Netskope Administrator's Guide

Overview

Netskope performs deep analytics of the cloud apps providing complete visibility of the apps i.e. uncover all cloud apps, view cloud apps across any endpoint or mobile device, drill down into apps, identify user actions within the app, content visibility etc. Netskope also enforces sophisticated policies for cloud apps enabling an administrator to write policies based on several variables such as users, AD groups, devices, locations, cloud apps, activity performed within cloud apps etc. When the criteria are matched the assigned action will be taken.

Getting Started

As an administrator, you have access to your tenant instance in Netskope. Admin UI provides full access to deploying and managing the Netskope solution.

Log in to your tenant instance in Netskope using the URL provided in the initial onboarding email sent from Netskope. Upon first log in, you will be prompted to change the admin password.

Managing Administrators

Netskope provides three administrator account types by default i.e. Tenant Admin, Delegated Admin, and Restricted Admin. Each admin type has different admin privileges. You can configure an admin user as one of the following admin account types.

Administrator Account Type	Description
Tenant Admin	The Tenant admin is the super admin for the organization and has full read-write access to all areas in the Netskope tenant UI. The Tenant admin can create other admin accounts.
Delegated Admin	Tenant admin should be able to delegate administration work to other admins by configuring an admin as a Delegated Admin. Delegated admins have all the privileges of the tenant admin except Delegated Admins cannot create other admin accounts.
Restricted Admin	Restricted Admins are read-only admins who are restricted access to view certain users and / or groups. You must create a role before you can create a restricted admin account. Roles are profiles that define what information the admin has access to. Roles are then assigned to the

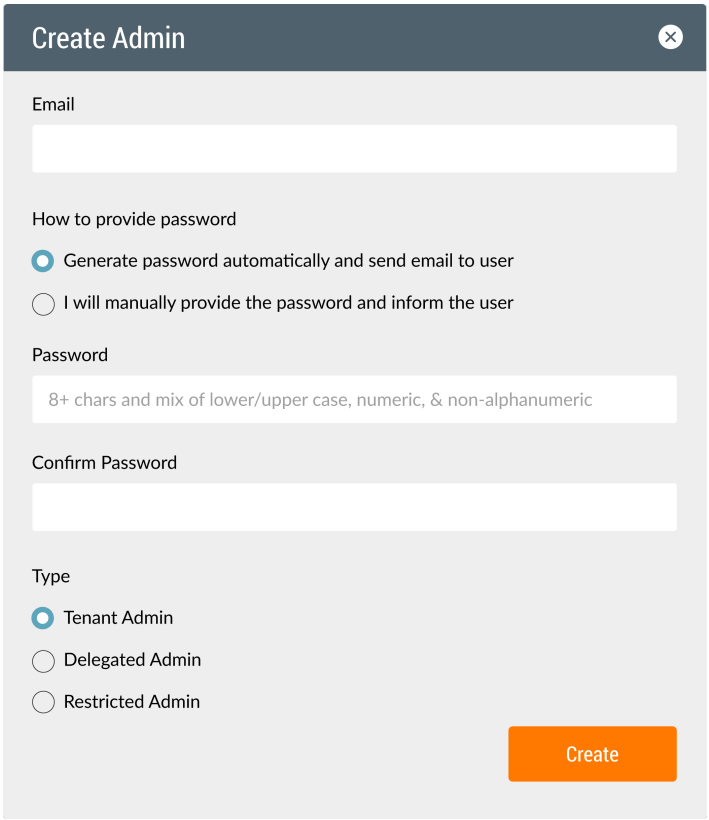
	restricted admin account. In addition to restricting the view to certain users and groups, tenant admins can also decide to obfuscate some of the sensitive data such as User-IPs or Source-IPs displayed in the UI for these users. The data obfuscation option can be specified in the role.

Creating Tenant Admins

Log in to the Netskope tenant UI as the tenant administrator.

1. Navigate to Settings > Administration > Admins.
2. Click Add.
3. Specify the email address of the admin user and choose the option, Generate password automatically and send email to user. This option automatically triggers an email to the admin. Alternatively, you can also choose the option to manually type a password.
4. Set the admin account type as Tenant Admin. Tenant Admins are not assigned any role.

The Administrator is prompted to change the password upon first log in. You can delete the admin user any time.



Creating Delegated Admins

Log in to the Netskope tenant UI as the tenant administrator.

1. Navigate to Settings > Administration > Admins.
2. Click Add.

3. Specify the email-address of the admin user and choose option “Generate password automatically and send email to user. This option will automatically trigger an email to the admin. Alternatively you can also choose option to manually type a password.
4. Set the admin account type as “Delegated Admin”. Delegated Admins are not assigned any role.

Administrator will be prompted to change the password upon first log in. You can delete the admin user any time

Creating Roles for Restricted Admins

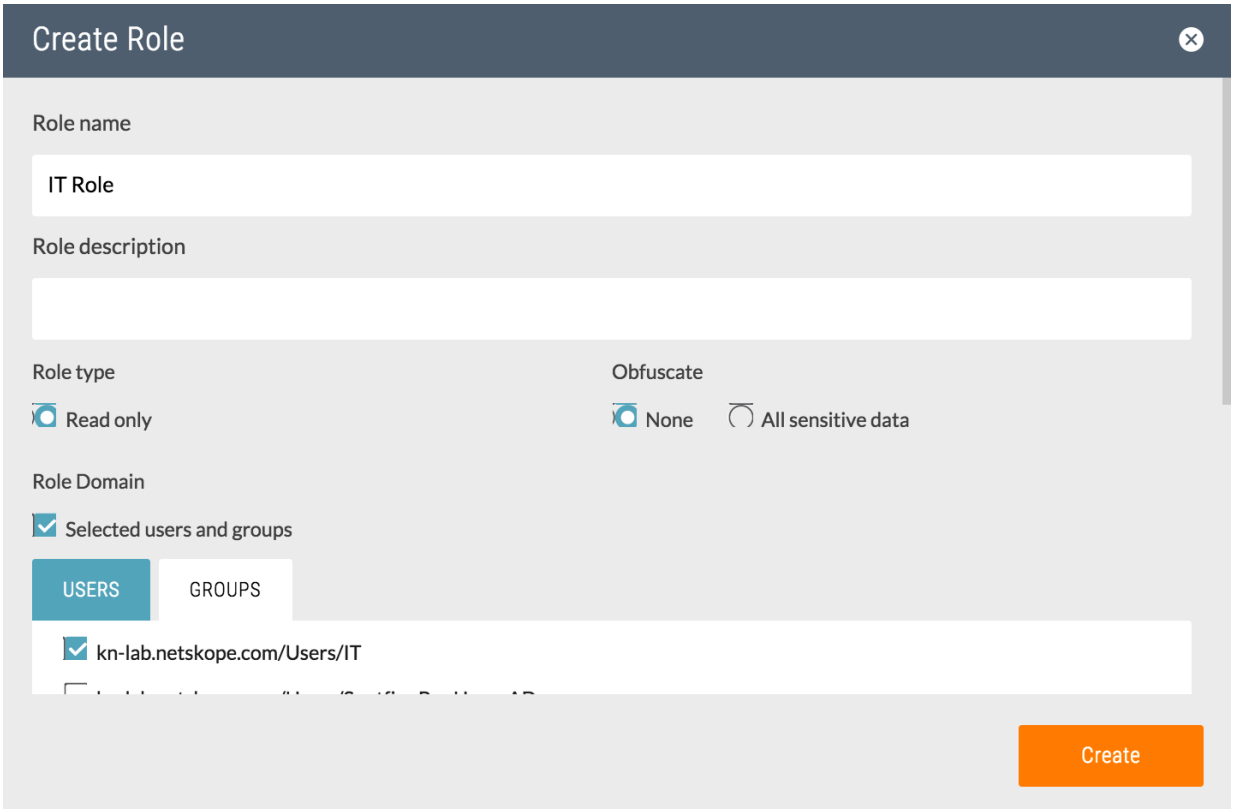
Log in to the Netskope tenant UI as the tenant administrator.

1. Navigate to Settings > Administration > Roles.
2. Click Create New.
3. Provide a Role name. Role type is set to “Read only” by default.
4. Specify the Role Domain. You can restrict the admin user to have access to only specific lists of users and / or groups. Default would be “All users and Groups”.
5. Optionally, you can choose the option to obfuscate all the Sensitive Data.

“Obfuscate”: If you choose the option to obfuscate “All the Sensitive Data”, restricted admins who are assigned this role cannot see sensitive data such as “username”, “src-IP” etc.

“Role Domain”: If you choose specific list of users or groups under Role Domain, Restricted admin who is assigned this role can only view the data pertaining to those users or the specific Active directory group i.e. view cloud apps usage for these users, create reports for these users etc. Restricted admin cannot view data of other users.

In the example below, IT group is chosen. IT group is the Active directory Group exported to the tenant instance in the Netskope cloud using AD Importer. You can also choose individual users.



NOTE: Users and groups can be automatically populated from the Microsoft Active Directory. This would require an AD Importer to be installed on a Windows system that can export the AD usernames and group names to customer's tenant instance in the Netskope cloud.

Assigning Roles to Restricted Admins

Log in to the Netskope tenant UI as the tenant administrator.

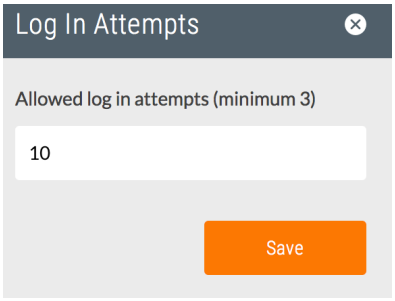
1. Navigate to Settings > Administration > Admins.
2. Click Add.
3. Specify the email-address of the admin user and choose option Generate password automatically and send email to user. This option will automatically trigger an email to the admin. Alternatively, you can choose the option to manually type a password.
4. Set the admin account type as Delegated Admin. Delegated Admins are not assigned any role.
5. Assign the role for the user.
6. Click Create to add the new admin.

The administrator is prompted to change the password upon first log in. You can delete the admin user or role at any time.

Admin Configuration

You can specify the number of log in attempts that can be allowed before the admin user is locked out of the UI. The default setting allows up to 5 failed login attempts.

To change the default navigate to Settings > Administration > Admins. On the right-hand side click the  icon to modify the allowed number of log in attempts.



Unlocking an Admin Account

The Tenant Admin can unlock other admin users if they are locked out of the UI. To unlock an admin,

1. Navigate to Settings > Administration >Admin.
2. Click the lock icon next to the admin user and unlock the account.

Configuring Single-sign-on for the Admin UI

The Netskope platform supports local and now SAML SP (Service Provider) workflow to provide authentication and authorization. This will allow for two-factor authorization supported by the IdP and eliminate the need to create local accounts for admins on the Netskope UI with the exemption of a tenant admin in case SSO is not available.

Logging in to the Portal

- User types in the tenant login URL (e.g. https://netskope.goskope.com)
- If SAML has **not** been configured for this tenant then the username/password page shows up as it does currently. User needs to authenticate locally.
- If SAML has been configured then Netskope will send a SAML "AuthnRequest" to the IdP. After the IdP authenticates the user, it will send an SAML Assertion back to Netskope with the admin's authentication (email address - NameID) and authorization (admin-role) credentials.
- On receiving the assertion we will check the authorization credentials. If authorization credentials are passed we will use that. If not then we will try to get the authorization attributes from our local tables. If we cannot find local authorization values either then we will report an error.

Configuration

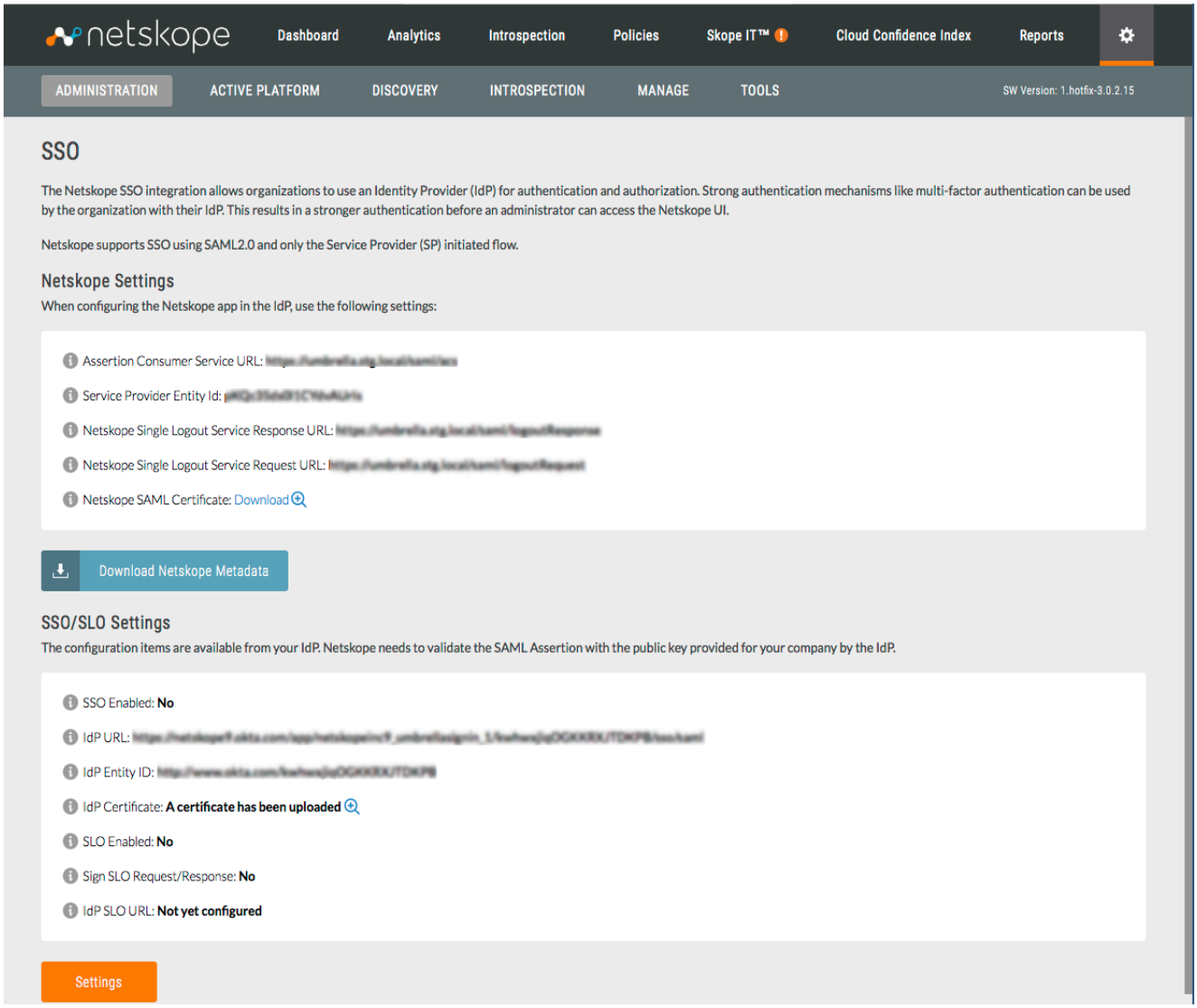
There are two sets of configuration, which has to be provided:

Netskope Configuration to be entered at the IdP (SSO Vendor)

- ACS (Assertion Consumer Service) URL - this is the URL to which the IdP will send the assertion after authenticating the user.

- entityId

These configuration parameters can be obtained from the tenant UI by navigating to Setting > Administration > SSO.



IdP related configuration to be entered in Netskope admin UI

You can obtain these from your SSO vendor.

- IdP Single Sign-On URL
- IdP Entity Id
- X.509 Certificate (IdP Public Key)

From the IdP/SSO vendor we expect a value "admin-role" to provide us with authorization info. This field can have the following values:

- "Tenant Admin"
- "Delegated Admin"
- previously created role in the portal for a "Restricted Admin"

Admin Role sent by IdP	Check against Local DB	Outcome
Nothing Sent	If the user is a provisioned user in the UI, then the admin account type configured for the user will be used to identify the privilege	Return error if no role found.
Tenant Admin	No	Login with role “Tenant Admin”

Delegated Admin	No	Login with role “Delegated Admin”
Read-only roles	Checked against roles configured in the tenant UI	f role name is found use that role. If not found return an error.

Single Logout

Netskope support Single Logout. When SSO is configured under SSO settings, user can be redirected to a specific logout page.

Timeout

Currently if the admin is idle for 30 minutes, the admin is logged out and sent to the login page. If SLO is enabled, we should now send him to the logout page configured under SLO settings.

Netskope Deployment modes

Netskope can be deployed in Offline (Discovery) mode or Inline (Active) mode. Discovery mode allows to discover the cloud apps in the network without having to deploy Netskope inline. In Active mode, cloud app traffic is actively steered to your tenant instance in the Netskope cloud

Offline Deployment methods

Deployment Method	**Details**
Log Discovery	Log upload provides quick and easy way to discover cloud apps in a customer’s environment. It also provides a baseline assessment of the risk to using these cloud apps. Customer can upload the log files from their enterprise Web proxy, Next generation firewalls and other devices. Netskope Log Collector can parse these logs to provide insight into the cloud apps being used i.e. who is using the app, what the app is, bandwidth and session usage, source and destination IP of cloud app traffic etc. There are several ways to upload the log for analysis. • Upload it to customer’s tenant instance in the Netskope cloud or • Upload it to a On-premise Secure cloud appliance • Upload to a On-premise Log Parser virtual appliance

Introspection	Netskope Introspection works by directly connecting to the Cloud app using the APIs published by the app. Introspection uses OAuth to gain delegated access to the app. Netskope's Introspection provides a complementary deployment model to provide Cloud Visibility, Policy, and Data Security Services by directly connecting to the cloud service using the APIs published by the cloud services. You can enable introspection for the following cloud apps: Box, Google Drive, One Drive, Sharepoint, Dropbox, Salesforce, Egnyte, Service Now
TAP mode	Netskope Appliance can be configured in TAP mode to integrate with PAN firewall or Bluecoat Proxy • Existing proxy or firewall sends a decrypted copy of SaaS App traffic to Netskope's probe • Complete visibility all the way down to Activities and DLP, but no policy enforcement • Qualified for Blue Coat and Palo Alto Networks

Netskope Active Platform

There are several ways to steer the cloud app traffic from enterprise network to customer's tenant instance in the Netskope cloud.

Deployment Method	Details
Client	User installs Netskope Agent on his Mac, Windows, or Android system. The Netskope Agent intercepts the HTTP and HTTPS traffic and steers the specified cloud app traffic to the customer's tenant instance in the Netskope cloud.
On-premise Secure Forwarder	Secure Forwarder is a customer premises virtual appliance enabling trusted access to the customer's tenant instance with a zero client software requirement. On the Internet-facing side, Secure Forwarder establishes a TLS tunnel to the customer's tenant instance and multiplexes client transactions with cloud app domains of interest over that tunnel. On it's client-facing side, Secure Forwarder becomes the destination for client requests to cloud app domains of interest. Secure Forwarder generates trusted certificates for those cloud app domains of interest, serving them up to the requesting clients to establish trusted path.

Proxy Chaining	Enterprise Proxy such as Bluecoat can be configured to forward cloud app traffic to Netskope Proxy in the cloud. • Existing proxy forwards relevant SaaS App traffic directly to Netskope's Cloud for Inspection and Policy Enforcement • No changes to existing endpoint configuration • Proxy cracks SSL open and adds **X-Authenticated-User** (userID) and **X-Forwarded-For** (endpoint IP) headers
iOS VPN Profile	iOS VPN profile is used for directing cloud app traffic of interest from an iOS device to Netskope cloud over VPN. iOS native on- demand VPN client is used for directing the traffic.
Reverse Proxy	The Netskope Reverse Proxy provides full visibility to a sanctioned app such as Box, Salesforce, etc. without requiring a software agent on the end point. Any SSO enabled app is supported. It works with SAML based SSO and ADFS.

Applications

Netskope performs deep analytics of the cloud apps providing complete visibility of the apps i.e. uncover all cloud apps, view cloud apps across any endpoint or mobile device, drill down into apps, identify user actions within the app, content visibility, etc.

Predefined Applications

Netskope has around 10000+ cloud apps in the database. These apps have an associated Cloud Confidence Index. Cloud Confidence Index measures the enterprise readiness of the cloud apps taking into consideration those apps security, auditability and business continuity. Each app is assigned a score of 0 – 100 and based on the score placed into one of five cloud confidence levels(ccl) "excellent," "high," "medium," "low," or "poor. CCL value is shown for each app.

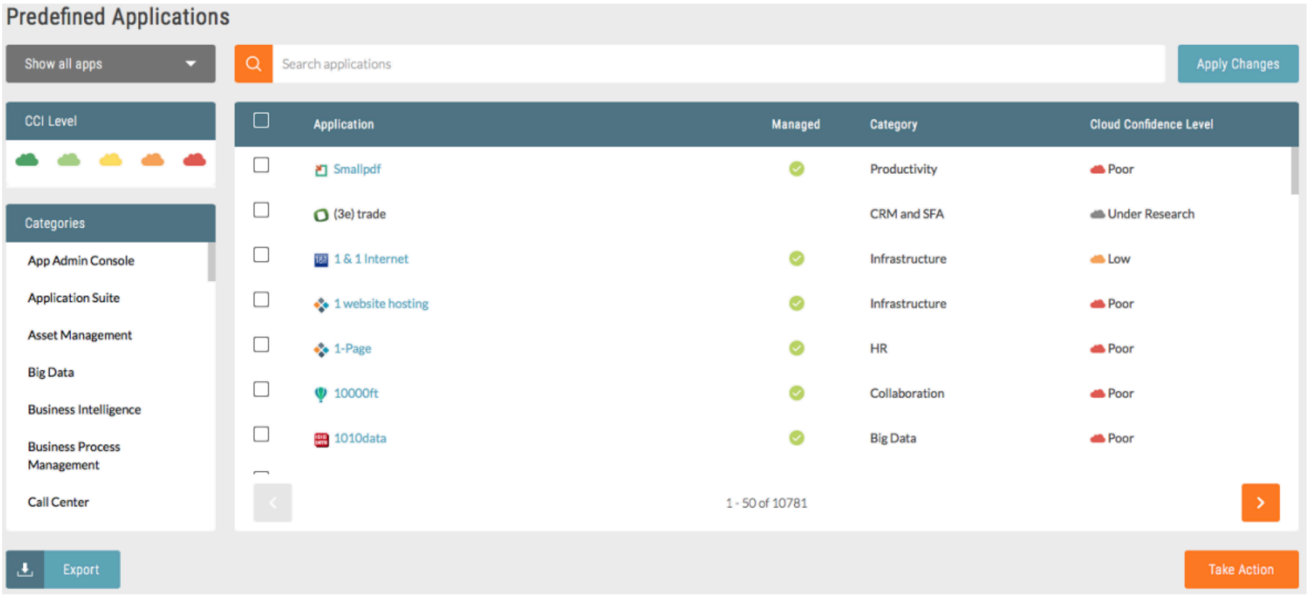
Cloud apps are grouped into categories as well.

By default all of the apps, except the consumer category, are added as managed apps. Customers can choose to manage or unmanage specific apps or app categories.

To add a managed app:

• Navigate to Settings > Manage > Applications > Predefined

• Click a category to display the list of apps in that category. The total number of apps in an app category displays at the bottom. You can further apply filters to show only the app with a specific CCL by choosing the CCI level on the left.



- You can also search for a specific app by typing the app name in Search bar.
- Choose the applications you want to manage and select Take Action > Manage.
- Use similar steps to add more cloud app categories or cloud apps.
- Once the apps are added click Apply changes at the top to save the configuration.
- Follow same steps to unmanage a specific app.

  Any configuration changes to managed apps are updated to the Secure Forwarder instantaneously and it's updated to the Netskope Client on Windows, Mac, Android Client, and the iOS VPN as well. Configuration updates to Windows, Mac, and the Android Client is not instantaneous and it can take up to an hour for the update.

- To view the list of Managed cloud apps, navigate to Settings > Manage >Applications > Predefined and select Show Managed apps from the dropdown.

- If you experience any issue with a specific app, you can choose to unmanage the app temporarily while you are working with Netskope support to resolve the issue with the specific app.

Certificate Pinned Applications

Several native apps are certificate pinned. These apps do not trust certificates if they are signed by 3rd party vendors. For example, if you go to google.com, your browser will trust the certificate if it's signed by Verisign, Digicert, etc. Some native applications do not allow it and ONLY trust their own certificates. If apps are certificate pinned, you can configure the Netskope client to either bypass or block these apps. If you select Bypass, the client will not steer traffic from the end point to the Netskope proxy in the cloud and apps will continue to work. If you select Block, the Netskope client blocks traffic. By default all apps are bypassed.

Certificate Pinned Apps don't allow SSL inspection and trusted certs are hardcoded.

It is not possible to intercept traffic for analytics. Alternatively you can use Netskope's introspection feature to connect to the sanctioned app instance for getting the visibility.

Options for Certificate pinned applications:

- Block Native App traffic
- Bypass Native App traffic
- Bypass if the endpoint is Managed
- Bypass and Tunnel (Outlook & Lync)

The bypass and tunnel option exists to allow connections to ip-filtered app instances.

Edit Certificate Pinned List

If apps are certificate pinned, you can configure the Netskope client to either bypass or block these apps. If you select Bypass, the client will not steer traffic from the end point to the Netskope proxy in the cloud and apps will continue to work. If you select Block, the Netskope client blocks traffic. By default all apps are bypassed.

Advanced Settings

Use this feature to configure the mode (Tunnel or Bypass) for app traffic from all accessing devices.

(1) Bypass + Direct: Selecting this means, bypass the configured apps / domains from the client.

(2) Bypass + Tunnel: Selecting this means, the client will tunnel the traffic from apps / domains but Netskope proxy will bypass it. This option is useful for domains associated with an SSO authentication service because these services use the source IP of the Netskope cloud to determine if Netskope protects access to the cloud app.

The following are the different actions and modes supported for the apps.

-three actions

--bypass

--bypass MD

--block

-two modes

--direct

--tunnel

-domains: add any domains that need to be bypassed but it should go through Netskope proxy just for the sake of SRC IP change. The traffic for this domain will still be bypassed...no DLP, No SkopeIT events
IMPORTANT: You must add any domains you add here to the Custom Domains list.

Navigate to plugin processes to add any additional processes that need to be bypassed.

Following options are possible:

1 Bypass+Direct: NS client itself will bypass the configured app (default behavior)

2 Bypass+Tunnel: NS Client will tunnel but NSProxy will bypass the app / domains. Add a use case for this.

3 Bypass MD + Direct: NS Client will bypass the app only if the device is Managed as per Device Classification policy otherwise block.

4 Bypass MD + Tunnel: NS Client will tunnel (to be bypassed by NSProxy) only if the device is Managed as per Device Classification policy otherwise block.

5 Block (mode and other options not allowed) : Client itself block the app traffic.

Policy Configuration

Inline Policy Configuration

Once administrator has visibility into the cloud Apps and the activities performed by the user within the cloud App; next step is to define policies to enforce the business rules. Policies allow you to enforce action (block or alert) based on Cloud apps, Cloud app categories, Users and groups, App Activity etc. In addition to this administrator can also define DLP Policies to inspect the traffic for data leak of sensitive and critical data.

Policies are expressed using a variety of variables. These variables define the matching criteria. When all criteria are matched the specified action is taken.

The following are the variables that can be defined on a policy. You can use one or more variables to define the policy. If any variable is not used in the policy it is considered as “Any”.

Match Criteria	Description
Groups	Active Directory Groups. These are the AD groups that are automatically populated to the Netskope cloud from the Enterprise AD server. Requires Netskope AD adapter to be installed on a server that is part of the domain to export the AD usernames and group names.
Users	Users created manually in the UI or Active directory users that are automatically populated from the enterprise AD server.
OU	Organization unit. This information is obtained from the exported AD groups

Devices (OS/Browsers/Device Classification)	Operating system (Mac, Linux, Windows, Android, iOS etc.) or browser used by end-users (Chrome, Firefox, Safari etc.). Device classification is applicable only for Netskope Client. Device can be classified as a managed or unmanaged device when using Netskope Client by performing certain registry checks, AD Domain checks etc. This is available under Settings -> Manage -> Device Classification
Network location	IP address or IP address range. This can be created under Objects -> Network location
Access method	Specify if the policy is applicable only for specific access methods i.e you can specify the policy is applicable only for traffic steered from Secure Forwarder or Reverse Proxy or Client or Mobile Profile
Geo location (Source countries or Destination countries)	Match on Source and/or Destination Country This also supports negate option. The match criteria include all the countries except the ones specified.
Applications or Categories	Choose an individual app (e.g. Dropbox) or an app category (e.g. cloud storage) as matching criteria.
App Instances	Some cloud apps have multiple instances of the app active at the same time e.g. Enterprise Google drive instance for an organization vs. personal instance. Add specific app instances to create policies that are specific to that instance of SaaS app. Refer to "Creating application instances" for details on creating application instances.
Cloud Confidence Index Level (CCI Level)	Cloud Confidence Index measures the enterprise readiness of the cloud apps taking into consideration those apps security, auditability and business continuity. Each app is assigned a score of 0 – 100 and based on the score placed into one of five cloud confidence levels "excellent," "high", "low," or "poor. CCI can be used as a matching criteria in the policy e.g., "Don't let users share content in Cloud Storage apps rated 'medium' or below "medium" CCI Level tab is shown when App category is chosen.
DLP	Specify the DLP profile that will be used for identifying DLP violations. DLP Profiles and Rules can be configured under Policies -> DLP

Activity	The activity tab is shown when App or App category is chosen. Netskope content analytics engine contains connector that can perform deep packet inspection to detect a specific cloud app and also to extract the relevant information about the activities performed in that app e.g. it can inform if the user downloaded a file, uploaded a file, shared a file and also the filenames etc.
Constraints Profile	Specify the name of the constraint profile to match for that specific activity. Constraints profiles are configured in the policy to define what the user is allowed to do for that specific activity (e.g. users are allowed to share only within the organization). Constraints profile is shown only for the activities, which supports it. Constraints profiles are defined under Policies -> Profiles -> Constraints

Action	• Alert – Inspects the session and performs deep analytics but no action is taken. It will generate an alert under the Alert tab • Block – Blocks the specified app session if all criteria are matched. For e.g. if the policy is configured to block only "download" activity for "Cloud Storage", only the download will be blocked. All other activities will be permitted. You can specify a default block page or a custom block page to be displayed when block action is taken. • Bypass – Bypasses the inspection once the criteria are matched. E.g. if you want to bypass all activities from being inspected except for login and logout, then choose all the activities except "Login Successful" and "Logout" and set the action as Bypass • User alert – This option is available only when DLP is configured in the policy. When user-alert action is chosen, you can specify a default user alert page or custom page to be displayed to the user when the policy is matched i.e. user had a DLP violation. The user justification page for user alert action will have the "Proceed" and "Stop Action" button. The "Proceed" button will allow the activity and generates a "upload/download" event with the user's justification reason whereas the "Stop Action" will just block the activity. • Quarantine –. If a user uploads a document that has DLP violation, an administrator can now take an action to quarantine the file. This will move the file to a quarantine folder for the administrator to review and take appropriate action. Administrator will then choose to allow the file to be uploaded or block the file form being uploaded. This option is available only when DLP is configured in the policy. Also the action can be taken only for upload activity • Encryption – Administrator can choose to encrypt files in the named instances of cloud apps that are sanctioned if it matches certain policy criteria. Encryption option is available only when an application instance of cloud app is chosen. Refer to the section "Creating Application instances on how to setup application instances. Encryption action can be taken only for upload activity. If any other activity is chosen e.g. download, encryption will not show under list of actions.

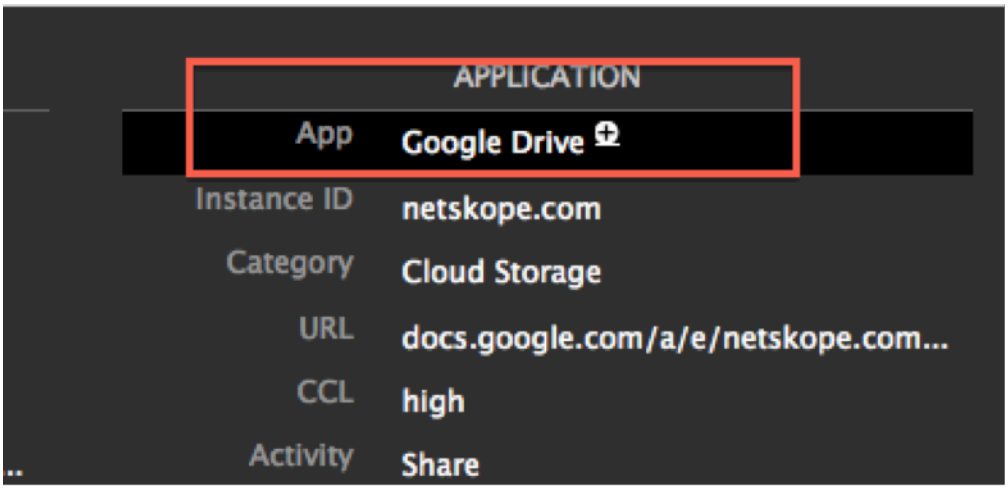
Creating Application instances

Some cloud apps have multiple instances of the app active at the same time e.g. Enterprise Google drive instance for an organization vs. personal instance.

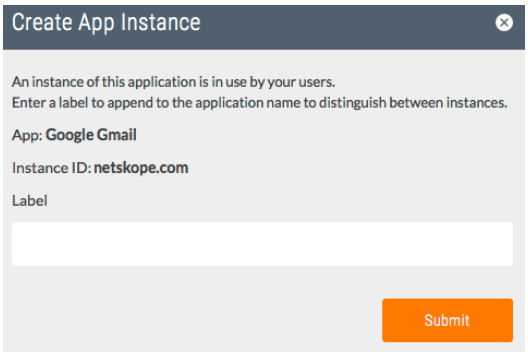
Netskope analytics engine tracks the instance-id for these apps. Administrator can create an app instance based on the instance-id and use the app instance name to create policies that are specific to that instance of the SaaS app.

Follow the steps below to create an appinstance name.

- Navigate to SkopeIT -> Expand the SkopeIT event
- Click the + Sign next to the app to create the app instance name. The SkopeIT event in the image below shows the Google Drive instance for Netskope.



- In the “Create app instance” window, provide a name for the app instance and click submit.



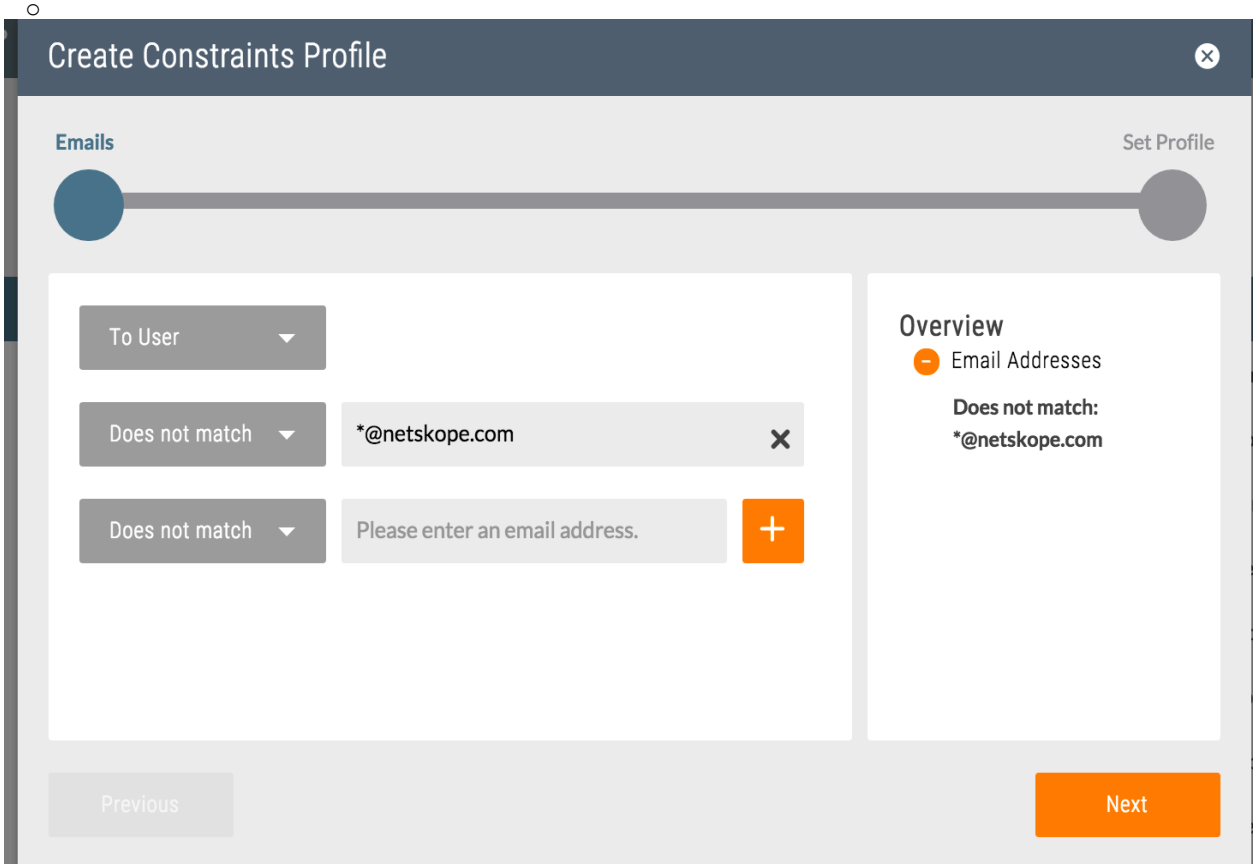
Once app instance is created it will now be available to be used in the policy

Constraints Profile

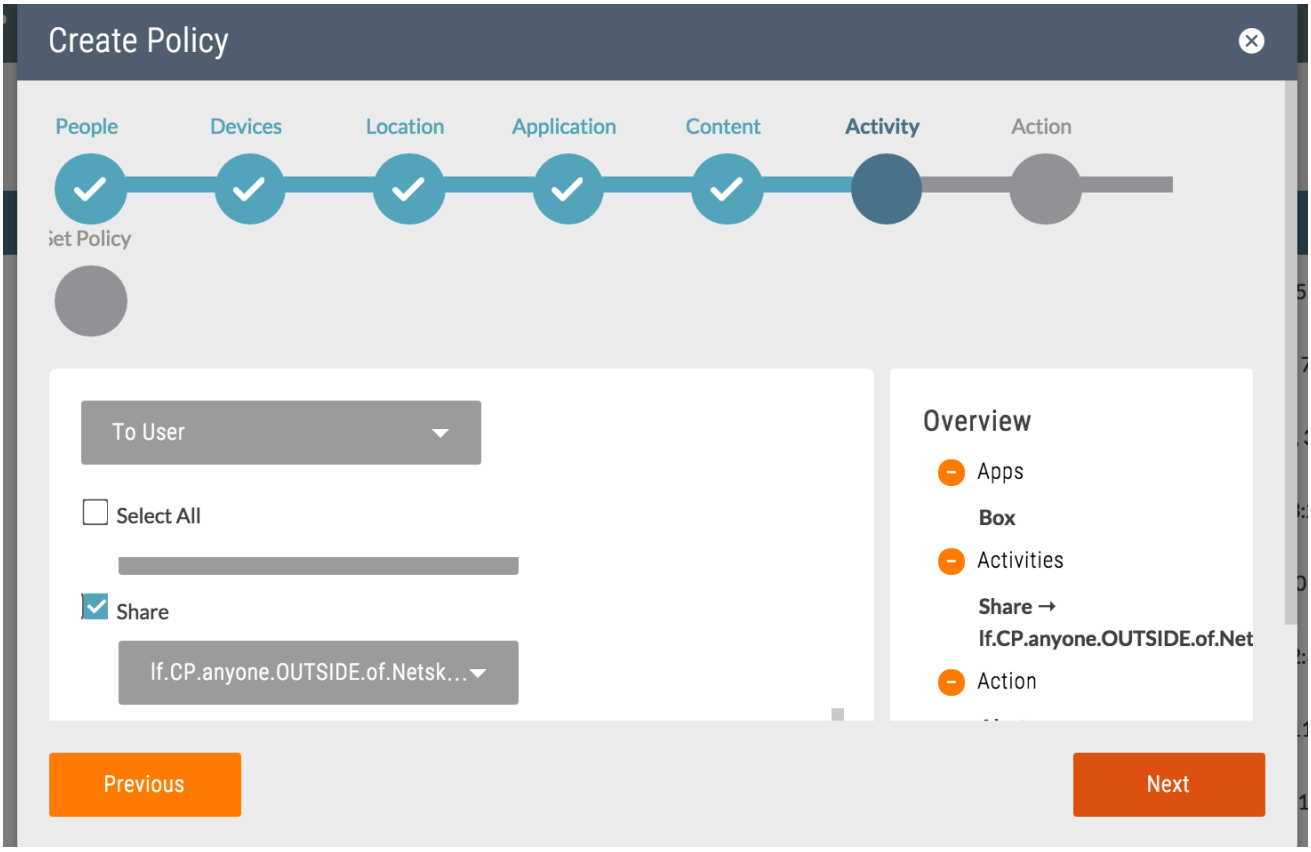
Constraints profile defines what the user is allowed to do for a specific activity in an App e.g. “Users are allowed to share contents only within the organization from Google Drive” or “Bypass inspection if the user is logging to their personal instance of Google mail”. Constrains profile are applicable only to Inline policies.

To create a new constraint profile,

- Navigate to Policies -> Profiles -> Constraints -> New Constraint Profile
- Choose if the constraint profile applies to “From User” or “To User”. I
  - If the administrator wants to block users from sharing files outside of the organization, in this case you will choose to create “To User” profile i.e. if the to_user does not match “@specificemaildomain.com”
  - If the administrator wants to bypass policy inspection when users log in from their personal email address to a personal box instance, then choose to create a constraint profile for “From user”. So if the from user does not match “@emaildomain.com”, then bypass the inspection
- Configure the email-address wild card to be matched.
  - In the example above if administrator wants to block users from sharing files outside of the organization, you would specify the email address “Does not match” the value “*@netskope.com”
- Provide a name and click “Create Constraints Profile”
-



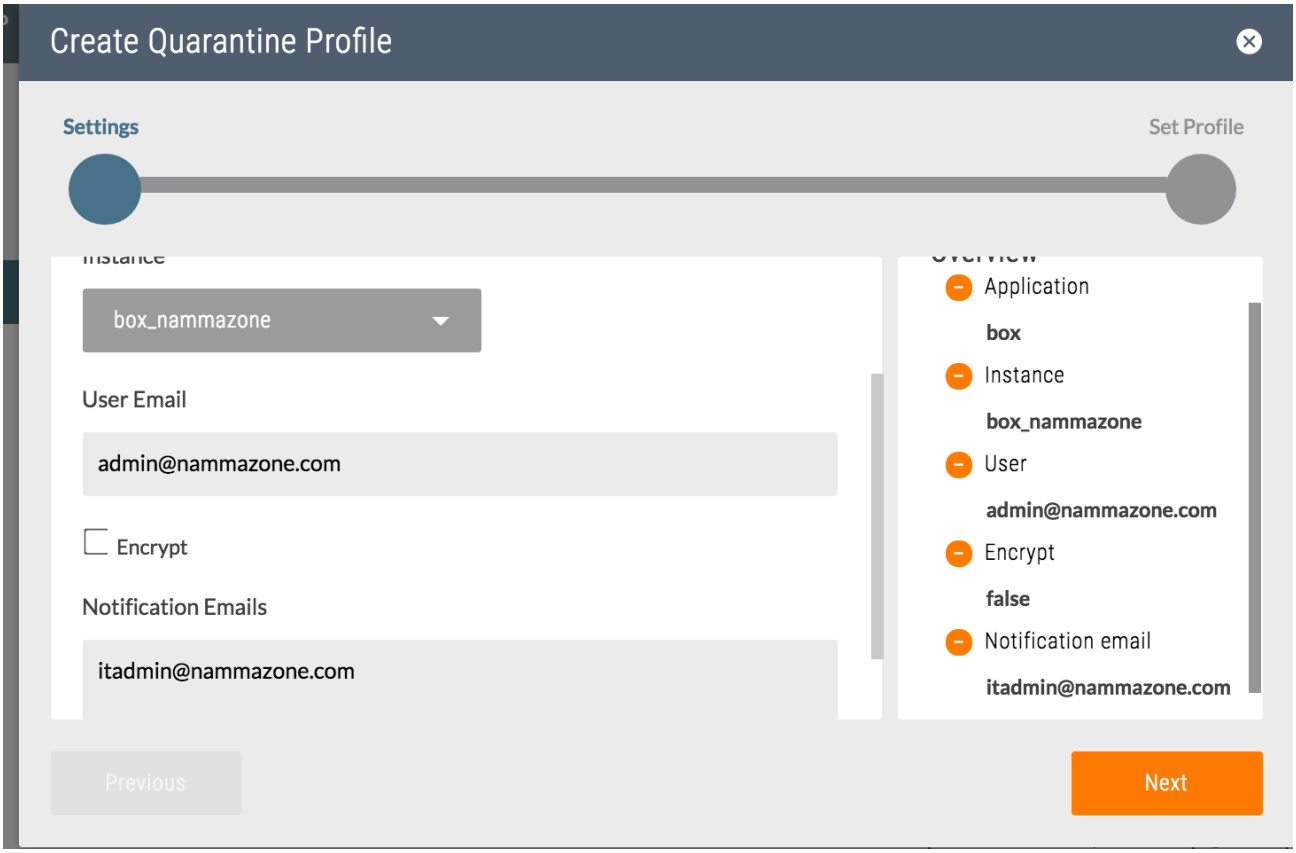
You can specify the constraints profile in the policy under Activity.



Quarantine Profiles

Quarantine Profiles are used for specifying where the file needs to be quarantined when there is a policy action of “quarantine”

To create quarantine profile, click on Profiles -> Quarantine -> New Quarantine Profile

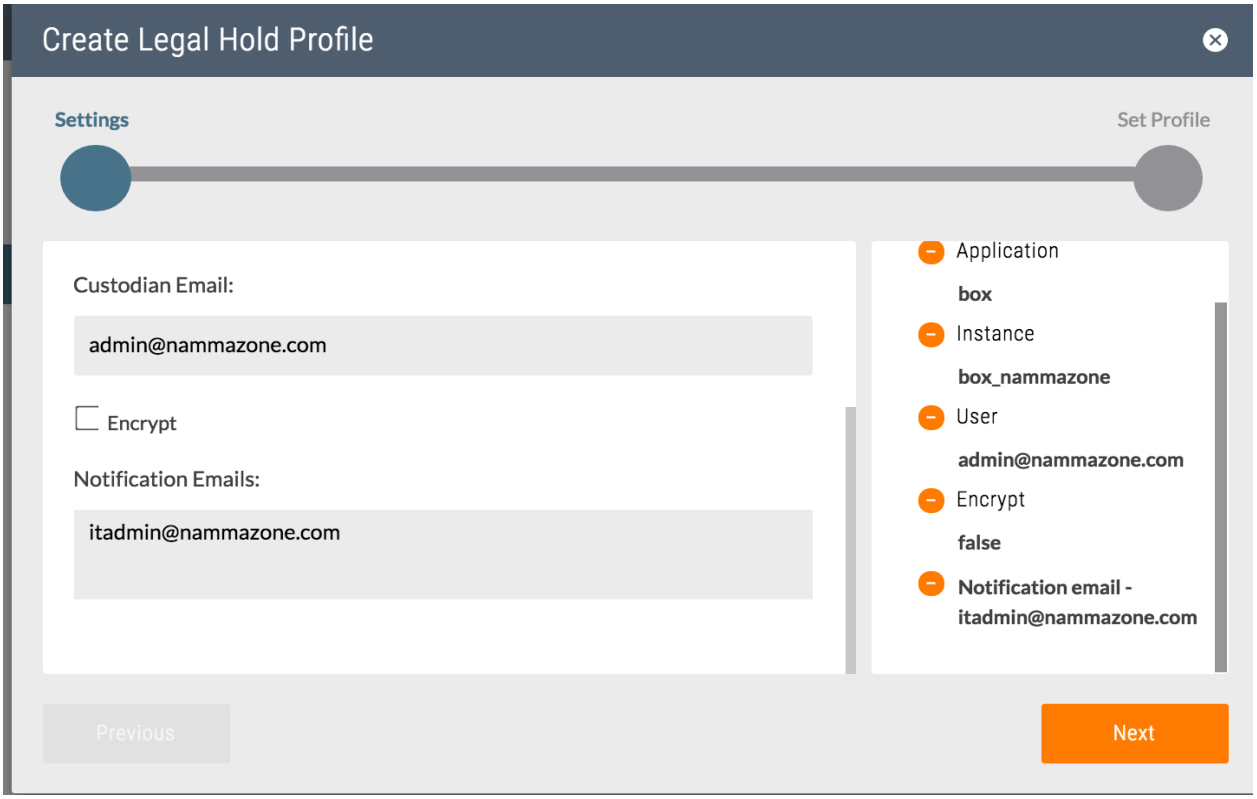


- Choose the app where you want the quarantined files to be uploaded. Today we support quarantined folders on Box, Google Drive and One Drive and Sharepoint app
- Choose the instance of the app previously created under Settings -> Introspection
- Choose the email address of the admin user
- Choose encrypt if the quarantined files has to be encrypted
- Choose the list of admins to be notified when a file is uploaded to quarantine folder

Legal-hold Profiles

A **legal hold** is a process that an organization uses to preserve all forms of relevant information when litigation is reasonably anticipated. Legal-hold Profiles are used for specifying where the files need to be held for legal purposes when action of "Legal Hold" is taken.

To create a Legal Hold profile, click Profiles -> Legal Hold -> New Legal Hold Profile



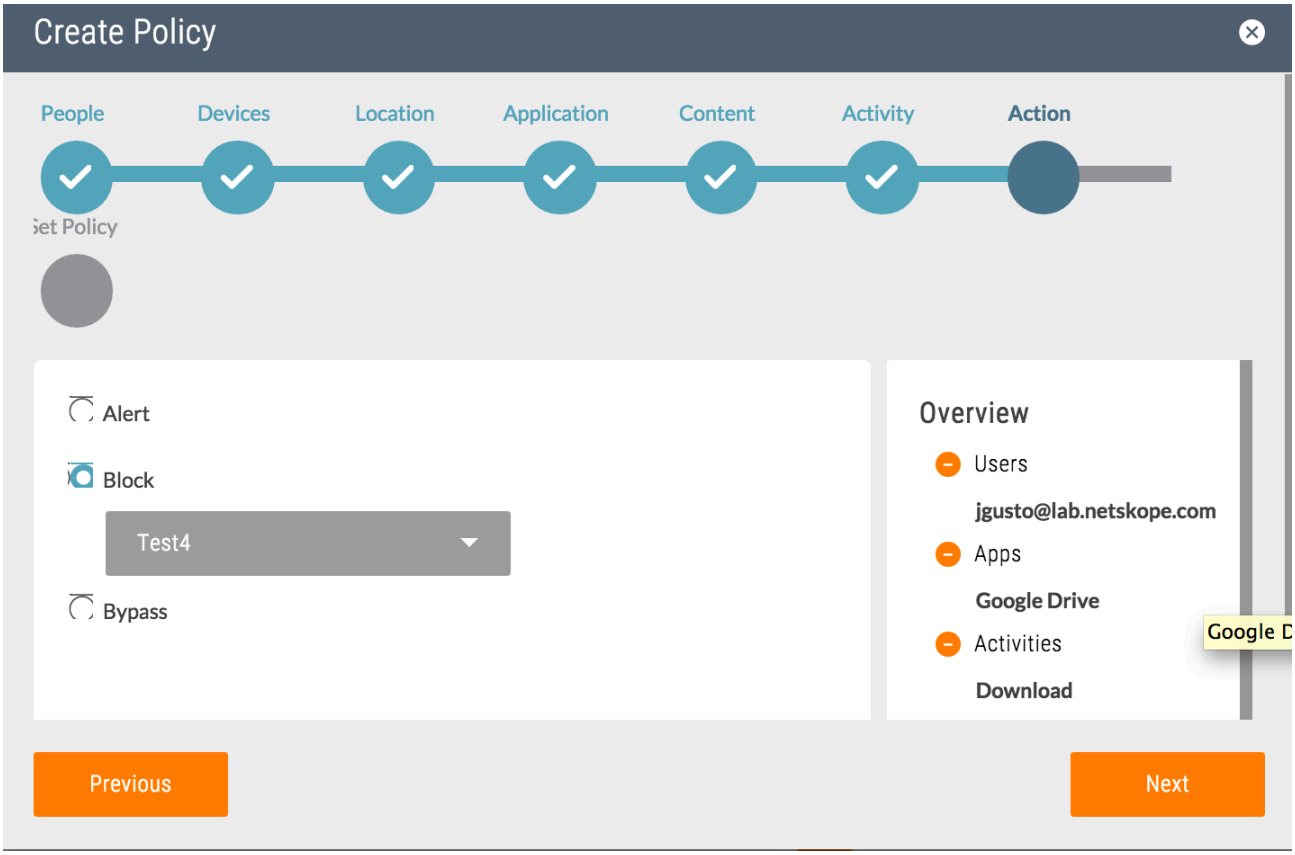
- Choose the app where you want the files to be uploaded for legal hold purposes. Today we support legal hold folders to be created on Box, Google Drive, One Drive and Salesforce app
- Choose the instance of the app previously created under Settings -> Introspection
- Choose the email address of the custodian
- Choose encrypt if the files to be held for legal purposes needs to be encrypted
- Choose the list of admins to be notified when a file is uploaded to legal hold folder

Policy Examples

Example 1:

Administrator wants to block certain users from downloading documents from Google Drive.

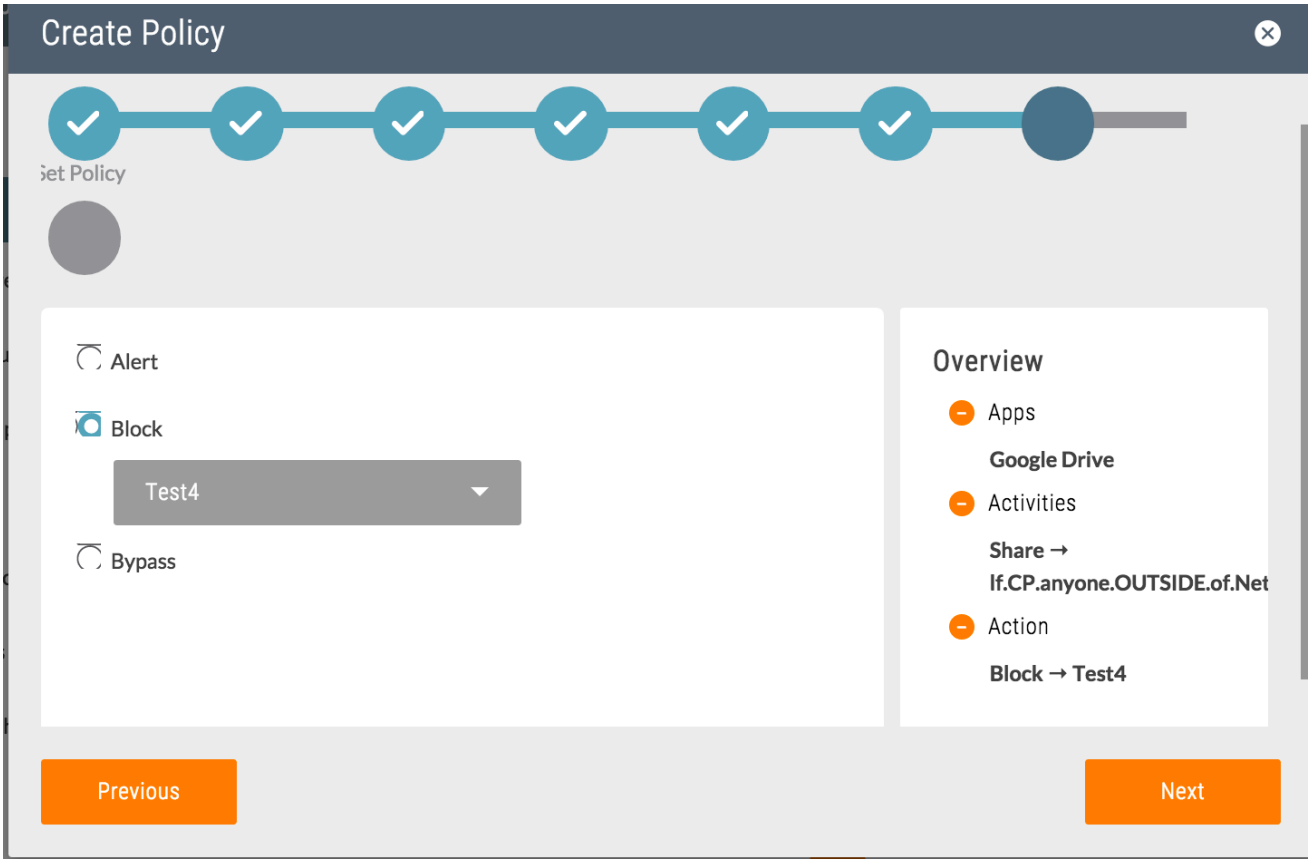
- Navigate to Policies -> Click Inline
- Select “New Policy” to create a new policy
- Choose Users -> Select a specific user name
- Choose Devices if you want to apply the policy to a specific browser or specific OS. Similarly choose Location if you want to restrict the policy to a specific network location. If not leave them as blank and click Next
- Select Application “Google Drive”
- Choose “Download” as the activity
- Select Block from the action tab and choose either a default or custom block page to be displayed to the user



Example 2:

- Administrator wants to block sharing for Google Drive to any user outside the organization.

- Navigate to Policies -> Click Inline
- Select “New Policy” to create a new policy
- Leave Users, Devices, Location blank as the policy is applied to all users
- Select Application “Google Drive”
- Choose “Share” as the activity, click on the dropdown menu to choose a constraint profile. In this case we want to block users from sharing outside of their organization. So choose a constraint profile that looks for email-address not equal to “*@domainname.com”
- Select Block from the action tab and choose either a default or custom block page to be displayed to the user



Note: You can click on any policy and drag it up or down to change the policy order.

DLP Policy Configuration

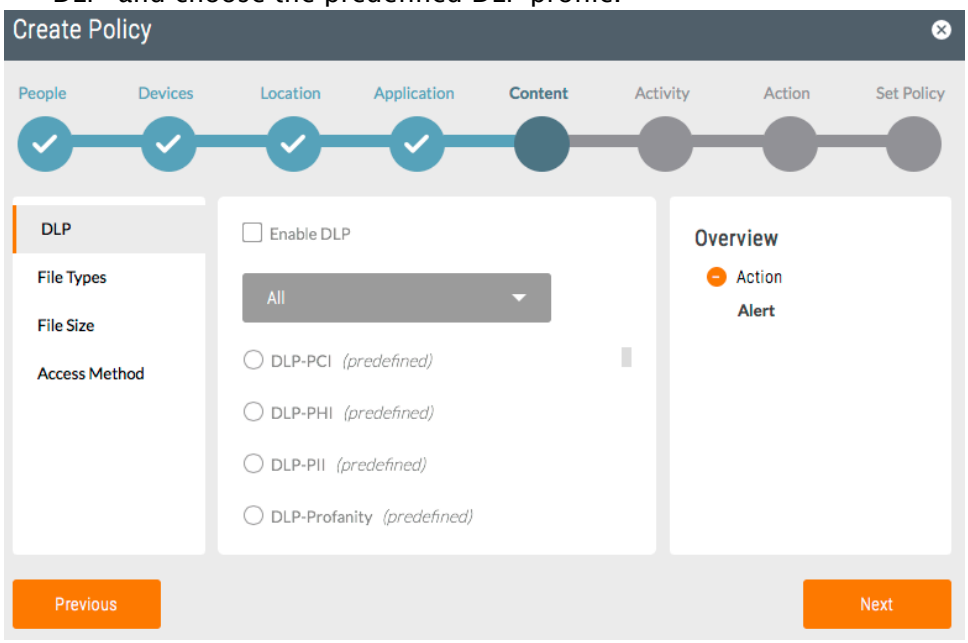
The Netskope Active™ platform provides a comprehensive DLP policy enforcement solution for cloud applications. The solution is ideal for addressing regulatory compliance requirements as well as protecting enterprise sensitive data. The DLP policy is based on profiles that specify the data identifiers to match in the content that is present in cloud app transactions. The platform comes with a predefined set of DLP profiles for well-known compliance regulations like PCI, PHI, PII etc. The platform also supports the creation of custom DLP profiles using a large dictionary of predefined data identifiers as well as custom regex expressions. The Netskope Active platform will scan file content to identify data leakage based on the configured DLP policy. There is a flexible set of policy actions that can be enforced if sensitive data is identified in the content.

Configuring DLP policy using Predefined DLP Profiles

You can use one of the predefined DLP profiles in the policy. This includes inspecting traffic for Payment Card Information (PCI); Personally-Identifiable Information (PII); Electronic Personal Health Information (ePHI), Profanity and Source code violations. Using pre-defined profiles will let you take advantage of established best practices and start preventing loss of

critical data in the cloud immediately without having to configure the system.

- Create a new policy or edit an existing policy. Under Content, choose “Enable DLP” and choose the predefined DLP profile.



- Click Submit to save the policy.
- Drag the policy up or down depending on the required policy order.
- Click on “Apply changes” to save the changes to the policy.

Note: You can click on any policy and drag it up or down to change the policy order.

Customizing DLP Policies

To create a custom DLP Policy, you need to create the DLP rules and DLP profile. For e.g. you can apply a custom DLP policy that looks for leakage of confidential document.

Refer to the next section for details on DLP rules and Profiles.

DLP Rules

DLP Rule contains one or more predefined data identifiers and/or custom data identifiers. DLP engine comes with a library of predefined data identifiers that can be used in the DLP rules for common terms that are required for detecting regulatory or sensitive data. Multiple data identifiers (predefined or custom) can be combined with Boolean operators (AND, OR) in a DLP Rule

Predefined DLP Rules and Predefined Data Identifiers

- To check the list of predefined DLP rules, navigate to Policies -> DLP -> Data Loss

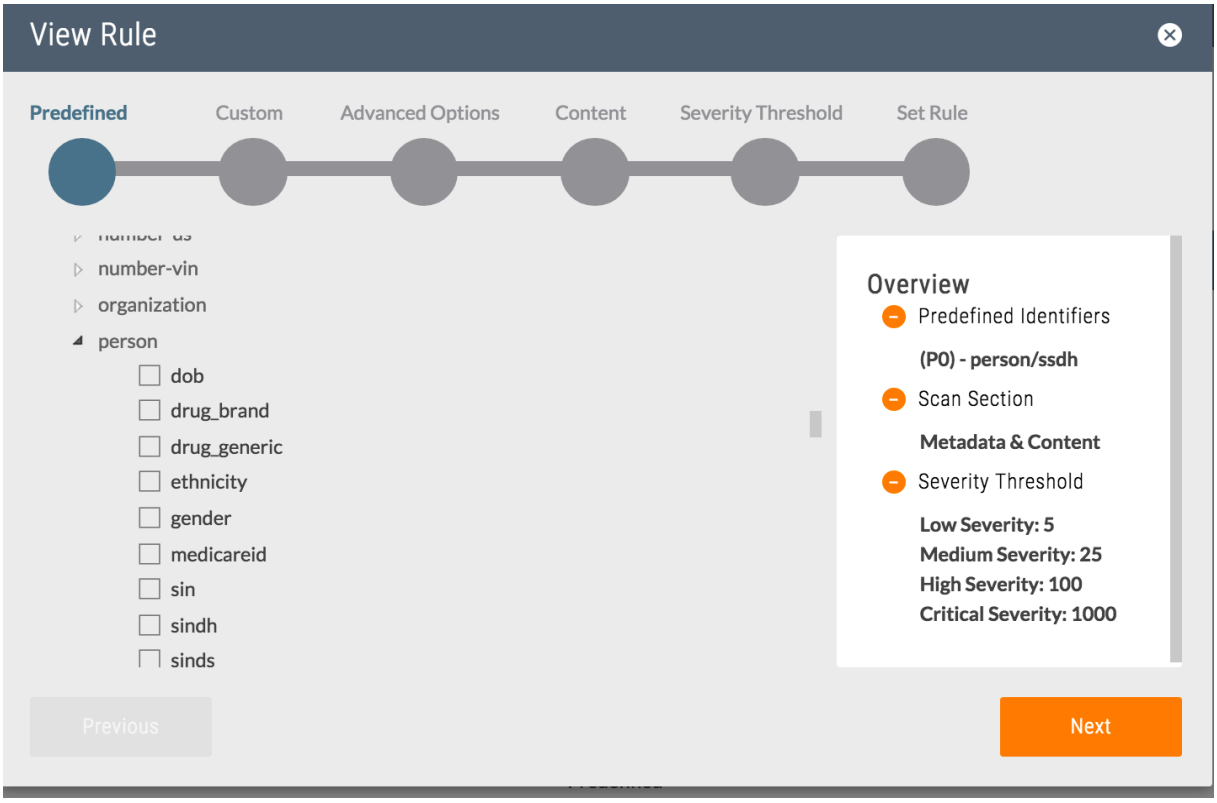
Prevention -> Rules

- To check the list of predefined data identifiers, navigate to Policies -> DLP -> Data Loss Prevention -> Rules -> Click on New Rule. This would show the list of all the predefined data identifiers available. You can mouse-over any of them to see the details.

Let us assume you want to match for data that contains SSN (dash delimited) and firstname and lastname of the user. Administrator can either choose to use a predefined DLP rule or create a custom DLP rule for this depending on the requirement.

There is a predefined DLP rule "Name-SSN(Dash Delimited)" which looks for a person name and Dash delimited SSN. This rule has the count threshold set to 5 occurrences. Refer to the image below for the details.

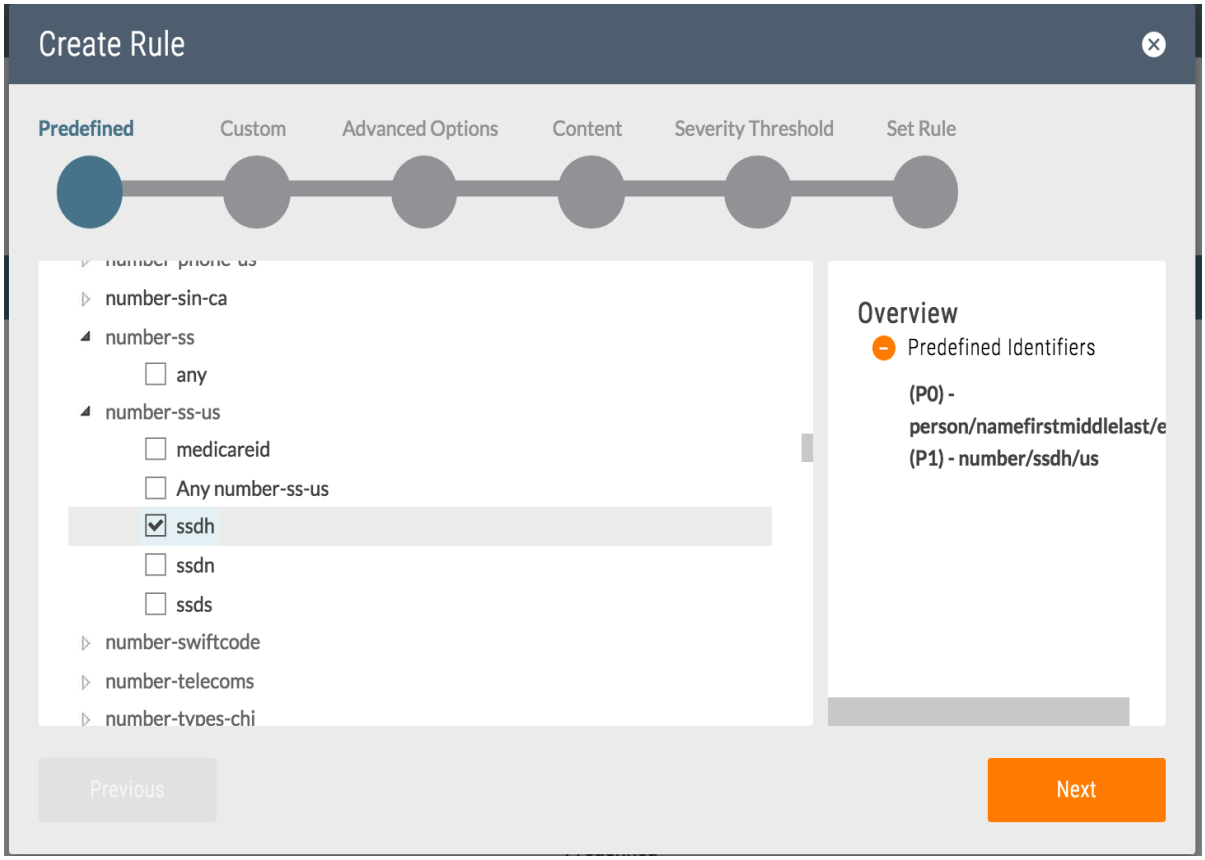
- Personal name and Dash delimited SSN are matched by predefined data identifier "**(P0) - person/ssdh**



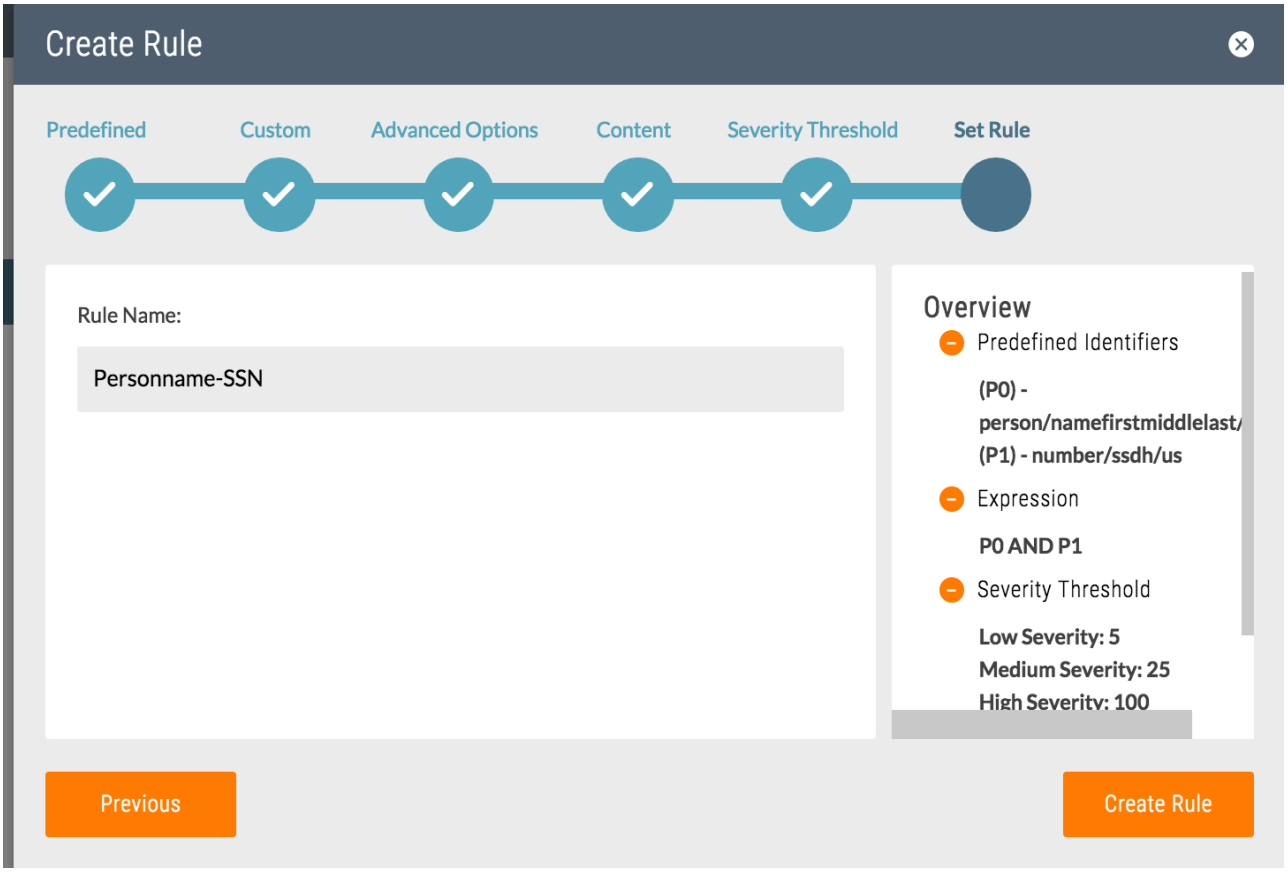
Custom DLP Rules using Predefined Data Identifiers

Use custom DLP rules when the predefined DLP rules do not match the requirement.

- Navigate to Policies -> DLP -> Data Leak Prevention -> Rules -> Click on New Rule
- Choose predefined data identifier “person-name-engus/namefirstlast”
- Choose predefined data identifier “number-ss-us/ssdh”. This will identify dash limited social security number. Mouse-over the name to see the description of the predefined data identifier.



- Click next to create any custom identifiers. For this specific example we do not need any custom identifier. So click next to move to the advanced options.
- Under Advanced Options, you can choose what Boolean expressions need to be applied for the predefined and custom identifiers. By default, if nothing is chosen, it is Boolean “AND” for all the identifiers.
- Select “Metadata and Content” to be scanned
- Click Next to configure the severity threshold. Alerts triggered by the DLP rule has an additional severity field, which displays the severity of the violation. Set the count equal to number of occurrences that should match before a DLP violation is triggered and also determines the severity of the DLP violation
- Provide a name for the DLP rule and choose “Create Rule”.
- Click on “Apply Changes” to save the changes.

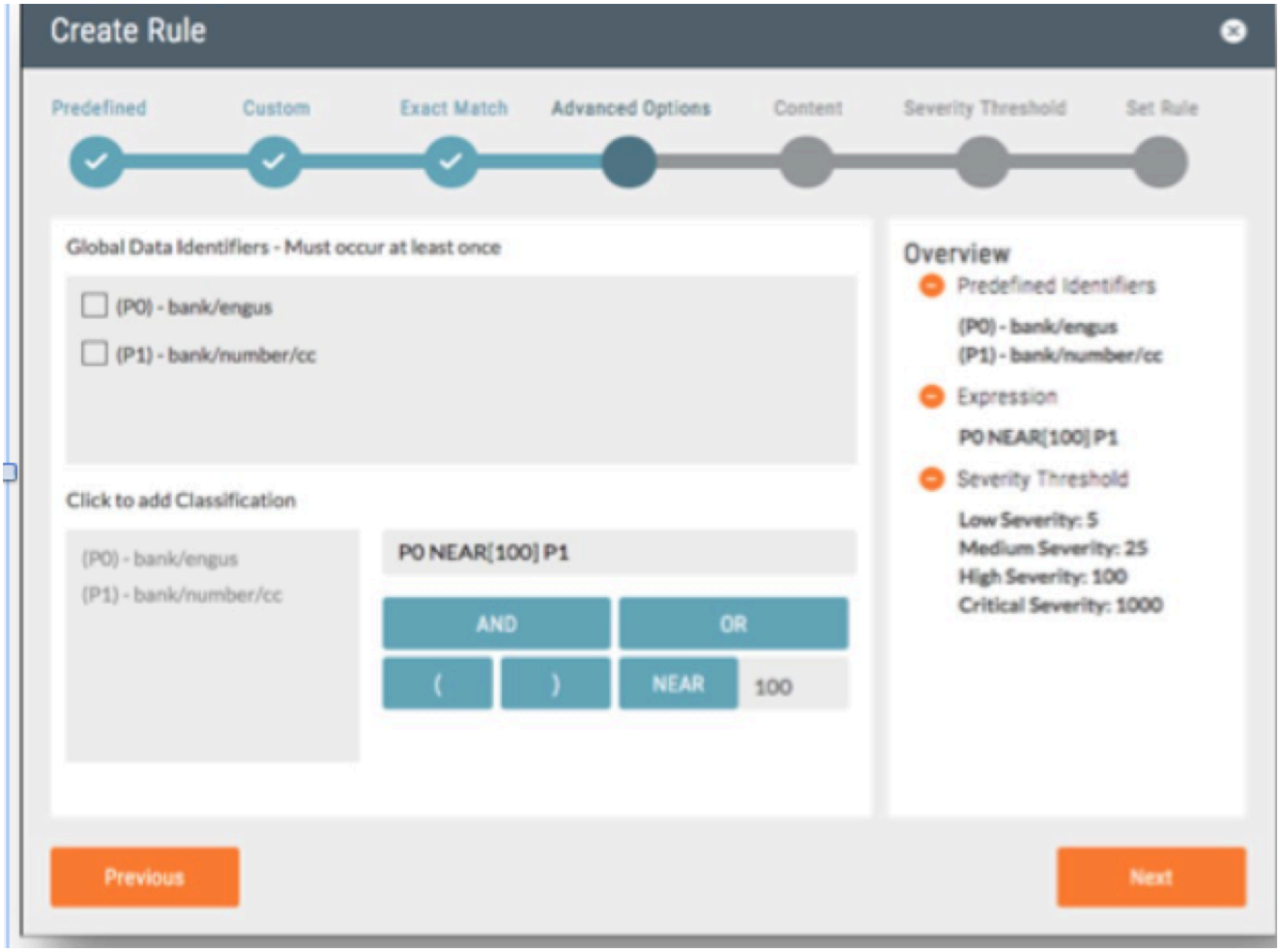


One not so obvious problem with the above rule is that the person name can be in the beginning of the document and a 9-digit number that looks like a SSN can be way at the end of the document and that would still satisfy the condition and trigger the rule. Introducing a proximity constraint can tighten the above rule. Refer to the next section for writing DLP rules using proximity constraint.

DLP Rules using Proximity Operator

Netskope's DLP proximity analysis checks for the presence of data identifiers within a certain distance of one another within a document. In order to achieve this a new operator for proximity called the 'NEAR' operator is introduced.

The NEAR operator is very similar to the AND operator except the NEAR operator will be specified with a character range for proximity check. In the above example the expressions P0 and P1 is required to be within 100 characters. Every NEAR operator can have it's own character range.



Similar to the AND operator the order in which these identifiers are found in the document will not matter. The rule will detect P0 followed by P1 as well as P1 followed by P0.

This proximity analysis allows flexibility as it can be seen from the below examples.

For explanation purposes we'll be using uppercase alphabets as identifiers (operands) and combining them with the AND, OR, and NEAR as operators.

Example 1: A and B needs to be within proximity of each other. Expression: (A NEAR B).

Example 2: A needs to be within proximity of either B or within proximity of C. Expression: ((A NEAR B) OR (A NEAR C)).

Example 3: A, B, and C proximity check is within 100 characters of each other. For example, John Smith's credit card is 4111-1111-1111-111 and expires on 11/10/2015; the distance between the first character of the first identifier and the last character of the last identifier should be within 100 characters. (Distance between 'J' of John and '5' of 11/10/2015 should be within 100 characters). The order of identifiers doesn't matter; the engine supports all combinations of A, B, andC.

Expression: (A NEAR B NEAR C).

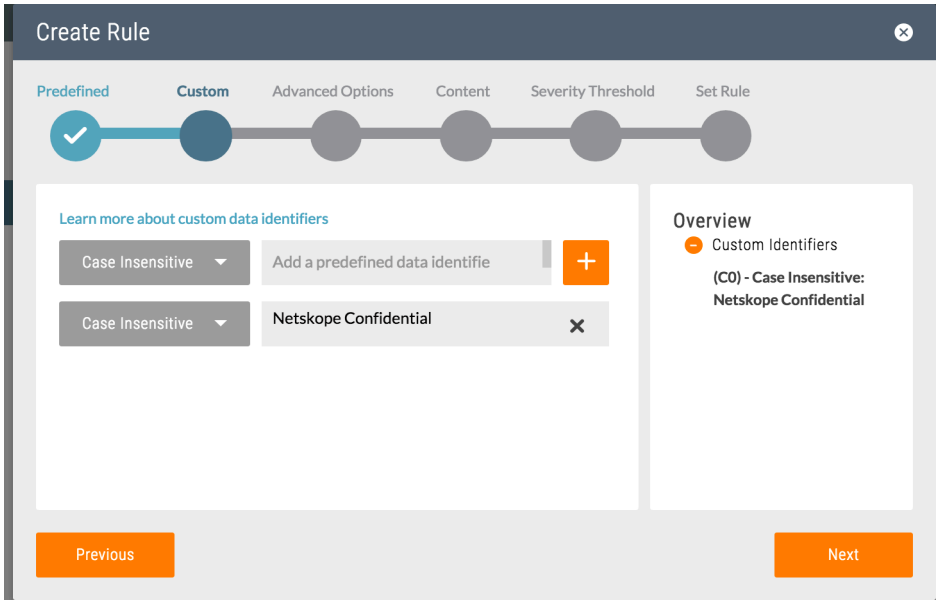
Example 4: A and B needs to be within the proximity of each other and there has to be either one of the identifiers C or D appearing any where in the document.

Expression: ((A NEAR B) AND (C OR D)).

> Note: C and D identifier should be configured as Global Data identifiers so they can match anywhere in the document

Custom DLP rule with custom identifier using keyword search

In the example below, DLP engine would look for keyword “Netskope Confidential” in the document.



Custom DLP Rules using regular expressions

This section describes the regular expressions syntax that DLP engine supports to define the regular expressions. The DLP engine parser interprets regular expression syntax nearly identically to the UNIX regular expression syntax. The engine’s regular expression syntax also includes some extensions for matching substrings.

Supported Operators

Table 1 lists the base regular expression operators available in the DLP engine and the pattern the operator matches.

Operator	Matched Pattern
\	Quote the next metacharacter.
^	Match the beginning of a line.
$	Match the end of a line.
.	Match any character (except newline).
|	Alternation
( )	Used for grouping to force operator precedence
[xy]	Character x or y
[x-z]	The range of characters between x and z
[^z]	Any character except z

Supported Quantifiers

Operator	Matched Pattern
*	Match 0 or more times
+	Match 1 or more times
?	Match 0 or 1 times
{n}	Match exactly n times
{n,}	Match atleast n times
{n,m}	Match atleast n times, but no more than m times

Metacharacters

Operator	Matched Pattern
\t	Match tab
\n	Match newline
\r	Match return
\f	Match form feed

\a	Match alarm (bell, beep and so on)
\e	Match escape
\v	Match vertical tab
\021	Match octal character (in this example, 21 octal)
\xF0	Match hex character (in this example, F0 hex)
\x{263a}	Match wide hex character (Unicode)
\w	Match word character (alphanum plus '_')
\W	Match non-word character
\s	Match whitespace character. This metacharacter also includes \n and \r
\S	Match non-whitespace character
\d	Match digit character
\D	Match non-digit character
\b	Match word boundary
\B	Match non-word boundary
\A	Match start of string (never match at line breaks)
\Z	Match end of string. Never match at line breaks; only match at the end of the final

Example 1: Simple regex to detect 16 digit credit card number

Regex: \d{4}-?\d{4}-?\d{4}-?\d{4}

\d – Checks for digit character.
{4} – Match exactly n times. It validates that there are exactly 4 digits.
-? – This would validate that the digits are occasionally separated by hyphen. ? indicates 0 or 1 times

This simple regex would validate it is 16 digit number occasionally separated by -.

Example matches: This regex would match 1234-5678-9123-4567 or 1234567891234567

Example 2: Regex to validate if the 16-digit credit card number is from a major credit card issuer

Matches major credit cards including: Visa (length 16, prefix 4) or MasterCard (length 16, prefix 51-55)

Regex: ^((4\d{3})|(5[1-5])\d{2})-?\d{4}-?\d{4}-?\d{4}

^ – Matches beginning of the line
4 – To validate if the first digit is 4. Visa card starts with 4
\d{3} – followed by 3 digits
| – Alternation is used for matching a single regular expression out of many possible regular expressions
(5[1-5]\d{2}) – Matches MasterCard prefix 51 to 55 followed by 2 digits
-? – This validates if the digits are occasionally separated by hyphens. ? Indicates 0 or

Example Matches: This would match 4001123456781234 or 5100123456781234

Example 3: Regex to check the medical record number

Assume you have a medical record number which is 16 characters long prefixed by word NWH to represent the patient record is from Northwestern Hospital, followed by first 3 letters of the first name and 3 letters of the last name, followed by 7 digits.

Regex: \b(NWH)-?[a-zA-Z]{3}-?[a-zA-Z]{3}-?\d{7}\b

\b – Match the word boundary (NWH)

– Looks for prefix NWH

-? – This is to check if 0 or 1 occurrence of "-" exists
[a-zA-z]{3} – Checks for three alphabet characters. It could be any character from a-z or A-Z
\d{7} – Check for seven digit character

Example matches: NWHCARVAN0000001 or NWH-TIM-BRO-0000002

DLP Profiles

DLP profile is defined as a collection of predefined or custom DLP rules. DLP profile can contain a single DLP rule or multiple DLP rules. When multiple DLP rules are defined they are considered as Boolean "OR" match. If any of the DLP rule matches then the DLP profile is matched.

DLP Predefined Profiles:

There are five predefined DLP profiles available to use in DLP policy. These profiles are built from rules that incorporate standard combinations of data identifiers. This includes Payment Card Information (PCI); Personally-Identifiable Information (PII); Electronic Personal Health Information (PHI), Source Code and Profanity.

DLP Custom Profiles

You can also create custom DLP profiles.

1. Navigate to Policies -> DLP -> Data Loss Prevention -> Profiles -> New Profile.

2. Choose one or more DLP rules.
3. Provide a name for the DLP profile and click Create profile.
4. Once profile is saved click Apply DLP changes to save the changes globally.

DLP Examples

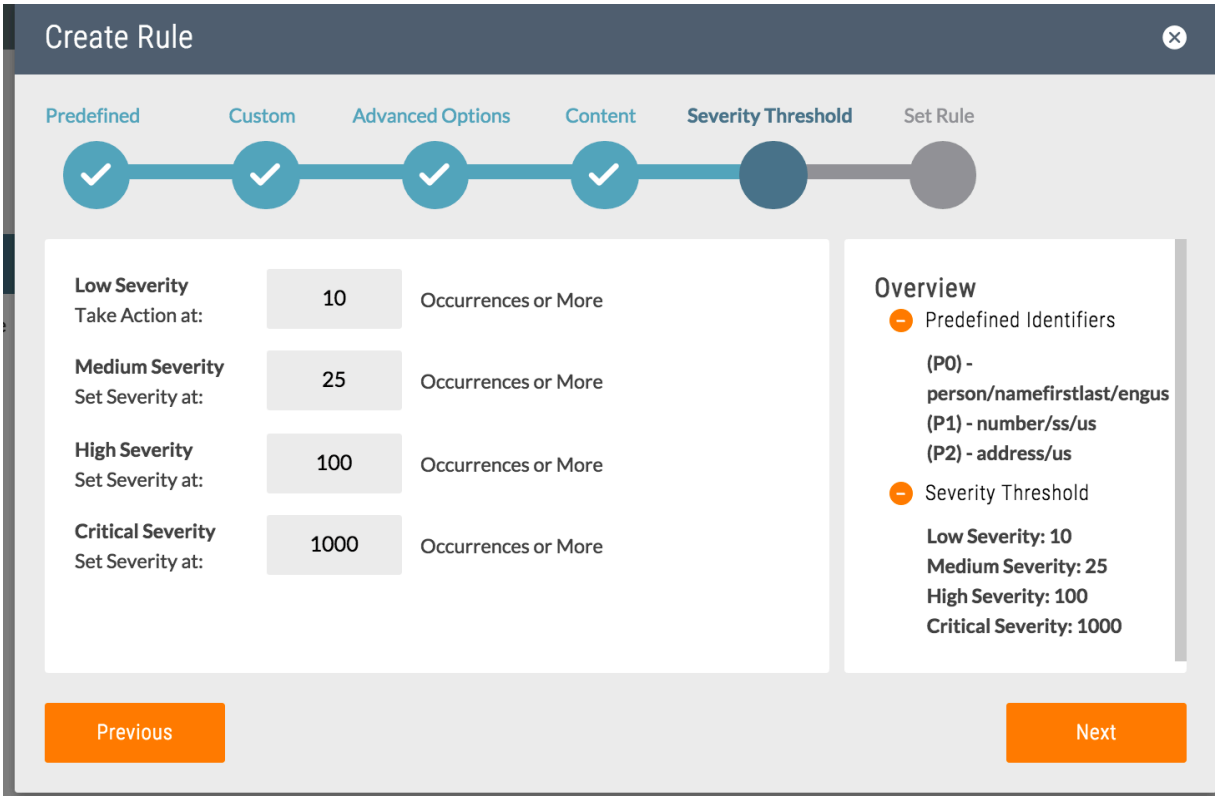
Enable DLP to inspect file uploads and file downloads on Google Drive.

- Match for any Personally identifiable data being sent. This includes User's first name and last name, SSN (dash delimited, space delimiter or no delimiter) and address.
- Look for any documents marked as "Confidential" that are uploaded
- Alert only if more than 10 occurrences are seen.

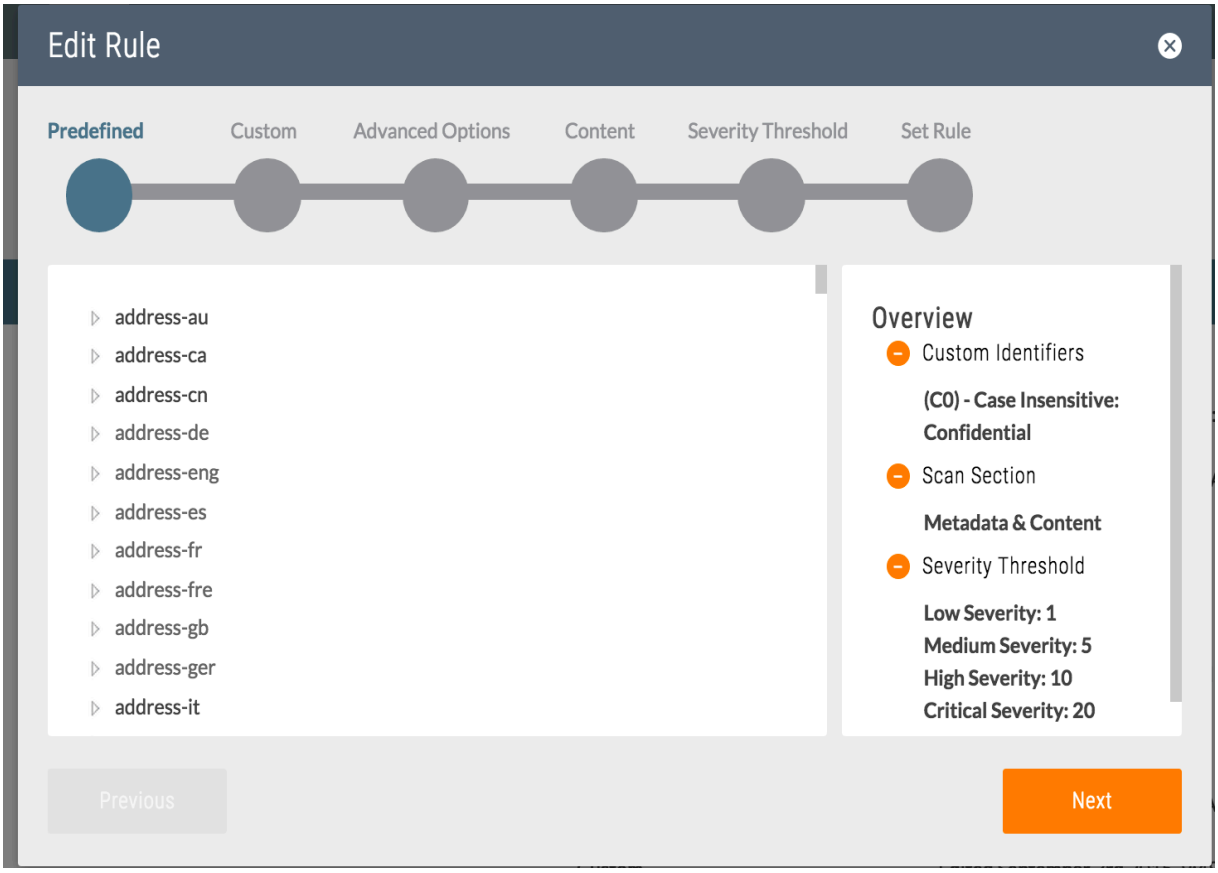
In order to achieve this, the first step is to create the DLP rules.

- Create a DLP rule that matches for the Personal identifiable information.
- Add the following Predefined data identifiers
  - Person-name-engus/namefirstlast -> Matches first & last name of the user
  - Number-ss-us -> Any number-ss-us-> Matches any social security number
  - Address-us -> Any address-us -> Matches US address
  - Change the count threshold to 10

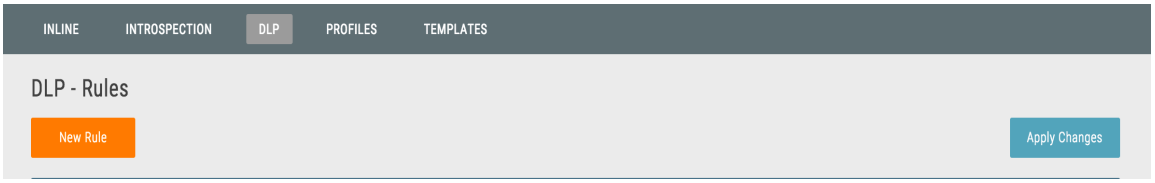
  Note: The data identifiers in DLP Rule are matched as Boolean "AND" if no Boolean expressions are specified i.e. all three values name, ssn, and address should be in the document for this to match.



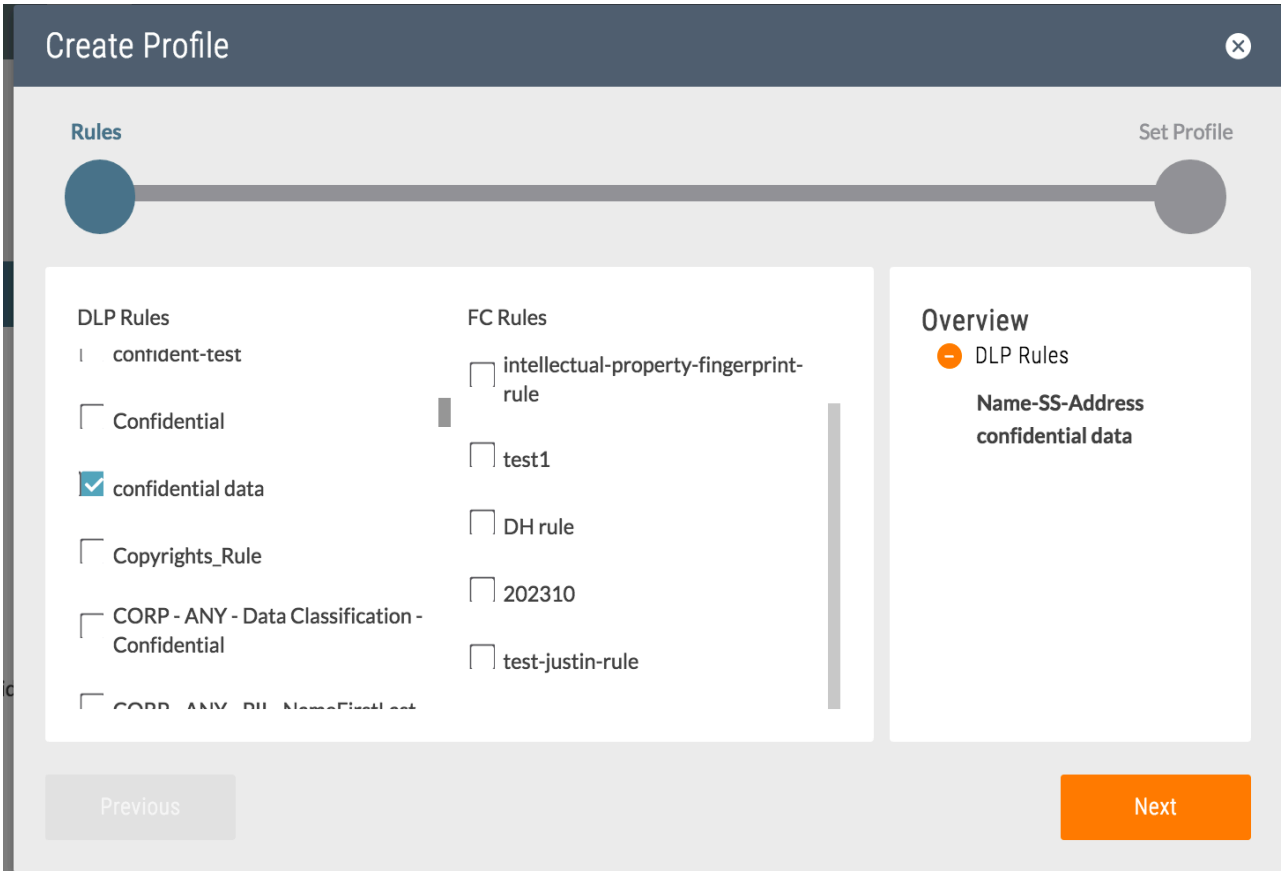
- Create a second DLP rule that matches for keyword “Confidential”
- Navigate to Policies–> DLP –> Data Loss Prevention –> Rules –> New Rule –> Add custom data identifier to match for keyword “Confidential”.
- Specify a rule name “confidential data”



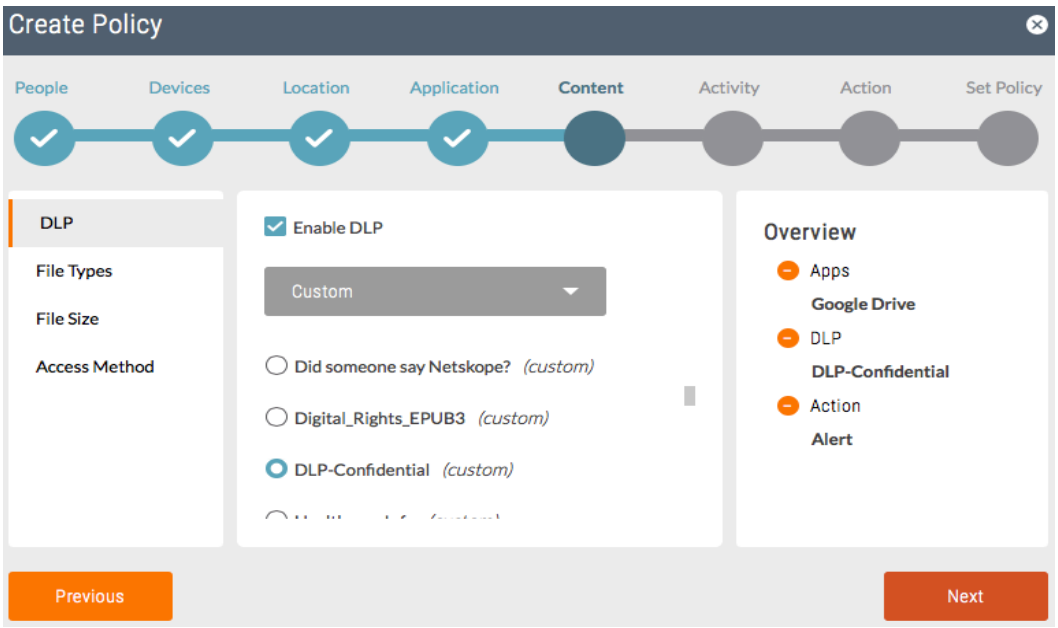
- Click “Apply changes” on the right hand corner to save the changes to DLP rules.



- Now create a DLP profile and add both the DLP rules added in the previous step.
- Provide a name and click “Create profile”
- Click “Apply changes” to save changes to DLP profile.



- Create a policy or edit a policy, under Inline, specify the DLP profile. Click Edit Policy or Create Policy to save the changes.

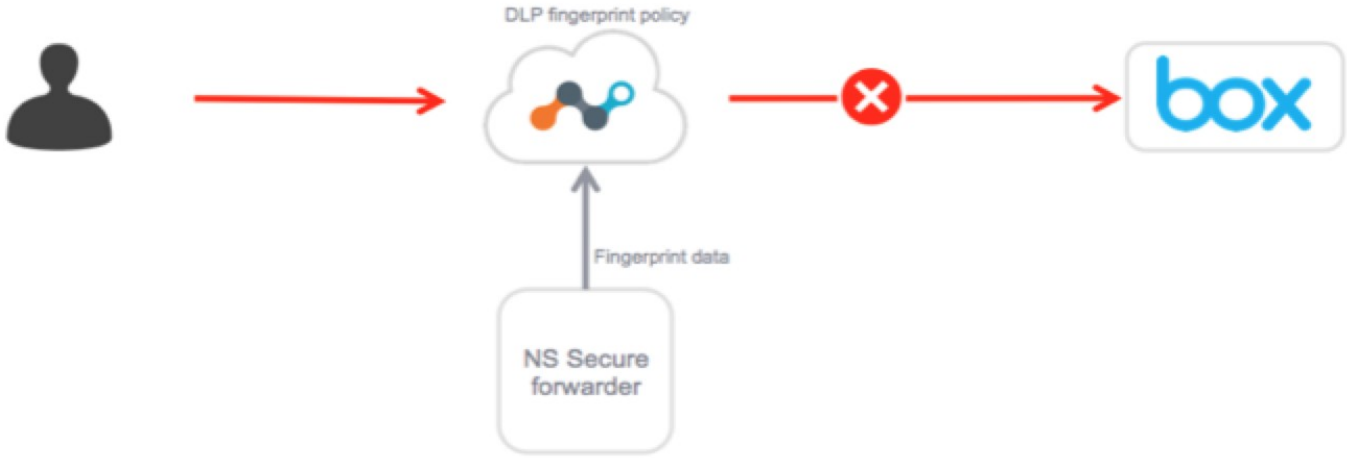


DLP Fingerprinting

DLP Fingerprinting is a methodology used to detect sensitive data in which the administrator provides a file to generate a fingerprint classification. The classification is then used to generate a DLP policy that checks whether a variant of the classification matches against an uploaded file.

DLP Fingerprinting allows administrators to protect confidential information by generating a unique DNA (classification) for sensitive files. This allows the Netskope DLP engine to create rules that capture variants or modified versions or the classified sensitive file.

The following diagram shows the DLP Fingerprinting workflow.



Fingerprint Use Cases

- Classifying an original document and creating a DLP rule/policy to trigger against modified versions
- Classifying a blank form and create a DLP rule / policy to trigger against forms completed with sensitive information.
- Creating a DLP rule / policy that will capture deliberate removal of confidential or private tags in a document.
- Fingerprinting is an alternative to create a set of individual rules to match a complex document.

Requirements and Limitations

- Files to be classified must be text-based. Common formats include: PDF, .doc,.txt, etc.
- File size limits:
  Max 100MB per file to generate a classification

  Max 15MB per file to trigger a DLP policy

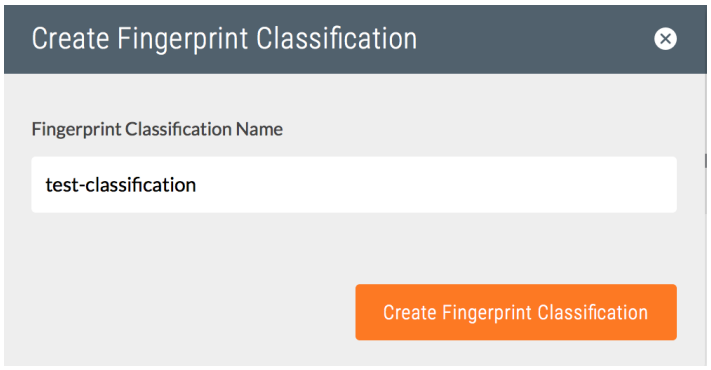
- The DLP policy will trigger only if the content match is at least 75% of the original classified file.

- The administrator will need access to Netskope tenant UI and have a Secure Forwarder connected to the tenant

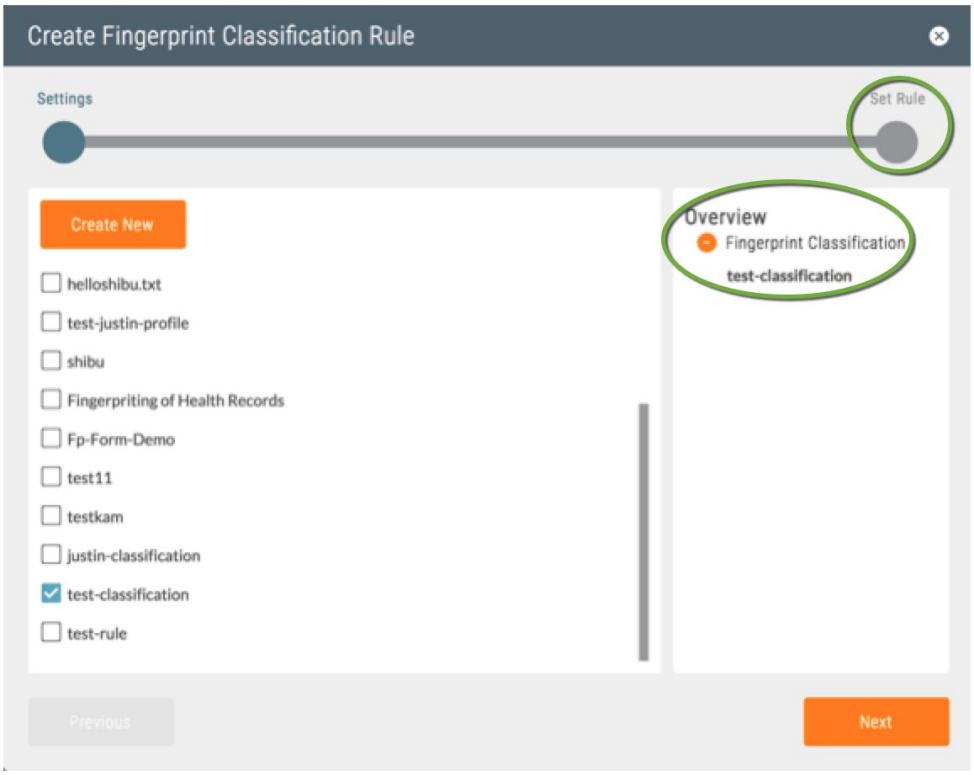
Creating a Fingerprint Classification Example Workflow

The following example walks you through the UI to create a Fingerprint Classification.

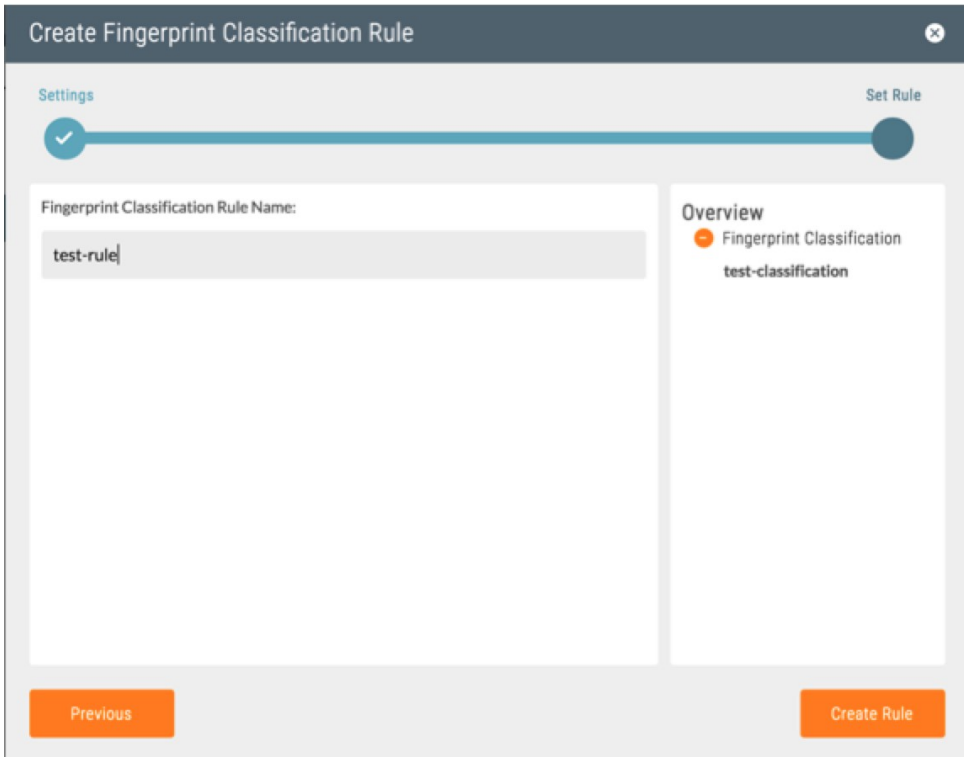
- Click Policies –> DLP-> Fingerprint Classification –> Profiles



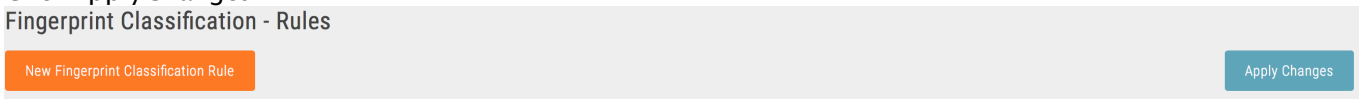
- The fingerprint classification profile created in the previous step needs to be added to a Rule. Click Policies –> DLP-> Fingerprint Classification –> Rules, Select the Fingerprint Classification profile



- Type a Fingerprint Classification Rule Name and click Create Rule.



- Click Apply Changes.



NOTE: Multiple classifications can be associated with a given fingerprinting rule.

- Upload the classified file to your Secure Forwarder. In this example, the file is called, sample_file.log.
- Run the following command in nsshell mode, after the file is uploaded to your Secure Forwarder

  nssecureforwarder> request dlpfingerprint generate classification test-classification path /tmp/sample_file.log

- **NOTE**: In place of test-classification, you should input the name of the DLP classification that you created in the previous step.

  Optionally, you can run the status command to validate the status of the fingerprinting.

  nssecureforwarder> request dlpfingerprint status

  Creating secure directory with prefix dlp in parent directory /tmp

  Starting process with command line ['/opt/ns/bin/nsdlp/nsdlp-fin- gerprint', '-c',u'test-classification', '-f', u'/tmp/sample_file.- log', '-o', '/tmp/dlpCSbJwN.25884']

  Process with pid 25893 for generating fingerprint has started

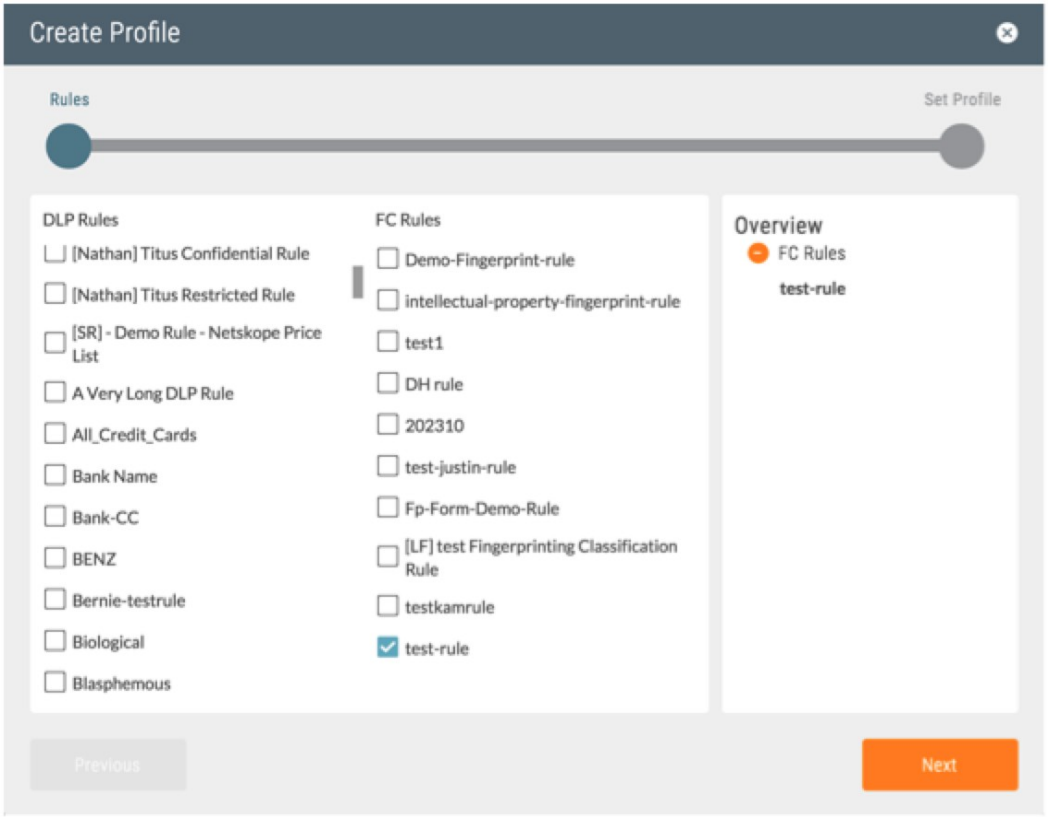
Process with pid 25893 for generating fingerprint has finished, return code 0

Uploaded classification journal file Uploaded

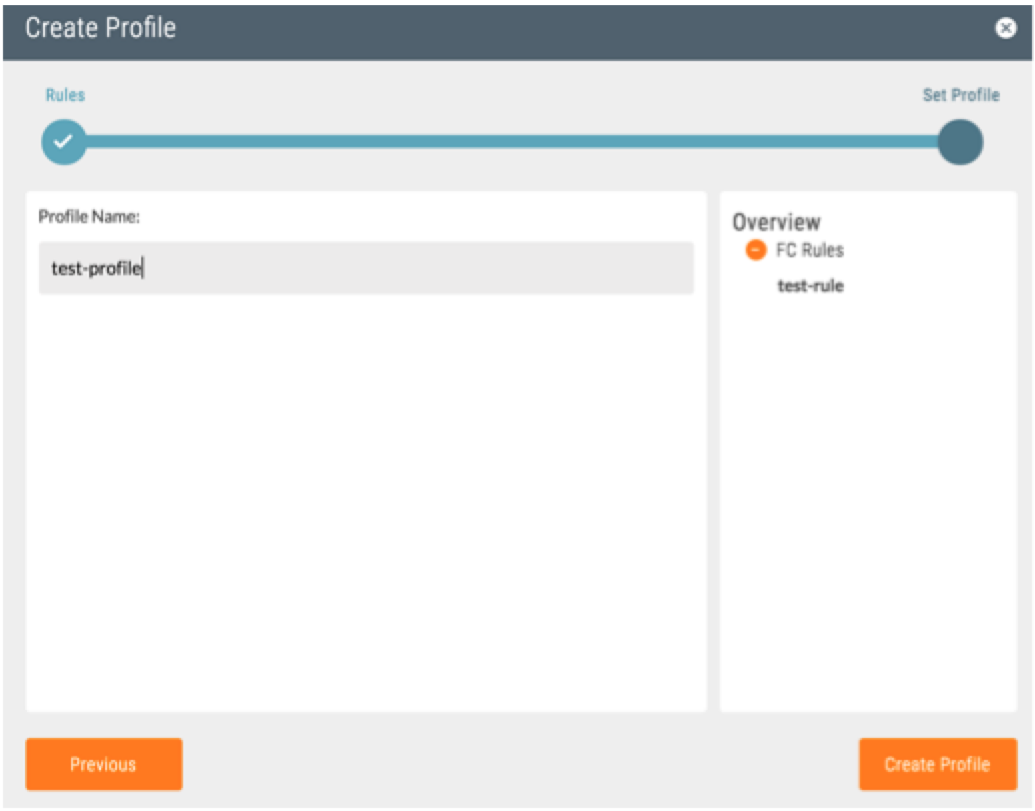
fingerprint keys journal file Fingerprint generation

complete

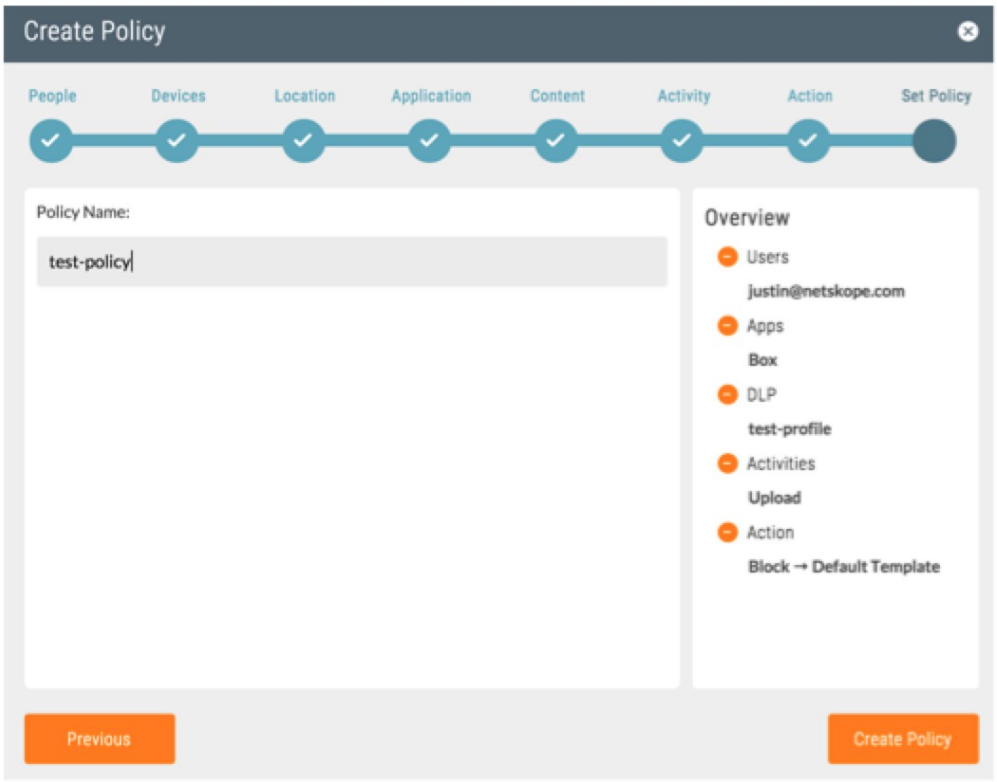
- Apply the new DLP fingerprinting rule to a DLP profile. Navigate to Policies -> DLP -> Data Loss Prevention -> Profiles -> New Profile. Select the Fingerprinting rule you created earlier.



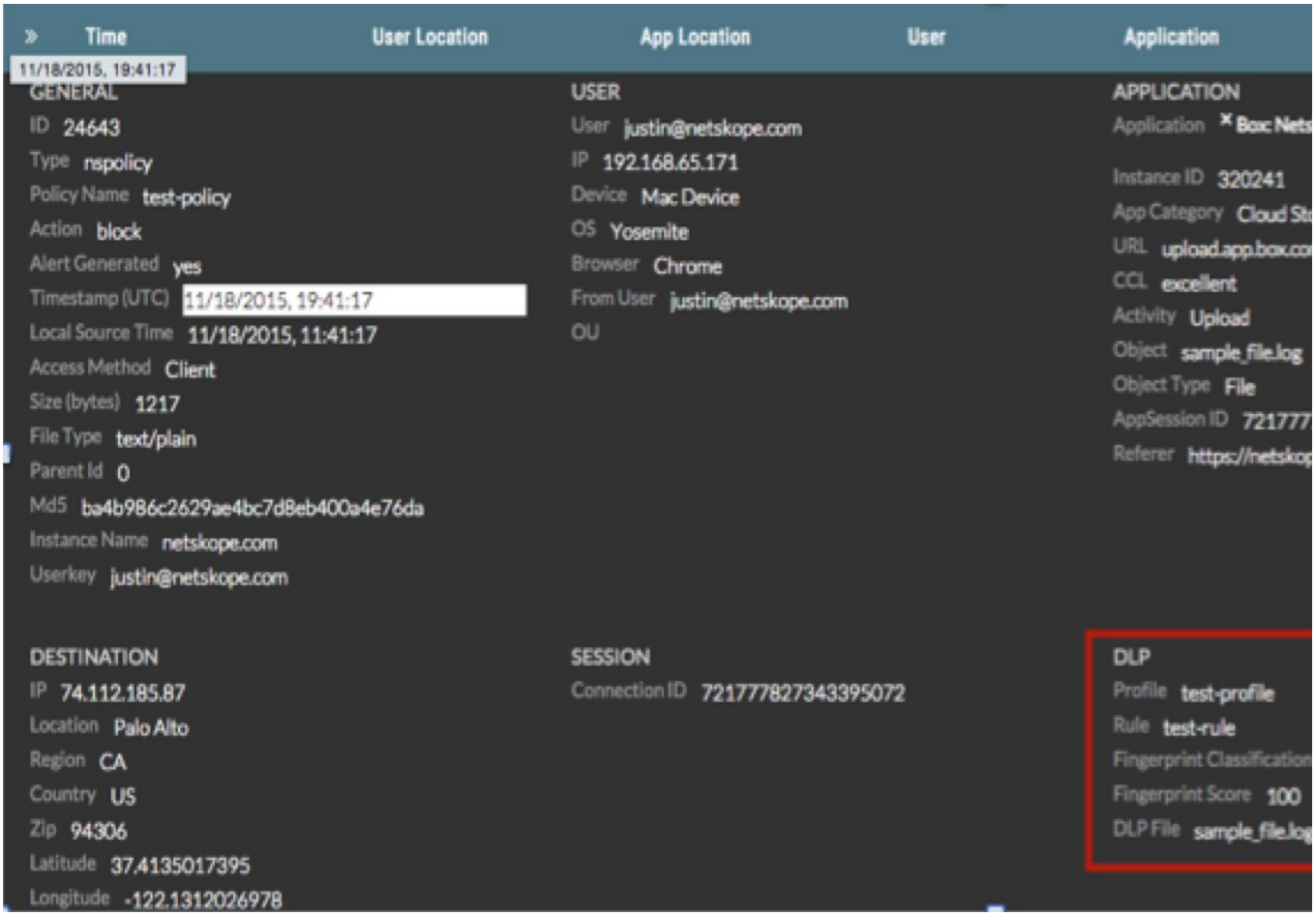
- Type a name for the profile and click Create Profile.



- Create an Inline policy with the new DLP Profile.



- Navigate to SkopeIT > Events to see an example of a blocked event, shown below.



DLP PDD

Overview

DLP Precise data detection (PDD) provides a mechanism to validate the presence or absence of the match result of an identifier against the data set provided by the user. Such a mechanism will reduce the false positives and guarantees precise data leak prevention of those of the entries in the data set.

Below are the couple sample use cases:

- Employee database where the intent is to prevent data leakage of SSN and Employee ID present in the database.

- A list of retail coupon codes formatted like credit card numbers but not valid credit card numbers. A credit card match result present in this data set will be ignored.

DLP PDD Workflow

The input data set should be in CSV format and the first row should contain the keyword or column name describing the data in its column. Essentially, each column name can be mapped to a DLP identifier for validation. This input data set will be uploaded to a secure forwarder which is on-premise virtual appliance deployed on customer's network. Once the data is uploaded to Secure Forwarder, each entry in the CSV will be SHA-256 hashed and sent to customer's tenant instance in the Netskope cloud.

Uploading data for DLP PDD

The input dataset will be uploaded to the Secure Forwarder. Please refer to the Secure forwarder installation guide for details on installing the virtual appliance.

- Upload the CSV file to a folder on the Secure Forwarder
- Run the following command from nsshell

  nsshell> request dlp-pdd upload file <filename> csv_delim <specify the delimiter> column_name_present <true or false>

  E.g
  request dlp-pdd upload file /home/nsadmin/fake_data_100.csv csv_delim ~ column_name_present true

  This command will generate hash for the data and upload it to customer's tenant instance in the Netskope cloud

- Verify the status of upload with command "request dlp-pdd status"

Configuring DLP Rules for DLP PDD

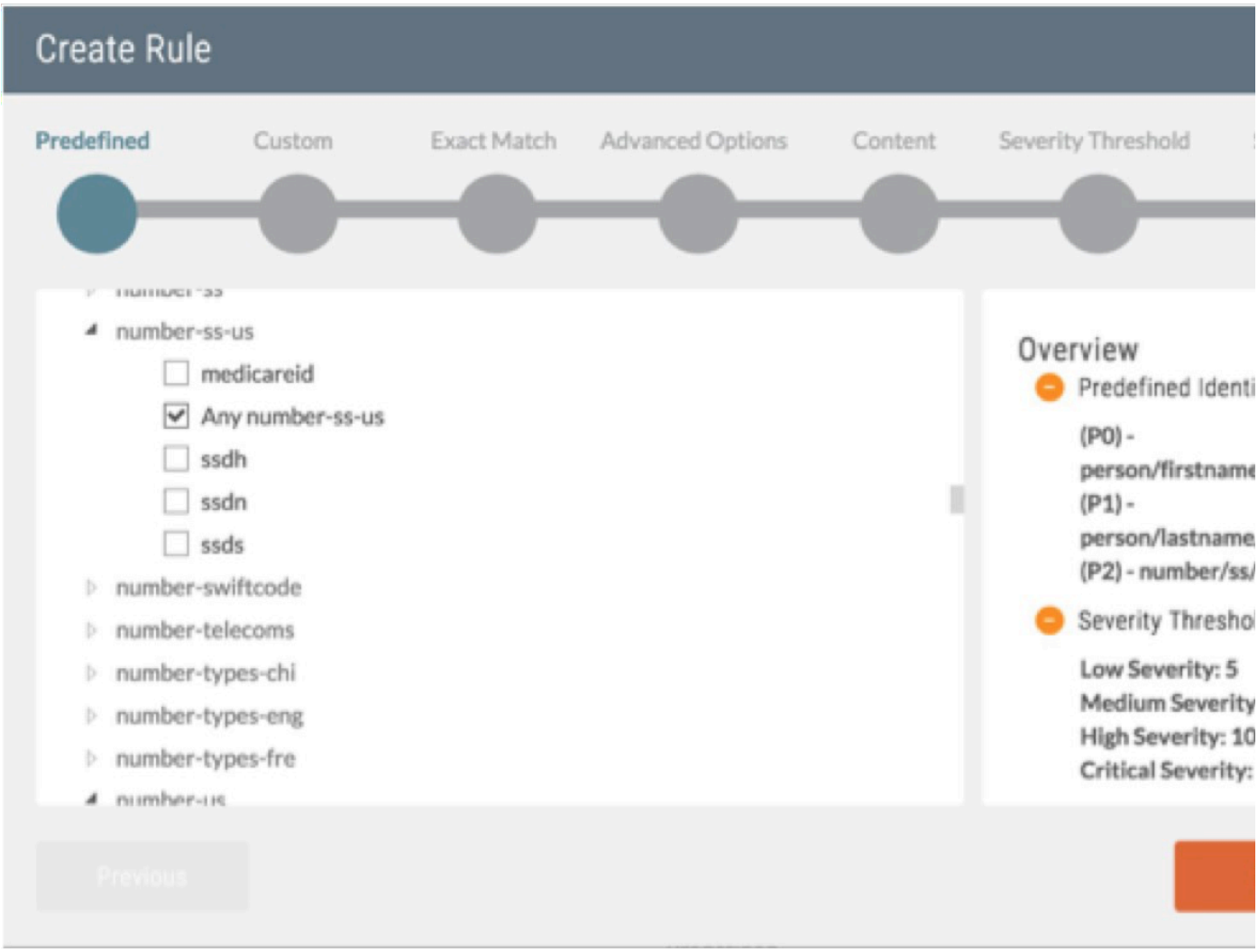
Once the hash is uploaded to customer's tenant instance in the Netskope cloud, you can now configure DLP rules to match the identifiers against the file upload

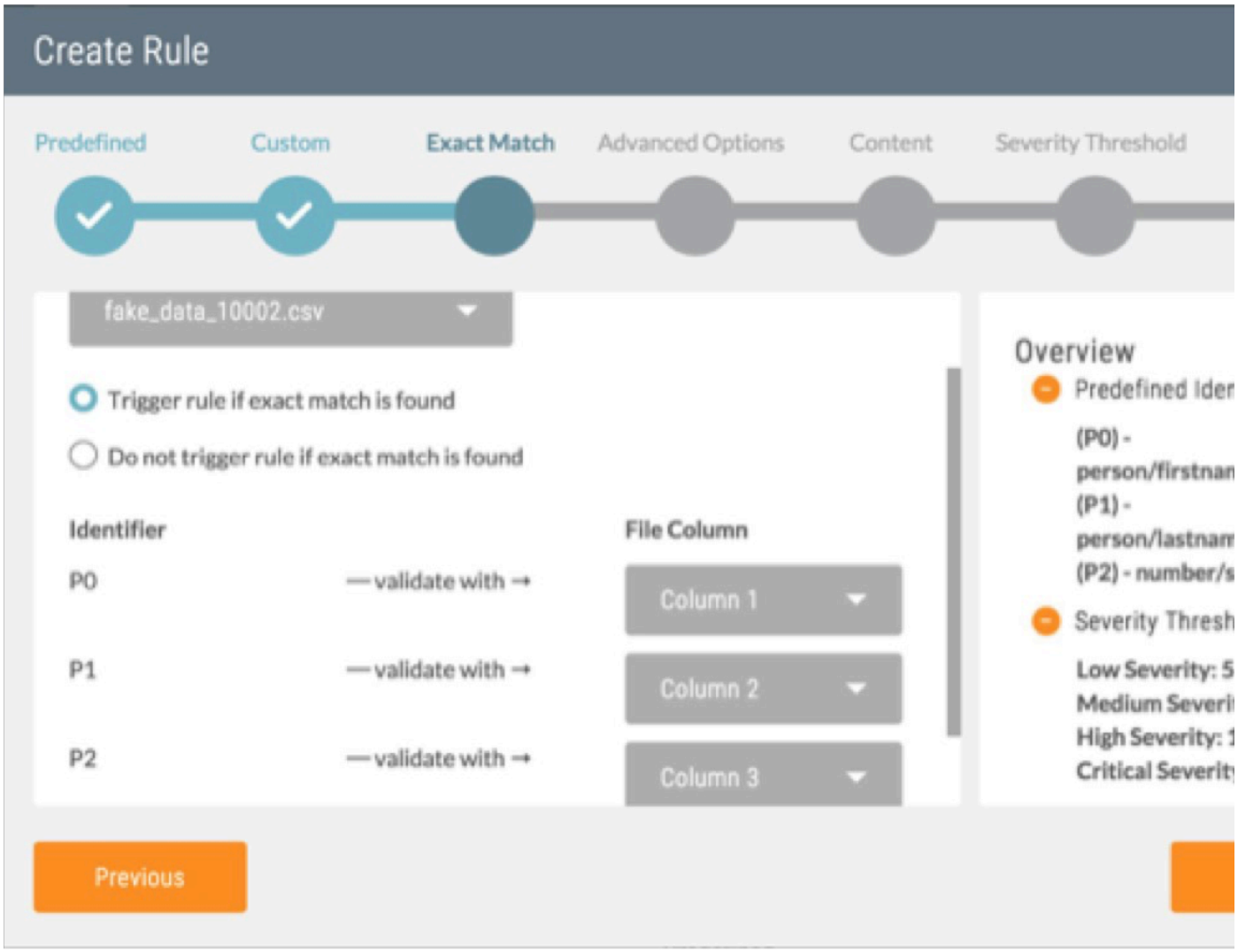
- Navigate to Policies > DLP > Rules

- Click New Rule

In this example, imagine you uploaded a file to secure forwarder that contained User firstname (Column 1), lastname (Column 2) and SSN dash delimited(Column 3). Each entry in the file will be SHA-256 hashed and uploaded to the tenant instance. In the DLP rule you need to match against the identifiers for firstname, lastname and SSN.

Choose Predefined identifiers, person-name-engus firstname and person-name- engus lastname and number-ss-us (Any number-ss-us). Choose ExactMatch, select the filename that was previously uploaded and map the column names to the identifier as shown in the screenshot below.





- Save the DLP rule and use this DLP rule created in the DLP profile.

Introspection Policies

Netskope Introspection (API Connectors) provide a complementary deployment model to provide Cloud Visibility, Policy and Data Security Services by directly connecting to the Cloud Service using the APIs published by the Cloud Service Provider.

You can enable introspection for cloud apps under Settings -> Introspection.

Introspection policies allow administrators to perform various automatic actions to user's files and folders within the cloud app. An Introspection policy can be used to scan content that resides in user's folders. DLP policies can be applied to detect DLP violations of data residing in the cloud app. This can be applied to data that is already residing in the cloud

app before the introspection was configured in Netskope as well as new data that is uploaded by the users.

An Introspection policy enables the following abilities:

- Visibility and discovery of sensitive data already residing within the cloud app instance and new data uploaded by users to the cloud app.
- Real time alerting of sensitive data
- The ability to force encryption of sensitive data.
- Ability to quarantine data or legal-hold the data for legal purposes
- Ability to change file permissions.

API Connector Policy Actions

Administrators can setup various actions to perform once a policy is triggered.

Netskope supports the following actions to mitigate risk exposure:

- Alert – Generates an alert under SkopeIT -> Alerts when the policy matches.
- Restrict Access – Depending on the app, there are different options available to restrict a publically or externally shared file. See the table below for details on different restriction options
- Change Ownership – this will make the designated administrator owner of files and folders for which the policy is hit.
- Encrypt – An administrator can choose to encrypt the files if it matches policy criteria. Encryption and must be enabled in your tenant to take advantage of this feature. Please contact support (support@netskope.com) if you do not see this as an action in the policies.
- Quarantine – If a user uploads a document that has DLP violation, an administrator can now take an action to quarantine the file. This will move the file to a quarantine folder for the administrator to review and take appropriate action (allow the file to be uploaded or block the file form being uploaded)
- Legal Hold – A **legal hold** is a process that an organization uses to preserve all forms of relevant information when litigation is reasonably anticipated. Admin can choose to have a copy of the file saved for legal purpose if it matches policy criteria.

The table lists the actions possible in Introspection policy in each app.

App	Alert	Change Ownership	Encrypt	Legal Hold	Quarantine	Restrict Access (to Owner)	Restrict Access to Internal	Restrict Access to specific domain	Restrict Access - Remove public links	Restrict collaborators to View only permissions	Rest collaratorDon' allovprintdownad
Box	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Google drive	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Microsoft Onedrive	Yes	No	Yes	Yes	Yes	Yes #	Yes #	Yes #	Yes #	No	No
Microsoft Sharepoint	Yes	No	Yes	No	No	Yes #	Yes #	Yes #	Yes #	No	No
Sales Force Unstructured data (Files)	Yes	No	No	Yes	No	No	No	No	No	No	No
Sales Force Structuted data (Chatter Messages and Chatte	Yes	No	No	Yes	No	No	No	No	No	No	No

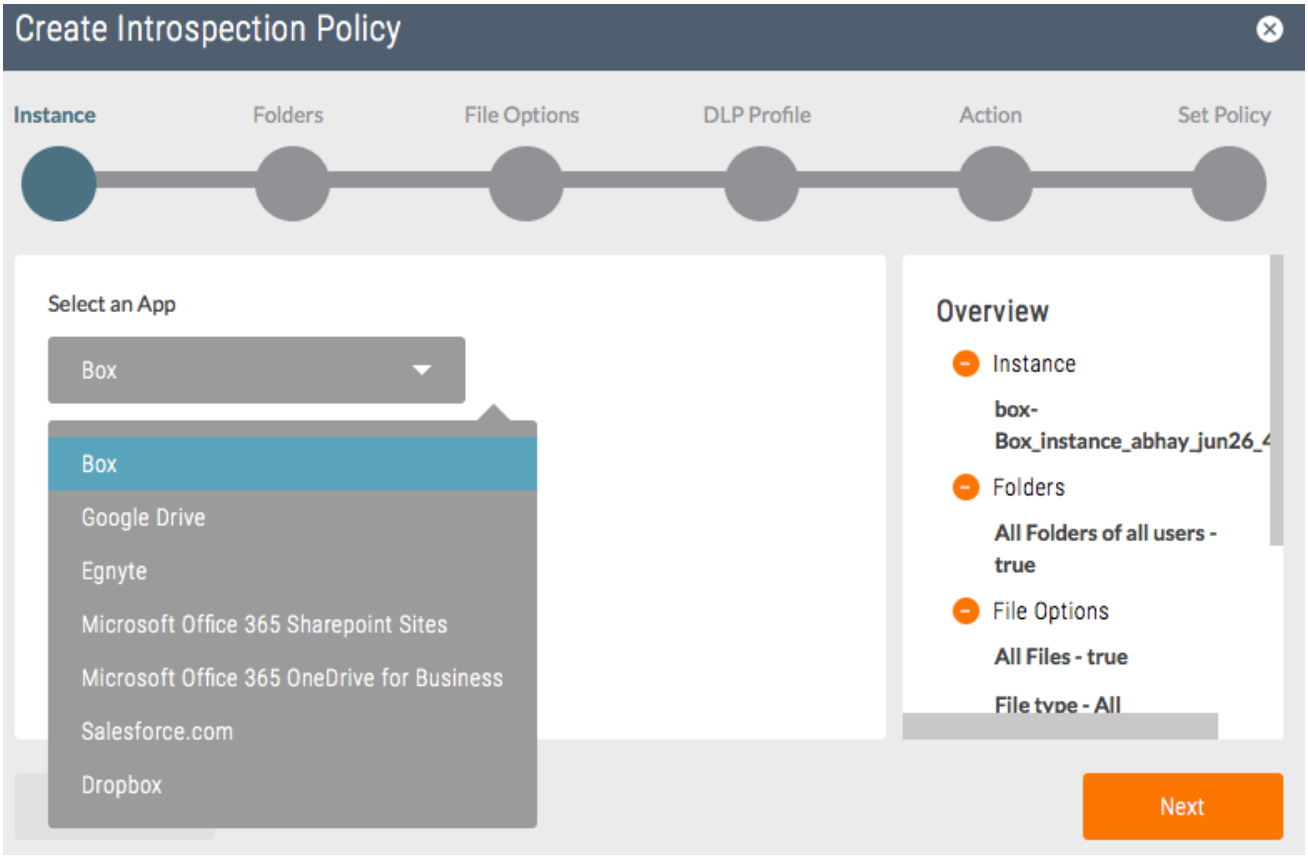
App	Alert	Change Ownership	Encrypt	Legal Hold	Quarantine	Restrict Access (to Owner)	Restrict Access to Internal	Restrict Access to specific domain	Restrict Access - Remove public links	Restrict collaborators to View only permissions	Rest t colla rato Don' allov print down ad
r Posts)											
Dropbox	Yes	No	Yes	No	No	No	No	No	No	No	No
Egnyte	Yes	Yes	Yes	No	No	No	No	No	No	No	No
ServiceNow	Yes	No	No	No	No	No	No	No	No	No	No

Configuring Introspection Policies

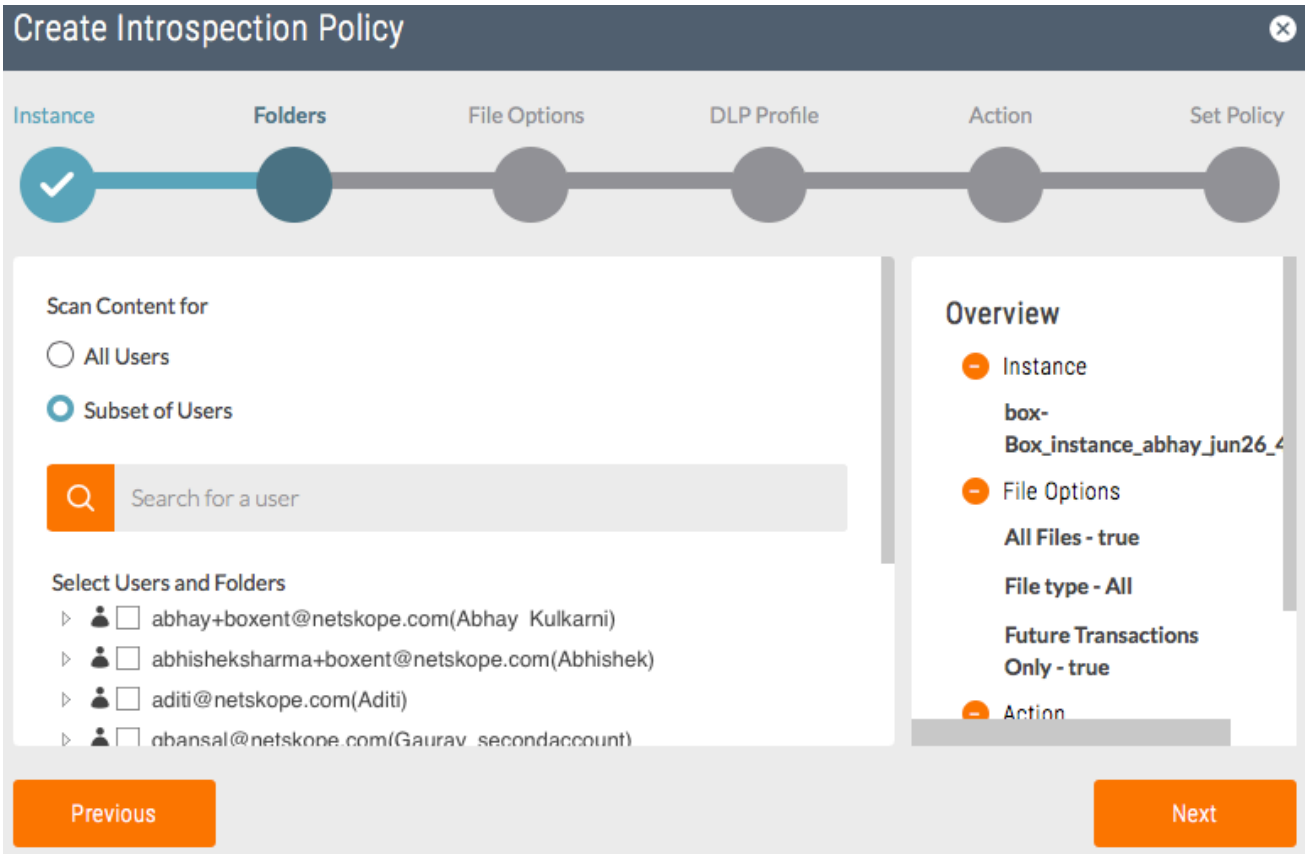
Organizations looking to discover existing content residing within your sanctioned cloud services like Box can do so by enabling the Introspection policies with the desired options and actions. To quickly setup a policy to discover content on your App instance you will need to browse to:

Policies > Introspection > New Policy

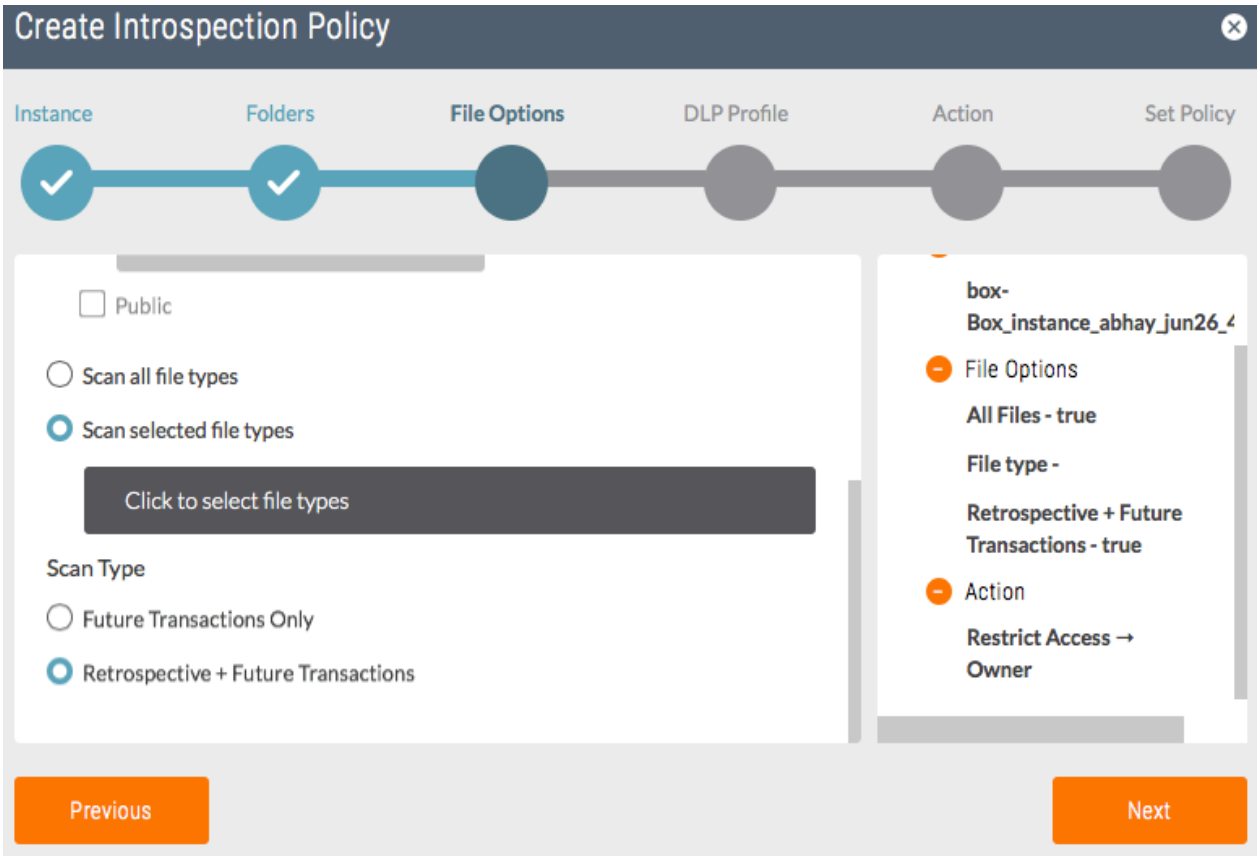
- In the policy UI select the App as well as the Application instance you would like to apply the policy to. Then Click Next.



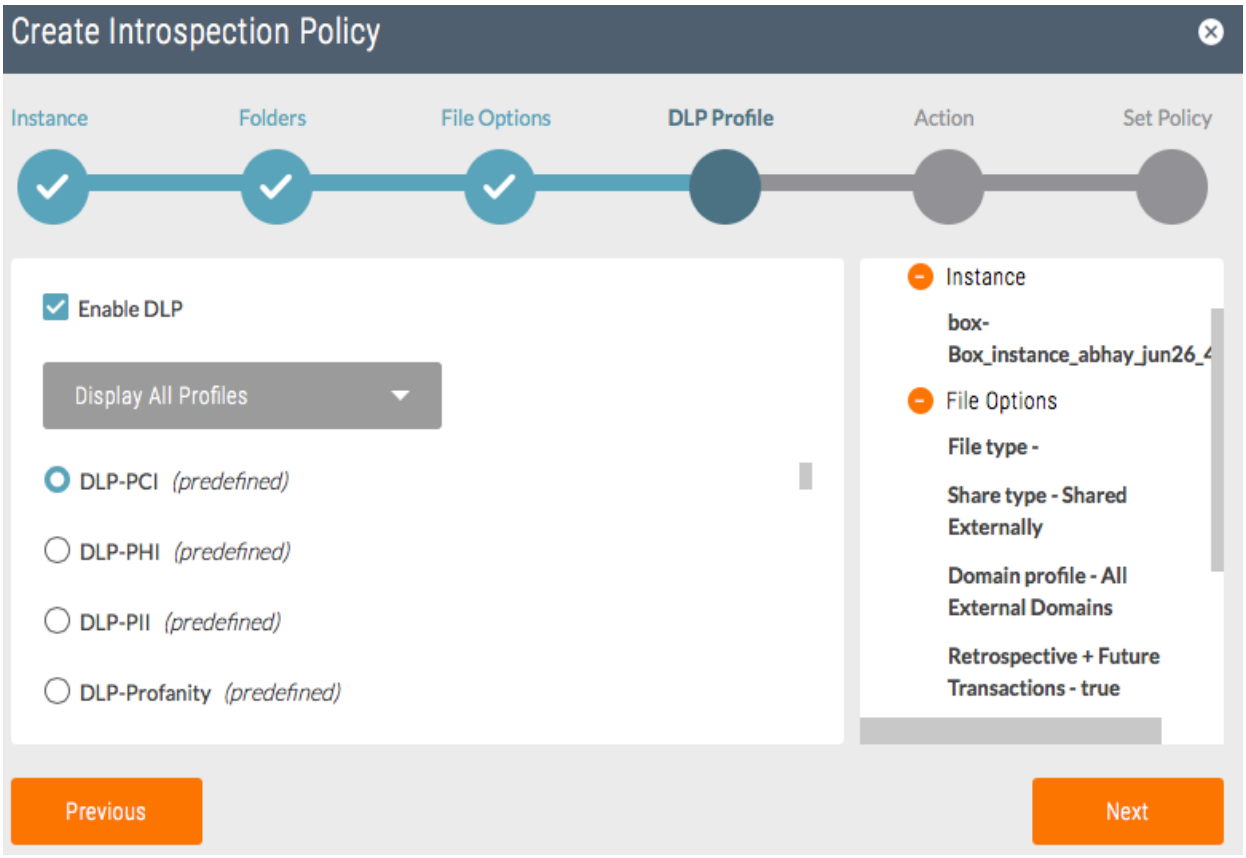
- On the Folders tab select the users you would like to apply this policy to. You can search for and select specific users (or specific folders within each user) or apply to all users. Note the list of all users (and folders of users) who have a Box account will be automatically be displayed. Click Next.



- On the File Options tab select the files you would like to scan. By selecting Scan Type > Retrospective + Future Transactions, DLP policies can be run against data that may have already been uploaded,to identify sensitive data that may lead to unintentional risky exposure. Click Next.

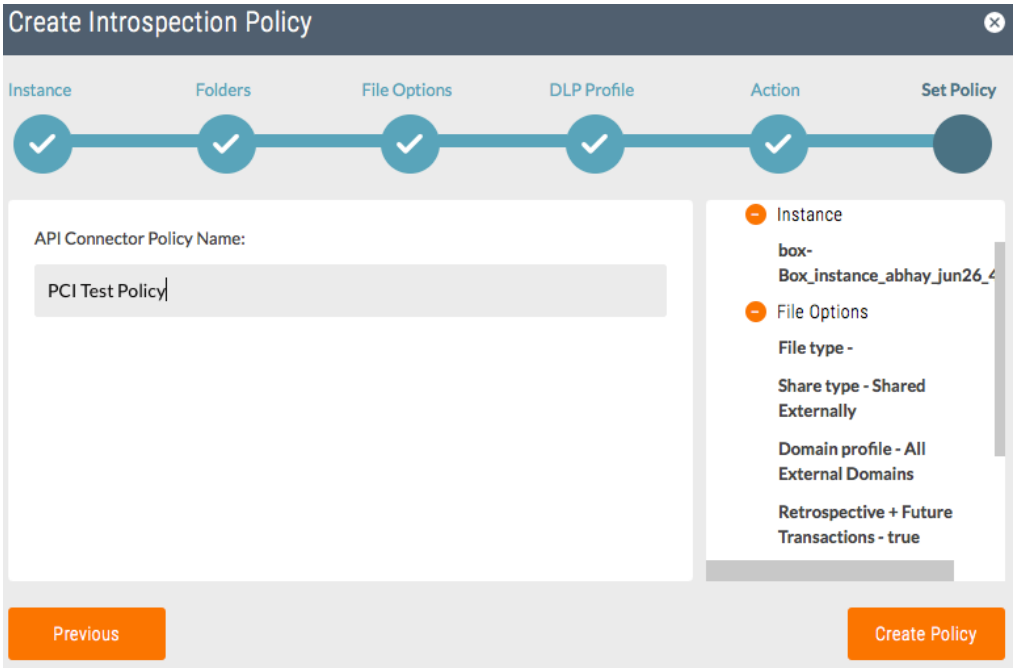


- On the DLP Profile tab select enable DLP and select the DLP policy you would like to enable. Refer to the DLP section for details on configuring DLP profiles and rules. Note if the DLP enable box is not checked and no policy is selected the action will be applied to all files matching the policy.. Click Next.



- On the Action tab select the action you would like to take such as Restrict Access, Encrypt, Alert, Quarantine, or Legal Hold. Click Next.

- On the Name tab, type the name you would like to use to identify this policy. Click Create Policy.



The policy that we just created will scan all files of all folders in the Box instance and alert any time there is any PCI content within the files.

Using REST API

Netskope provides REST API to extract the cloud apps data from SkopeIT events, alerts and reports.

Netskope REST API uses an auth token to make authorized calls to the API. The token is available in the tenant UI under Settings → Tools -> Rest API.

The token should be passed in every REST API call for the tenant. Netskope's REST APIs provide access to resources via URI paths. HTTP GET is the only supported method.

The format is as follows:

https://<tenant-name>.goskope.com/api/v1/<endpointname>?token=<token>&<queryparameters>

Valid endpoint names and query parameters are described below. The token passed is the token obtained from the tenant UI.

HTTP Responses

Netskope REST API uses JSON format for all the responses with the following error codes:

HTTP Response Code	Explanation
200	Success
403	Unauthorized
404	Not found
500	Internal server error
503	Service under maintenance

HTTP Endpoints

The following lists the various endpoints in the Netskope REST API.

https://<tenant-name>.goskope.com/api/v1/events

This endpoint returns events extracted from SaaS traffic and or logs. Valid query parameters are:

Event

Parameter	Value constraints	Description
query	Valid event query. Refer Appendix 1 for details on the query language. Appendix 2 provides the list of all the event fields	This acts as a filter for all the cloud app events in the events database.
type	connection|application|audit	Select connection events or application events. Application events are triggered for user actions inside the cloud app. Connection events are triggered for the http/https connection.
timeperiod	3600 | 86400 | 604800 | 2592000	Last 60 mins | Last 24 Hrs | Last 7 Days | Last 30 Days

starttime	Unix epoch time	Restrict events to those that have timestamps greater than this. Needed only if timeperiod is not passed.
endtime	Unix epoch time	Restrict events to those that have timestamps less than or equal to this. Needed only if timeperiod is not passed.
limit	Positive integer less than 5000	Limit the number of events returned (useful for pagination in combination with skip)
skip	Positive integer	Skip over some of the events (useful for pagination in combination with limit)

https://<tenant-name>.goskope.com/api/v1/alerts

This endpoint returns alerts generated by Netskope, including policy, DLP and watch list alerts. Policy alerts are triggered when traffic matches policy. DLP alerts are generated when there is a DLP violation triggered by the policy. Watch list alerts are triggered when watchlist matches.

Valid query parameters are:

Parameter	Value constraints	Description
query	Valid event query. Refer Appendix 1 for details on the query language.	This acts as a filter for all the alert events in the events database.
type	policy|dlp|watchlist|quarantine	Selects Policy, DLP, Quarantine or Watch list alerts. If nothing passed then it gets alerts of all types.
timeperiod	3600 | 86400 | 604800 | 2592000	Last 60 mins | Last 24 Hrs | Last 7 Days | Last 30 Days

starttime	Unix epoch time	Restrict events to those that have timestamps greater than this. Needed only if timeperiod is not passed.
endtime	Unix epoch time	Restrict events to those that have timestamps less than or equal to this. Needed only if timeperiod is not passed.
limit	Positive integer less than 5000	Limit the number of events returned (useful for pagination in combination with skip)
skip	Positive integer	Skip over some of the events (useful for pagination in combination with limit)

https://<tenant-name>.goskope.com/api/v1/report

This endpoint returns the result of a report generated on one of the fields on the summarization database. Valid query parameters are:

Parameter	Value constraints	Description
query	Valid event query. Refer Appendix 1 for details on the query language	This acts as a filter on all the entries in the database
type	application|connection|alert	Selects application events, connection events or alerts(policy, dlp, quarantine, watchlist)
groupby	application|user|device|activity	Note: Activity is only available for type = application or alert
timeperiod	3600 | 86400 | 604800 | 2592000	Last 60 mins | Last 24 Hrs | Last 7 Days | Last 30 Days
starttime	Unix epoch time (rounded off to nearest period)	Restrict events to those that have timestamps greater than this. Needed

		only if timeperiod is not passed.
endtime	Unix epoch time (rounded off to nearest period)	Restrict events to those that have timestamps less than or equal to this. Needed only if timeperiod is not passed.
limit	Positive integer less than 5000	Limit the number of events returned (useful for pagination in combination with skip)
skip	Positive integer	Skip over some of the events (useful for pagination in combination with limit)

https://tenant.goskope.com/api/v1/userconfig

This endpoint returns the user configuration items for specified users. You can retrieve the IOS mobile profile or Netskope Agent config for an user. Valid query parameters are:

Parameter	Value constraints	Description
email	valid emailID	This is the email ID of the user for whom the iOS profile or agent config is to be fetched
configtype	valid values are 'ios' and 'agent'	If the value is ios then the ios profile of the user is returned and if the value is 'agent' then the branding info for the user (the contents of the nsbranding.json) is returned

The response format is same as what is specified in the 'Response' section above, just that the data will be an array with just one json entry with the format:

For configtype 'ios'

- { "email" : "a@mycompany.com", "profile" : "....." }

  For configtype 'agent'

- { "email" : "a@mycompany.com",
  "brandingdata" : {"SFCheckerHost":"sfchecker.goskope.com",.....,"OrgName":"Shire"} }

Note that the iOS profile data will be xml string, the users of this API are recommended to get the data and store it in a file, and this file would be the iOS profile config file. As the profile size is big (50+ KB), fetch of only one profile at a time is supported.

https://tenant.goskope.com/api/v1/logstatus

Parameter	Value Constraints	Description
Filename	-	Name of log file. If not passed then a list of log files will be returned.
timeperiod	3600 | 86400 | 604800 | 2592000	Last 60 mins | Last 24 Hrs | Last 7 Days | Last 30 Days
starttime	Unix epoch time (rounded off to nearest period)	Restrict events to those that have timestamps greater than this. Needed only if time period is not passed.
endtime	Unix epoch time (rounded off to nearest period)	Restrict events to those that have timestamps less than or equal to this. Needed only if time period is not passed.
limit	Positive integer less than 5000	Limit the number of events returned (useful for pagination in combination with skip)
skip	Positive integer	Skip over some of the events (useful for pagination in combination with limit)

Examples

Query for application events for the past 24 hours

https://tenant1.goskope.com/api/v1/events?token=<token-number>&type=application&timeperiod=86400

- Endpoint name used is event

- Set type= application
- Set timeperiod = 86400

Query for all the application events for “app eq Dropbox” for the past 24 hours

https://tenant1.goskope.com/api/v1/events?token=<token-number>&query=app%20eq%20Dropbox&type=application&timeperiod=86400

- set query=app eq Dropbox
  Note: Set the URL encoded values for the query. app%20eq%dropbox

Query for all the DLP alerts for the past 24 hours

https://tenant1.goskope.com/api/v1/alerts?token=<token-number>&type=dlp&timeperiod=86400

- Endpoint name is alert
- set type=dlp
- set timeperiod=86400

Query for DLP violations grouped by user

https://tenant1.goskope.com/api/v1/report?token=<token-number>&query=alert_type eq DLP&type=alert&groupby=user&timeperiod=2592000

- set endpoint name as report
- set query=’alert_type eq DLP’ to query for DLP alerts
- set type=alert to query for DLP alerts
- set groupby=user

DLP Quarantine

The enterprise administrator may define an inline DLP Policy and associate a quarantine profile with this policy with action set to ‘Quarantine’. When DLP policy is triggered on a file upload, the file will now be quarantined. The file is blocked from being actually uploaded to the intended cloud app and it is deposited into the administrator designated "quarantine folder".

The administrator can designate a Box cloud app folder as the designated quarantine folder for that enterprise in order to store the "quarantined" files. The administrator can define in each quarantine profile, a person (or a set of persons), as identified by their email address(es), as the designated approvers for the quarantined files.

When a file is determined to be "quarantined", the user is served with a special "quarantine page" which notifies the user that their file was "quarantined" and to contact the "approver" whose email address is listed in the "quarantine page" for further information. The approver can now inspect the quarantined files on Box Quarantine folder and take further remedial action such as blocking or allowing this file to be uploaded

DLP Quarantine workflow using API

a. Administrator can use the REST API to query list of alerts generated in the Netskope cloud with action of Quarantine.

https://tenant1.goskope.com/api/v1/alerts?token=<token-number>&type=quarantine&timeperiod=86400

This will return all the alerts generated by DLP policy with action of Quarantine. Each event will have a field called "quarantine_file_id".

b. Administrator can now use API to allow or block the upload of this quarantined file. If the file is approved, the Netskope cloud solution will send out an email to the original user who had tried to upload the file informing them that their file is now allowed to be uploaded to their intended destination and they can proceed to uploading it again. If the file is blocked then administrator has to send an email to the user out-of-band to indicate the remedial action to be taken by the user.

To allow the file to be uploaded:

GET /quarantine/action?action=allow_file_1&dest=https%3A%2F%2Ftenant.goskope.com&fileid=<quarantine_file_id>

E.g

https://tenant.goskope.com/quarantine/action?action=allow_file_1&dest=https%3A%2F%2Ftenant.goskope.com&fileid=22558027549

You will see a http response "Future uploads of this file by user <username> to application <appname> will be allowed.

To block the quarantined file from being uploaded:

GET /quarantine/action?action=block_file_1&dest=https%3A%2F%2Ftenant.goskope.com&fileid=<quarantine_file_id>

E.g
https://tenant.goskope.com/quarantine/action?action=block_file_1&dest=https%3A%2F%2Ftenant.goskope.com&fileid=22558027549
You will see a http response "Future uploads of this file by user <username> to application <appname> will be blocked

To view the details of the event:

GET /quarantine/action?action=view_event_1&dest=https%3A%2F%2Ftenant.goskope.com&fileid=<quarantine_file_id>

E.g
https://tenant.goskope.com/quarantine/action?action=view_event_1&dest=https%3A%2F%2Ftenant.goskope.com&fileid=22558027549