DLP Configuration Guide

About This Document

This guide outlines the essential steps to configure Versa Networks' Data Loss Prevention (DLP), helping you quickly deploy and manage policies to protect sensitive data across your network and cloud applications.

Versa Networks' Network DLP provides comprehensive data protection across multiple communication channels including email, web, chat, SaaS applications, and cloud storage. With native SSL/TLS inspection, it applies DLP policies to encrypted traffic and supports a wide range of file types and metadata, including OCR for PDFs and images.

Versa's unified policy engine ensures consistent management across its security and DLP services from a single interface. Integrated with CASB capabilities, it delivers deep visibility and control over sensitive data in both on-premises and cloud environments.

Its intuitive UI, built-in templates, best practices, and analytics make it easy to deploy and manage, while supporting compliance with standards like HIPAA, PCI and GDPR.

Document Information

Title	**DLP Configuration Guide**
Author	Versa Professional Services
Version	V 1.0

Disclaimer

Information contained in this document regarding Versa Networks (the Company) is considered proprietary.

Before you begin

Before you proceed with the steps outlined in this document, please ensure you've met the following pre-requisites.

- The provider administrator must complete your tenant configuration. If you haven't received this information, please get in touch with your Managed Service Provider or Account Manager for assistance.
- You have the Enterprise Administrator (Tenant Admin) credentials for the Versa SASE portal, also called the Concerto User Interface.

How DLP is Configured in Versa

Versa's DLP configuration follows a modular, layered approach — building complex protections from simple, reusable components. The process consists of defining and combining key building blocks in a nested structure:

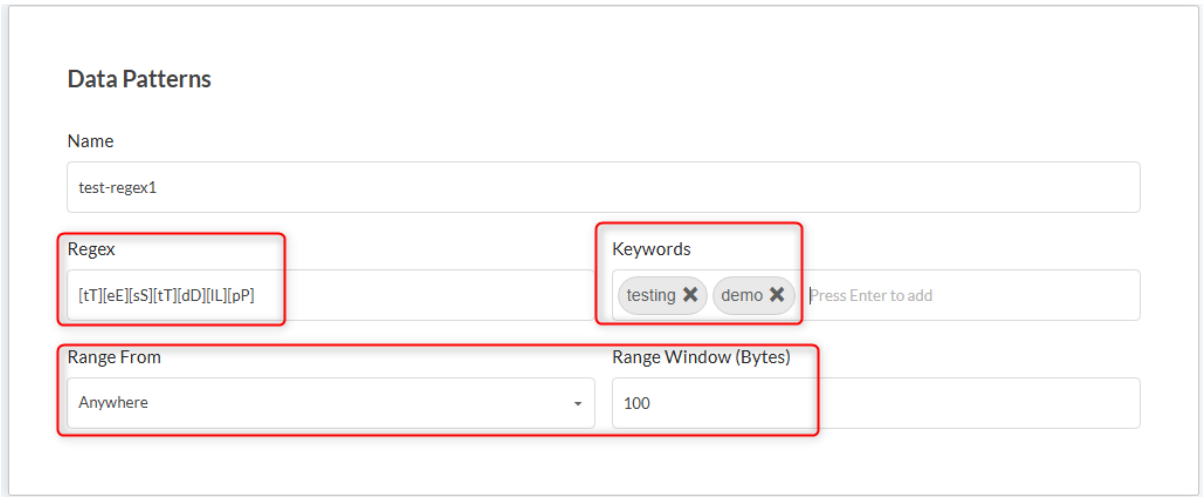
Data Patterns

These are the most granular elements of the DLP system. A Data Pattern typically consists of a regular expression (regex) used to detect specific values such as keywords, patterns (e.g., credit card numbers), or sensitive terms. Administrators can define custom patterns or use Versa's rich library of predefined ones.

Recommendations:

- Keyword and Regex both are mandatory for predefined, custom patterns, and a data pattern will only match if at least one of the defined keywords is present together with a value that matches the defined regex, within the defined range, as shown in the example below.

-The Range Window (Bytes) parameter defines how many bytes around a detected keyword or regex match are inspected to validate context. A value of ***100–200 bytes*** *is generally recommended as it balances accuracy and performance; smaller windows (50–100 bytes) work well when patterns are close together, while larger windows (up to 500 bytes) may be needed if attributes are separated by more text. As a best practice, start with 100 bytes and adjust only if broader context is required.*



Data Protection Profiles

At the next level, Data Protection Profiles group multiple Data Patterns using logical expressions such as AND, OR, NOT, or proximity operators like NEAR. This allows for the creation of more nuanced conditions to match complex data leakage scenarios. Both custom and predefined patterns can be referenced in a profile.

Operator	**What it does**	**Pseudo-syntax**	**Matches**	**Doesn't match**
AND	All referenced patterns must be present	PATTERN_A AND PATTERN_B	Text contains both an EMAIL and a CREDIT_CARD	Only EMAIL or only CREDIT_CARD
OR	Any one of the patterns is enough	PATTERN_A OR PATTERN_B	Either PAN or AADHAAR appears	Neither appears
NOT	Excludes matches that contain a pattern	PATTERN_A AND NOT PATTERN_B	CREDIT_CARD present but no CORP_EMAIL_DOMAIN	Both CREDIT_CARD and CORP_EMAIL_DOMAIN present
NEAR	Two patterns must occur within n words of each other (any order)	PATTERN_A NEAR/5 PATTERN_B	"card number is 4111… email me" (≤5 words apart)	"card number … [30 words] … email"

Recommendations:

- Recommended to configure a Boolean expression with at least 2 or 3 patterns(userdef/predef) with any of the operators.

- A maximum of 10 data patterns can be added to data protection profiles.

- Versa DLP has Predefined Data Protection Profiles, a built-in database of data expressions & rules which are used to classify the data. These expressions or rules are updated with SPACK upgrades, and it is designed to detect most occurrences of sensitive/regulatory data, but not all.

DLP Rules

DLP Rules consume one or more Data Protection Profiles and define how and when inspection occurs. Each rule includes:

- **Inspection Method**:
    - *Content Analysis*: Efficient scanning of data-in-motion using prefilters.
    - *File DLP*: Inspects based on file attributes (filaname, filesize range and/or hash value).
    - *OCR*: Applies policy to text extracted from image-based files.
    - *EDM*: Matches data against exact entries in a user-supplied dataset.
    - *Document Fingerprinting*: Matches documents based on predefined sensitive forms.
- **File Types**: Specify which file types are subject to inspection.
- **Direction/Context**: Specify whether the rule applies to uploads, downloads, or both. Also clarify whether it applies to the header, body, and/or attachments.
- **Actions**: Determine what happens when a match is found — *block*, *alert*, *allow*, etc.

Recommendation: - Do not select Header in DLP policy until it's required.

DLP Profile

Finally, DLP Profiles aggregate multiple DLP Rules into a single configuration object. These profiles are then applied within policies to enforce DLP across the desired traffic paths.

This nested and reusable design allows organisations to scale DLP policies efficiently while maintaining clarity and control over policy logic.

Use Case 1: (PII) Aadhaar Card Numbers and Indian Mobile Numbers Policy

This use case demonstrates how Versa Networks' Data Loss Prevention (DLP) can be configured for ACME-ONE, a global enterprise concerned about the leakage of **personally identifiable information (PII)**.

The HR and Compliance departments at ACME-ONE frequently process documents containing **Indian Aadhaar card numbers** and **Indian mobile phone numbers**, both of which are considered sensitive **PII**. To prevent the accidental or intentional exfiltration of this information, the organisation wants to block outbound transfers (such as external emails with attachments using **Gmail** or **Outlook**) whenever:

- The file or message contains Aadhaar-related keywords (e.g., Aadhaar, UIDAI) and matches Versa's predefined Aadhaar number detection pattern.
- **OR** the file or message contains Indian mobile number patterns.
- **AND** more than 10 Aadhaar numbers **or** more than 10 Indian mobile numbers are found within the same file or transaction.

Using Versa's integrated DLP engine, ACME-ONE defines a DLP policy named **"PII Protection Policy"** with the following conditions:

Policy Name	**Conditions**	**Details**
PII Protection Policy	Aadhaar-related keyword & Aadhaar number pattern **AND** >10 Aadhaar numbers in a single file/transaction **OR** Indian mobile number pattern **AND** >10 Indian mobile numbers in a single file/transaction	1) Detect Aadhaar details using keywords combined with Versa's predefined Aadhaar pattern. 2) Detect Indian mobile numbers using Versa's predefined mobile number pattern. 3) Trigger when more than 10 Aadhaar **or** Indian mobile numbers are detected in the same file/transaction upload. Actions include blocking, logging, or quarantining as per the DLP policy.

Pre-requisites

- SSE Gateway with VSPA, VSIA or both enabled.
- Authentication via Active Directory (LDAP used in our scenario)

- TLS Decryption enabled for the cloud applications defined for testing.

Configuration steps

The DLP configuration consists of the following four steps, which are described in detail below:

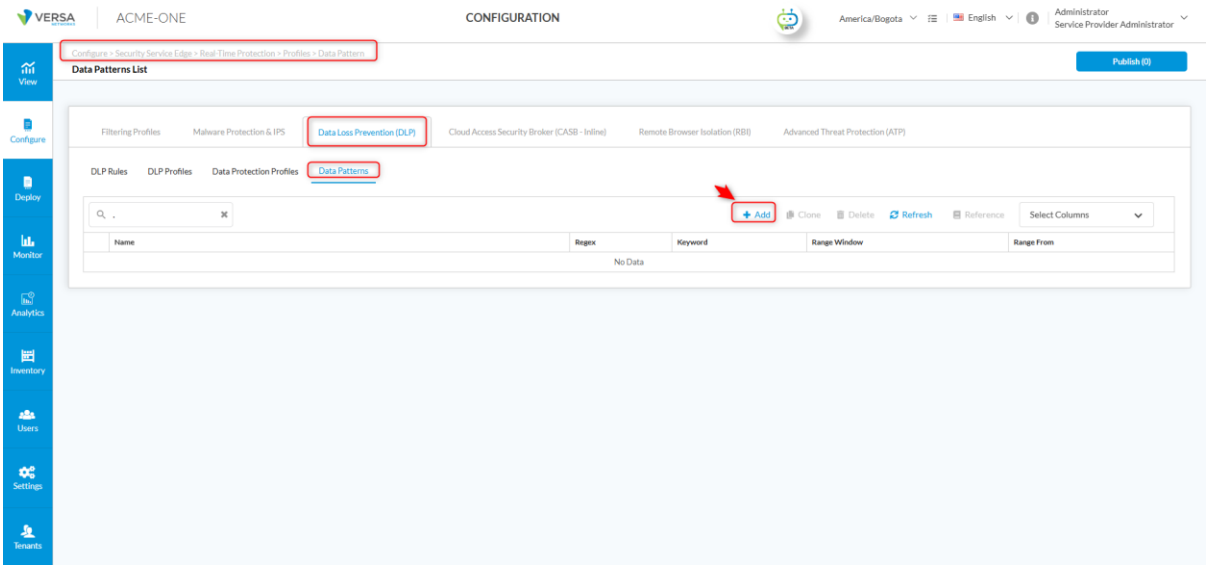
1. Create DLP objects
    - Create a **Data Protection Profile** (detection patterns, dictionaries, fingerprinting, etc.).
    - Create a **DLP Rule** (conditions that trigger DLP checks).
    - Create and assign a **DLP Profile / Policy** (the policy that ties the data profile and rules to enforcement actions).
2. **Create TLS decryption rule** for the cloud apps you will test (Gmail and Outlook).
3. **Create real-time protection rule** in the Internet Protection Policy that applies the DLP profile to the cloud apps defined in Step 2.
4. **Perform tests and validate the behaviours.** Execute test cases, verify detection and enforcement, and record results.

Step 1: Create DLP objects

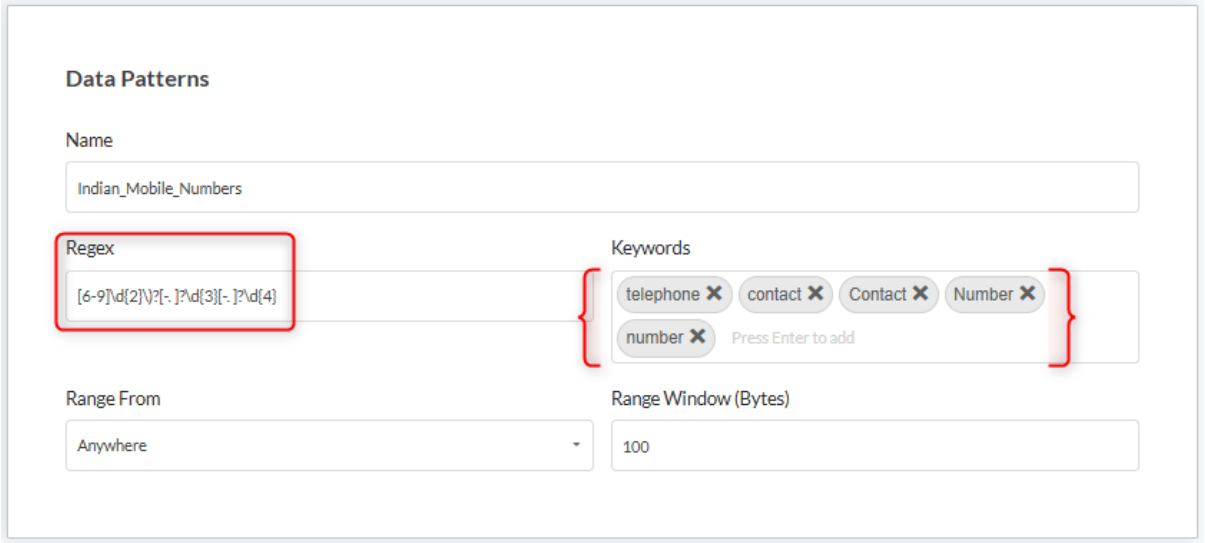
Creating a Data Pattern for Indian Mobile numbers

Navigate to

Configure **>** ***Security Service Edge*** **>** ***Real-Time Protection*** **>** ***Profiles*** **>** ***Data Patterns. Click*** **+** ***Add***, as shown in the image below.



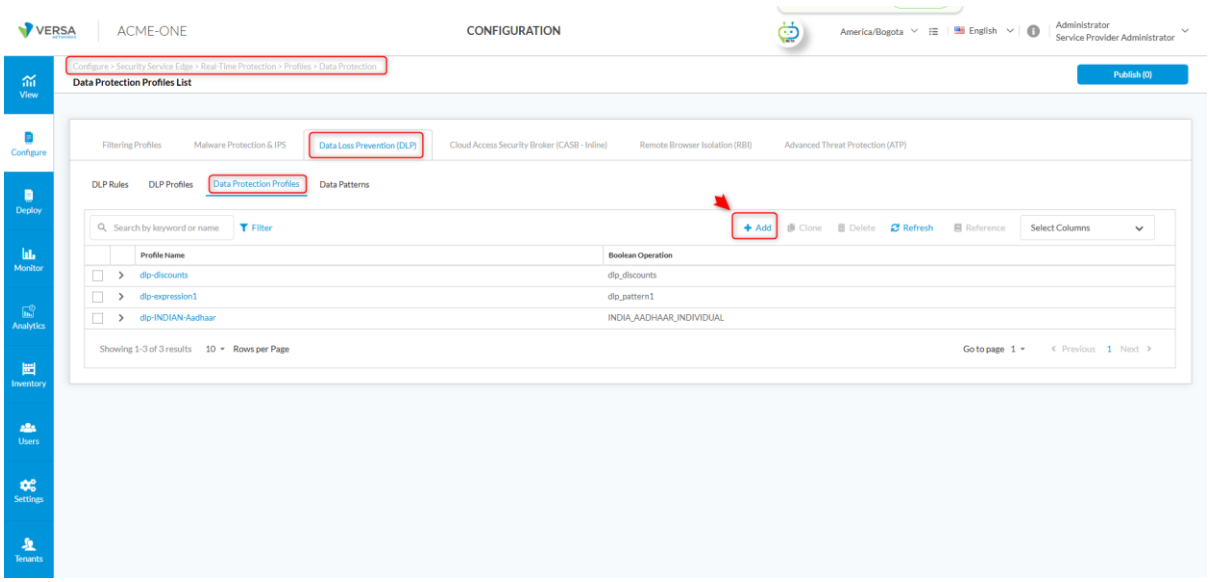
Next, we define the values with a simple regex for Indian mobile numbers, making sure the keywords are included and related to the content, just as shown in the image below. Finally, click on Save.



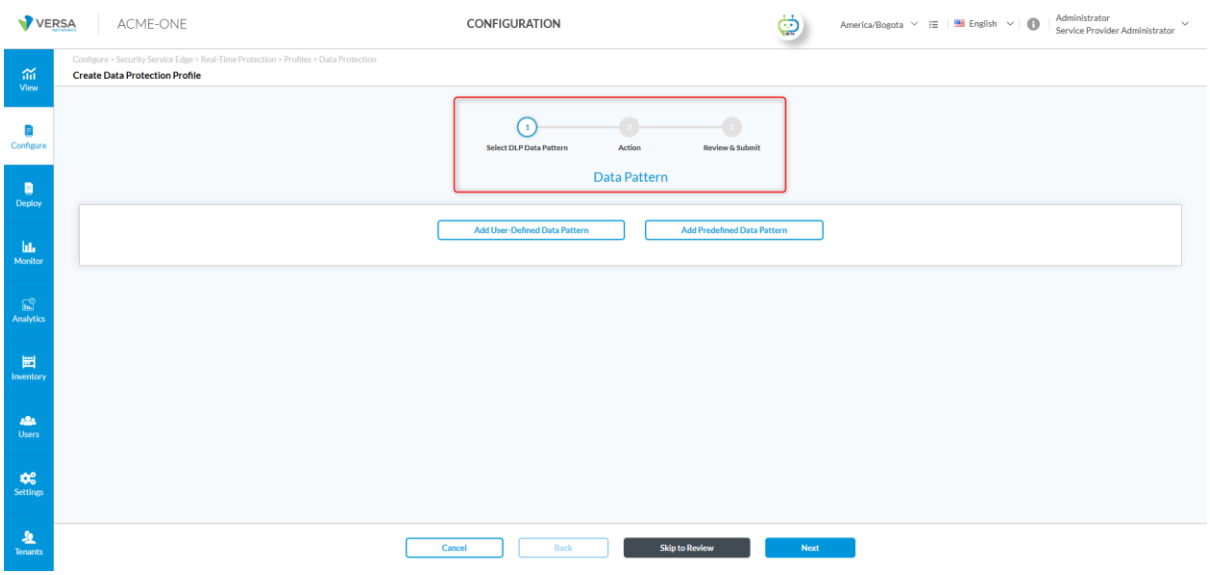
Creating a Data Protection Profile

Navigate to

Configure > Security Service Edge > Real-Time Protection > Profiles > Data Protection. Click + Add, as shown in the image below.



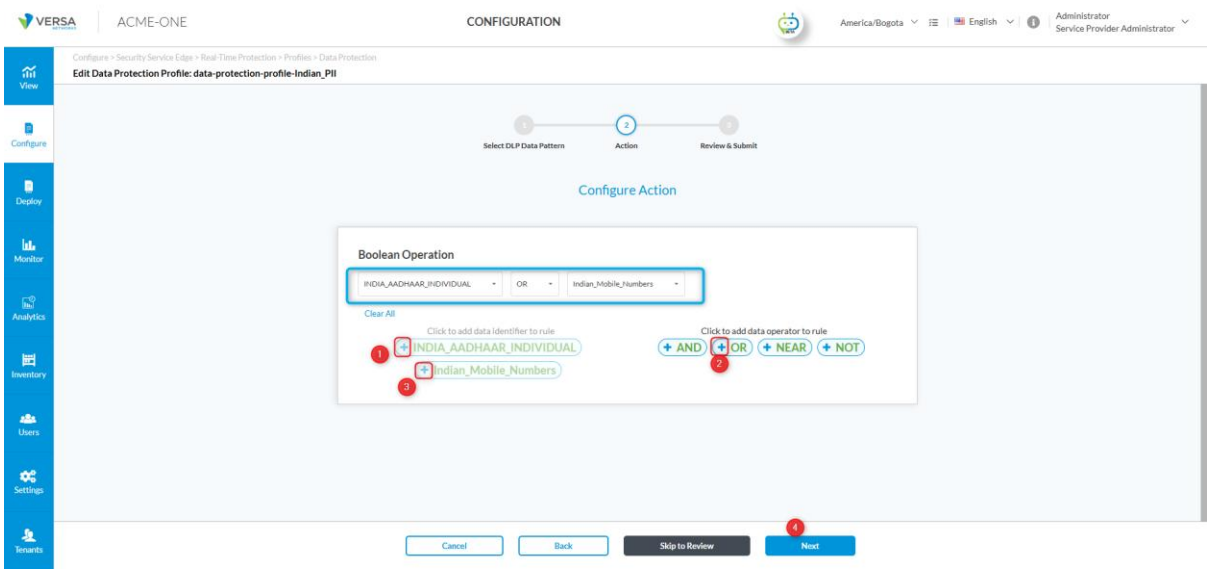
Next, complete the three configuration steps shown in the image below.



Select DLP Data Pattern: Select Add Predefined Data Pattern and search for the one you need. In this example, enable **INDIA_AADHAAR_INDIVIDUAL**, then click Save. Then click on Add User-Defined Data Pattern and enable **Indian_Mobile_Numbers** then click on Save.

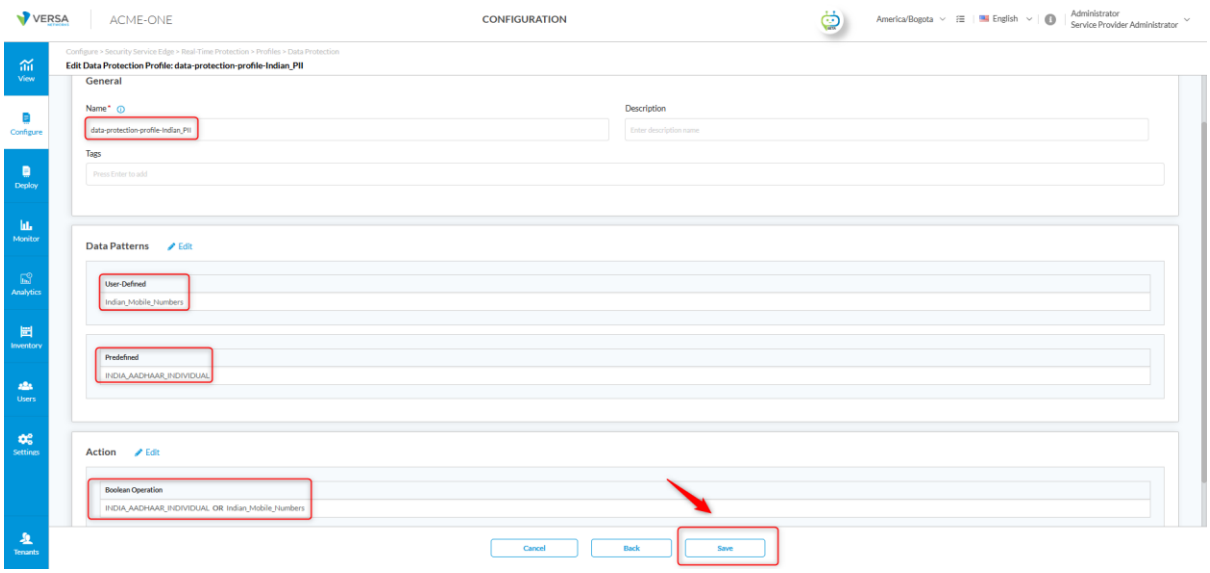
Action: Click the + icon next to the data identifier *INDIA_AADHAAR_INDIVIDUAL* to add it to your Boolean expression. Then, insert the OR operator and click the + icon again to add *Indian_Mobile_Numbers*. See the image below.

See the image below.



Once the data identifier has been added, click Next to continue.

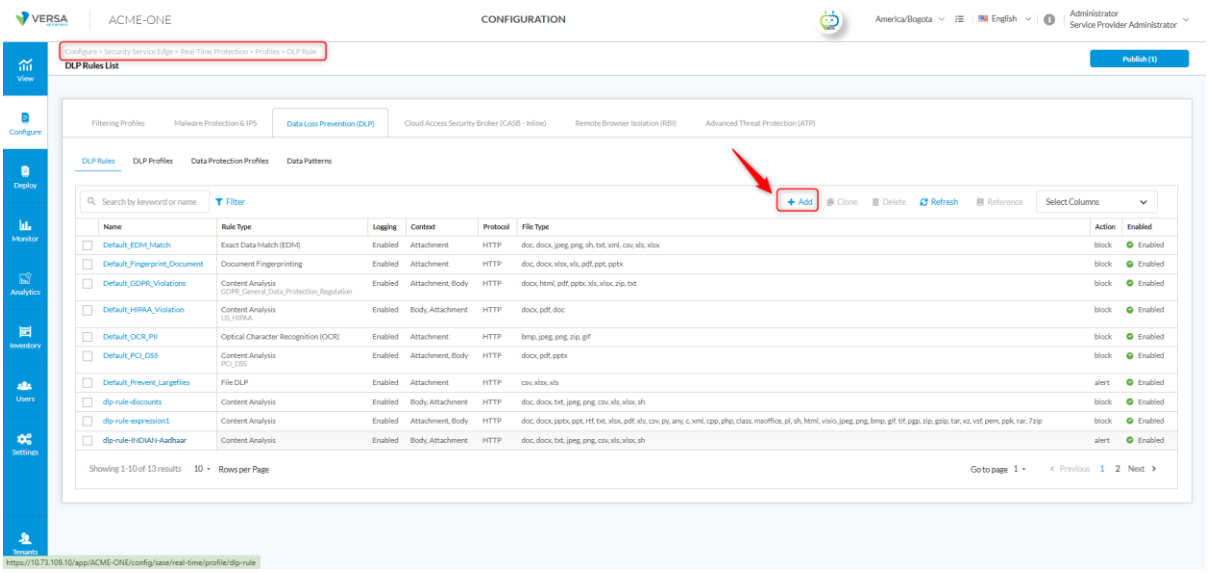
Review & Submit: Assign a name to your Data Protection profile and click **Save**.



Create DLP Rule:

Navigate to **Configure > Security Service Edge > Real-Time Protection > Profiles > DLP Rule**.

Click **+ Add**, as shown in the image below.



You will now see a menu to select the type of DLP rule. In our case, select **Content Analysis**. For details on the different types of DLP rules, refer to **Appendix A *(DLP Rule Types)***.

After selecting **Content Analysis**, six configuration steps will appear:

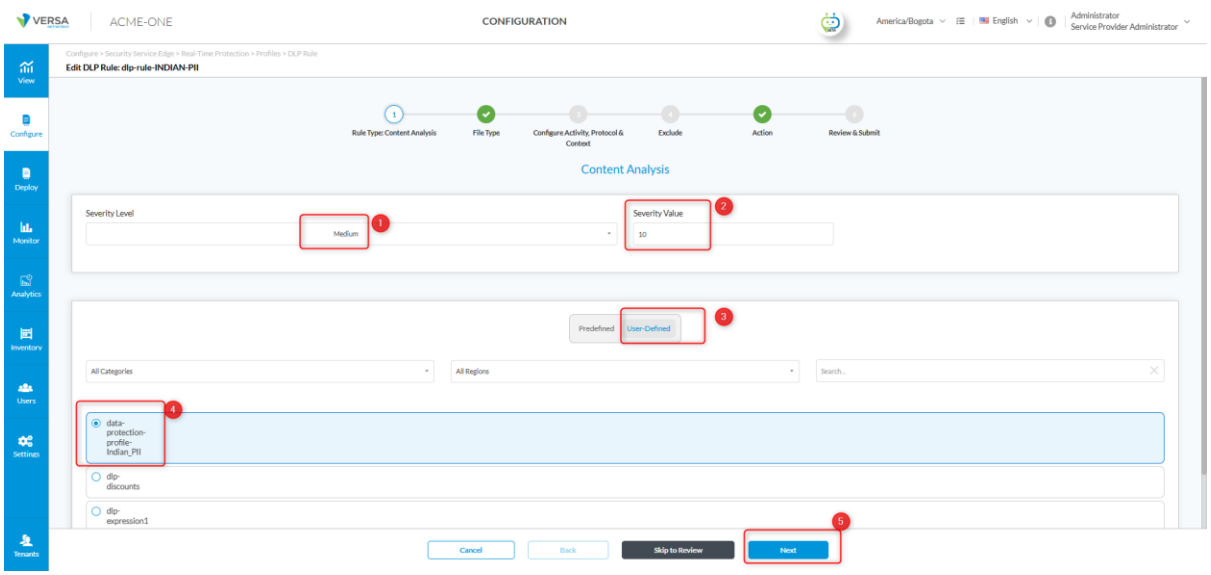
Rule Type: Content Analysis

1. **Severity Level:** Select the severity assigned to the DLP event. Each level has a default value: Low = 1, Medium = 10, High = 20, Critical = 30. The default value for each level specifies the number of occurrences needed to trigger the rule. In the current case, select **Medium**.

2. **Severity Value:** Define a custom number of occurrences required to trigger the rule (Overwrites the default value associated with the Severity level). The counter starts from 0. For example, if you set the value to 10, the rule will trigger beginning from the 11th DLP event. In this example, no value needs to be set since the Severity Level is set to Medium.

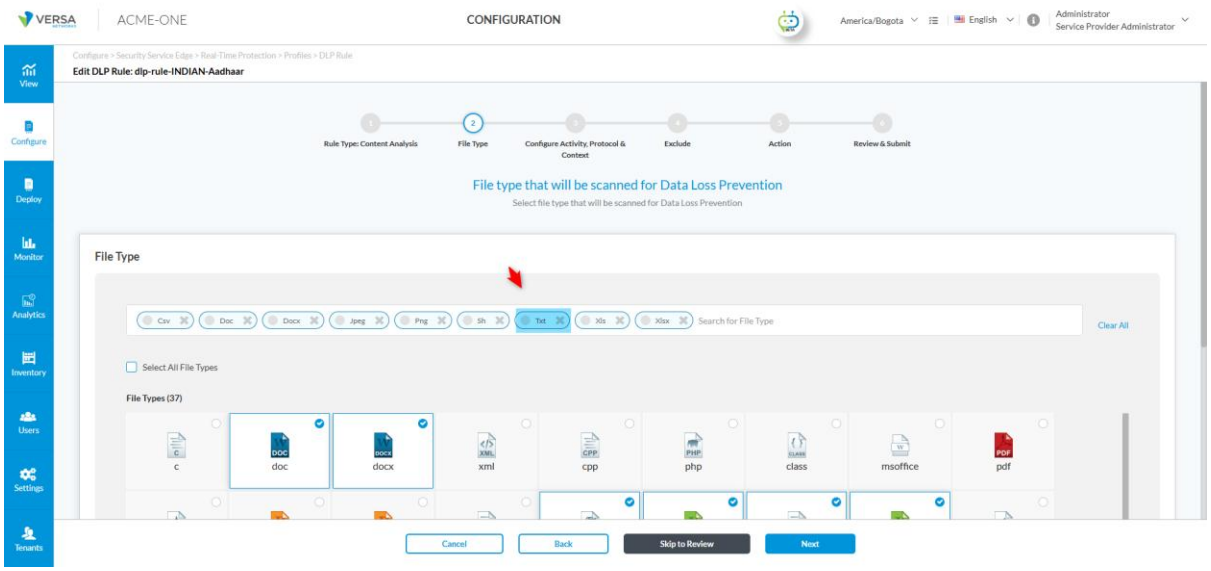
3. **Predefined/User Defined:** Select **User Defined** and then choose the **Data Protection Profile** we created earlier, named data-protection-profile-AADHAAR.

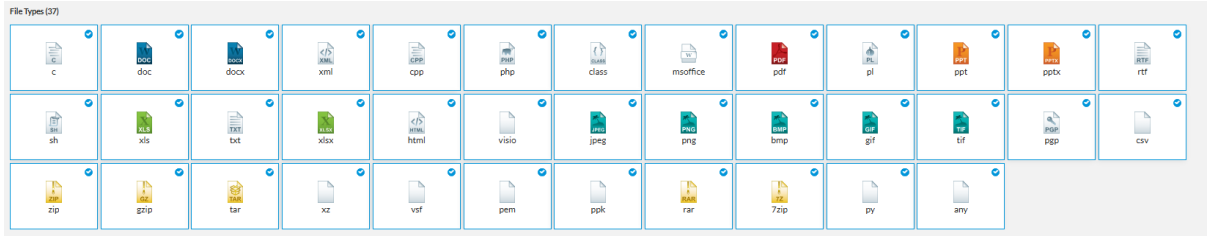
4. Click **Next** to continue.



File Type: Select the file types you want to inspect. For this use case select the checkbox **Select All File Types**.:

Click on **Next** to continue.



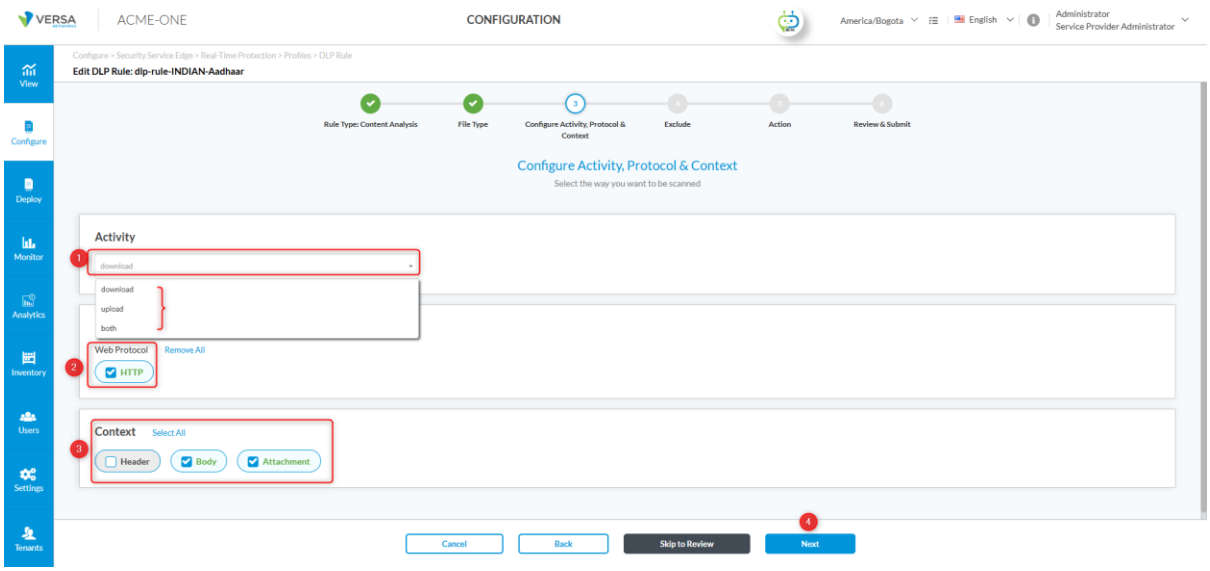


Configure Activity, Protocol & Context:

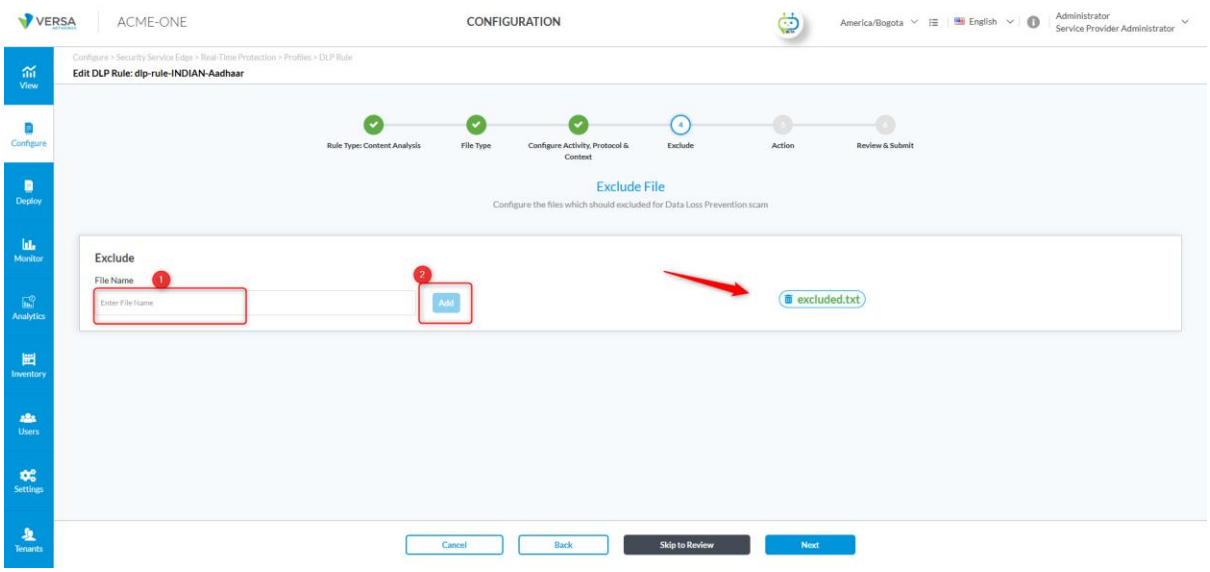
1. **Activity:** Select the activity to which the DLP module will be applied. In our case, select **Upload**. This reflects the activity when someone is trying to exfiltrate data.

2. **Web Protocol:** Select HTTP.

3. **Context:** Defines which part of the packet or message will be inspected. For this example, select **Attachments** and **Body**.



Exclude: Specify the file name(s) that should be excluded from DLP inspection.

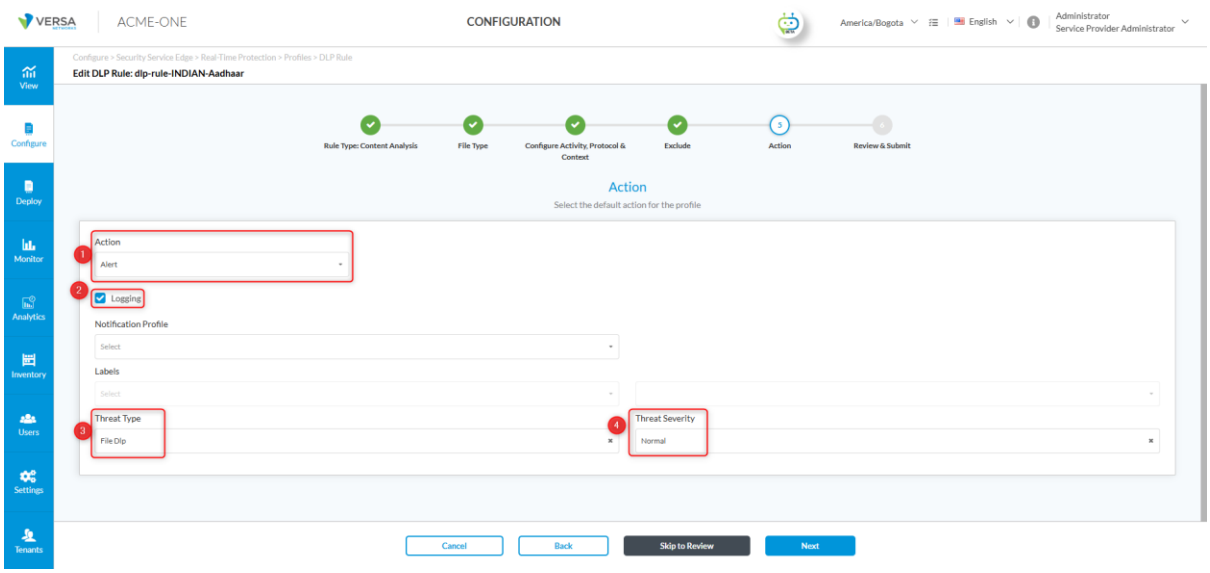


Action: Define the action to be executed when the rule is triggered. Several options are available, such as:

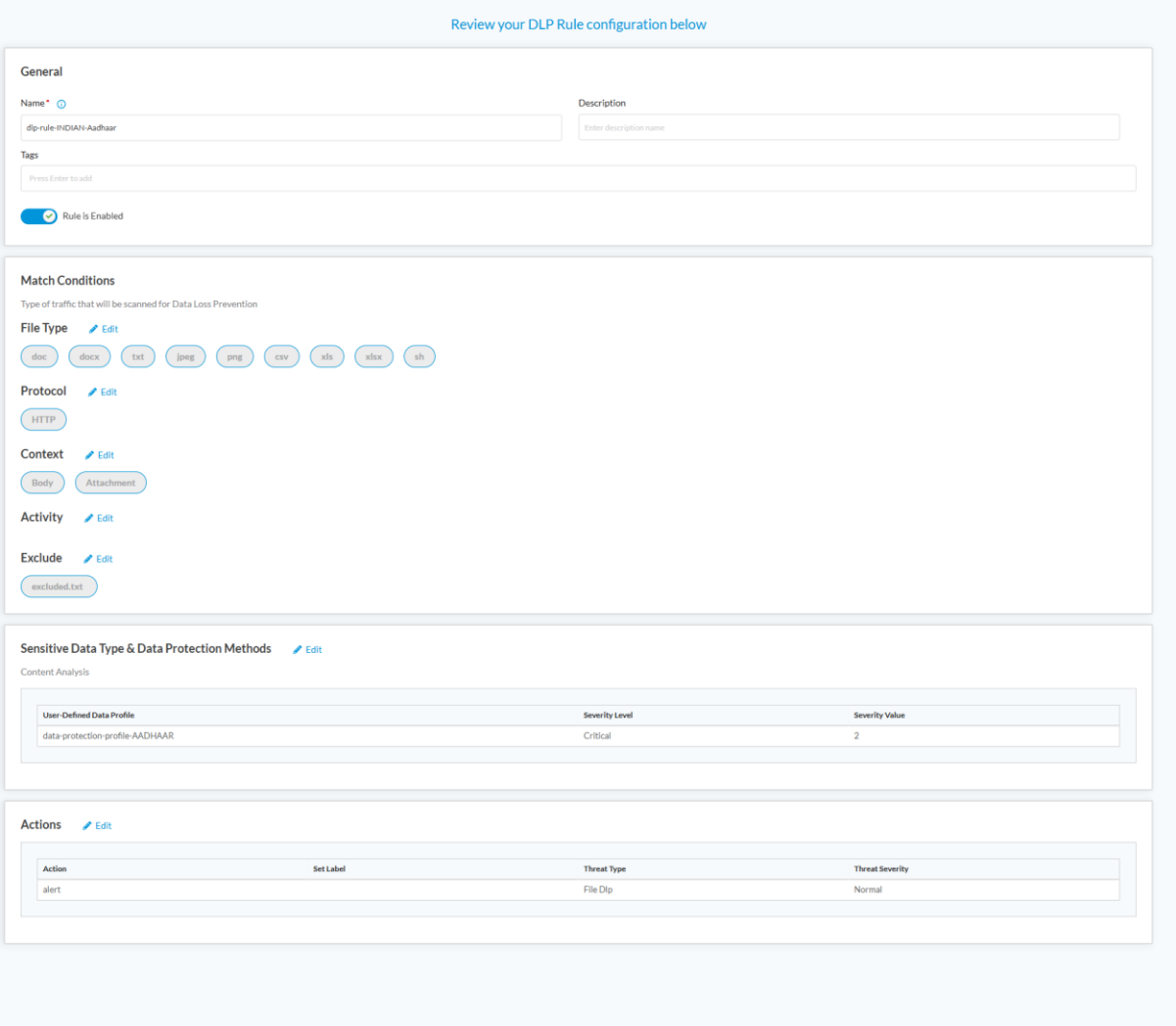
- Allow

- Alert
- Block
- Reject

In our case, we will select **Alert** because we only want a log to be generated in the platform without blocking the user or displaying any pop-up messages. This option is commonly used when tuning DLP rules. For more information on the different actions, refer to **Appendix B: *DLP Rule Actions*.**



Review & Submit: Verify that your rule matches the example shown in the image below, then click **Save**.

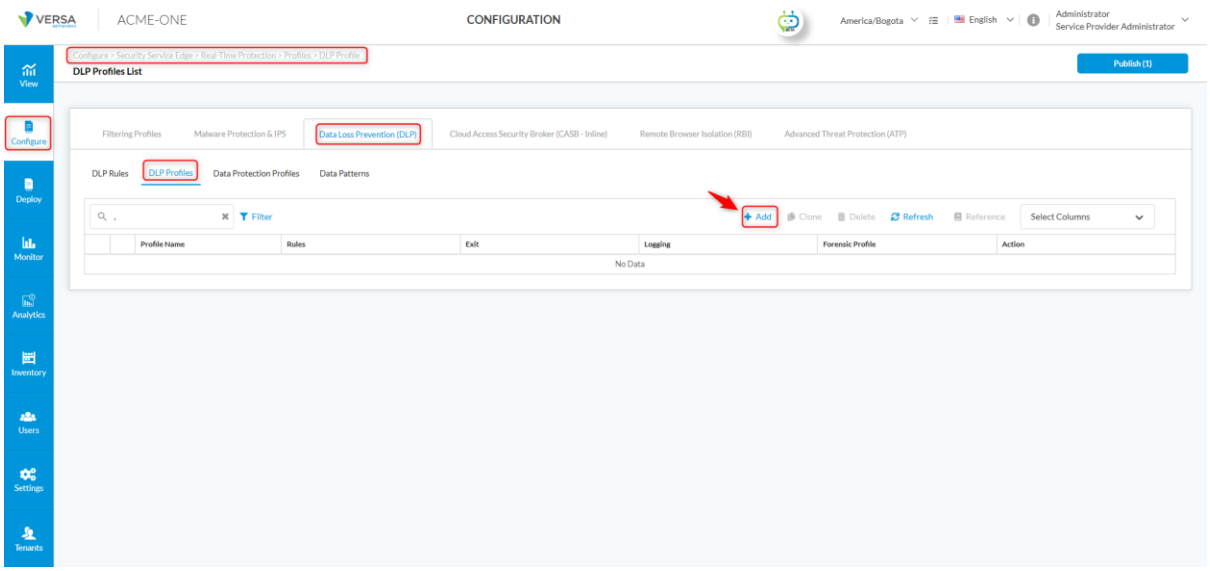


Create the DLP Profile:

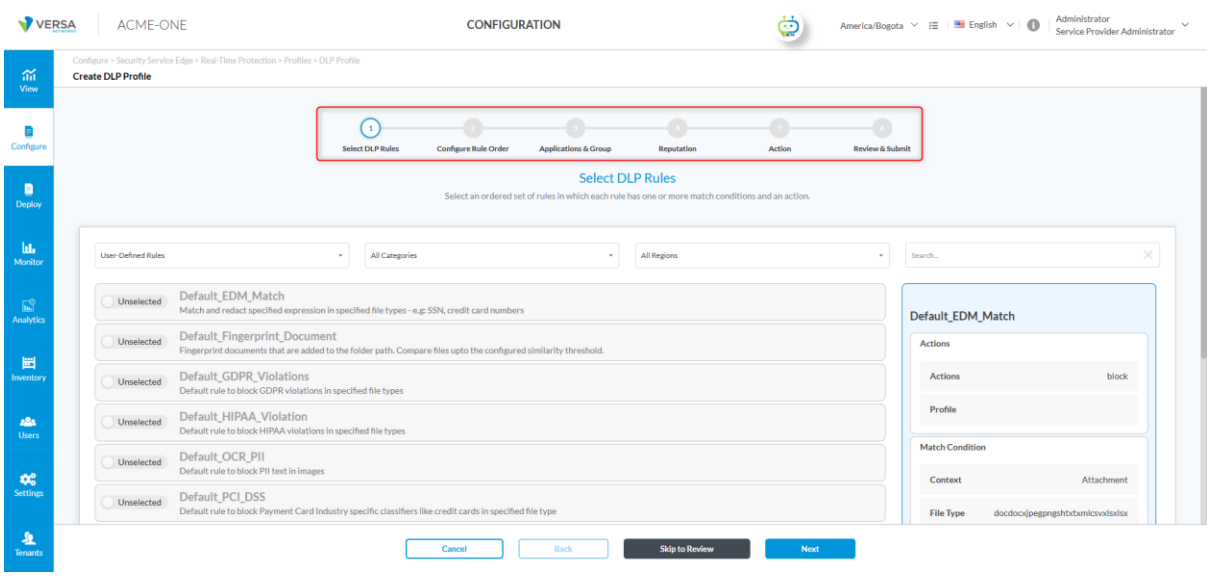
Navigate to

Configure > Security Service Edge > Real-Time Protection > Profiles > DLP Profile.

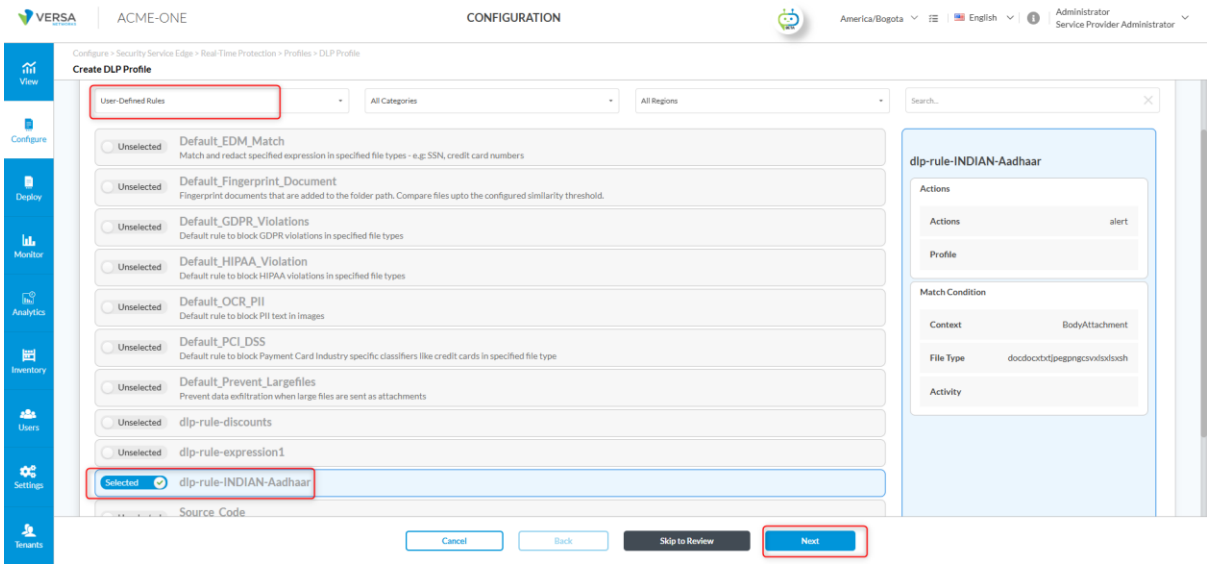
Click + Add, as shown in the image below.



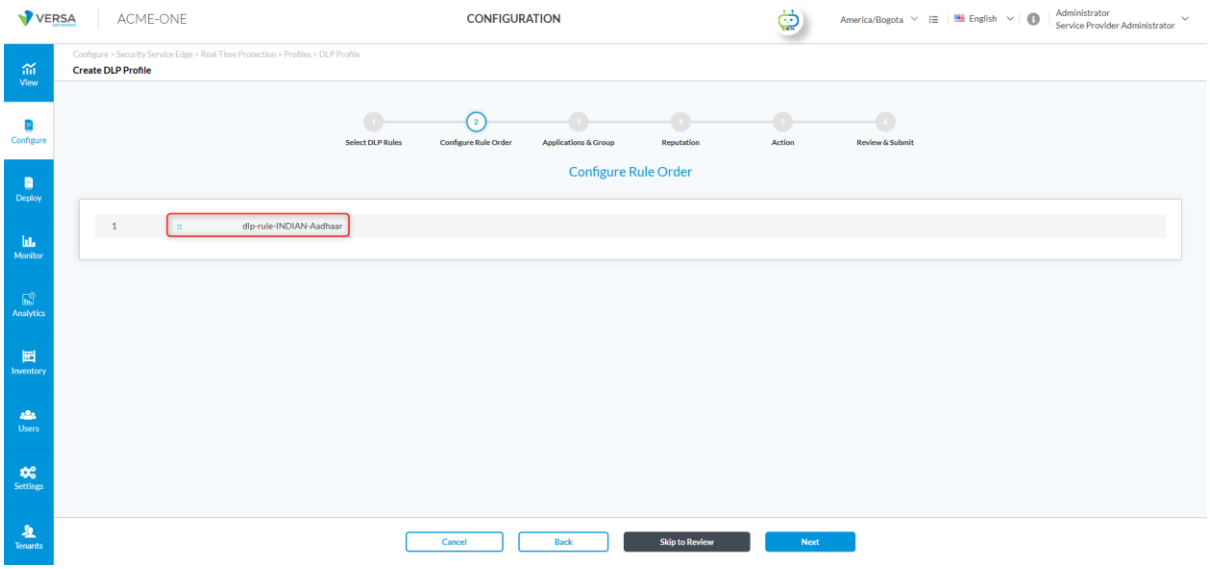
Complete the six configuration steps shown in the following image.



Select DLP Rules: In the **User Defined Rules** section, search for the rule you created earlier, select it, and click **Next**. It should look like the example shown in the image below.



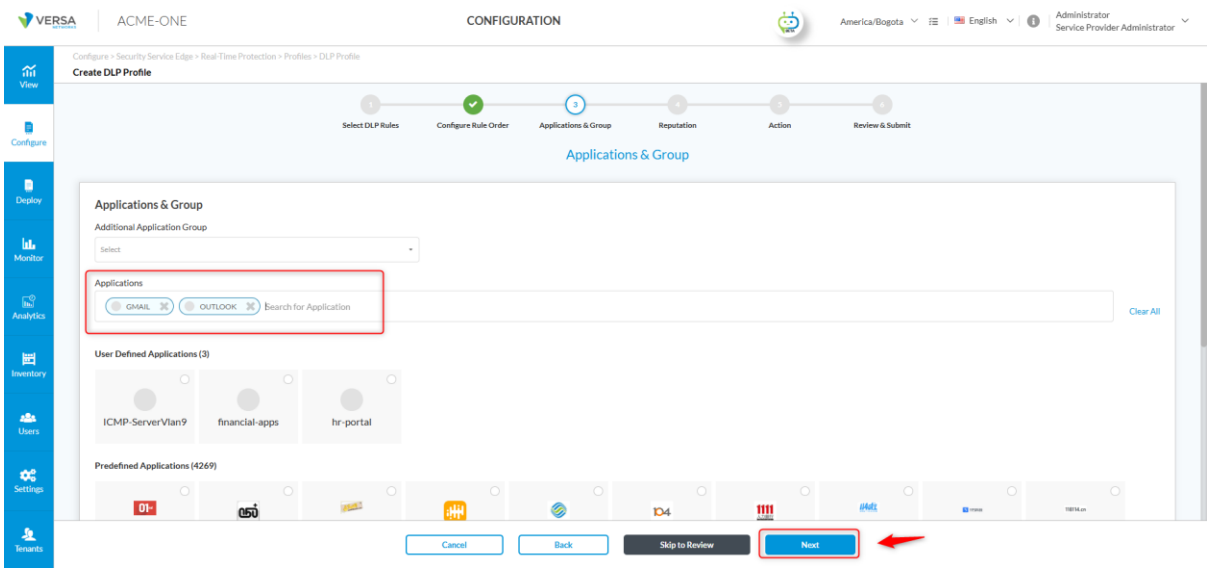
Configure Rule Order: You can select any rule and move it up or down to change the DLP processing order. The rule at the top is processed first, and the one at the bottom is processed last. In our case, this does not apply since we have selected only a single rule.



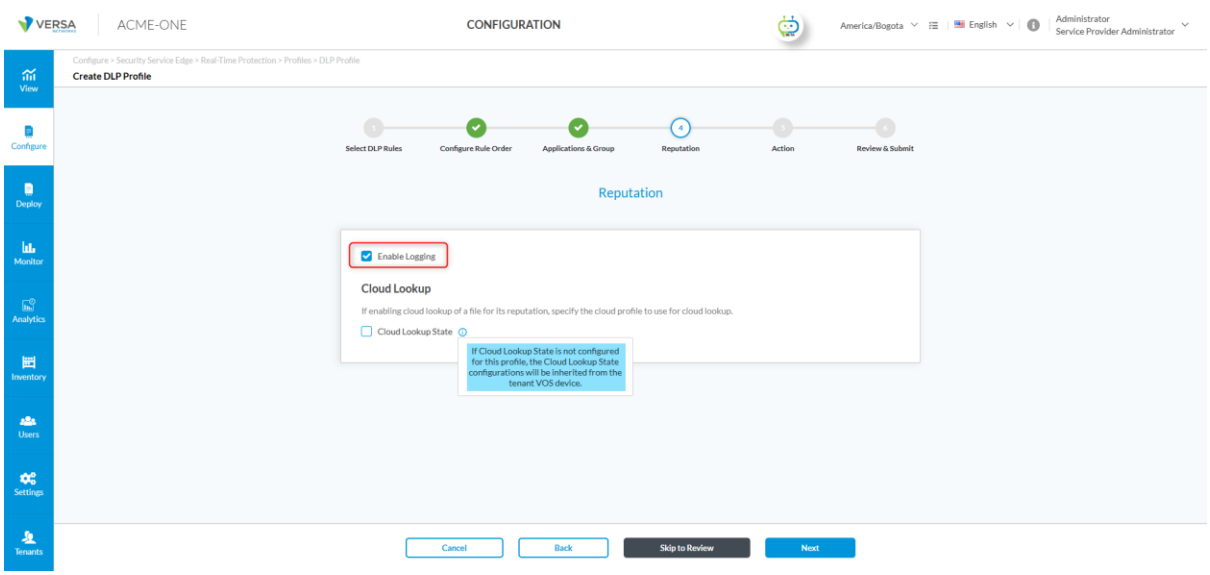
Applications & Group: In the **Applications** search field, search for each application to which the DLP profile will be applied. In our case, select **Gmail** and **Outlook**, then click **Next**, as shown in the image below.

***Notes**: - In cases where not all dependent applications are known, adding the generic applications **HTTPS** or **HTTP** to the DLP profile may help. However, this approach is not technically guaranteed to work and could impact unrelated traffic. Therefore, rules applied in real-time protection should remain as specific as possible.*

*- In some cases, you may also need to add dependent applications when dealing with SaaS apps. For example, Gmail relies on additional services such as **gstatic.com** to load resources like icons, scripts, or image previews (e.g., when sending or viewing image attachments). Without allowing these dependencies, the SaaS application may not function correctly.*



Reputation: Select the **Enable Logging** option to store website reputation events, as shown in the image below. **Cloud Lookup** is not required. Click **Next**.



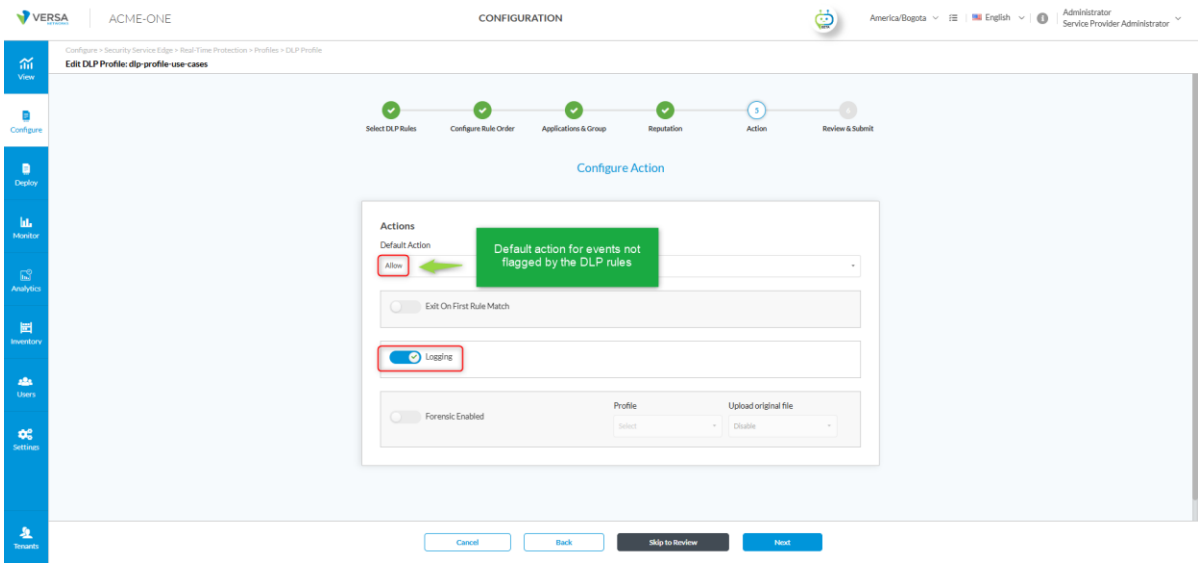
Action: Specify the following as shown in the screenshot below:

Actions: Set the default action to **Allow**. The default action is applied if none of the scanned data matches a rule.

Logging: Click on the toggle button to enable logging.

Exit on First Rule Match: Leave the default action set to **disabled**.

Note: if multiple DLP rules are configured, this option should be disabled to ensure that all rules are applied to the same session.



Review & Submit: Assign a name, then review the configuration and click the **Save** button.

Step 2: Create the TLS decryption rule for the cloud applications we will test (Gmail and Outlook).

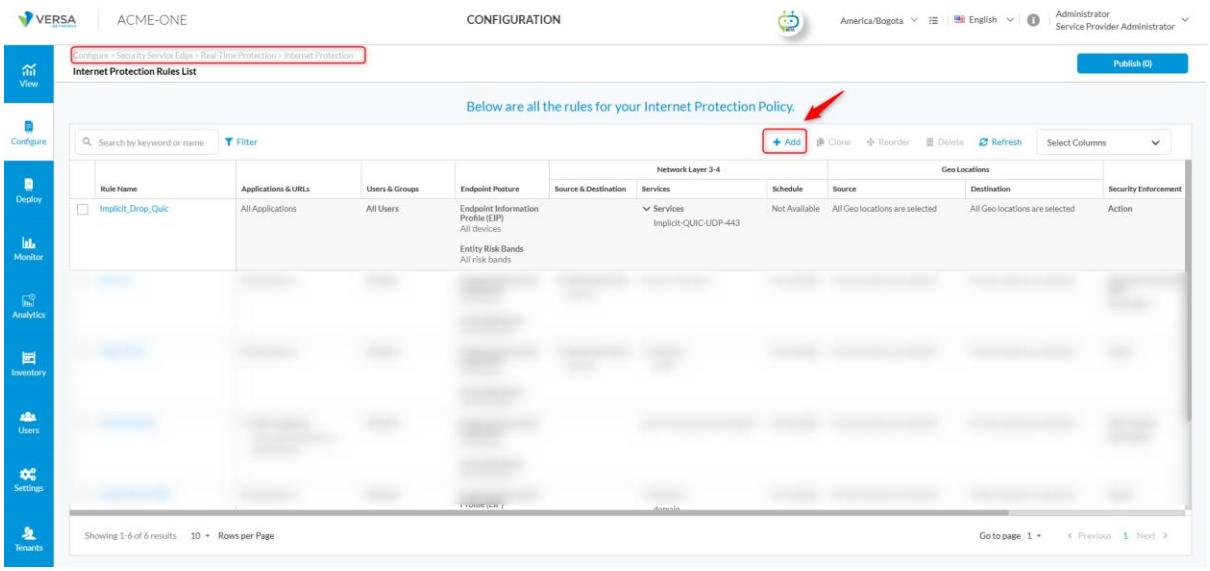
To ensure that payloads can be inspected and DLP policies applied, a TLS decryption rule must exist for the cloud applications being tested (e.g., Gmail and Outlook).

If you need the detailed step-by-step configuration for creating this rule, refer to **Appendix C: TLS Decryption Rule Configuration**.

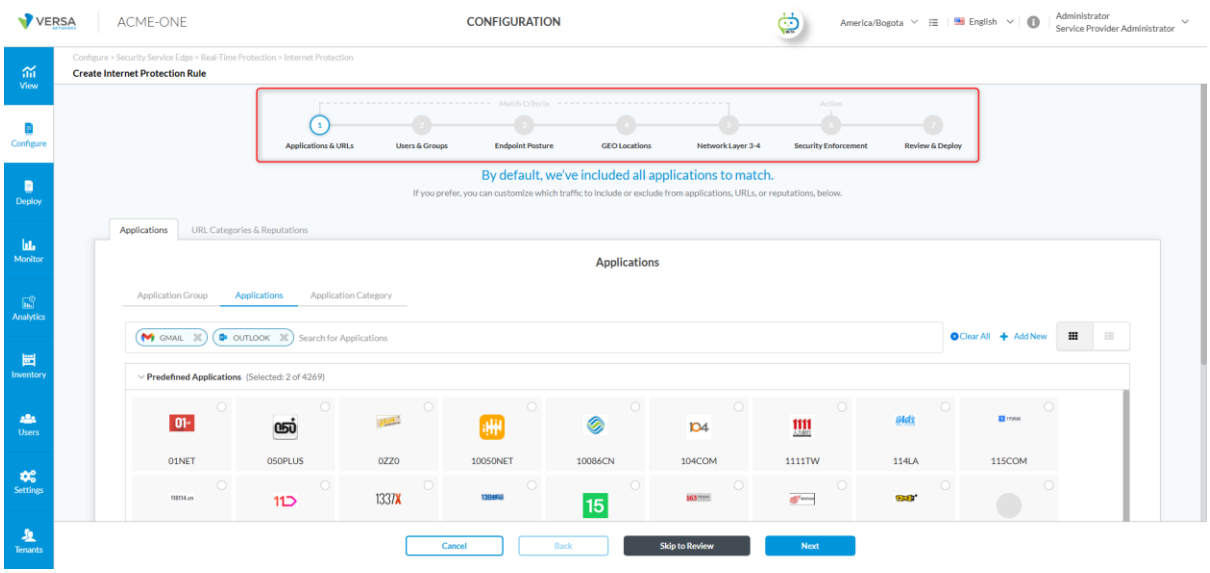
Step 3. Create the real-time protection rule using the DLP profile on the cloud apps defined earlier.

Navigate to ***Configure*** > ***Security Service Edge*** > ***Real-Time Protection*** > ***Internet Protection.***

Click + ***Add***, as shown in the image below.



Then, complete the seven configuration steps shown in the following image.



Applications & URLs: Select the applications to which we will apply our DLP module. In our case, we choose Gmail and Outlook.

Users & Groups: Select our test group and then click **Next**. In our case, it can be the (VIP) group coming from our LDAP-AD.

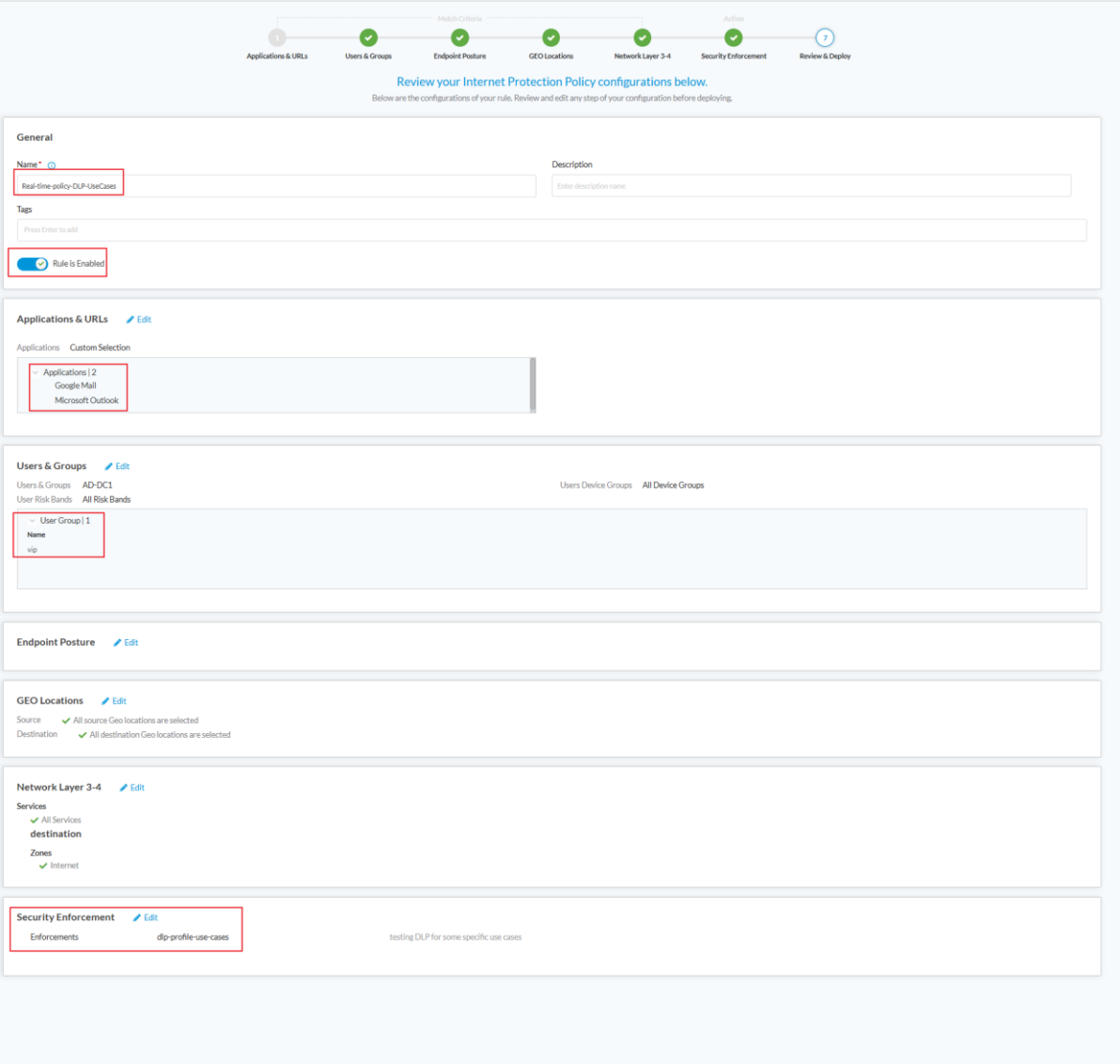
Endpoint Posture: You can apply Endpoint Information Profiles and Entity Risk Bands; however, in our case, leave the default settings to apply none and click **Next**.

Geolocation: You can filter by Source or Destination Geo Location. In our case, we leave the default setting to **All** and click **Next**.

Network Layer 3-4: You can filter by services (Layer 4) such as HTTP, HTTPS, DNS, ICMP, etc. You can also filter by Source & Destination (Layer 3). However, leave the default values and click **Next**.

Security Enforcement: Click on the **Security Profiles** option, then select **Data Loss Prevention**. Toggle the switch to enable it, then choose the profile named **dlp-profile-use-cases**, which is the one we created. Click **Next**.

Review & Validate: Review the configuration (see image below), click **Save**, and select **add this rule at the top of the rule list**.



Finally, publish the changes applied in Concerto and proceed with the verifications.

Step 4. Perform tests and validate the behaviour.

To perform tests, we need to understand which key pair values will cause our selected Data Pattern (**INDIA_AADHAAR_INDIVIDUAL**) to match our data samples. This is part of our Predefined **DLP Patterns**

DLP Pattern Name: INDIA_AADHAAR_INDIVIDUAL

Keywords: (aadhaar|aadhaar card)

Pattern Conditions:

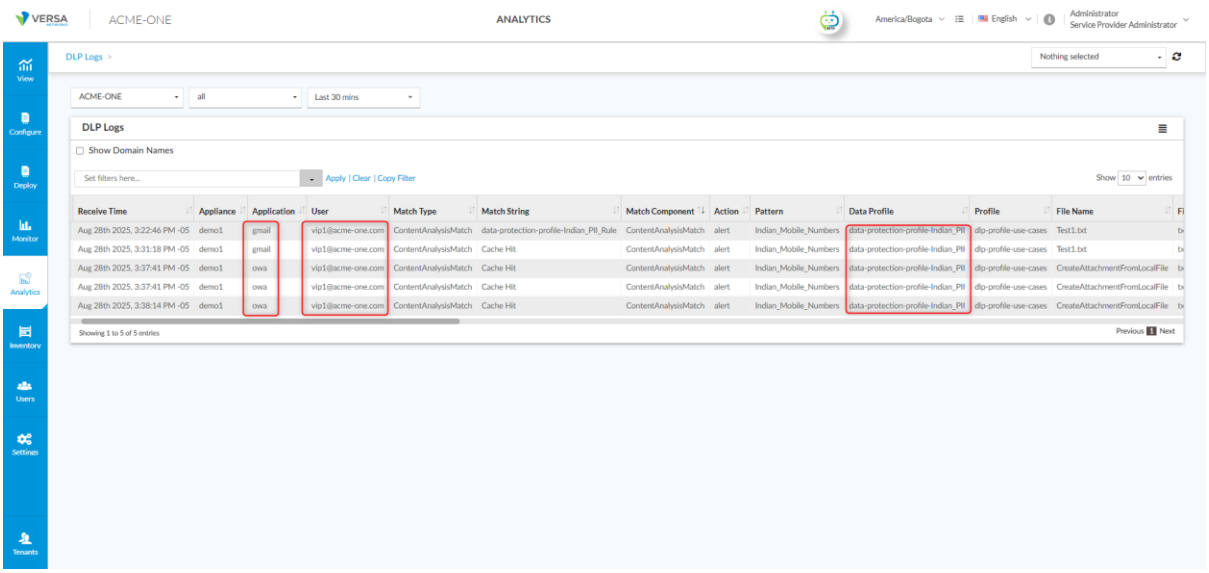
- Detects a **12–digit Aadhaar number** that starts with digits 2–9.
- Supports different formatting styles, such as continuous digits (123412341234) or with separators (e.g., 1234-5678-9123 or 1234 5678 9123).
- Ensures the detected number is not part of a larger alphanumeric string.

Based on the above and also considering our custom data pattern created in Step 1, we generated some samples to create the .txt file and run the tests.

Filename: Test1.txt

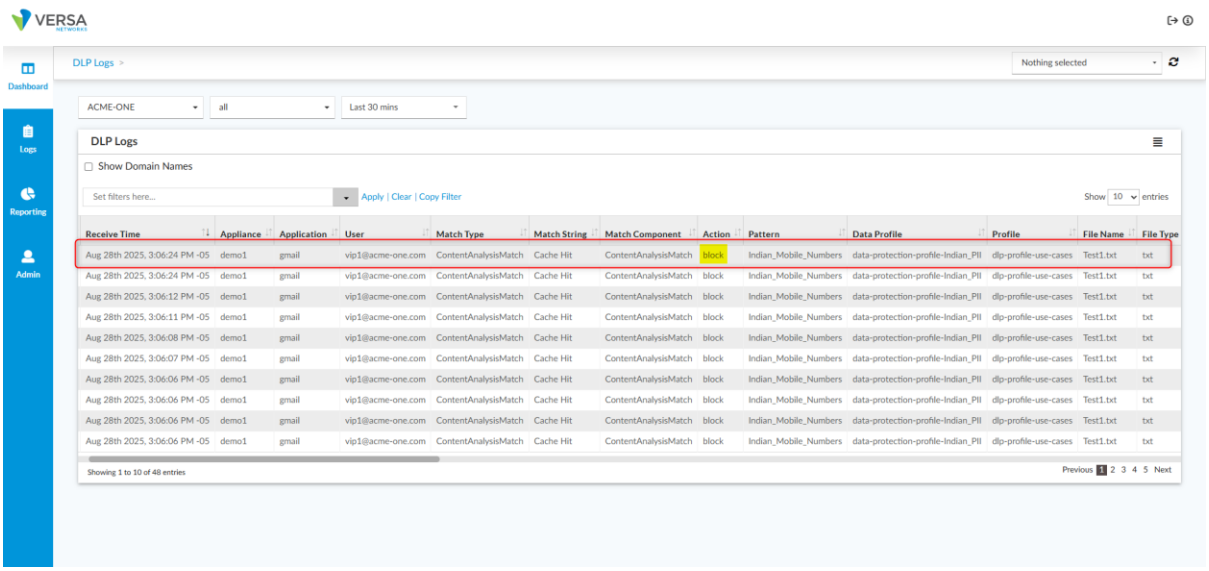
Aadhaar Numbers: 6472 4756 5971 6904 5289 0788 7885-6256-1067 8950-0527-1593 019114027248 7617-8729-4609 855106136654 111048062360 8558 4853 3876 462740952344 763753879522 679336449441 1255 3766 1539 2904-0323-2864 7932-7598-9884 7285 2101 3902 618131683916 4168-9830-2972 0595-3528-6334 7088 6925 2334 Mobile Numbers: 8168718125 +91 6883553941 08511396286 08087536420 0-9344714963 91 9050767250 0-6642953071 9772829100 0-7555887505 9497707487 +919947360842 +919086832700 6361279769 +91 8772342864 07606012845 919099828766 8773658291 9555473795 91-9465257534 91-6948732713

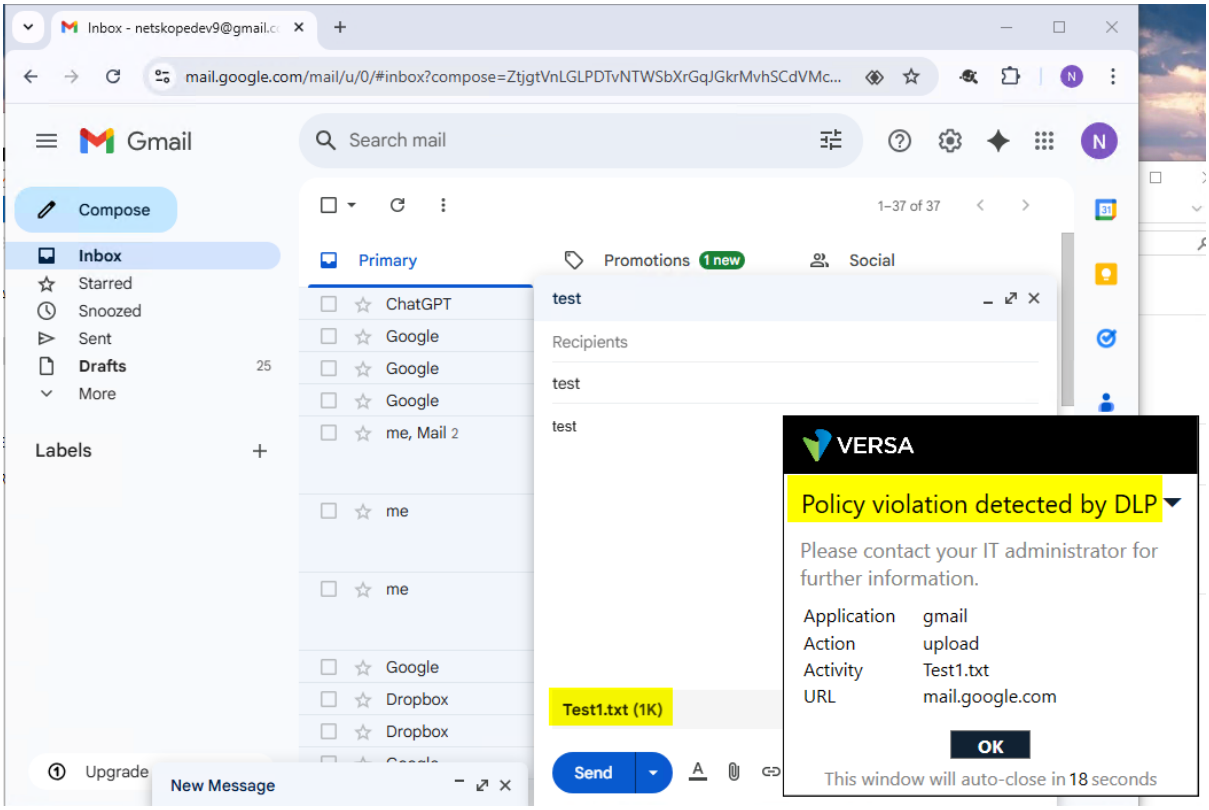
Now, compose an email from Gmail or Outlook and attach **Test1.txt**, which should be allowed because the **Alert** action does not block but generates an alert log for the DLP event. When checking the logs in **Concerto > Analytics > DLP Logs**, you should see something similar to the images below.



Switch from Alert to Block Action

With the DLP rule validated as working properly, change the action from **Alert** to **Block** for this DLP rule (Refer to Step 1, Create DLP Rule to make this change). As a best practice, DLP rules are usually deployed in **Alert** mode first to fine-tune detections, and only then switched to **Block** mode once they are validated. When using **Block**, the logs will reflect the blocked action instead of an alert. In addition, the user session will be dropped, and the client will display a pop-up notification with the violation message, as shown below.




Inbox - netskopedev9@gmail.c
mail.google.com/mail/u/0/#inbox?compose=ZtjgtVnLGLPDTvNTWSbXrGqJGkrMvhSCdVMc...
Gmail
Search mail
Compose
Inbox
Starred
Snoozed
Sent
Drafts 25
More
Labels
1–37 of 37
Primary
Promotions 1 new
Social
ChatGPT
Google
Google
Google
me, Mail 2
me
me
Google
Dropbox
Dropbox
Upgrade
New Message
test
Recipients
test
test
Test1.txt (1K)
Send
VERSA
Policy violation detected by DLP
Please contact your IT administrator for further information.
Application gmail
Action upload
Activity Test1.txt
URL mail.google.com
OK
This window will auto-close in 18 seconds

Use Case 2: Protecting Confidential HR Forms with Fingerprint DLP

This use case demonstrates how ACME-ONE leverages **Fingerprint-based DLP** in Versa Networks to protect sensitive HR documents that must not leave the corporate environment.

The HR department at ACME-ONE manages a **"Confidential Employee Disciplinary Form"**, which contains predefined fields such as:

- Employee Name
- Employee ID
- Date of Incident
- Description of Violation
- Manager Comments
- HR Review Outcome

Although the specific details in each form may vary, the overall structure, layout, and field labels remain consistent.

To prevent the **exfiltration of these documents through web-based uploads to cloud storage services such as SharePoint and Dropbox**, Versa's Fingerprint DLP engine is configured to detect **document similarity** against a registered template of the "Confidential Employee Disciplinary Form."

Using Versa's integrated DLP engine, ACME-ONE defines a DLP policy named **"Confidential HR Form Protection"** with the following conditions:

Policy Name	Conditions	Details
HR Form Protection Policy	Document fingerprint match with ≥ 50% similarity	1) Register the "Confidential Employee Disciplinary Form" as a fingerprinted document in Versa DLP. 2) Trigger the policy if outbound traffic contains a **web upload attempt** of a file with ≥ 50% similarity to the fingerprinted template via SharePoint or Dropbox. 3) Actions include Alerting, blocking and logging.

Pre-requisites

- SSE Gateway with VSIA enabled.
- Authentication via Active Directory (LDAP used in our scenario)
- TLS Decryption enabled for the cloud applications defined for testing.

Configuration steps

The DLP configuration consists of the following steps, which are described in detail below:

1. Create DLP objects
    - Create a **DLP Sub-Folder** and **upload the confidential file.**
    - Create a **DLP Rule** (conditions that trigger DLP checks).
    - Create and assign a **DLP Profile / Policy** (the policy that ties the data profile and rules to enforcement actions).
2. **Create TLS decryption rule** for the cloud apps you will test (**SharePoint** and **Dropbox**).
3. **Create real-time protection rule** that applies the DLP profile to the cloud apps defined in Step 2.
4. **Perform tests and validate the behaviour.** Execute test cases, verify detection and enforcement, and record results.

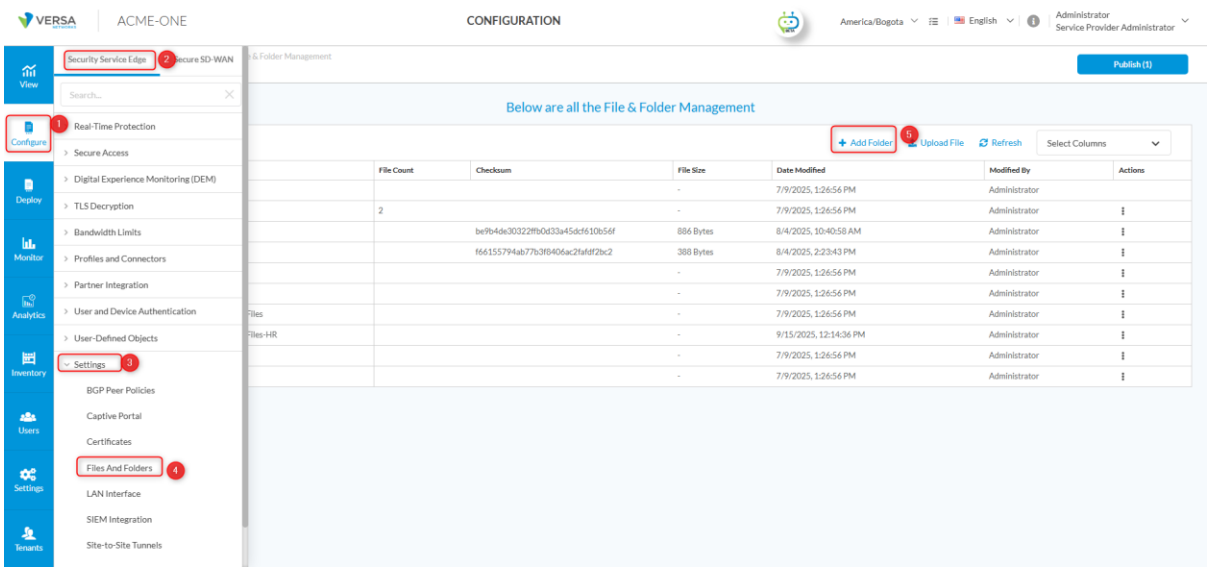
Step 1: Create DLP objects

For our rule type (**Document Fingerprinting**), we need to create a folder where the confidential document will be stored. This document will be used to generate corresponding fingerprint hash. We must also define and upload the confidential file. Once this is completed, we can define the DLP rule by selecting the folder that already contains our file and then proceed with the standard configuration steps that we will demonstrate.

Create Folder:

Navigate to **Configure > Security Service Edge > Settings > Files and Folders**.

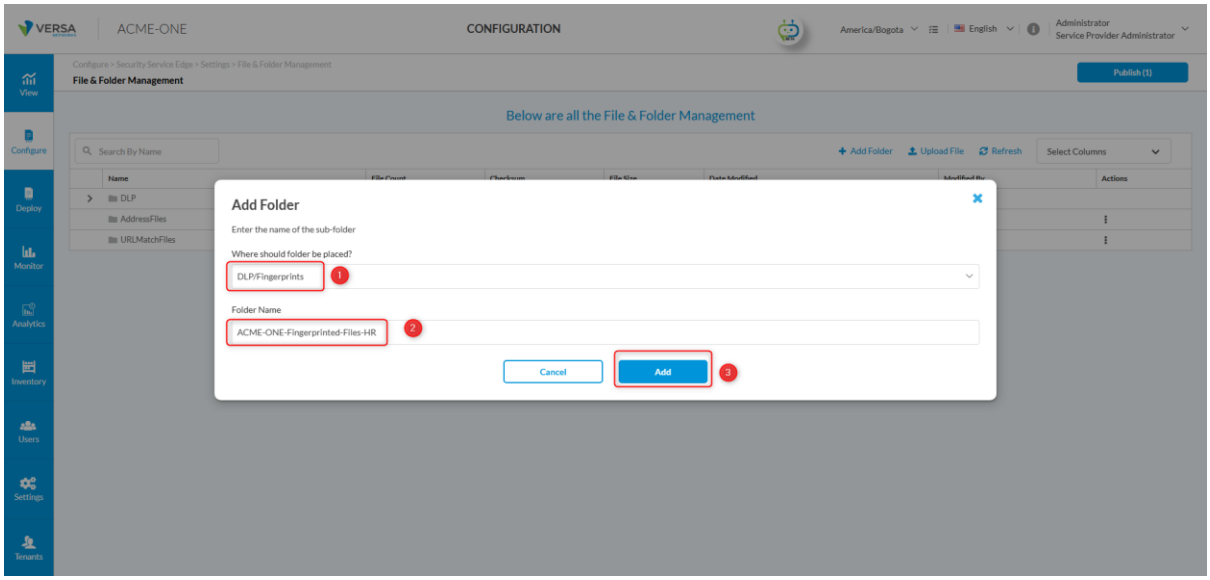
Click **+ Add**, as shown in the image below.



Next, a window called **Add Folder** will appear with two sections to configure:

- **Where should folder be placed?**: From the dropdown list, select **DLP/Fingerprints**.
- **Folder Name**: Enter a descriptive name, for example: **ACME-ONE-Fingerprinted-Files-HR**.

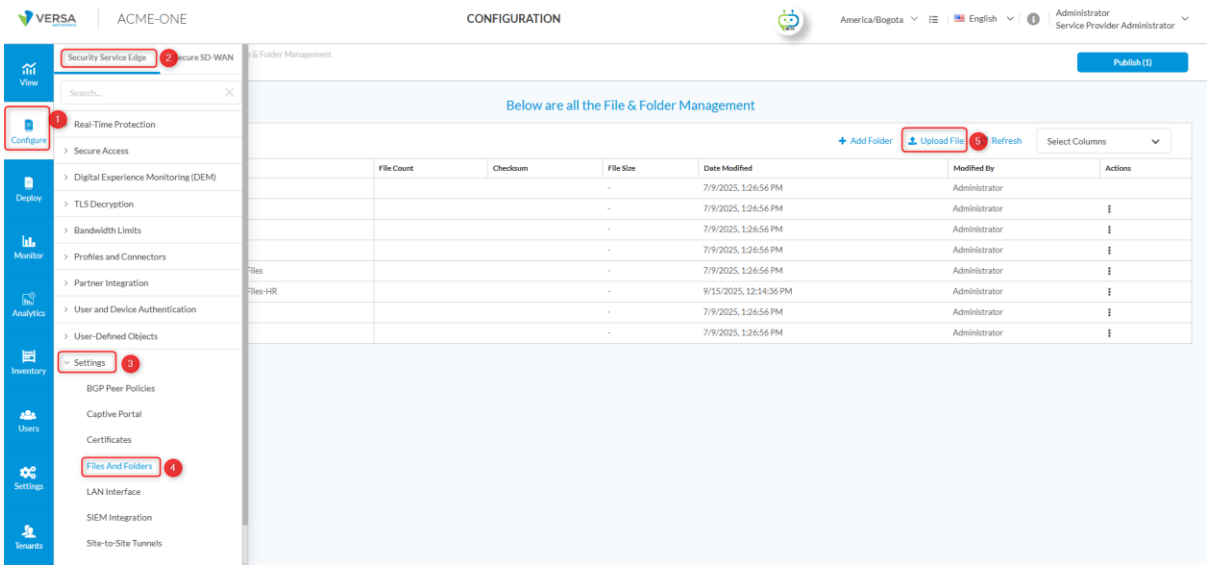
Once completed, the configuration window will look as follows:



Upload File:

Navigate to **Configure > Security Service Edge > Settings > Files and Folders**.

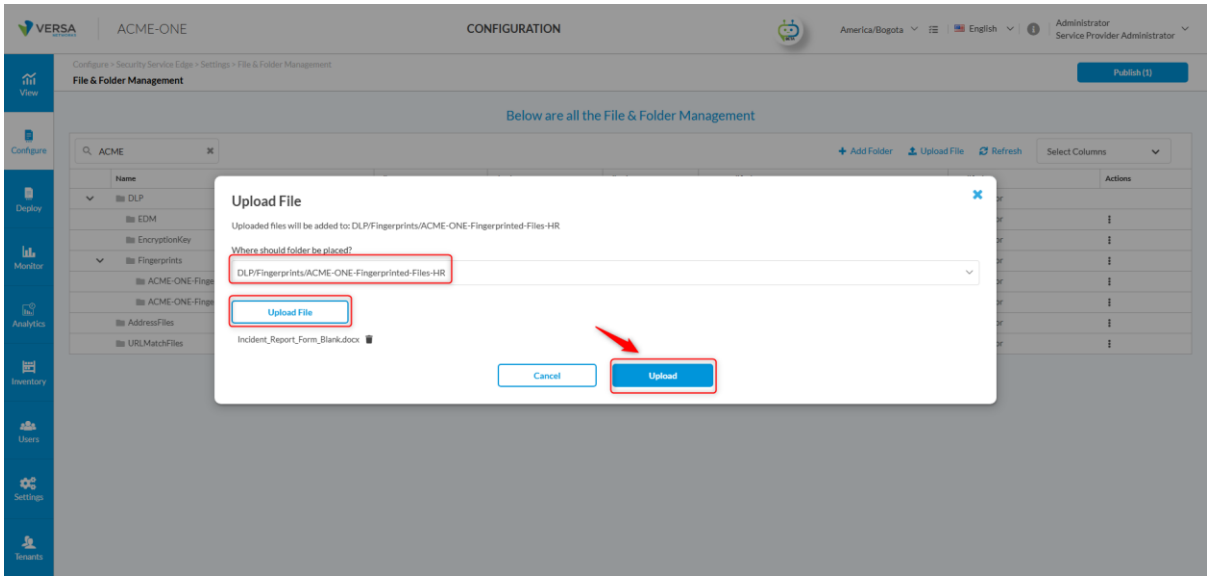
Click **+ Upload File**, as shown in the image below.



Next, a window called **Upload File** will appear with three sections to configure:

- **Hash the file:** We can leave the default option selected (checked).
- **Where should folder be placed?**: From the dropdown list, select **DLP/Fingerprints/ACME-ONE-Fingerprinted-Files-HR** which is the sub-folder we defined before.
- **Upload File**: Click and select the file from the corresponding location. In our case we are uploading the file

Once completed, the configuration window will look as follows:

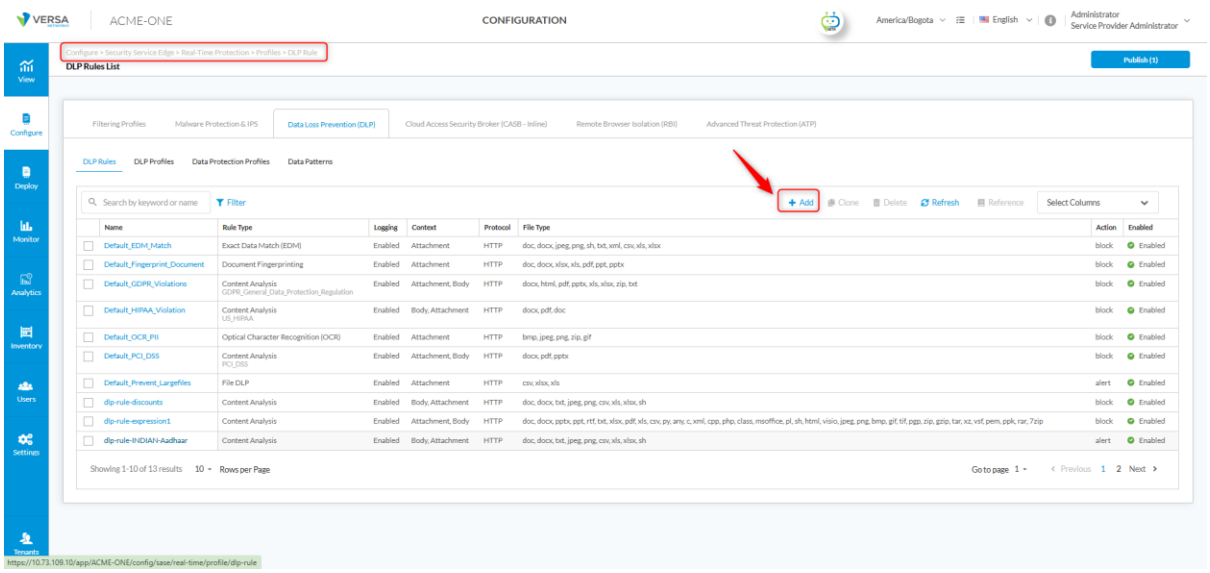


Finally, click on **Upload** to complete the process.

Create DLP Rule:

Navigate to **Configure > Security Service Edge > Real-Time Protection > Profiles > DLP Rule**.

Click **+ Add**, as shown in the image below.



You will now see a menu to select the type of DLP rule. In our case, select **Document Fingerprinting**. For details on the different types of DLP rules, refer to **Appendix A *(DLP Rule Types)***.

After selecting **Document Fingerprinting**, six configuration steps will appear:

Document Fingerprinting:

Folder Name: Click on the dropdown list and select the folder ACME-ONE-Fingerprinted-Files-HR.

Similarity Threshold: Defines the minimum level of content overlap required between an uploaded user document and the reference (sample) document. For example, if the threshold is set to 60% and the computed similarity is 70%, the document will be considered a match. Conversely, if the threshold is set to 80%, the same document would not be considered a match. For this case, please select 50%.

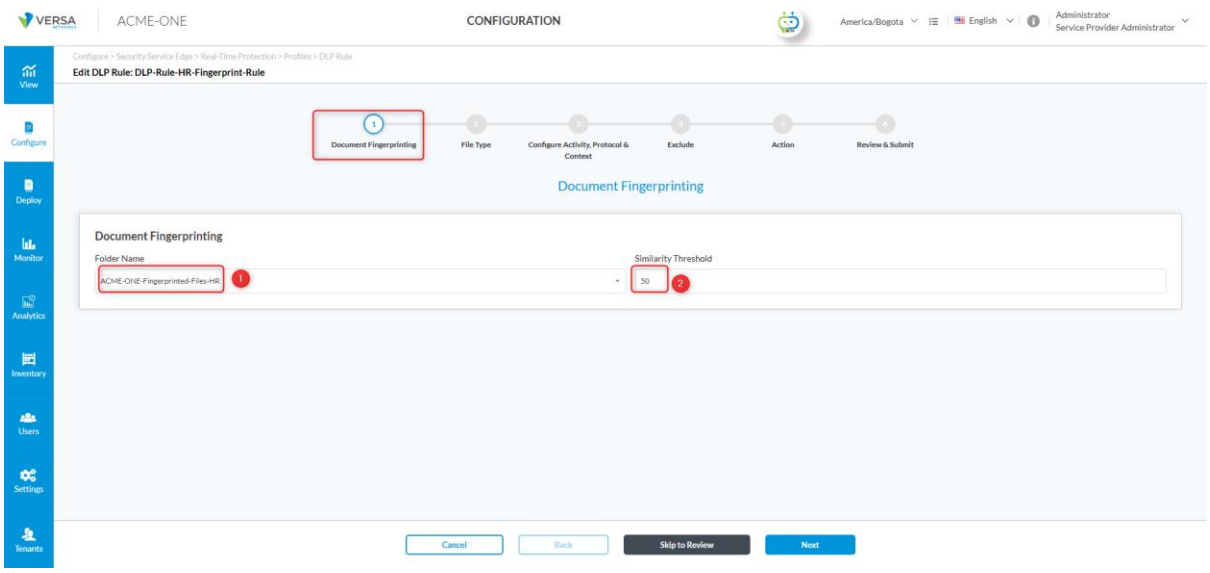
Once completed, the configuration window will look as follows:

Notes:

*- **Avoid False Matches on Blank Forms**: If the computed similarity is **95% or higher**, Versa assumes the uploaded document is effectively blank or unmodified, and the document will not be considered a match. Ensure user-filled forms include sufficient new content to lower the similarity below 95%, enabling meaningful evaluation.*

*- **Recommended Thresholds for Fully Completed Forms**: For user-submitted, fully completed forms, set the similarity threshold between **30% and 60%** to detect and match against the original template reliably.*

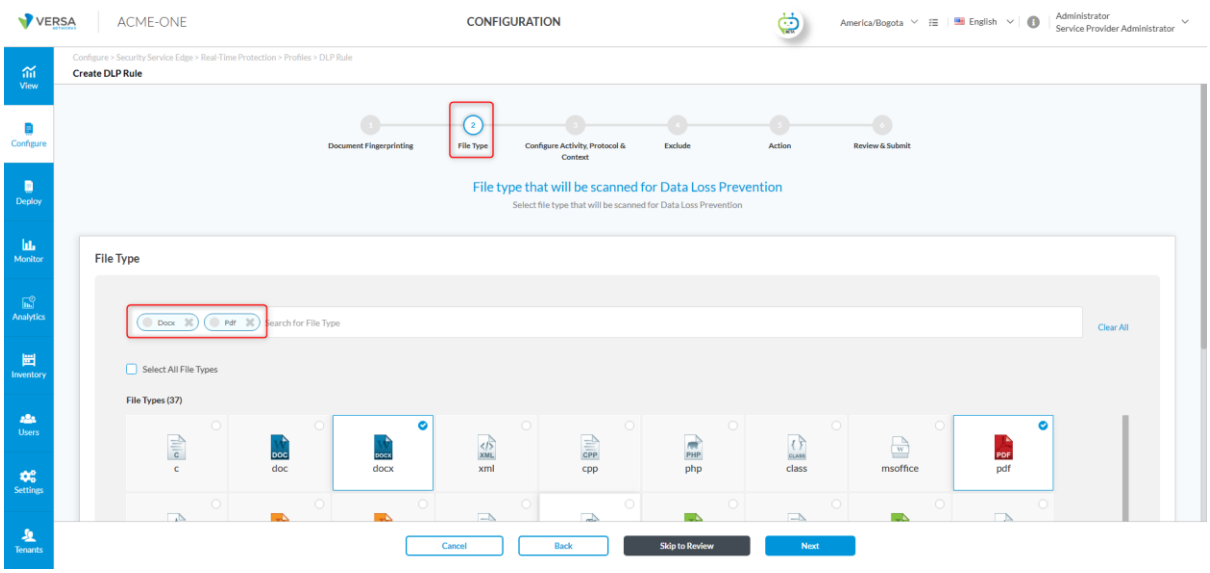
*- **Tailor the Threshold**: Adjust the similarity threshold based on form type and expected variation. Use **lower thresholds** for structured, fully completed forms and **higher thresholds** for loosely modified templates.*



Click **Next** to continue.

File Type: Select the file types you want to inspect. For this use case select: **.docx** and .pdf.

***NOTE**: - **Supported File Types**: **PDF, DOC, and DOCX**.*



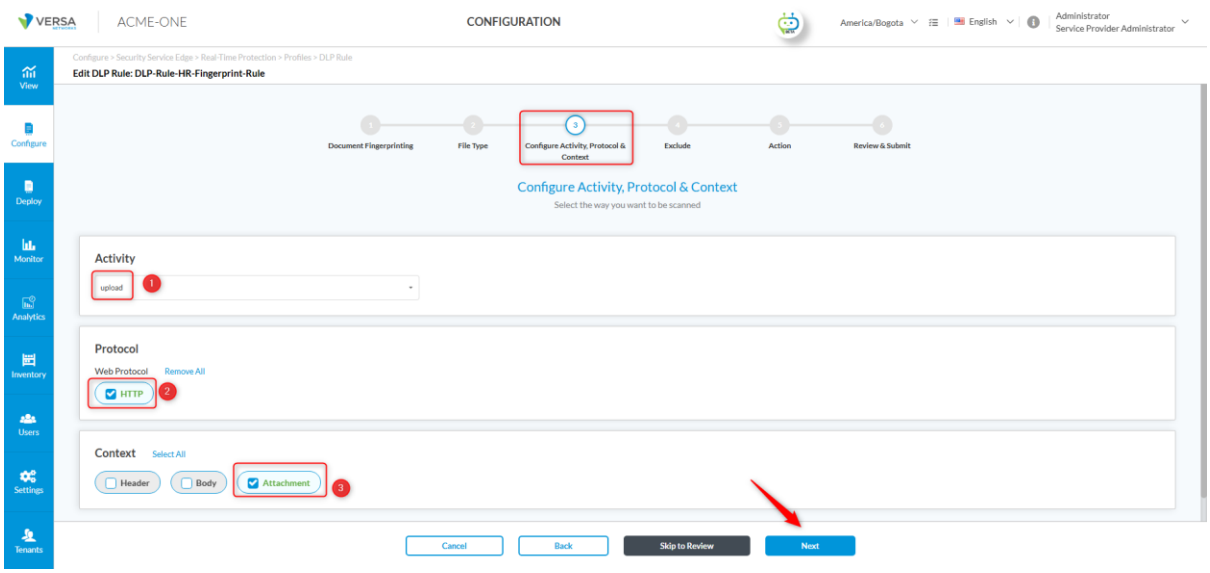
Click on **Next** to continue.

Configure Activity, Protocol & Context:

Activity: Select the activity to which the DLP module will be applied. In our case, select **Upload**.

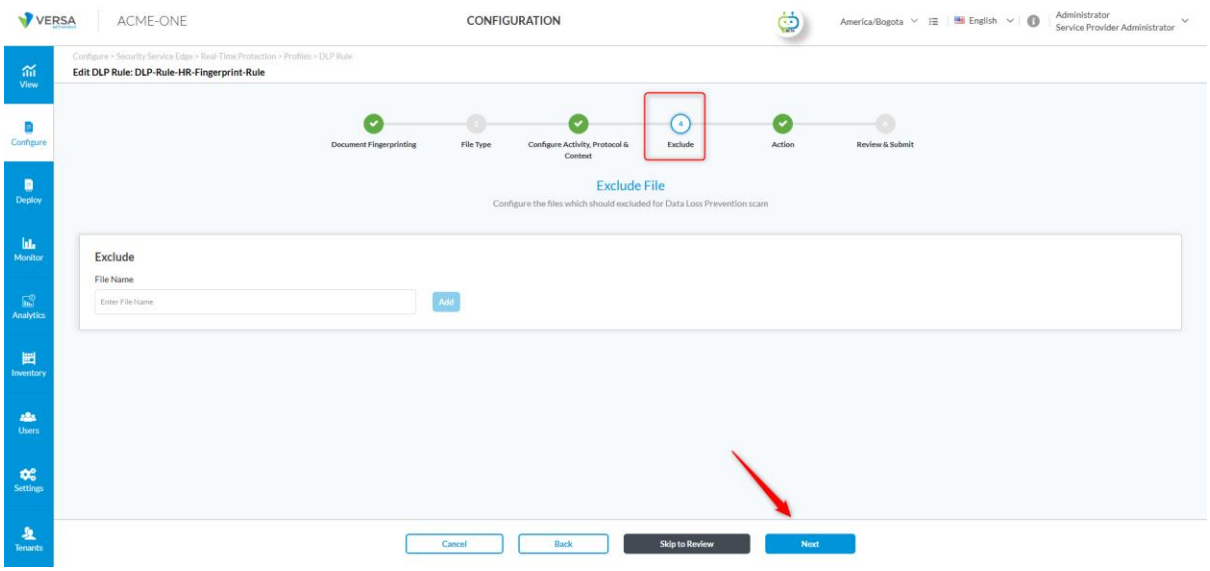
Web Protocol: Select **HTTP**.

Context: Defines which part of the packet or message will be inspected. For this example, select **Attachments**.



Exclude: We can skip this step since the use case does not require excluding any files.

Click on **Next** to continue.

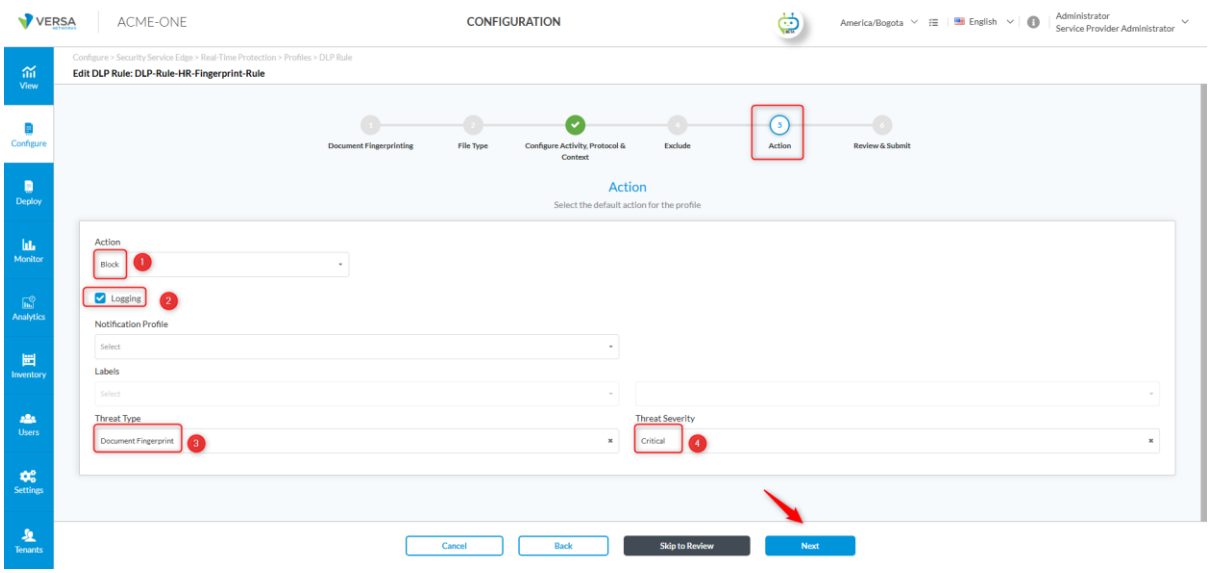


Action:

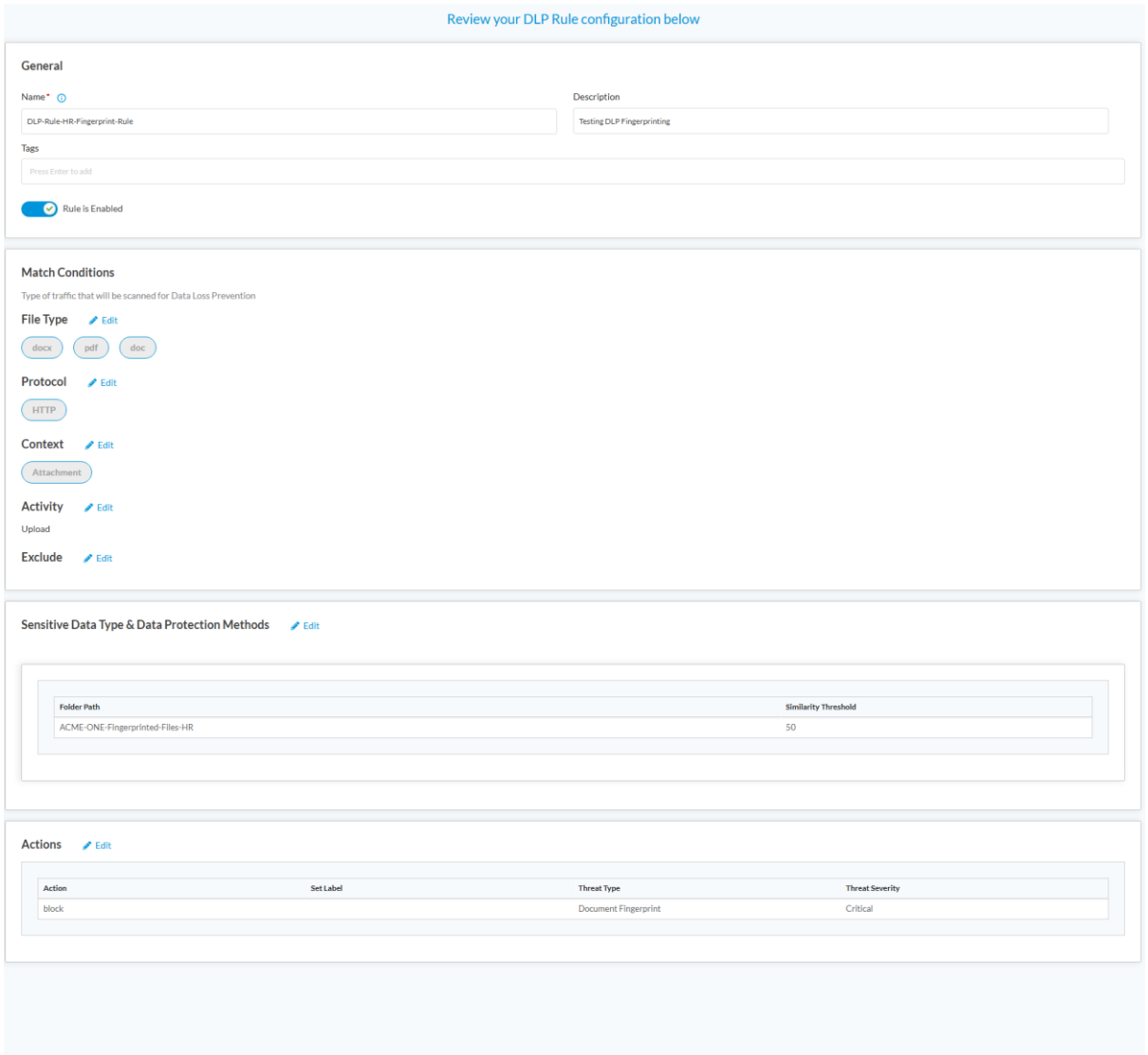
Define the action to be executed when the rule is triggered. Several options are available including:

- Allow
- Alert
- Block
- Reject

In our case, we will select **Block**. For more information on the different actions, refer to **Appendix B: *DLP Rule Actions*.**



Review & Submit: Verify that your rule matches the example shown in the image below, then click **Save**.

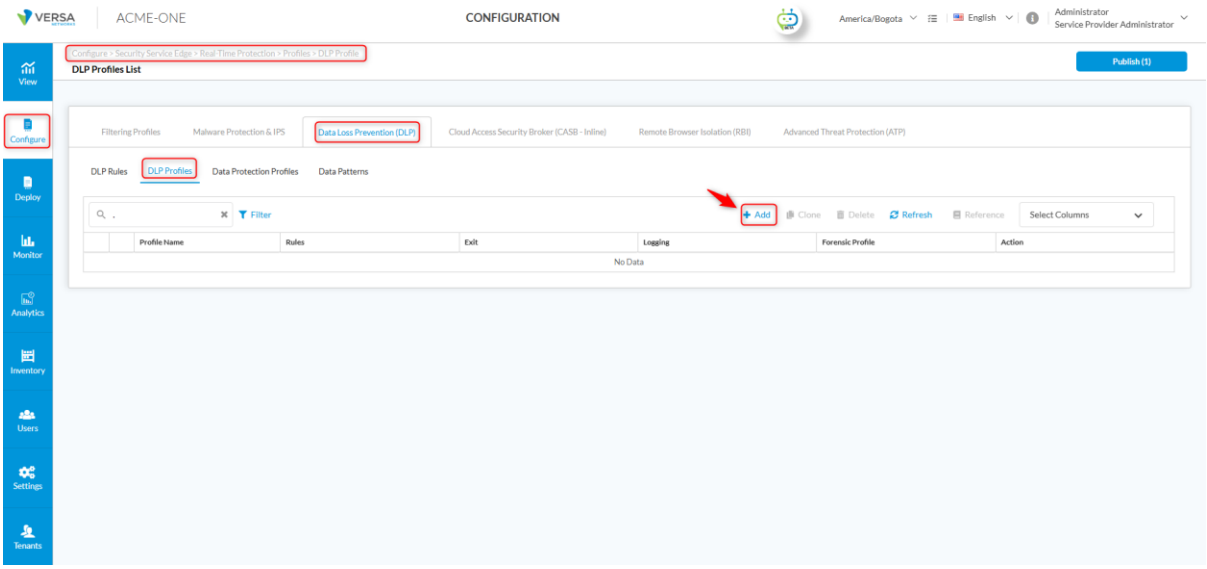


Create the DLP Profile:

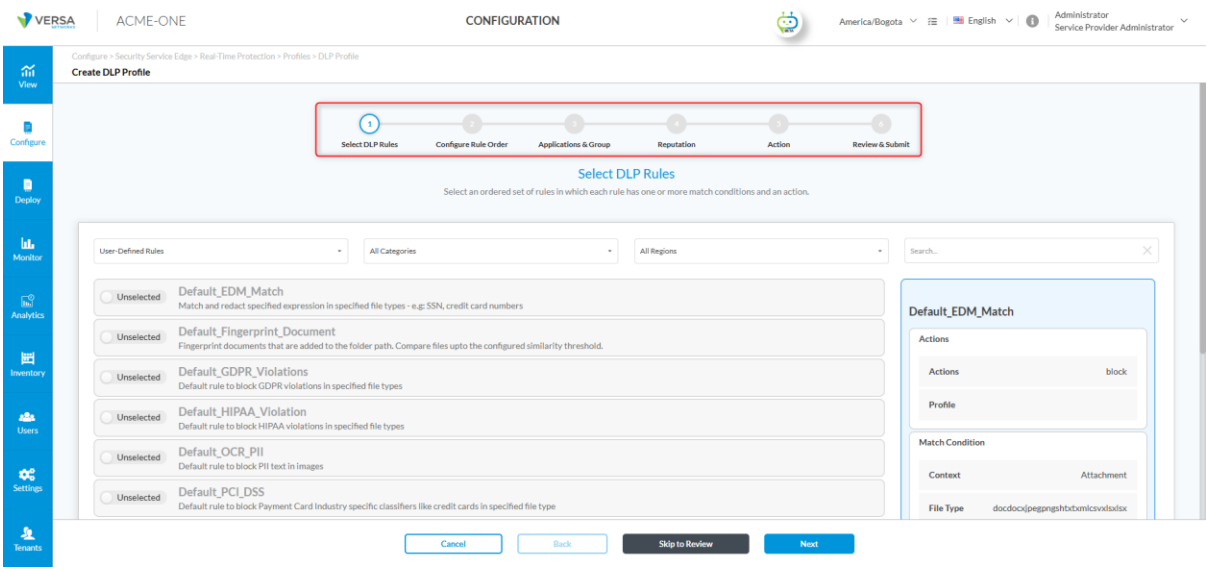
Navigate to

Configure > Security Service Edge > Real-Time Protection > Profiles > DLP Profile.

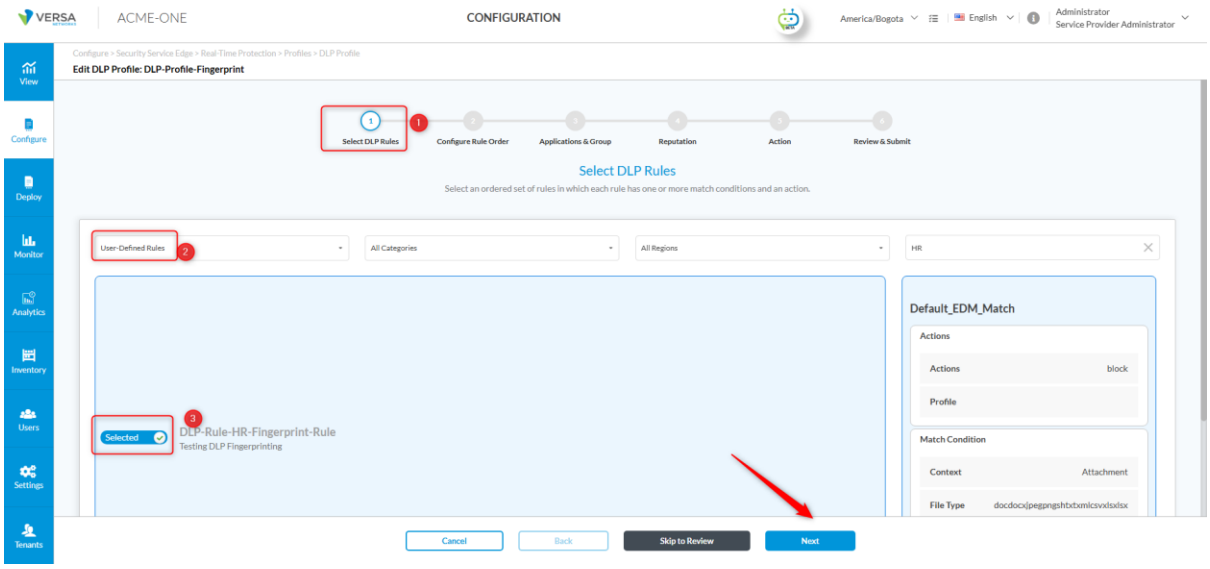
Click + Add, as shown in the image below.



Then, complete the six configuration steps shown in the following image.



Select DLP Rules: In the **User Defined Rules** section, search for the rule you created earlier.Select it and click **Next**. It should look like the example shown in the image below.



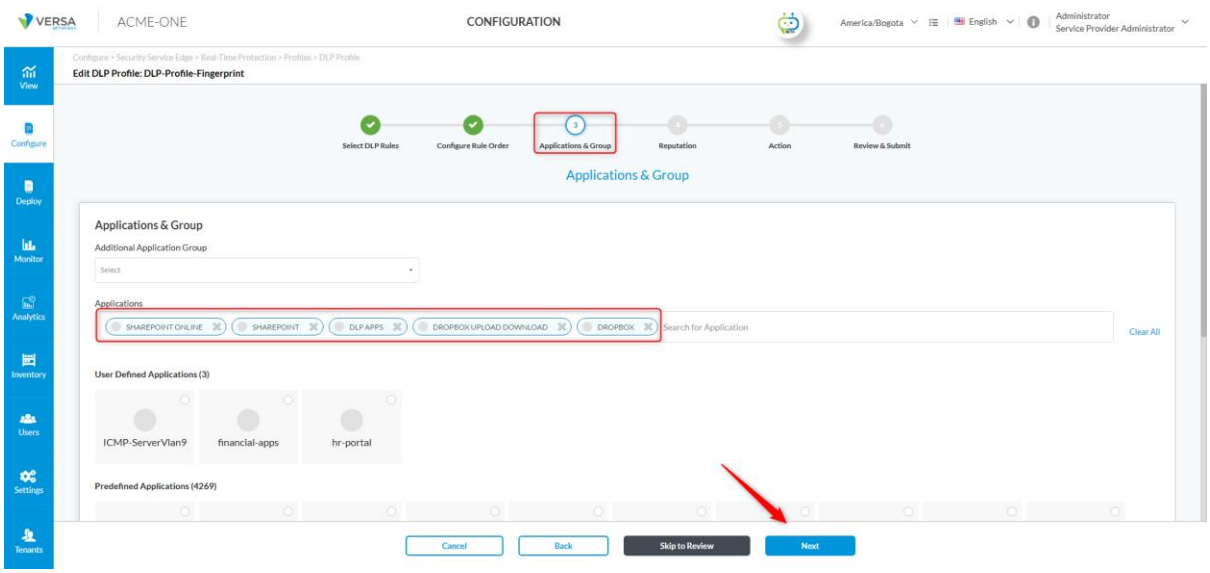
Configure Rule Order: We can skip this step since only a single rule has been selected, so click **Next** to continue.

Applications & Group: In the **Applications** search field, search for each application to which the DLP profile will be applied. In our case, select the related apps for **SharePoint** and **Dropbox**, then click **Next**, as shown in the image below.

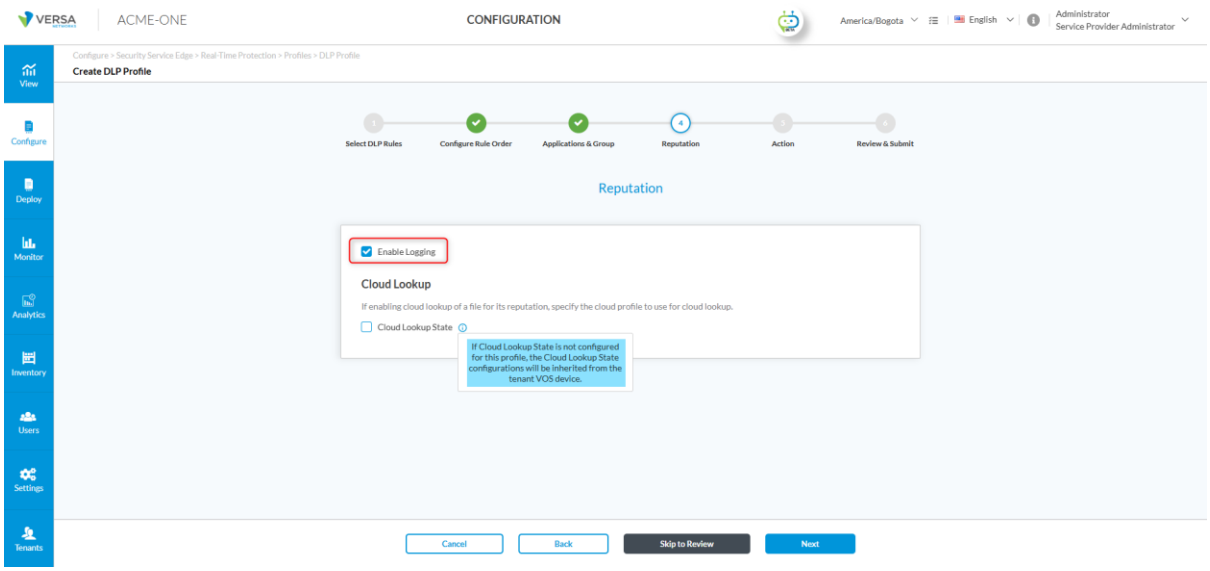
Notes:

*- In cases where not all dependent applications are known, adding the generic applications **HTTPS** or **HTTP** to the DLP profile may help. However, this approach is not technically guaranteed to work and could impact unrelated traffic. Therefore, rules applied in real-time protection should remain as specific as possible.*

*- In some cases, you may also need to add dependent applications when dealing with SaaS apps. For example, Gmail relies on additional services such as **gstatic.com** to load resources like icons, scripts, or image previews (e.g., when sending or viewing image attachments). Without allowing these dependencies, the SaaS application may not function correctly.*



Reputation: Select the **Enable Logging** option to store website reputation events, as shown in the image below. **Cloud Lookup** is optional; for more information, you can visit the following link: How to Configure Cloud Lookup.



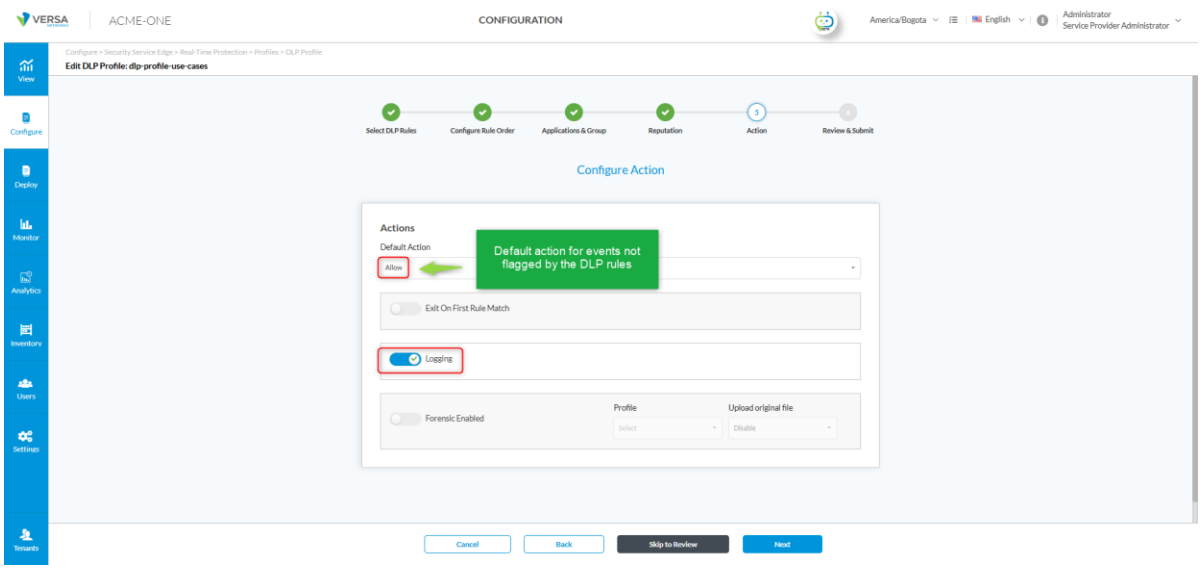
Action:

Actions: Set the default action to **Allow**. The default action is applied if none of the scanned data matches a rule.

Logging: Click on the toggle button to enable logging.

Exit on First Rule Match: Leave the default action set to **disabled**.

Note: if multiple DLP rules are configured, this option should be disabled to ensure that all rules are applied to the same session.



Review & Submit: Review the configuration, then click the **Save** button.

Step 2: Create the TLS decryption rule for the cloud applications we will test (SharePoint and Dropbox).

To ensure that payloads can be inspected and DLP policies applied, a TLS decryption rule must exist for the cloud applications being tested (e.g., SharePoint and Dropbox).

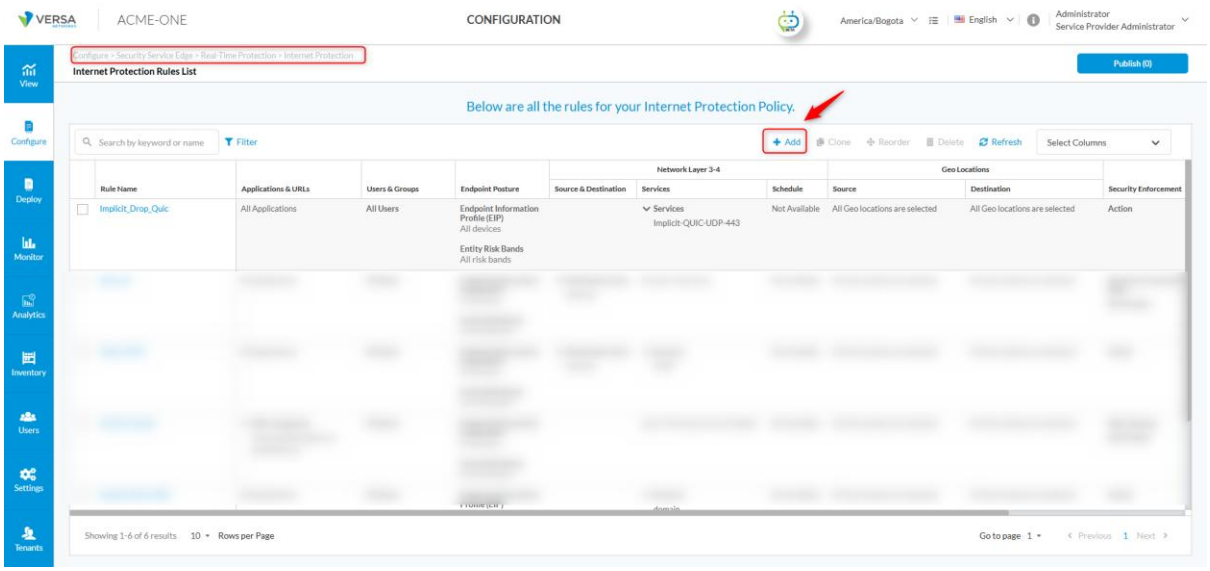
If you need the detailed step-by-step configuration for creating this rule, refer to **Appendix C: TLS Decryption Rule Configuration**.

Step 3. Create the real-time protection rule using the DLP profile on the cloud apps defined earlier.

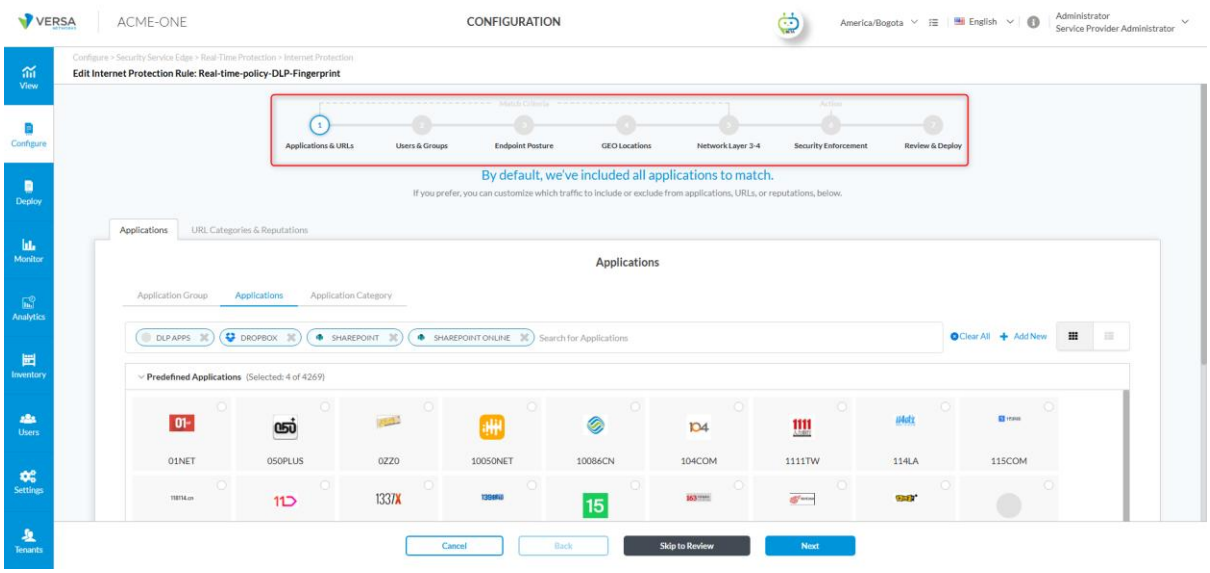
Navigate to

Configure > Security Service Edge > Real-Time Protection > Internet Protection.

Click + Add, as shown in the image below.



Then, complete the seven configuration steps shown in the following image.



Applications & URLs: Select the applications to which we will apply our DLP module. In our case, we choose SharePoint and Dropbox.

Users & Groups: Select our test group and then click Next. In our case, it can be the (VIP) or (HR) group coming from our LDAP-AD.

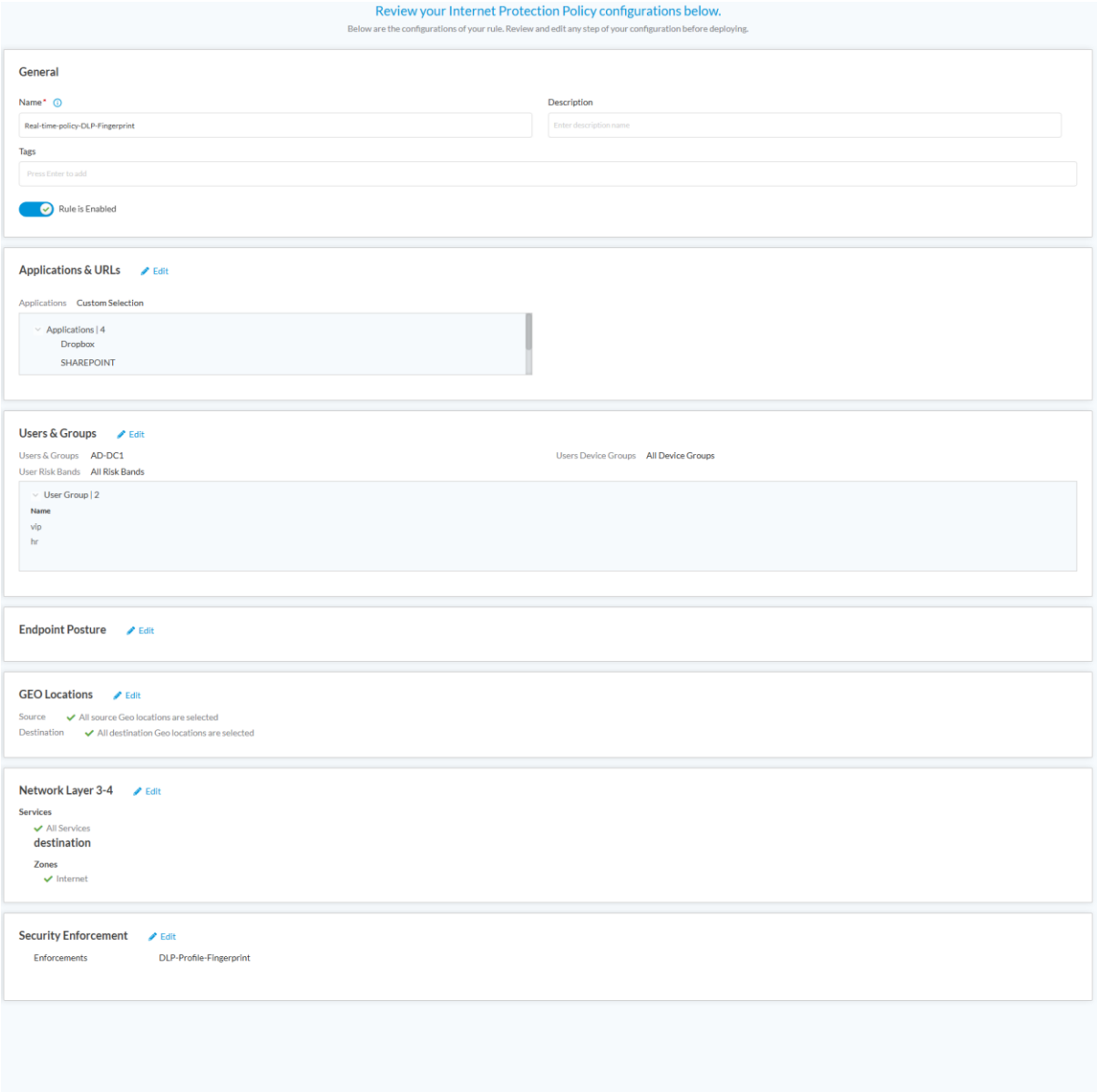
Endpoint Posture: You can apply Endpoint Information Profiles and Entity Risk Bands; however, in our case, leave the default settings to apply none and click **Next**.

Geolocation: You can filter by Source or Destination Geo Location. In our case, we leave the default setting to **All** and click **Next**.

Network Layer 3-4: You can filter by services (Layer 4) such as HTTP, HTTPS, DNS, ICMP, etc. You can also filter by Source & Destination (Layer 3). However, leave the default values and click **Next**.

Security Enforcement: Click on the **Security Profiles** option, then select **Data Loss Prevention**. Toggle the switch to enable it, then choose the profile named **DLP-Profile-Fingerprint**, which is the one we created. Click **Next**.

Review & Validate: Review the configuration (see image below), click **Save**, and select **add this rule at the top of the rule list**.



Finally, publish the changes applied in Concerto and proceed with the verifications.

Step 4. Perform tests and validate the behaviour.

To perform the tests, we only need to upload from SharePoint and Dropbox the test file that corresponds to the confidential form once completed. Below, you can see the original (blank) and the one used in the test (filled).

Filename: Incident_Report_Form_Blank.docx

Confidential Employee Incident Report Form

This form is intended for the reporting of workplace incidents and policy violations. All submissions are confidential and will be reviewed by the HR Compliance Department. Please complete all required sections. Additional evidence or extended narratives should be attached as separate documents. Do not exceed the provided space in each section.

Section 1 – Employee Information

Employee Name: _____

Department: _____

Position: _____

Date of Incident: ___ / ___ / ____

Section 2 – Type of Violation

Please check one or more categories that best describe the violation (mandatory selection):
[ ] Code of Conduct
[ ] Confidentiality Breach
[ ] Workplace Harassment
[ ] Safety Violation
[ ] Other (please specify) _____

Section 3 – Description of Violation

Provide a concise summary of the violation in 3–4 sentences maximum. If additional details are needed, attach a supporting document.

Description (do not exceed space provided):
_____
_____
_____

Section 4 – Witnesses

List up to 2 witnesses with name and department. Additional names must be attached separately.

1. _____

2. _____

Section 5 – Co-Workers Involved

List any co-workers directly involved in the incident. Specify their role or relation to the case.

1. _____

2. _____

Section 6 – Acknowledgement

By signing this form, the reporting employee confirms that the information provided is accurate to the best of their knowledge. The HR Compliance Department will review the case and take the appropriate action as outlined in company policy.

Employee Signature: _____ Date: ___ / ___ / ____

Filename: Incident_Report_Form_Filled.docx

Confidential Employee Incident Report Form

This form is intended for the reporting of workplace incidents and policy violations. All submissions are confidential and will be reviewed by the HR Compliance Department. Please complete all required sections. Additional evidence or extended narratives should be attached as separate documents. Do not exceed the provided space in each section.

Section 1 – Employee Information

Employee Name: John Doe

Department: IT Security

Position: Senior Security Analyst

Date of Incident: 09 / 12 / 2025

Section 2 – Type of Violation

Please check one or more categories that best describe the violation (mandatory selection):
[X] Confidentiality Breach
[ ] Code of Conduct
[ ] Workplace Harassment
[ ] Safety Violation
[ ] Other (please specify) _____

Section 3 – Description of Violation

Provide a concise summary of the violation in 3–4 sentences maximum. If additional details are needed, attach a supporting document.

Description:
On September 12th, 2025, an employee was observed uploading a confidential HR policy document to a personal Dropbox account. The file contained sensitive disciplinary procedures. The incident was detected by the DLP monitoring system and reported for investigation.

Section 4 – Witnesses

List up to 2 witnesses with name and department. Additional names must be attached separately.

1. Jane Smith – HR Department

2. Michael Brown – IT Department

Section 5 – Co-Workers Involved

List any co-workers directly involved in the incident. Specify their role or relation to the case.

1. Alice Johnson – Co-worker who shared the document link internally.

2. N/A

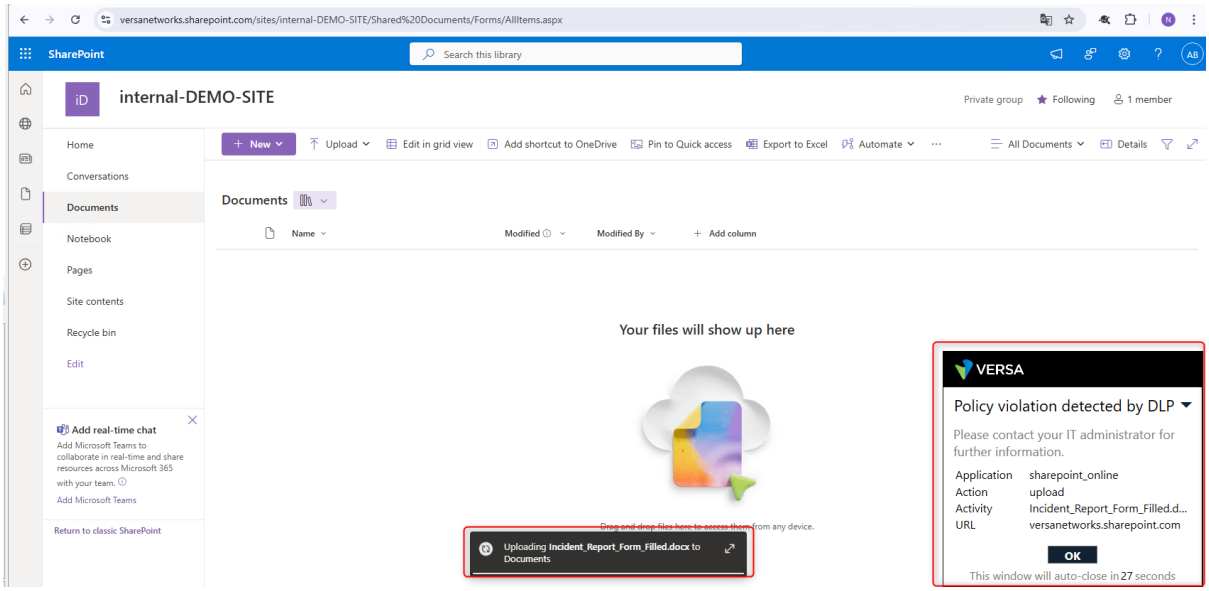
Section 6 – Acknowledgement

By signing this form, the reporting employee confirms that the information provided is accurate to the best of their knowledge. The HR Compliance Department will review the case and take the appropriate action as outlined in company policy.

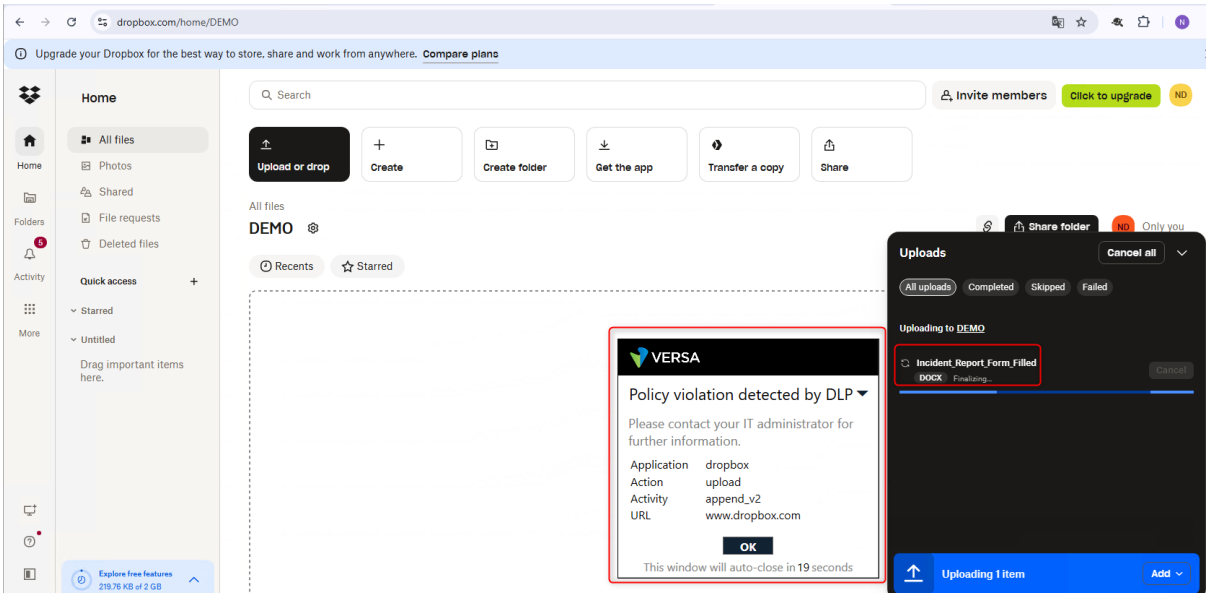
Employee Signature: John Doe Date: 09 / 12 / 2025

Now, Upload from SharePoint or Dropbox the file called *Incident_Report_Form_Filled.docx*, which should be blocked because the **Block** action was selected. See the images below.

SharePoint test

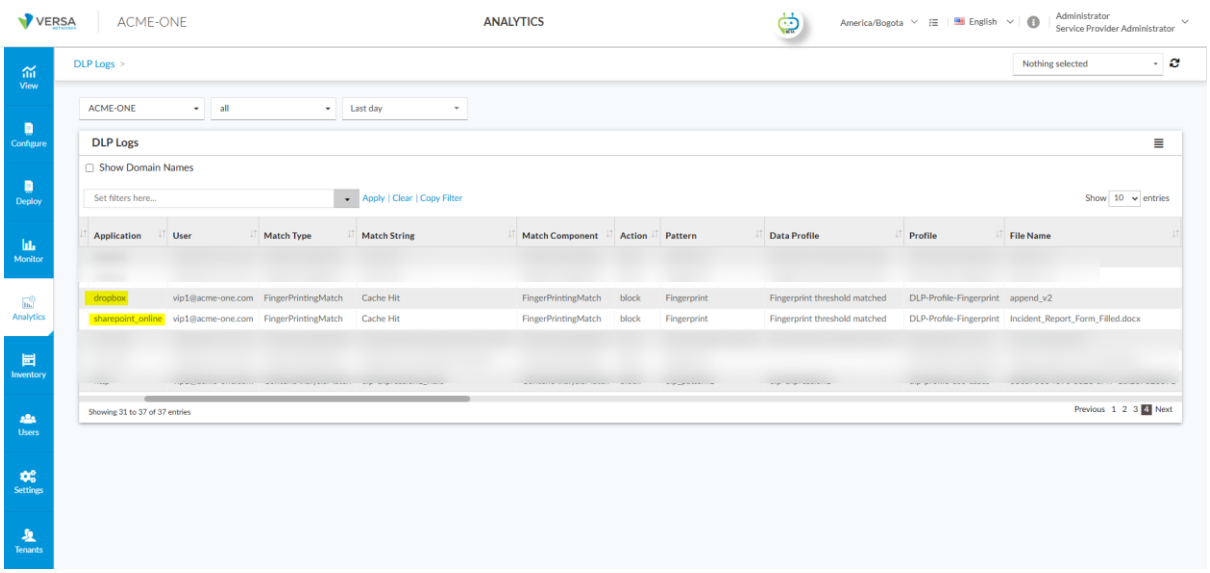


Dropbox test



You can find the sample in Appendix D – *Incident_Report_Form_Filled.docx*.

When checking the logs in **Concerto > Analytics > DLP Logs**, you should see something similar to the images below.



Use Case 3: VIP Customer Data Protection with EDM-Based DLP

This use case demonstrates how ACME-ONE leverages **EDM-based DLP** in Versa Networks to prevent sensitive customer records from being leaked by employees in Finance or VIP Management. These employees regularly access the **VIP Customers Database** and frequently use cloud collaboration platforms and email services.

The Finance and VIP Management departments at ACME-ONE manage a **VIP Customers Database** containing highly sensitive information, such as:

- Customer Full Name
- Customer ID / Account Number
- Email Address
- Phone Number
- Contract Reference Number

Since these records represent ACME-ONE's top customers, preventing their unauthorized disclosure is a business-critical requirement. Unlike fingerprinting entire forms, **EDM provides field-level matching against the structured database**, ensuring that even partial extracts (e.g., a CSV export) are detected.

To reduce the risk of intentional or accidental exfiltration via platforms commonly used by Finance and VIP staff, Versa's EDM DLP engine is configured to detect matches against the registered VIP customer database when data is transmitted through:

Cloud storage apps: SharePoint web, Dropbox web.

Email services: Outlook (Office 365), Gmail

Using Versa's integrated DLP engine, ACME-ONE defines a DLP policy named **"VIP Customer Data Protection"** with the following conditions:

Policy Name	Conditions	Details
VIP Customer Data Protection	EDM match with ≥ 1 field hit from VIP database	1) Register the VIP customer database as an EDM source in Versa DLP. 2) Trigger the policy if outbound traffic contains data matching any field from the EDM source via SharePoint, Dropbox, Outlook, or Gmail. 3) Actions include **Blocking, and Logging**.

Pre-requisites

- SSE Gateway with VSIA enabled.
- Authentication via Active Directory (LDAP used in our scenario)
- TLS Decryption enabled for the cloud applications defined for testing.

Configuration steps

The DLP configuration consists of the following steps, which are described in detail below:

1. Create DLP objects
    - Create a **DLP Pattern for USA mobile numbers, Contract id and Customer id.**
    - Create a **DLP Rule** (conditions that trigger DLP checks).
    - Create and assign a **DLP Profile / Policy** (the policy that ties the data profile and rules to enforcement actions).
2. **Create TLS decryption rule** for the cloud apps you will test (**SharePoint, Dropbox, Outlook** and **Gmail**).
3. **Create real-time protection rule** that applies the DLP profile to the cloud apps defined in Step 2.
4. **Perform tests and validate the behaviour.** Execute test cases, verify detection and enforcement, and record results.

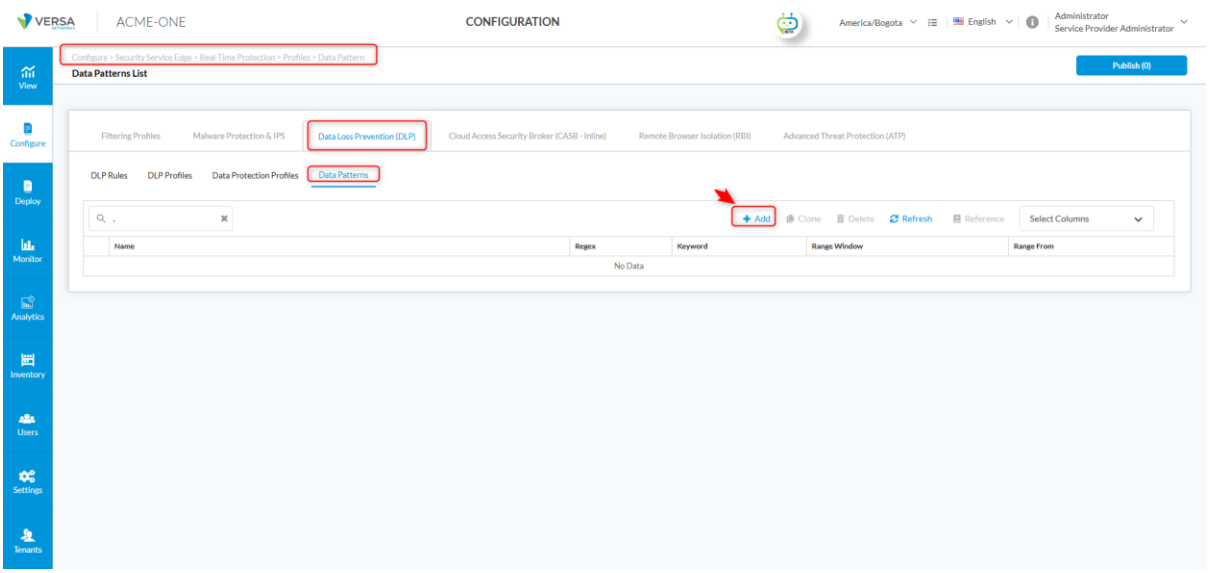
Step 1: Create DLP objects

For our use case (**EDM – Exact Data Match**), we need to upload our database through Concerto and then select the columns that contain sensitive information, mapping each column to a data pattern (either predefined or customized). It is important to have already defined any custom data patterns to be used, before reaching this step. In our case, we will define a custom data pattern for USA mobile numbers, contract IDs, and customer IDs, and we will use a predefined one for emails. After that, we will define the DLP rule, where we must configure the Boolean expression that determines the match condition.

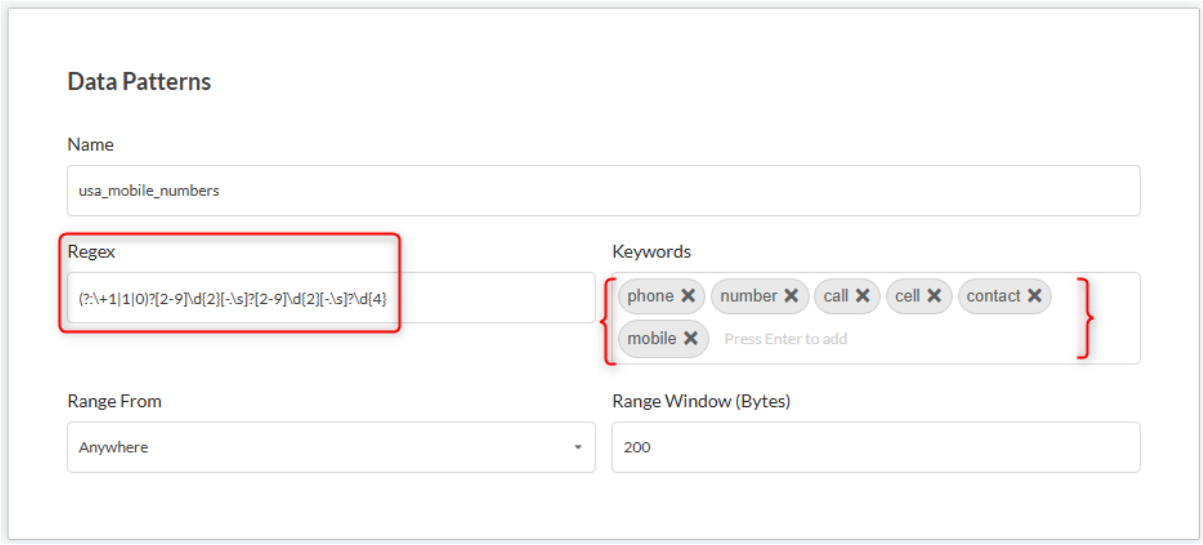
Creating a Data Pattern for USA Mobile numbers

Navigate to

Configure > ***Security Service Edge*** > ***Real-Time Protection*** > ***Profiles*** > ***Data Patterns. Click*** + ***Add***, as shown in the image below.



Next, we define the values with a simple regex for USA mobile numbers, making sure the keywords are included and related to the content, just as shown in the image below. Finally, click on Save.

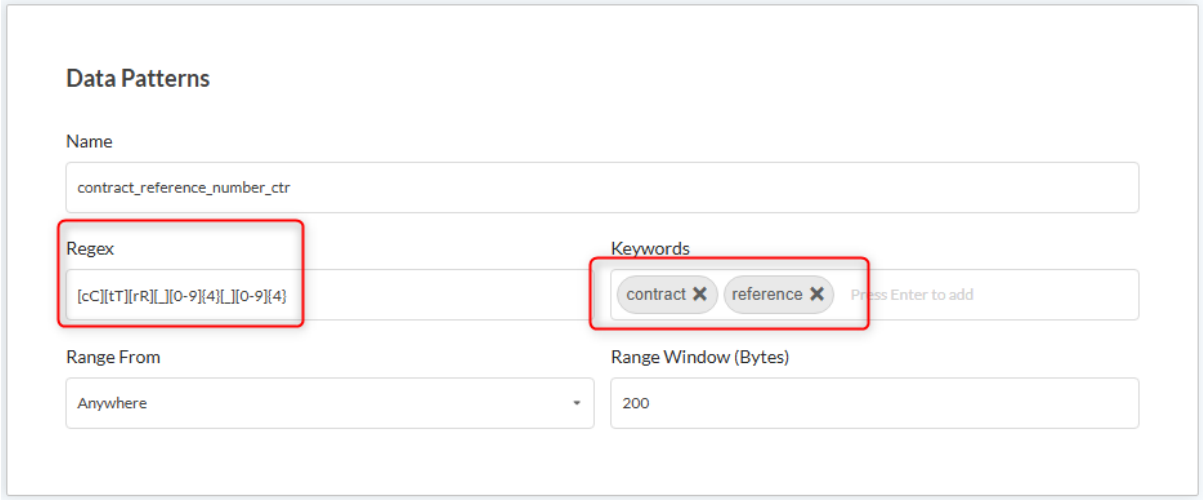


Creating a Data Pattern for Contract id

Navigate to

Configure > Security Service Edge > Real-Time Protection > Profiles > Data Patterns. Click + Add.

Next, we define the values with a simple regex for Contract id based on our Database , making sure the keywords are included and related to the content, just as shown in the image below. Finally, click on Save.

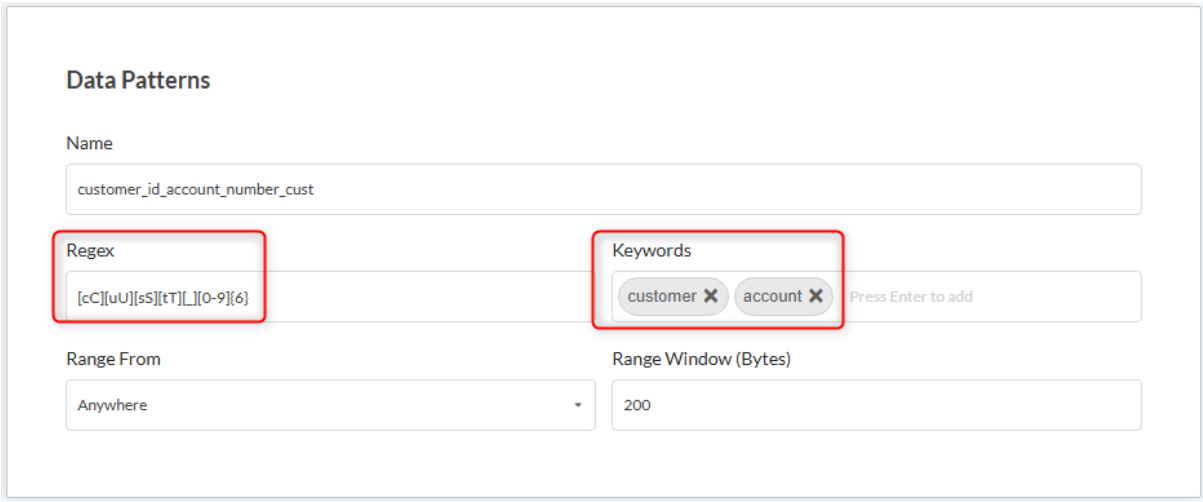


Creating a Data Pattern for Customer id

Navigate to

Configure > Security Service Edge > Real-Time Protection > Profiles > Data Patterns. Click + Add.

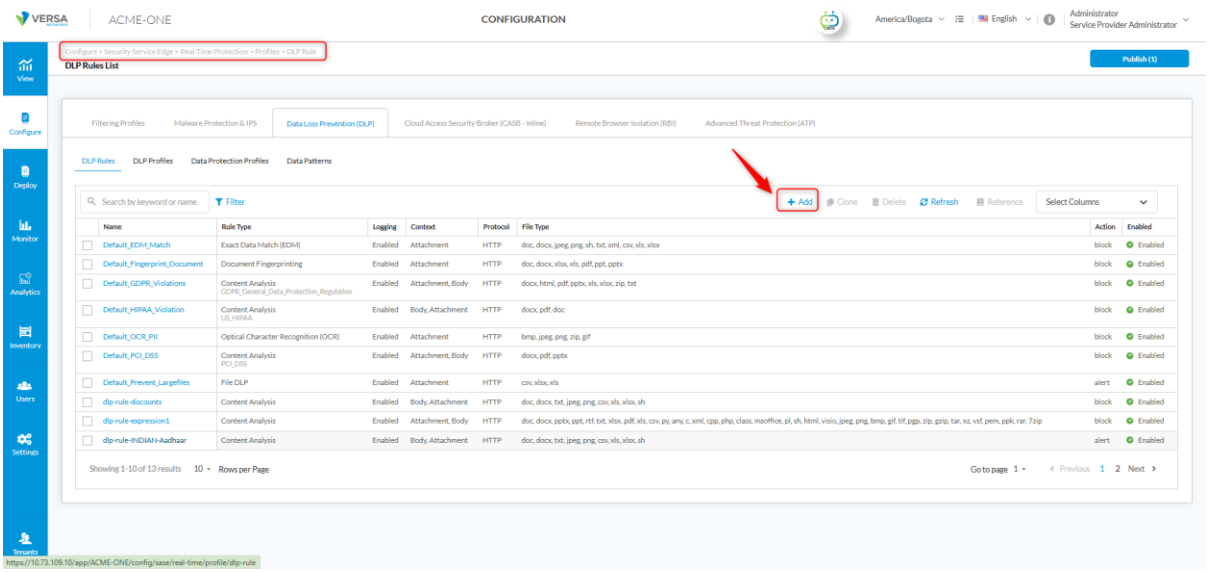
Next, we define the values with a simple regex for Customer id based on our Database , making sure the keywords are included and related to the content, just as shown in the image below. Finally, click on Save.



Create DLP Rule:

Navigate to **Configure > Security Service Edge > Real-Time Protection > Profiles > DLP Rule**.

Click **+ Add**, as shown in the image below.



You will now see a menu to select the type of DLP rule. In our case, select **Exact Data Match (EDM)**. For details on the different types of DLP rules, refer to **Appendix A *(DLP Rule Types)***.

After selecting **Exact Data Match (EDM)**, six configuration steps will appear. We will describe them below:

Exact Data Match:

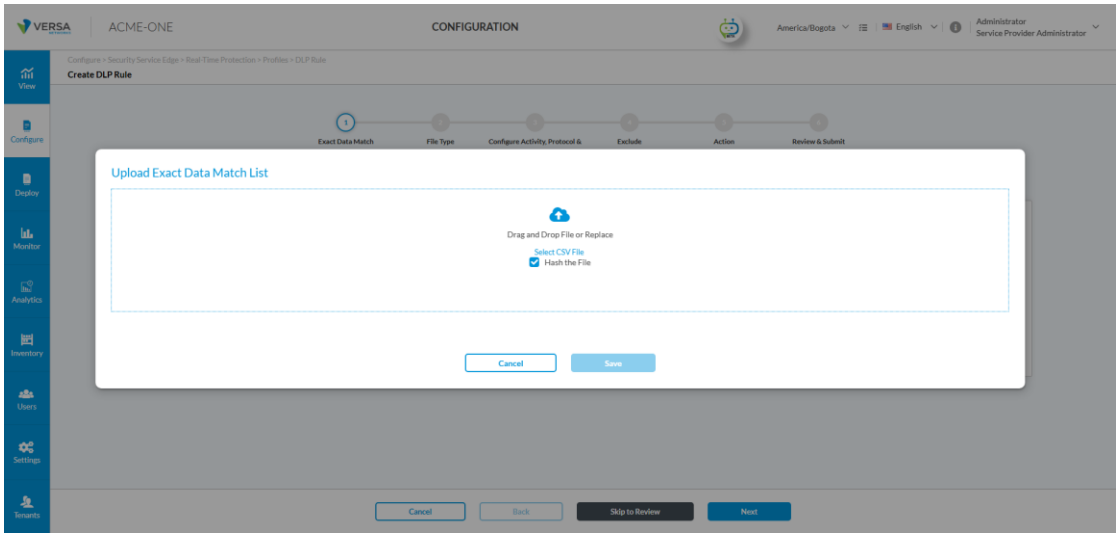
1. **Expression:** We have the following three options:

   Create Expression: The user defines a boolean expression without relying on a database. This expression can use either predefined or customized data patterns.

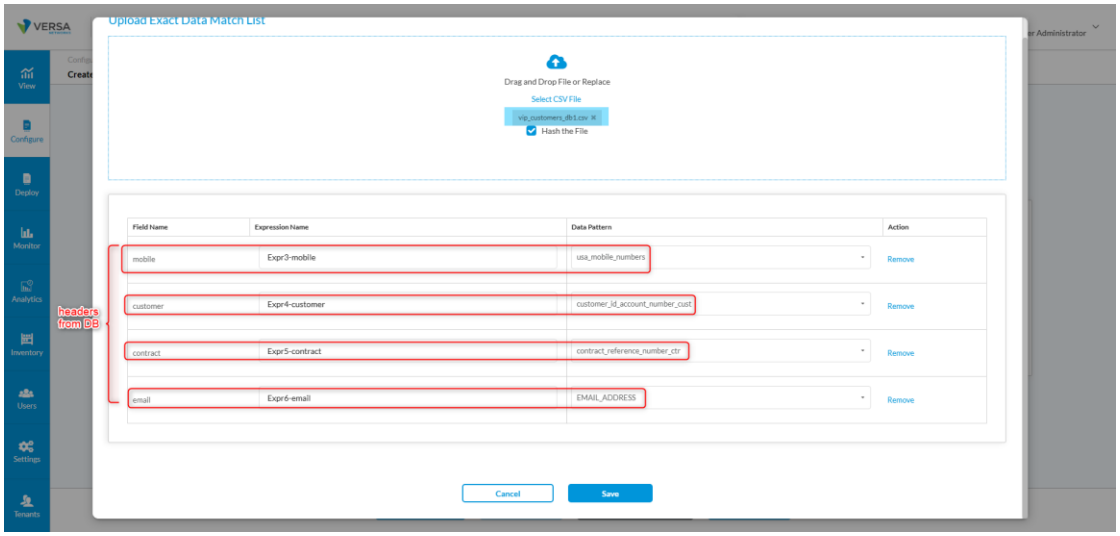
   Upload File: Allows us to upload our database file, and Versa will automatically display the column headers so the user can decide which ones to use and which data pattern to associate with each of them. For example, if the database has a column with email addresses, that column can be mapped to Versa's predefined data pattern for emails.

   Select File Name: Allows us to select a file that was previously uploaded to Versa under the *File and Folders* path.

   For our case, we will use the option **Upload File**, and the following screen will appear. We can keep the *Hash the File* option enabled, which is selected by default for security reasons. However, if in the future the Administrator wants to download the original database from Concerto, this option must be unchecked; otherwise, the downloaded file will only contain the hashed values.

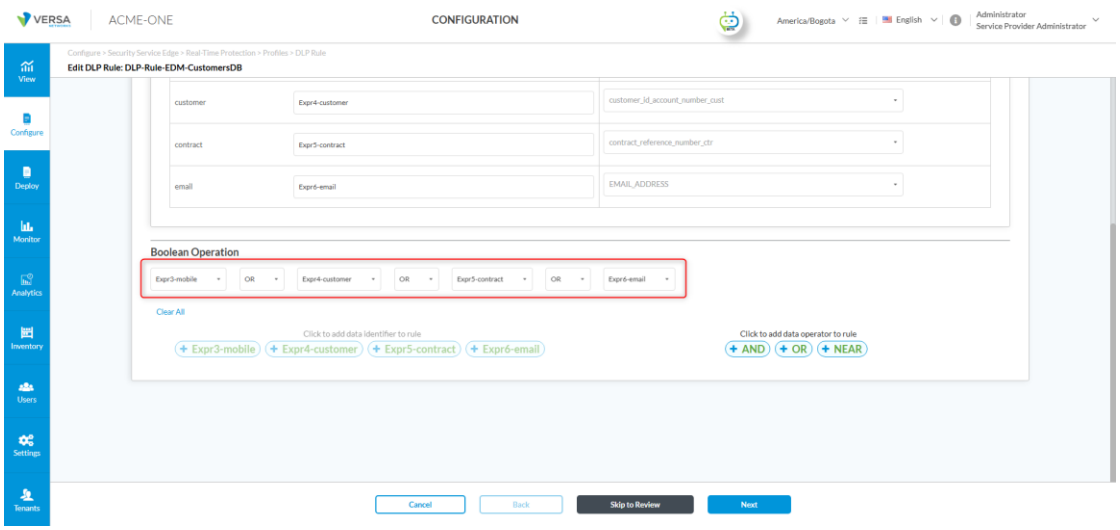


Next, we either drag and drop the database file or click to select it manually. In our case, we upload the file named *vip_customers_db1.csv*. We then proceed to remove the columns that are not relevant to our use case and map each remaining column to the corresponding DLP data pattern created earlier, as shown in the image below.



Click **Save** to continue.

2. **Boolean Operation:** After completing the previous step, we proceed to define the boolean expression that will determine the match condition. For example, in our case, we will use a simple expression that applies an OR to all the expression name headers, as shown in the image below.

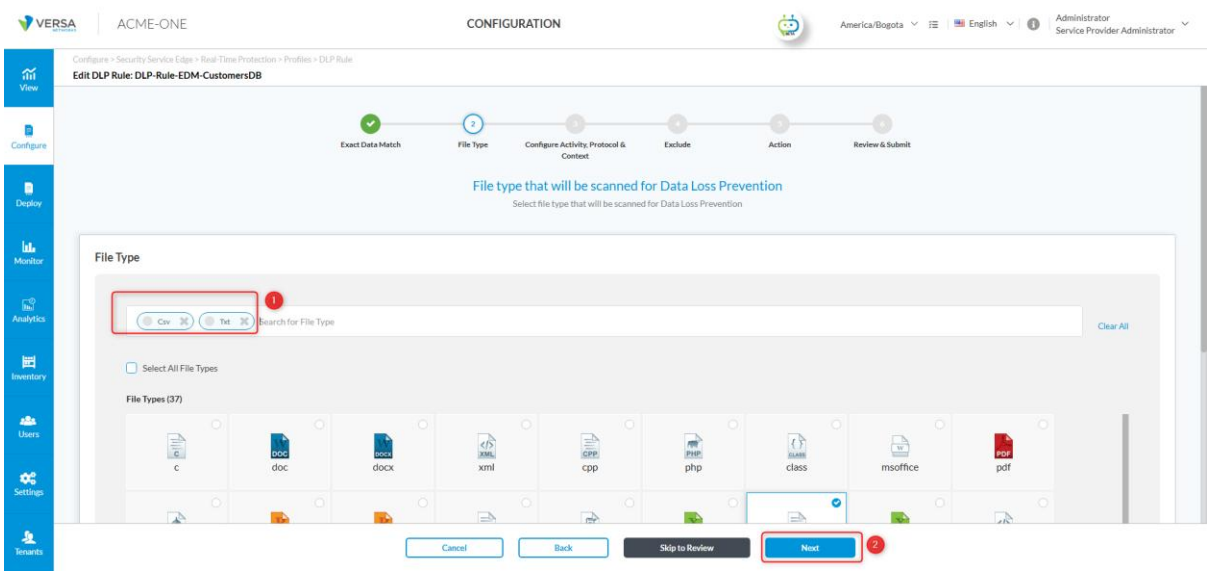


3. Click **Next** to continue.

File Type: Select the file types you want to inspect. For this use case, select: .csv and .txt.

NOTE: Supported File Types are CSV, Excel and Text.

Click on **Next** to continue.

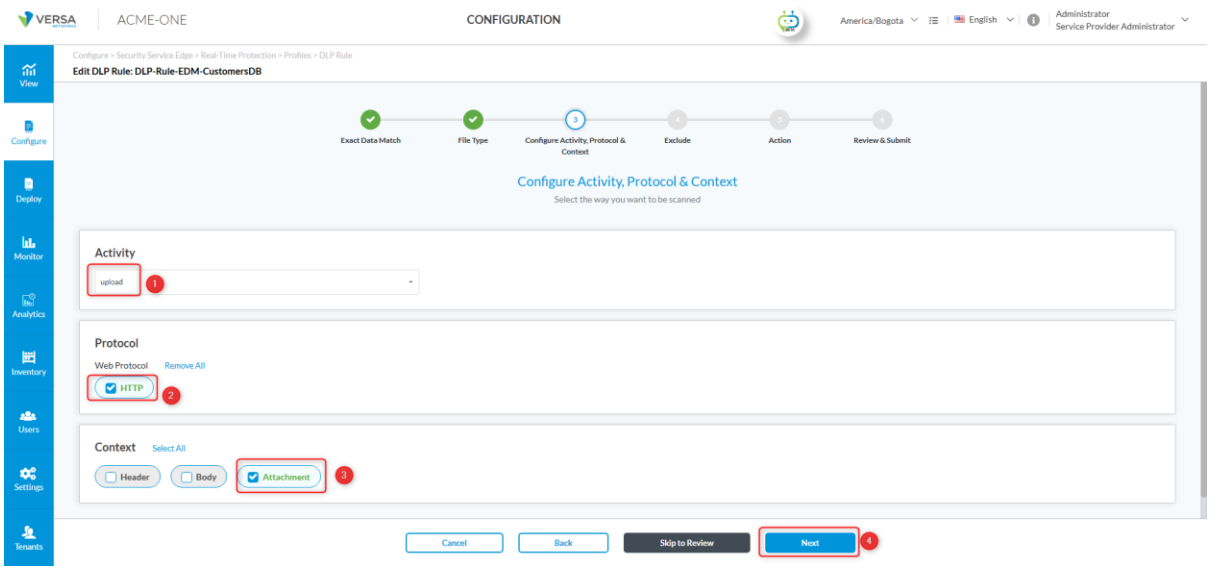


Configure Activity, Protocol & Context:

1. **Activity:** Select the activity to which the DLP module will be applied. In our case, select **Upload**.

2. **Web Protocol:** Select HTTP.

3. **Context:** Defines which part of the packet or message will be inspected. For this example, select **Attachments**.

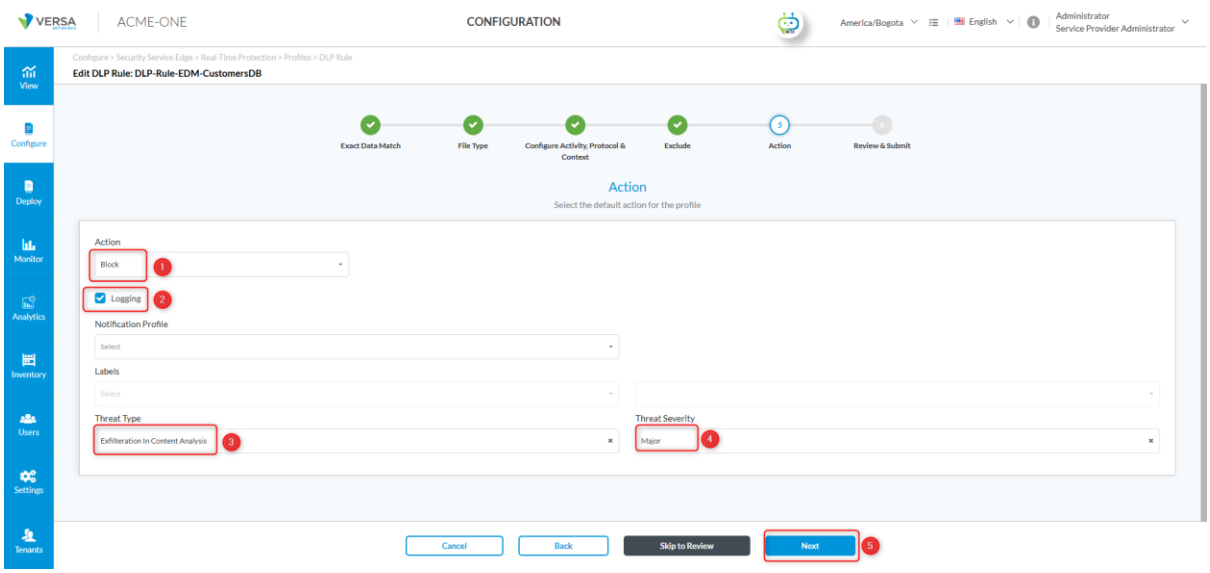


Exclude: Specify the file name(s) that should be excluded from DLP inspection. In our case there is no need to exclude any files so we can leave this field blank and click **Next**.

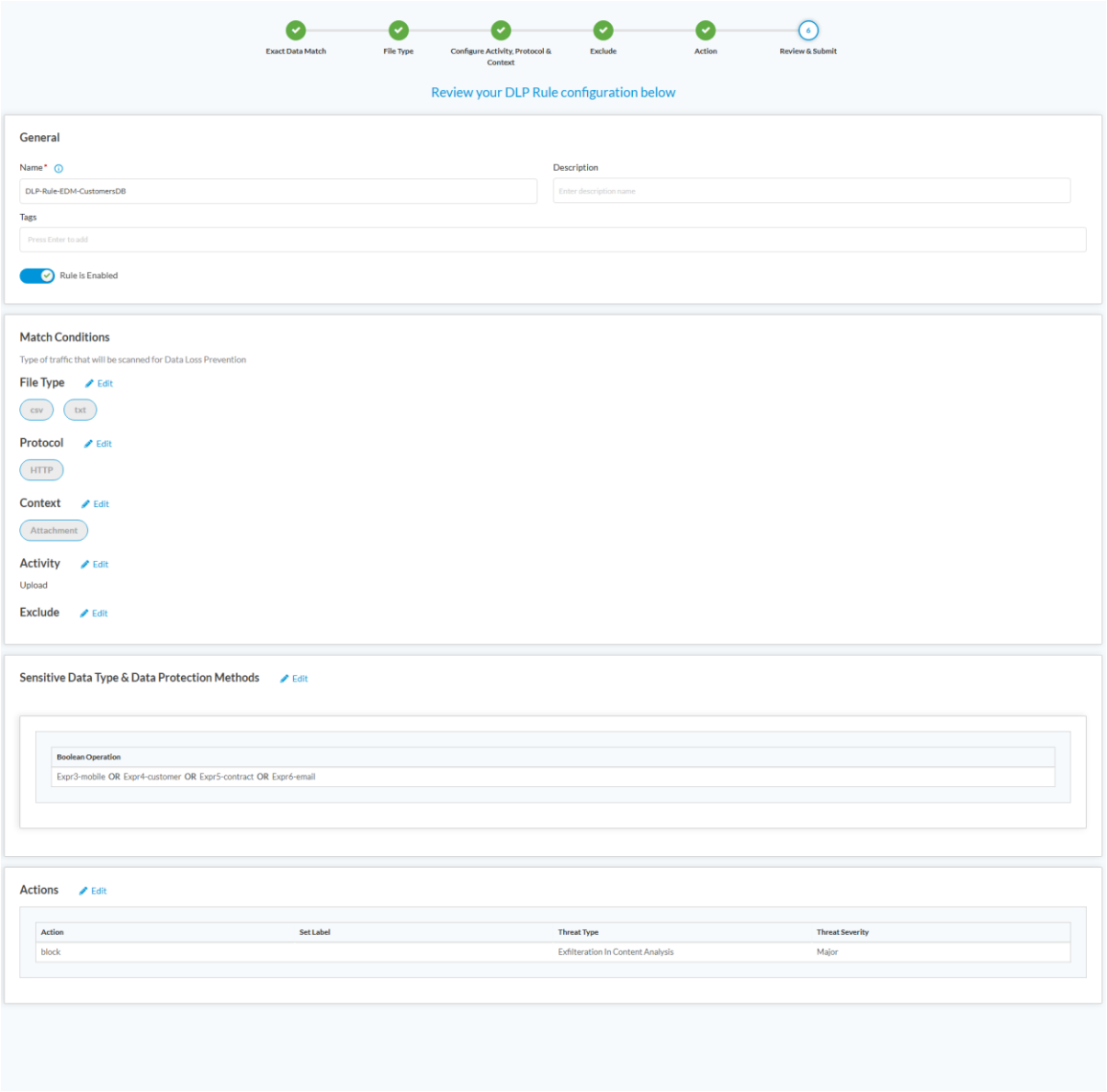
Action: Define the action to be executed when the rule is triggered. Several options are available, including:

- Allow
- Alert
- Block
- Reject

In our case, we will select **Block**. For more information on the different actions, refer to **Appendix B: *DLP Rule Actions*.**



Review & Submit: Verify that your rule matches the example shown in the image below, then click **Save**.

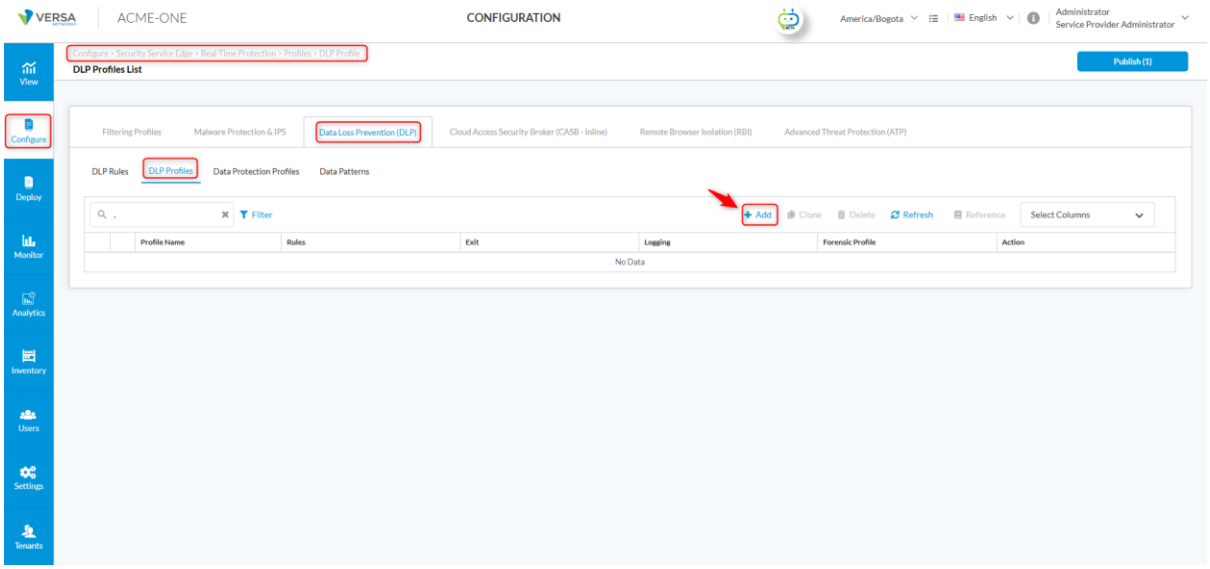


Create the DLP Profile:

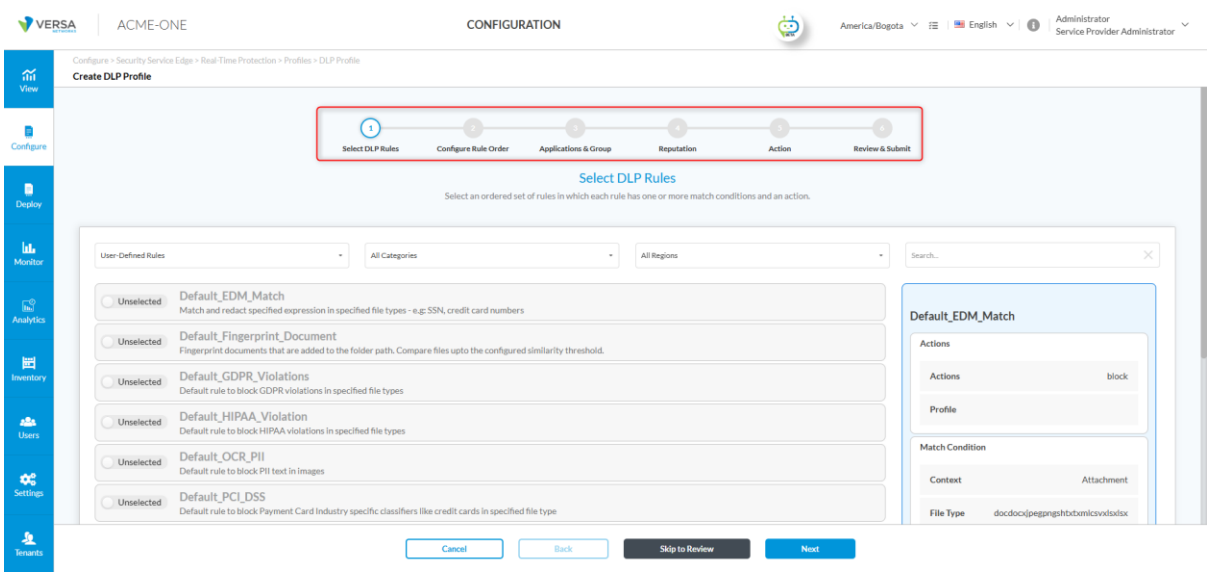
Navigate to

Configure > Security Service Edge > Real-Time Protection > Profiles > DLP Profile.

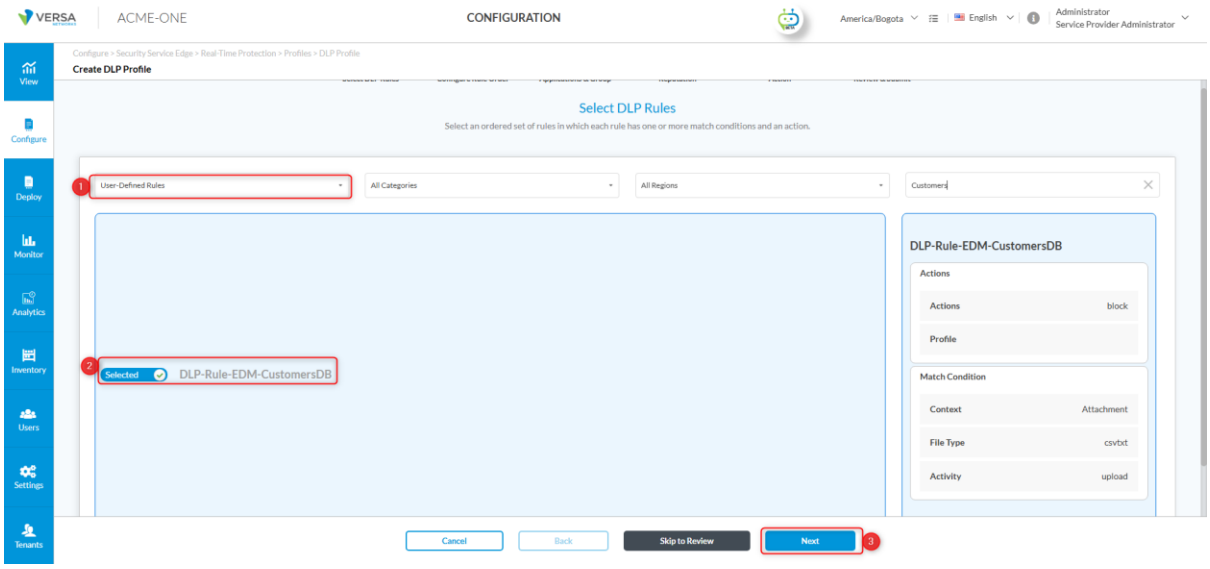
Click ***+ Add***, as shown in the image below.



Then, complete the six configuration steps shown in the following image.



Select DLP Rules: In the **User Defined Rules** section, search for the rule you created earlier, select it, and click **Next**. It should look like the example shown in the image below.



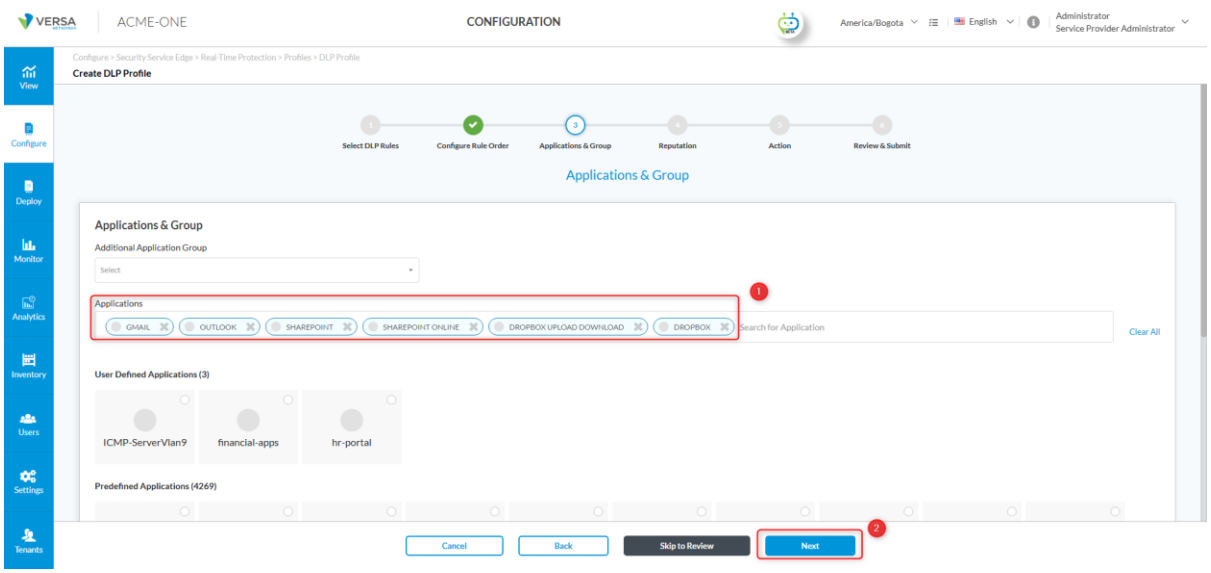
Configure Rule Order: Order does not apply for this use case since we have selected only a single rule, so click **Next**.

Applications & Group: In the **Applications** search field, search for each application to which the DLP profile will be applied. In our case, select **Gmail**, **Outlook**, **SharePoint** and **Dropbox** then click **Next**, as shown in the image below.

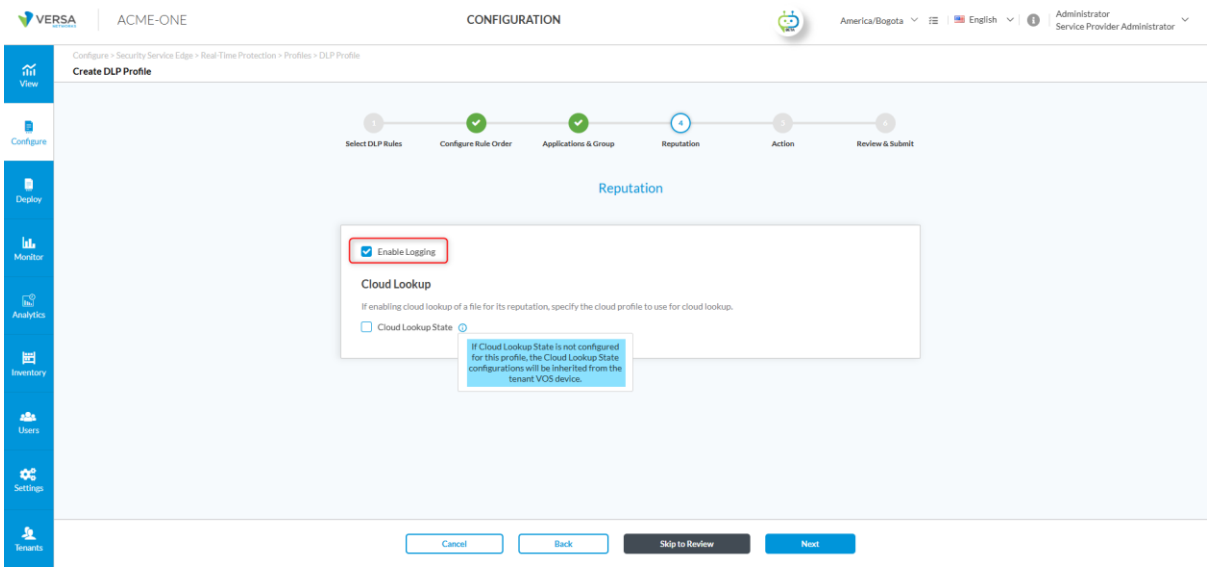
Notes:

*- In cases where not all dependent applications are known, adding the generic applications **HTTPS** or **HTTP** to the DLP profile may help. However, this approach is not technically guaranteed to work and could impact unrelated traffic. Therefore, rules applied in real-time protection should remain as specific as possible.*

*- In some cases, you may also need to add dependent applications when dealing with SaaS apps. For example, Gmail relies on additional services such as **gstatic.com** to load resources like icons, scripts, or image previews (e.g., when sending or viewing image attachments). Without allowing these dependencies, the SaaS application may not function correctly.*



Reputation: Select the **Enable Logging** option to store website reputation events, as shown in the image below. **Cloud Lookup** is optional; for more information, you can visit the following link: [How to Configure Cloud Lookup](#).



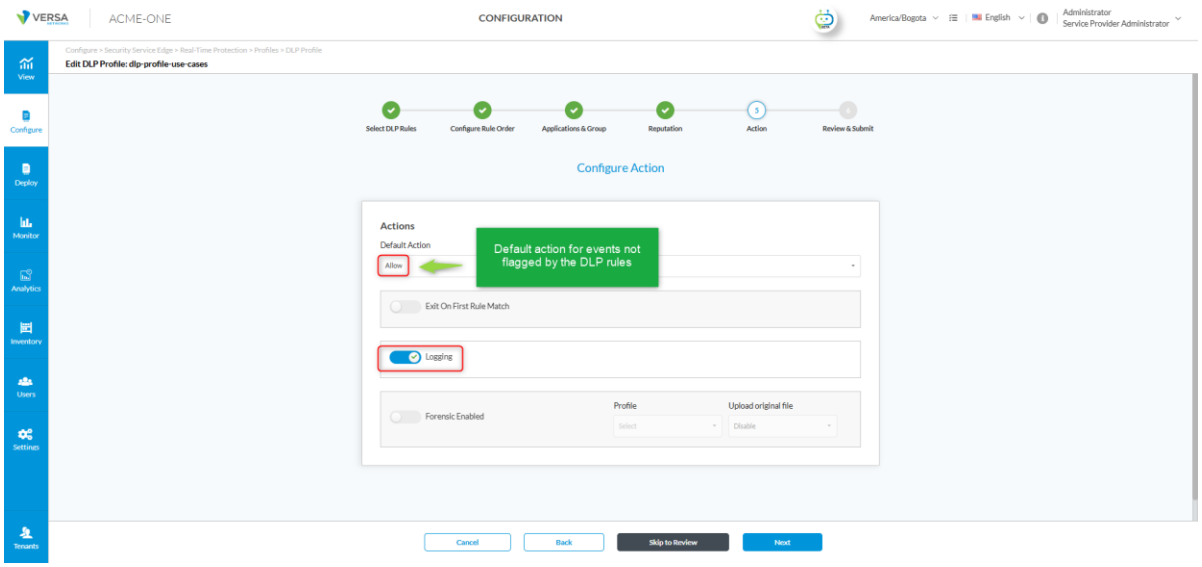
Action:

Actions: Set the default action set to **Allow**. The default action is applied if none of the scanned data matches a rule.

Logging: Click on the toggle button to enable logging.

Exit on First Rule Match: Leave the default action set to **disabled**.

Note: if multiple DLP rules are configured, this option should be disabled to ensure that all rules are applied to the same session.



Review & Submit: Assign a name, then review the configuration and click the **Save** button.

Step 2: Create the TLS decryption rule for the cloud applications we will test (Gmail, Outlook, SharePoint and Dropbox).

To ensure that payloads can be inspected and DLP policies applied, a TLS decryption rule must exist for the cloud applications being tested (e.g., Gmail, Outlook, SharePoint and Dropbox).

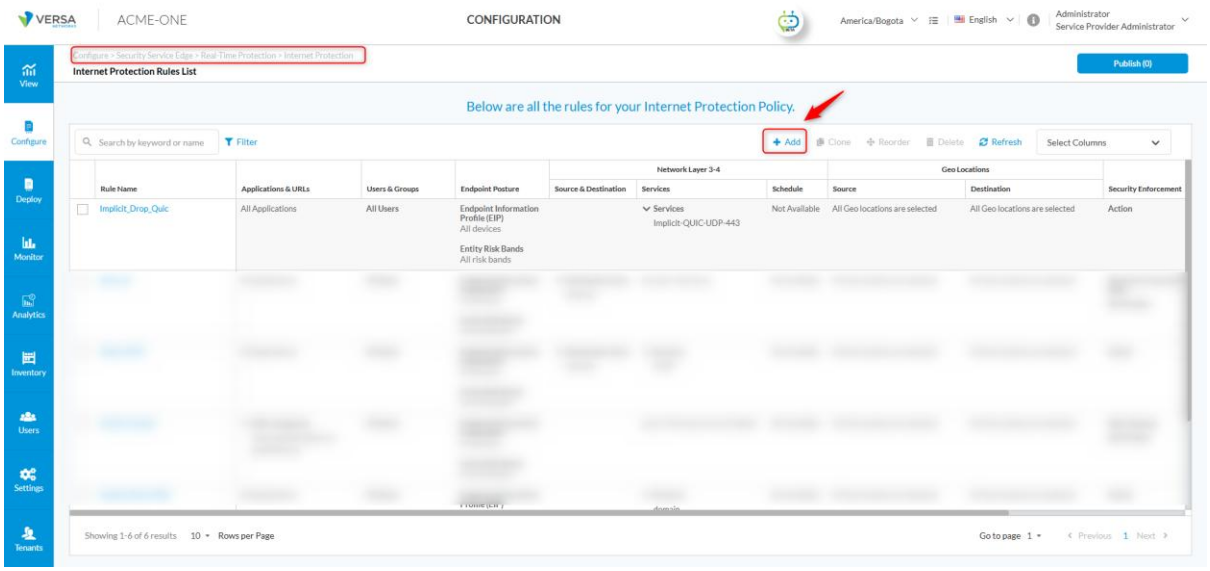
If you need the detailed step-by-step configuration for creating this rule, refer to **Appendix C: TLS Decryption Rule Configuration**.

Step 3. Create the real-time protection rule using the DLP profile on the cloud apps defined earlier.

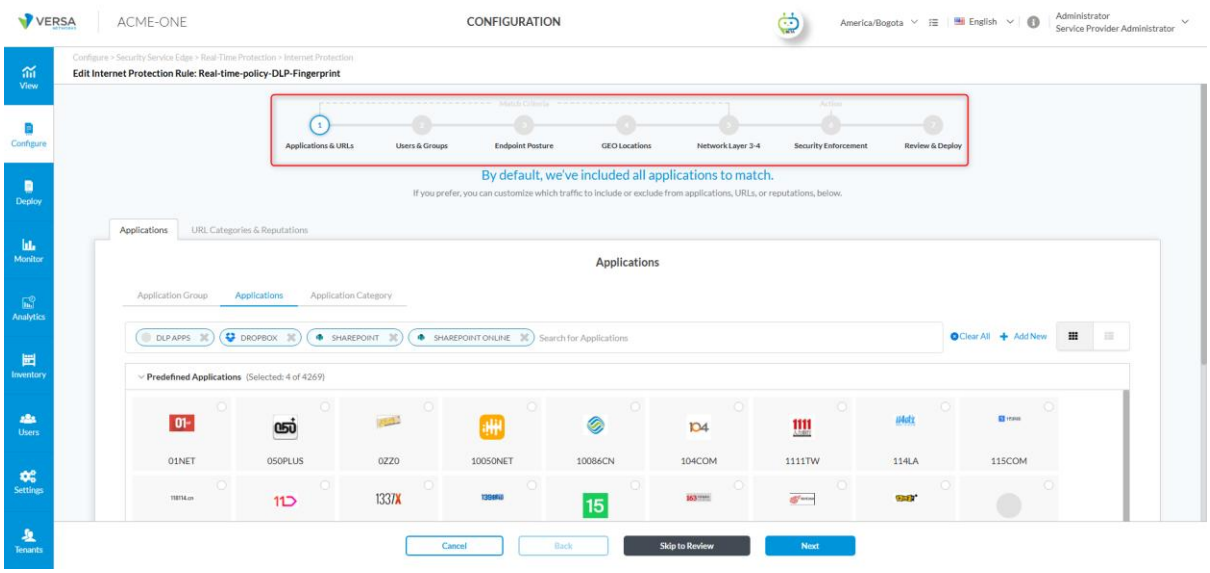
Navigate to

Configure > Security Service Edge > Real-Time Protection > Internet Protection.

Click + Add, as shown in the image below.



Then, complete the seven configuration steps shown in the following image.



Applications & URLs: Select the applications to which we will apply our DLP module. In our case, we choose Gmail, Outlook, SharePoint and Dropbox.

Users & Groups: Select our test group and then click Next. In our case, it can be the (VIP) or (Finance) group coming from our LDAP-AD.

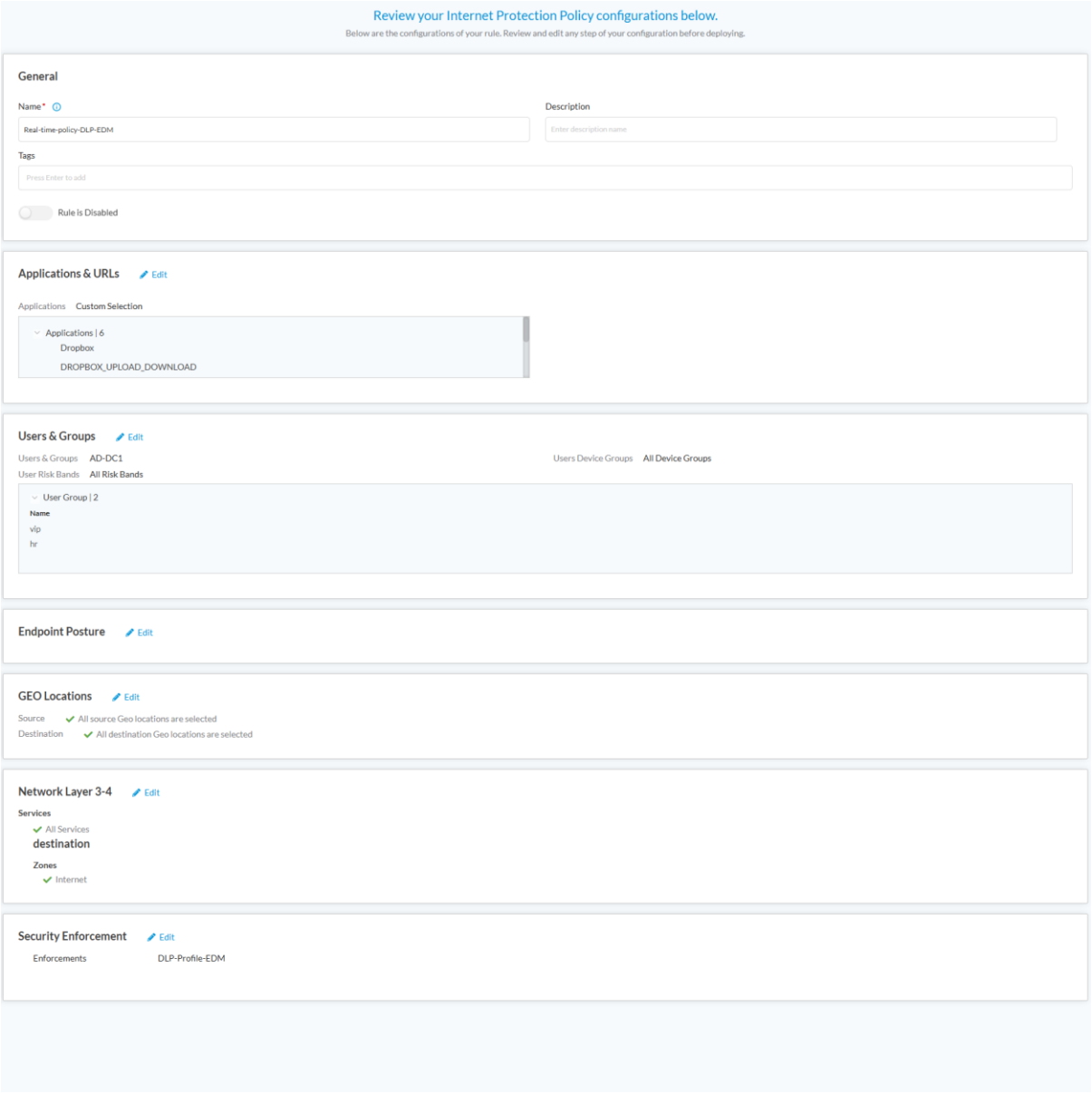
Endpoint Posture: You can apply Endpoint Information Profiles and Entity Risk Bands; however, in our case, leave the default settings to apply none and click **Next**.

Geolocation: You can filter by Source or Destination Geo Location. In our case, we leave the default setting to **All** and click **Next**.

Network Layer 3-4: You can filter by services (Layer 4) such as HTTP, HTTPS, DNS, ICMP, etc. You can also filter by Source & Destination (Layer 3). However, leave the default values and click **Next**.

Security Enforcement: Click on the **Security Profiles** option, then select **Data Loss Prevention**. Toggle the switch to enable it, then choose the profile named **DLP-Profile-EDM**, which is the one we created. Click **Next**.

Review & Validate: Review the configuration (see image below), click **Save**, and select **add this rule at the top of the rule list**.



Finally, publish the changes applied in Concerto and proceed with the verifications.

Step 4. Perform tests and validate the behaviour.

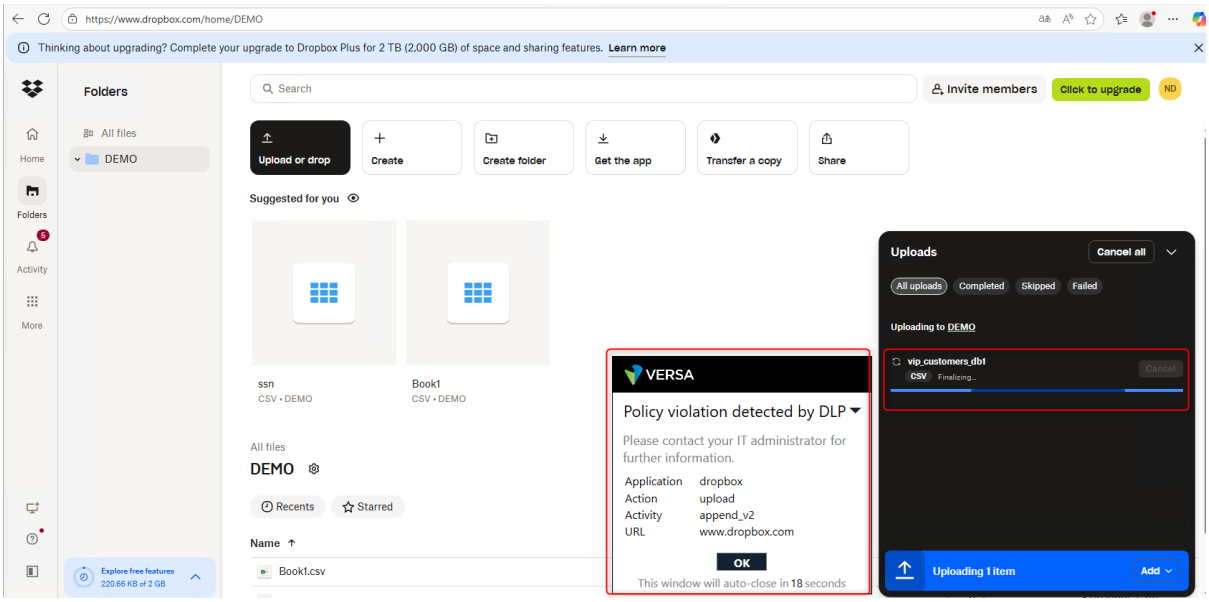
To perform the tests, we only need to upload a test file from Gmail, Outlook, SharePoint, or Dropbox that contains partial information from the original database. For simplicity, we are going to use the same file we used for the database (*vip_customers_db1.csv*). Below, you will see a portion of the data contained in the CSV.

vip_customers_db1.csv

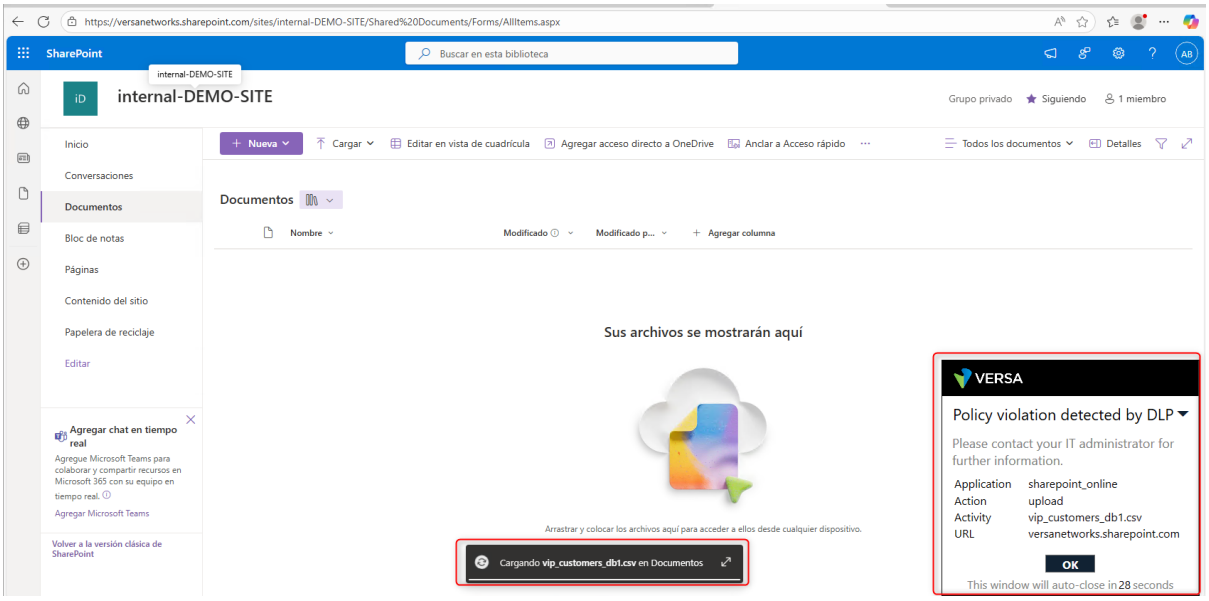
firstname,lastname,gender,mobile,customer,contract,email
Ava,Jackson,Male,3140474786,CUST_000001,CTR_1001_0001,ava.jackson@initech.com
Ava,Harris,Female,7359869480,CUST_000002,CTR_1001_0002,ava.harris@acmeenergy.com
Lucas,Lee,Female,9411336152,CUST_000003,CTR_1001_0003,lucas.lee@hooli.com
Olivia,Lee,Male,7110163088,CUST_000004,CTR_1001_0004,olivia.lee@wayneenterprises.com
Daniel,Johnson,Female,2647706560,CUST_000005,CTR_1001_0005,daniel.johnson@wayneenterprises.com
Emma,Taylor,Male,5041660904,CUST_000006,CTR_1001_0006,emma.taylor@umbrella-corp.com
Daniel,Martinez,Male,3286054734,CUST_000007,CTR_1001_0007,daniel.martinez@initech.com
Ethan,Harris,Male,4032561166,CUST_000008,CTR_1001_0008,ethan.harris@aurora-services.com
Daniel,Diaz,Male,4129341454,CUST_000009,CTR_1001_0009,daniel.diaz@globex.com
Emma,Allen,Female,4604552725,CUST_000010,CTR_1001_0010,emma.allen@cascadeinc.com

Now, Upload from Gmail, Outlook, SharePoint or Dropbox the file created with the data mentioned before, which should be blocked because the **Block** action was selected. See the images below.

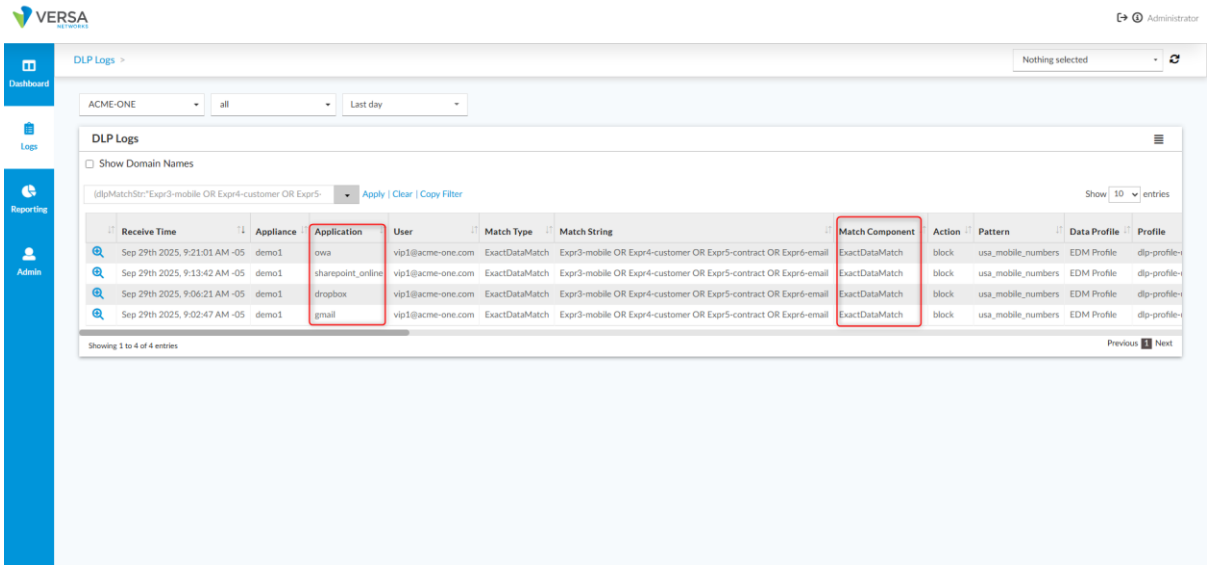
Dropbox test



SharePoint test



When checking the logs in **Concerto** > **Analytics** > **DLP Logs**, you should see something similar to the images below.



Use Case 4: Collaboration Chat Monitoring with DLP for Bad Words

This case demonstrates how **ACME-ONE** leverages **DLP profiles in Versa Networks** to detect and flag inappropriate or non-compliant language in collaboration tools, specifically **Slack** chats. The objective is to monitor communication channels for the use of prohibited terms, ensuring compliance with corporate policies and maintaining a professional environment.

The **Collaboration and HR departments** at ACME-ONE are responsible for monitoring employee chat activity for the following categories of concern:

- Use of offensive, discriminatory, or profane language (bad words).
- Custom-defined terms that reflect ACME-ONE's internal compliance policies (e.g., code words, sensitive project names, or restricted topics).

Versa's DLP engine allows combining **predefined bad words dictionaries** with **custom keyword lists**, ensuring that both general profanity and organization-specific terms are detected in Slack chat messages.

To reduce the risk of misconduct or policy violations in internal collaboration, Versa's DLP engine is configured to **inspect chat content from Slack (web and desktop app)** and apply DLP actions when matches are detected.

Using Versa's integrated DLP engine, ACME-ONE defines a DLP policy named **"Bad Words and Inappropriate Language Monitoring"** with the following conditions:

Policy Name	Conditions	Details
Bad Words and Inappropriate Language Monitoring	Match on predefined Bad Words dictionary **OR** custom keyword list	1) Enable Versa's predefined dictionary for profanity/offensive language. 2) Create a custom keyword list with terms specific to ACME-ONE's compliance rules (e.g., project code names, restricted slang). 3) Apply the policy to outbound and internal chat traffic within **Slack**. 4) Actions include Alerting, Logging, and optional Blocking.

Configuration steps

The DLP configuration consists of the following steps, which are described in detail below:

1. Create DLP objects
    - Create a **DLP Pattern for custom Badwords.**
    - Create a **DLP Rule** (conditions that trigger DLP checks).
    - Create and assign a **DLP Profile / Policy** (the policy that ties the data profile and rules to enforcement actions).
2. **Create TLS decryption rule** for the cloud apps you will test (**Slack**).
3. **Create real-time protection rule** that applies the DLP profile to the cloud apps defined in Step 2.
4. **Perform tests and validate the behaviour.** Execute test cases, verify detection and enforcement, and record results.

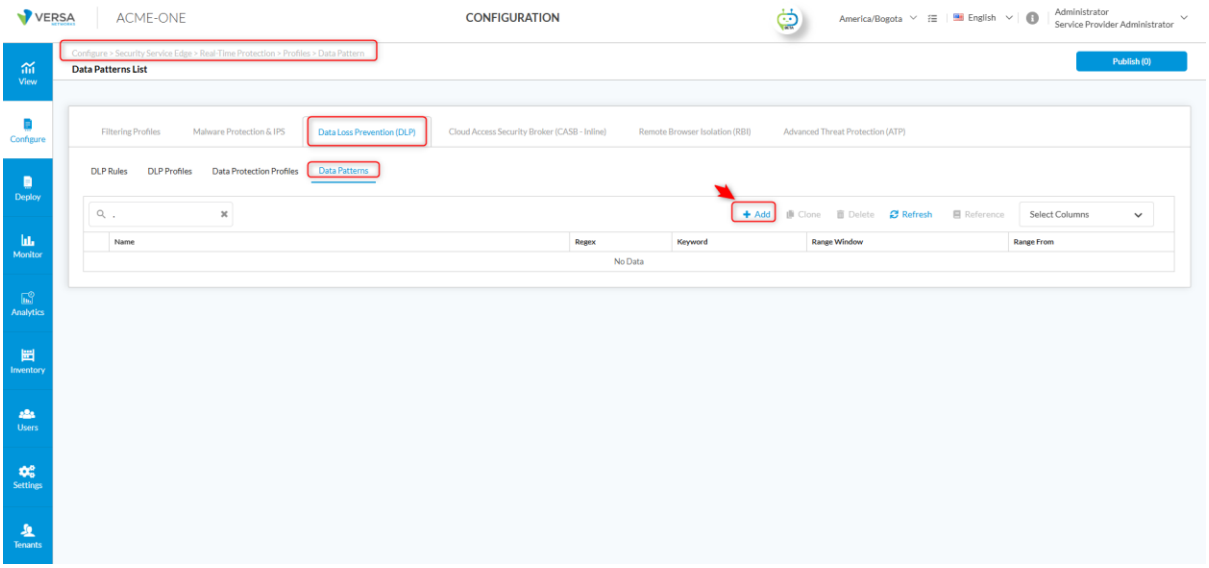
Step 1: Create DLP objects

For this use case (Content Analysis), we will use the predefined Bad Words data pattern and create an additional custom pattern if needed. These patterns will be referenced in the DLP rule, where a Boolean expression (e.g., *Predefined_BadWords OR Custom_BadWords*) defines the match condition.

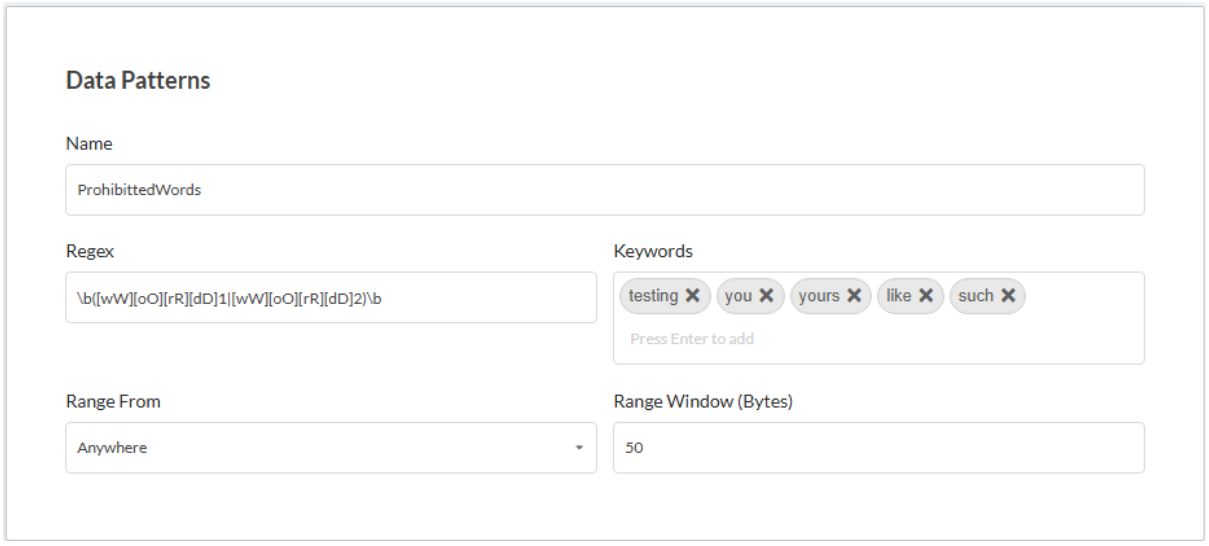
Creating a Data Pattern for Bad Words

Navigate to

Configure > Security Service Edge > Real-Time Protection > Profiles > Data Patterns. Click + Add, as shown in the image below.



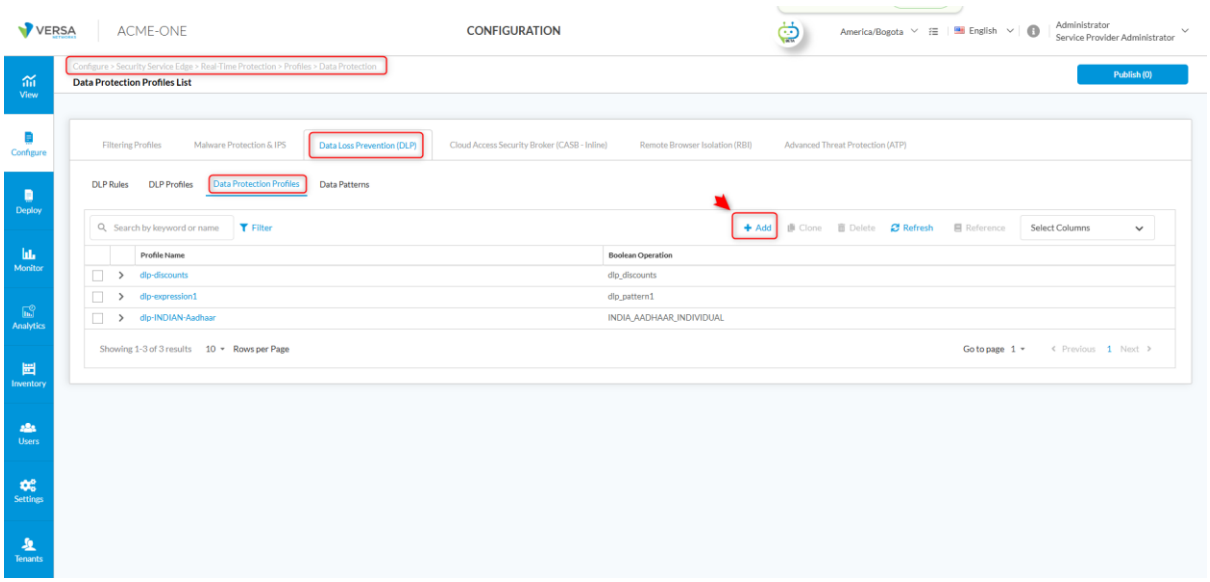
Next, we define the values with a simple regex for Bad Words, making sure the keywords are included and related to the content, just as shown in the image below. Finally, click on Save.



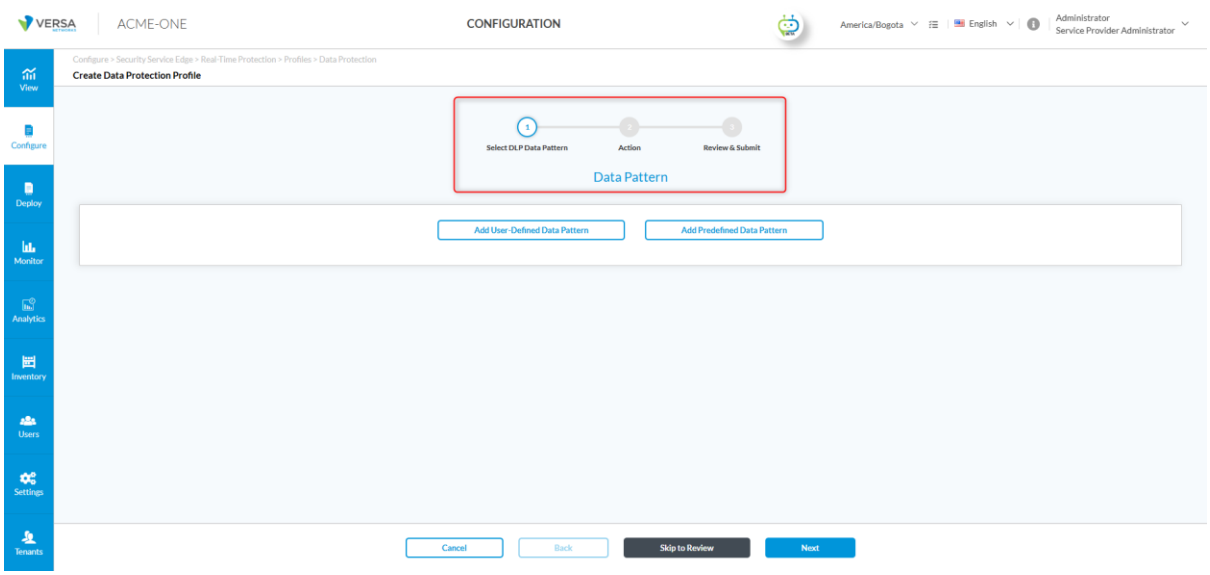
Creating a Data Protection Profile

Navigate to

Configure > Security Service Edge > Real-Time Protection > Profiles > Data Protection. Click + Add, as shown in the image below.



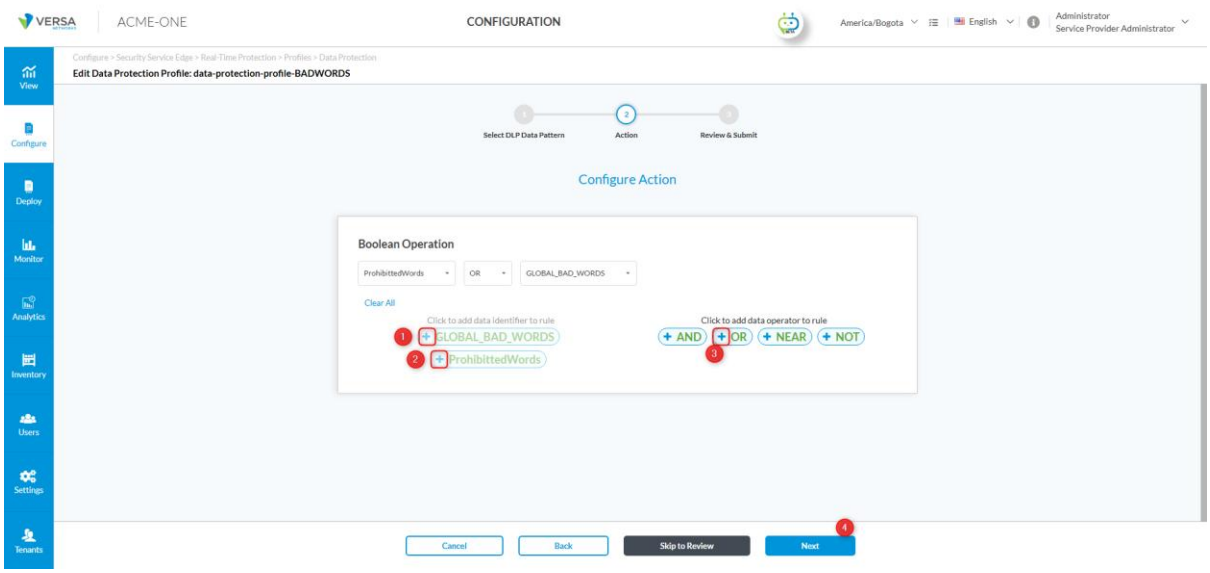
Next, complete the three configuration steps shown in the image below.



Select DLP Data Pattern: Select Add Predefined Data Pattern and search for the one you need. In this example, enable **GLOBAL_BAD_WORDS**, then click Save and then click on User-Defined Data Pattern and enable **ProhibittedWords (**created in the last step) Next click on Save

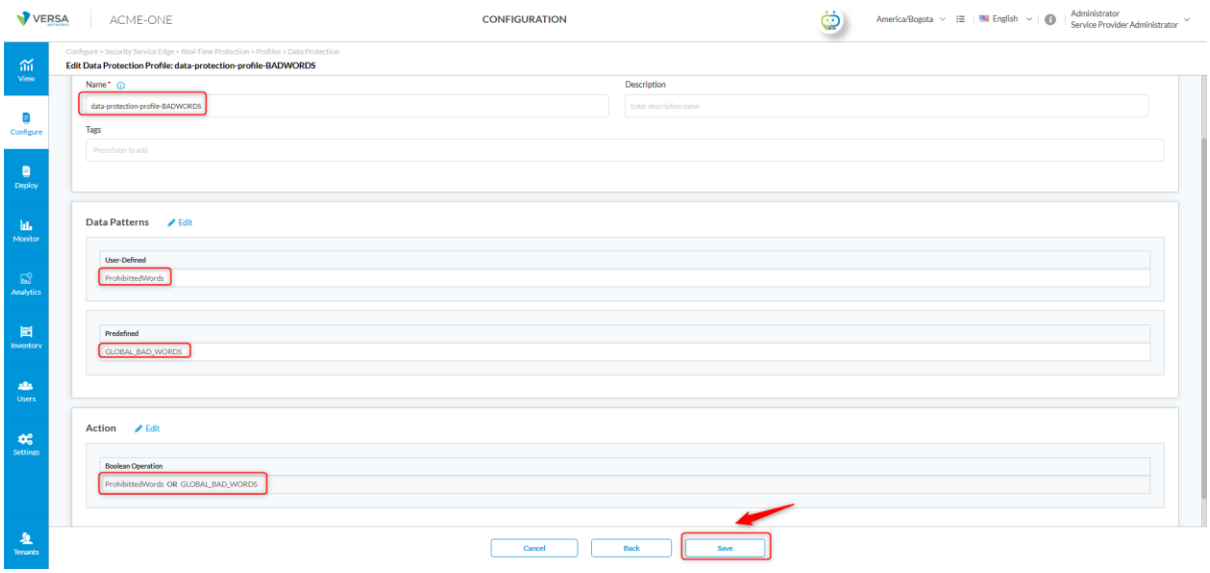
Action: Click the + icon next to the data identifier *GLOBAL_BAD_WORDS* to add it to your Boolean expression. Then, insert the OR operator and click the + icon again to add *ProhibittedWords*. See the image below.

See the image below.



Once the data identifier has been added, click Next to continue.

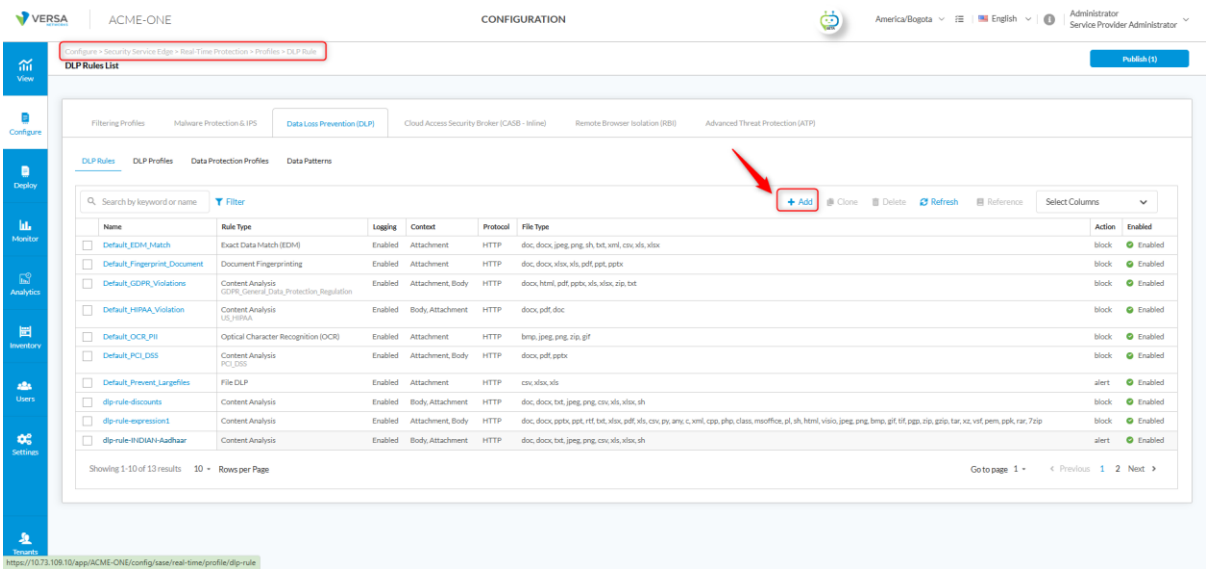
Review & Submit: Assign a name to your Data Protection profile and click **Save**.



Create DLP Rule:

Navigate to **Configure > Security Service Edge > Real-Time Protection > Profiles > DLP Rule**.

Click **+ Add**, as shown in the image below.



You will now see a menu to select the type of DLP rule. In our case, select **Content Analysis**. For details on the different types of DLP rules, refer to **Appendix A *(DLP Rule Types)***.

After selecting **Content Analysis**, six steps will appear. We will describe them below:

Rule Type: Content Analysis

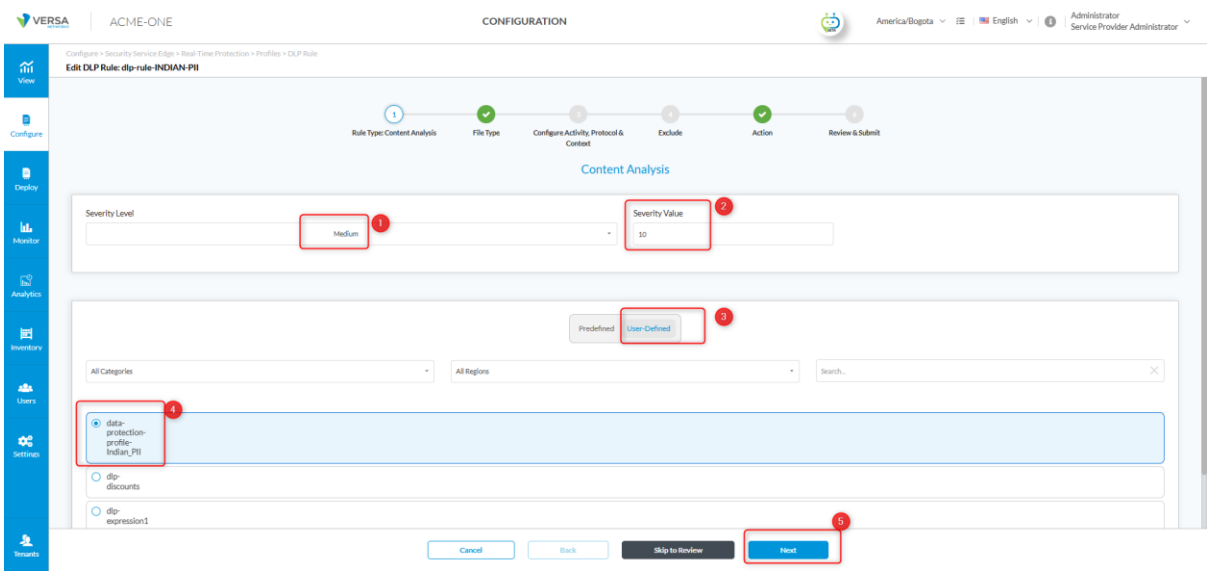
5. **Severity Level:** Select the severity assigned to the DLP event. Each level has a default match threshold: Low = 1, Medium = 10, High = 20, Critical = 30. For this example, choose **Medium**.

6. **Severity Value:** Define a custom number of occurrences required to trigger the rule. The counter starts from 0. For example, if you set the value to 10, the rule will trigger starting from the 11th DLP event. In this case, set the value to **10**.

7. **Predefined/User Defined:** Select **User Defined** and then choose the **Data Protection Profile** we created earlier, named data-protection-profile-AADHAAR.

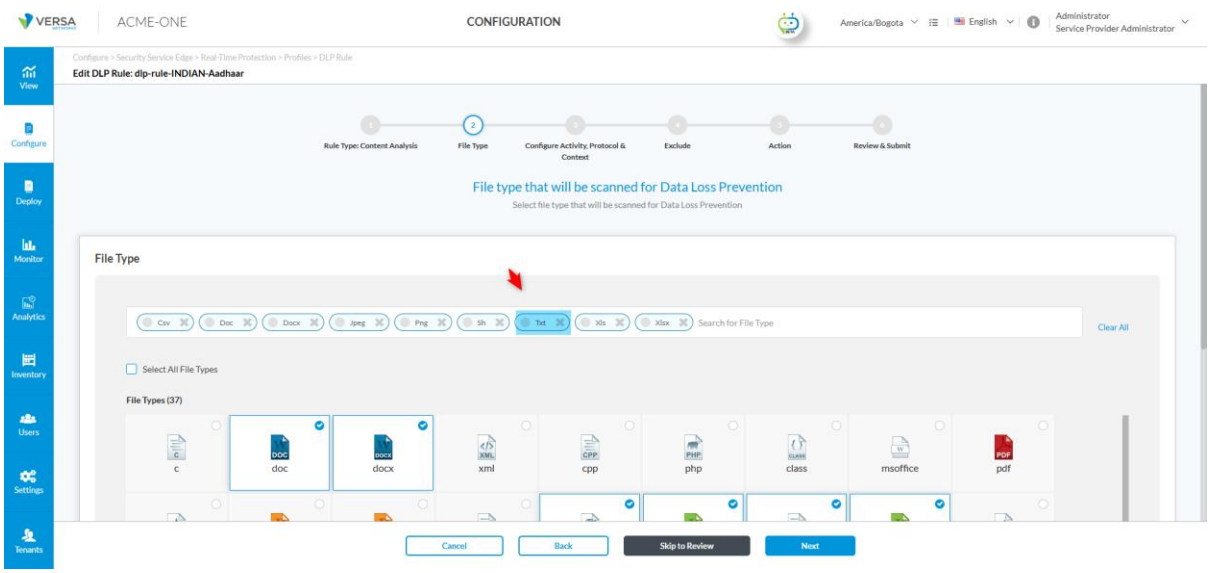
8. Click **Next** to continue.

Note: In DLP, the Severity Level defines the default number of matches required to trigger a rule (Low=1, Medium=10, High=20, Critical=30). If a custom Severity Value is set, it overrides the default threshold (e.g., High=20 but Value=5 → triggers after 5 occurrences).

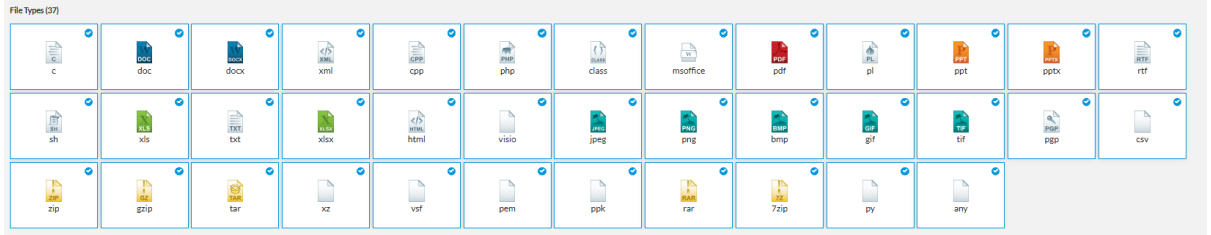


File Type: Select the file types you want to inspect. For this use case select: **.txt**, .doc, .docx, .csv, etc.

Click on **Next** to continue.



Note: In the image below, you will see the file types supported for DLP.

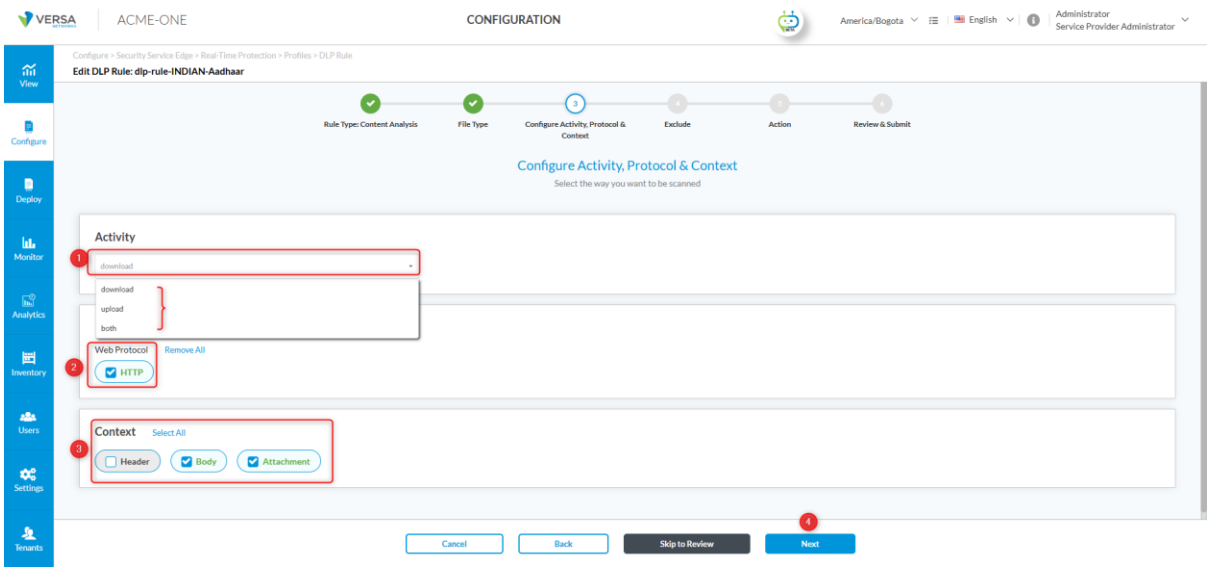


Configure Activity, Protocol & Context:

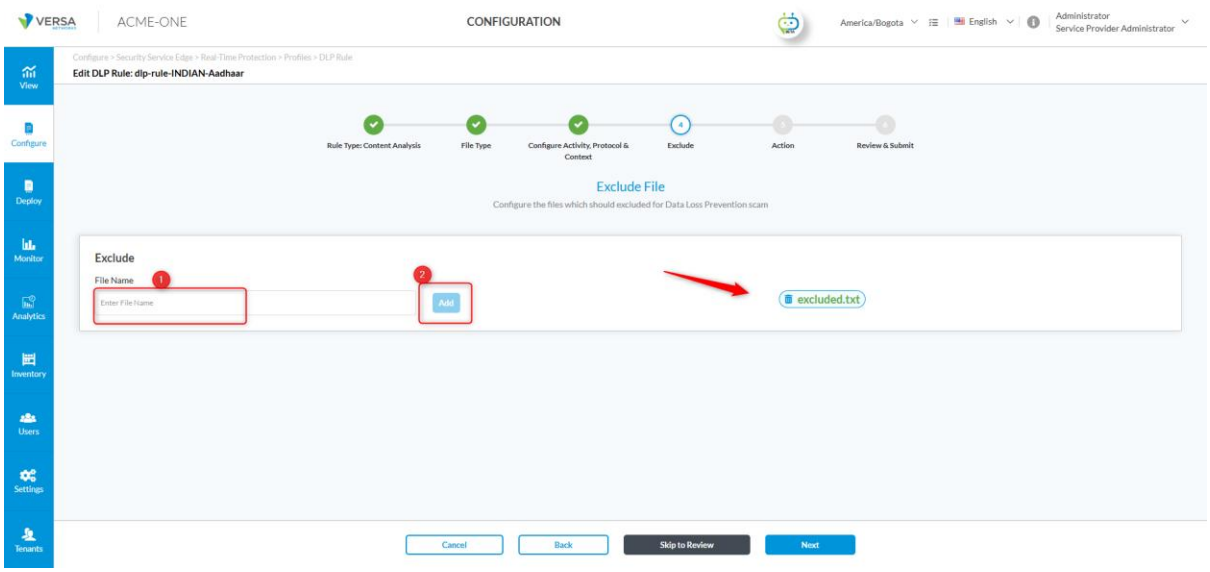
4. **Activity:** Select the activity to which the DLP module will be applied. In our case, select **Upload**.

5. **Web Protocol:** Select HTTP.

6. **Context:** Defines which part of the packet or message will be inspected. For this example, select **Attachments** and **Body**.



Exclude: Specify the file name(s) that should be excluded from DLP inspection.

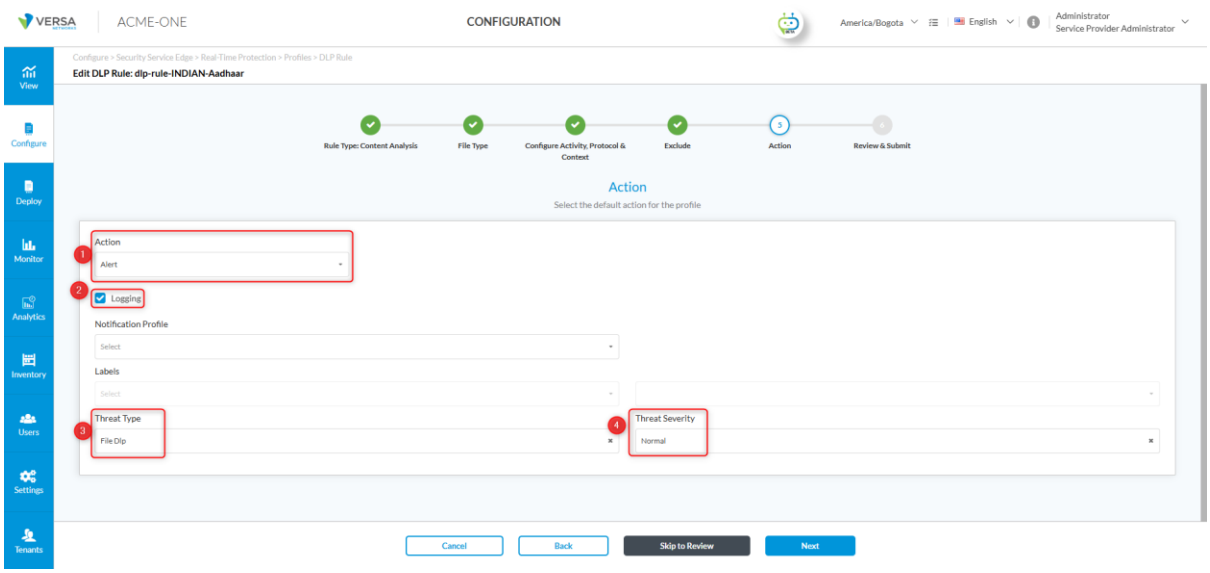


Action: Define the action to be executed when the rule is triggered. Several options are available, such as:

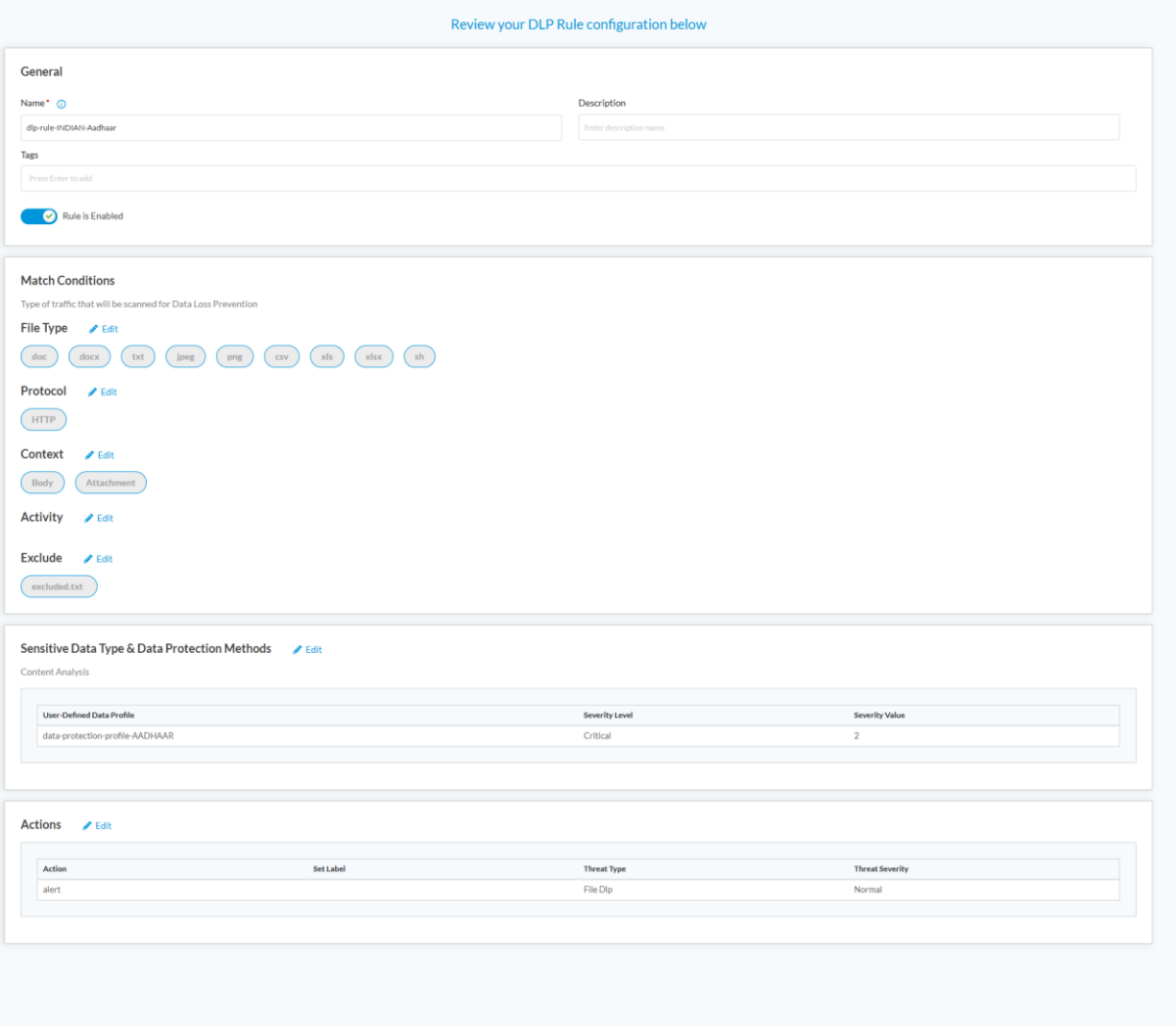
- Allow

- Alert
- Block
- Reject
- Reject

In our case, we will select **Alert** because we only want a log to be generated in the platform without blocking the user or displaying any pop-up messages. This option is commonly used when tuning DLP rules. For more information on the different actions, refer to **Appendix B: *DLP Rule Actions*.**



Review & Submit: Verify that your rule matches the example shown in the image below, then click **Save**.

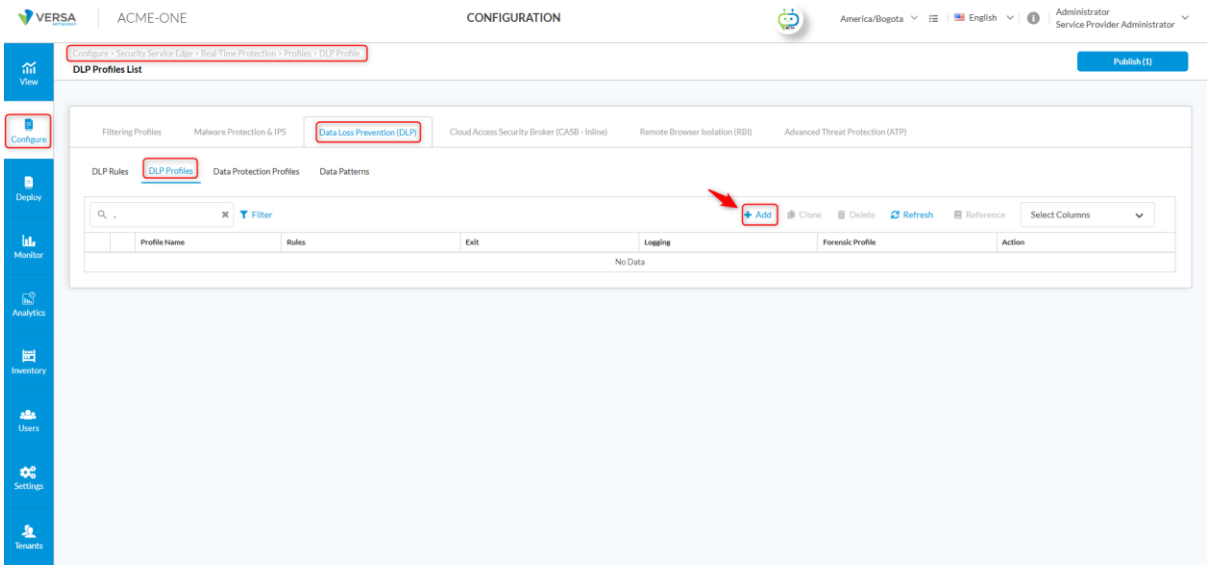


Create the DLP Profile:

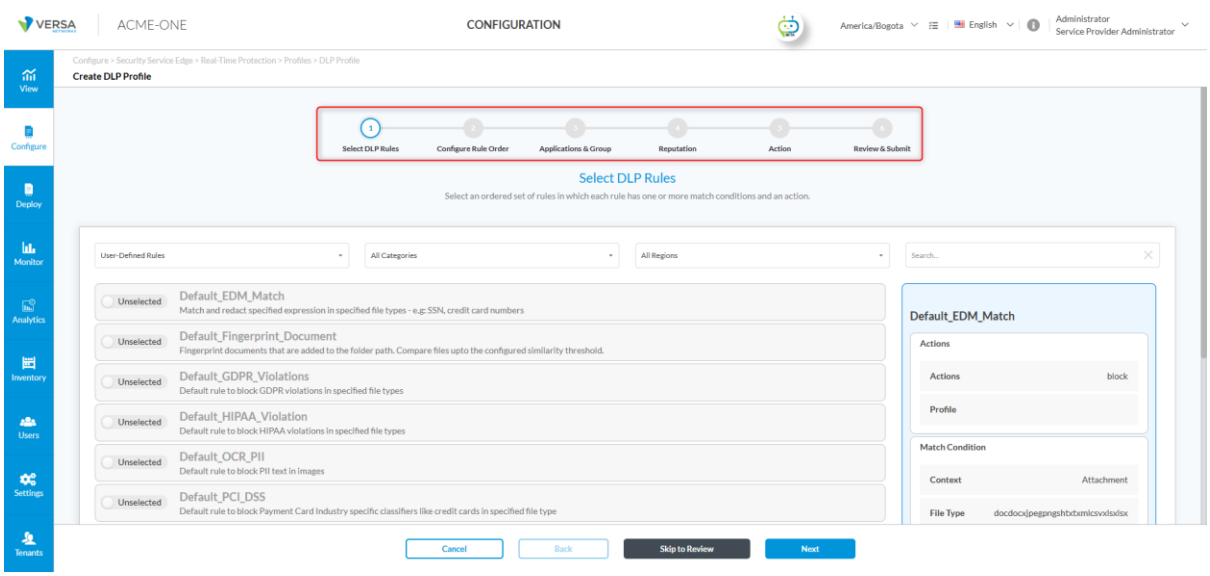
Navigate to

Configure > Security Service Edge > Real-Time Protection > Profiles > DLP Profile.

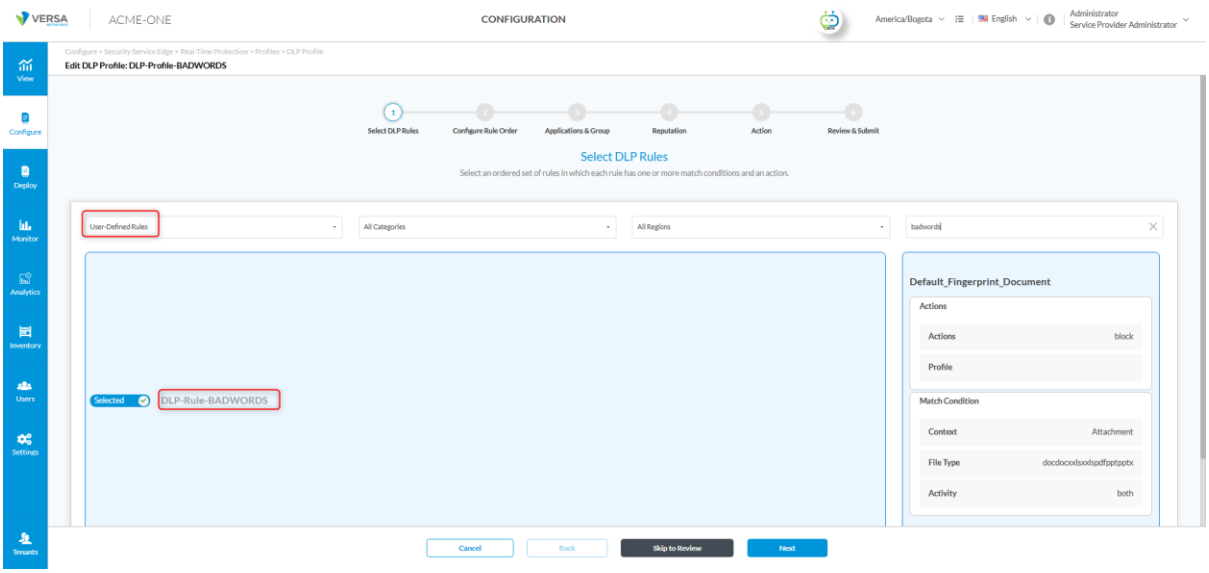
Click + Add, as shown in the image below.



Then, complete the six steps shown in the following image.



Select DLP Rules: In the **User Defined Rules** section, search for the rule you created earlier, select it, and click **Next**. It should look like the example shown in the image below.

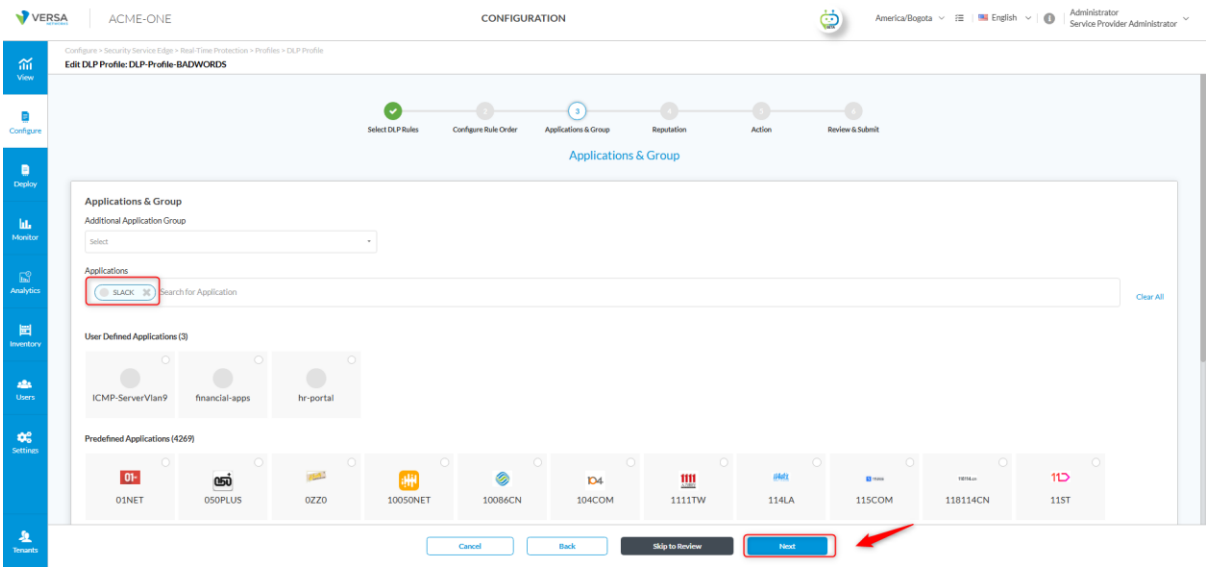


Configure Rule Order: Order does not apply since we have selected only a single rule.

Applications & Group: In the **Applications** search field, search for each application to which the DLP profile will be applied. In our case, select **Slack**, then click **Next**, as shown in the image below.

*Notes: - In cases where not all dependent applications are known, adding the generic applications **HTTPS** or **HTTP** to the DLP profile may help. However, this approach is not technically guaranteed to work and could impact unrelated traffic. Therefore, rules applied in real-time protection should remain as specific as possible.*

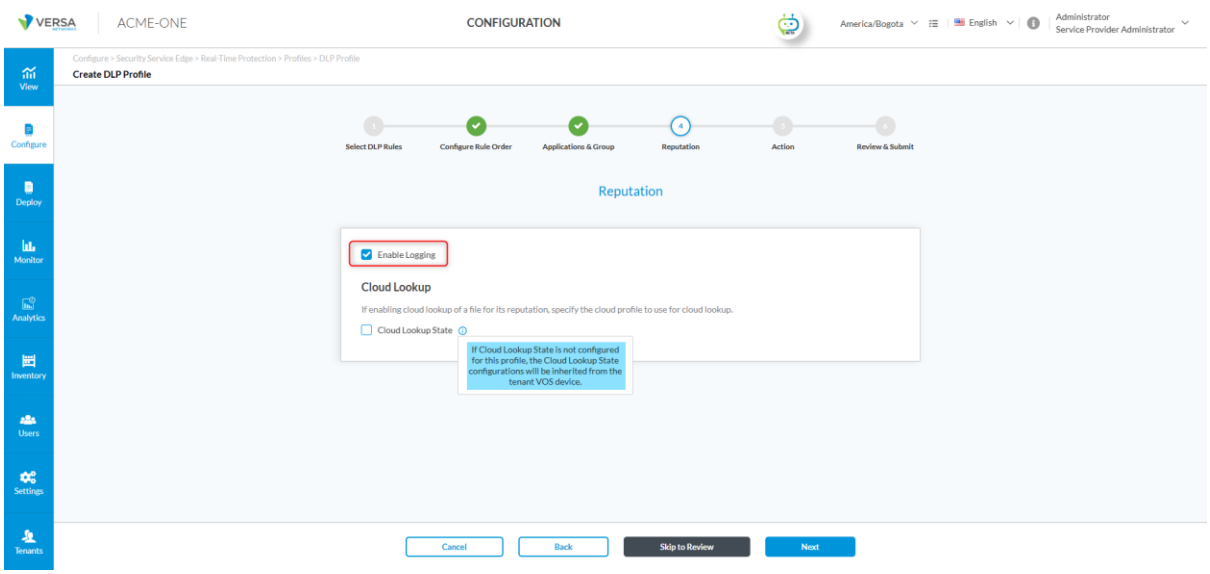
*- In some cases, you may also need to add dependent applications when dealing with SaaS apps. For example, Gmail relies on additional services such as **gstatic.com** to load resources like icons, scripts, or image previews (e.g., when sending or viewing image attachments). Without allowing these dependencies, the SaaS application may not function correctly.*



Reputation: In Versa, *Reputation* refers to a local URL database used to categorize websites and assign reputation scores for web filtering. This local database allows quick lookups for the most common and popular websites.

Additionally, Versa offers the option to enable **Cloud Lookup** to complement the local database.

For our use case, select the **Enable Logging** option to store website reputation events, as shown in the image below. **Cloud Lookup** is optional; for more information, you can visit the following link: [How to Configure Cloud Lookup].



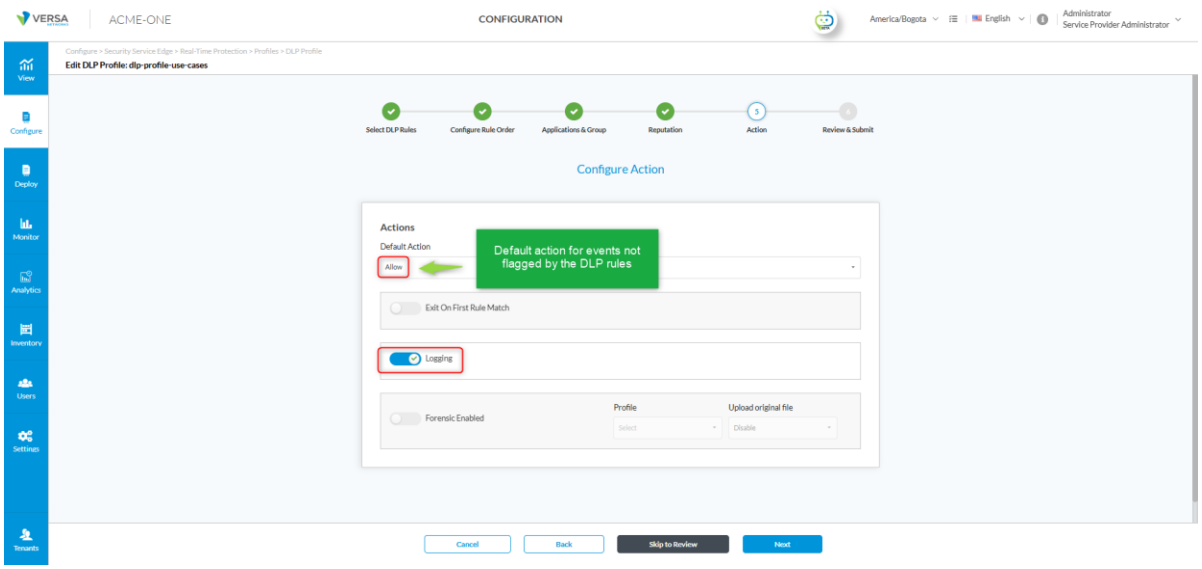
Action:

Actions: Set the default action set to **Allow**. The default action is applied if none of the scanned data matches a rule.

Logging: Click on the toggle button to enable logging.

Exit on First Rule Match: Leave the default action set to **disabled**.

Note: if multiple DLP rules are configured, this option should be disabled to ensure that all rules are applied to the same session.



Review & Submit: Assign a name, then review the configuration and click the **Save** button.

Step 2: Create the TLS decryption rule for the cloud applications we will test (Slack).

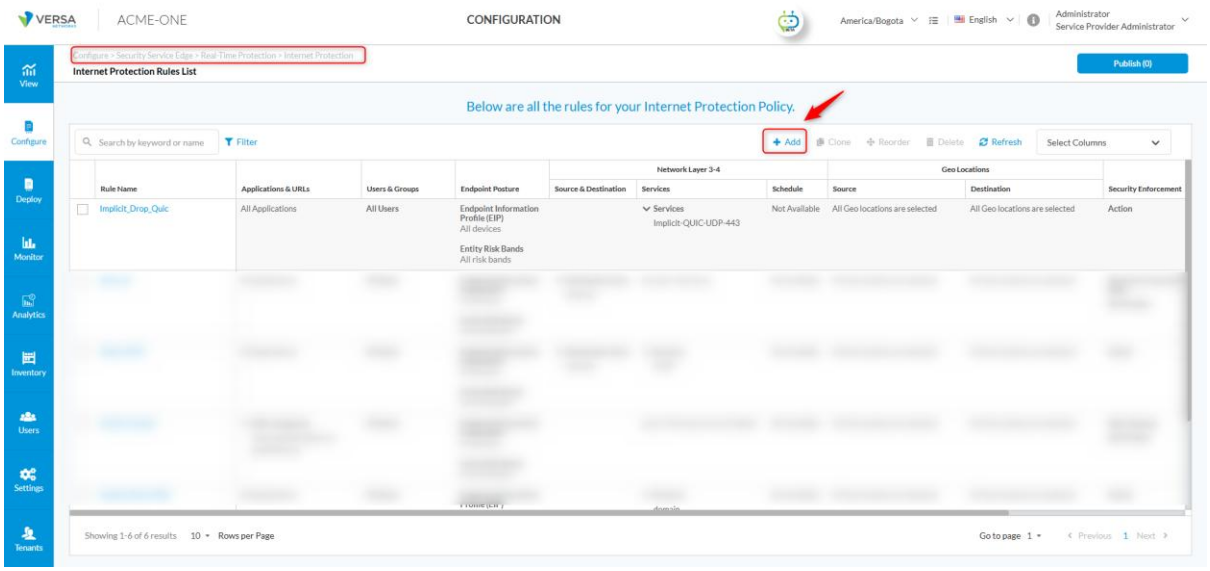
To ensure that payloads can be inspected and DLP policies applied, a TLS decryption rule must exist for the cloud applications being tested (e.g., Slack).

If you need the detailed step-by-step configuration for creating this rule, refer to **Appendix C: TLS Decryption Rule Configuration**.

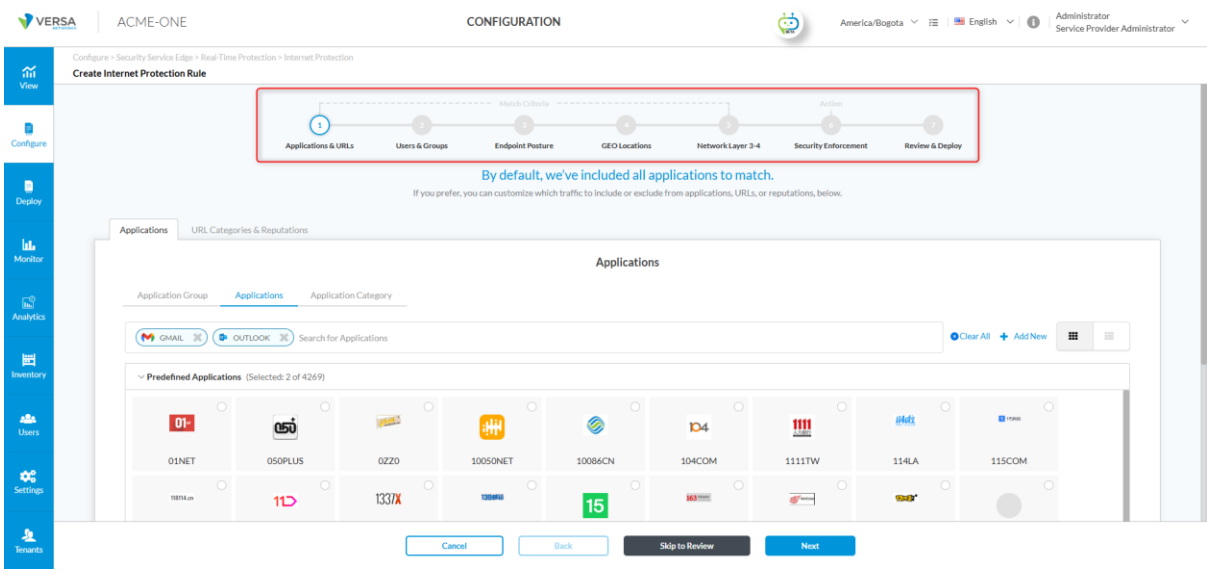
Step 3. Create the real-time protection rule using the DLP profile on the cloud apps defined earlier.

Navigate to ***Configure > Security Service Edge > Real-Time Protection > Internet Protection.***

Click + Add, as shown in the image below.



Then, complete the seven steps shown in the following image.



Applications & URLs: Select the applications to which we will apply our DLP module. In our case, we choose Slack.

Users & Groups: Select our test group and then click Next. In our case, it can be the (VIP and HR) group coming from our LDAP-AD.

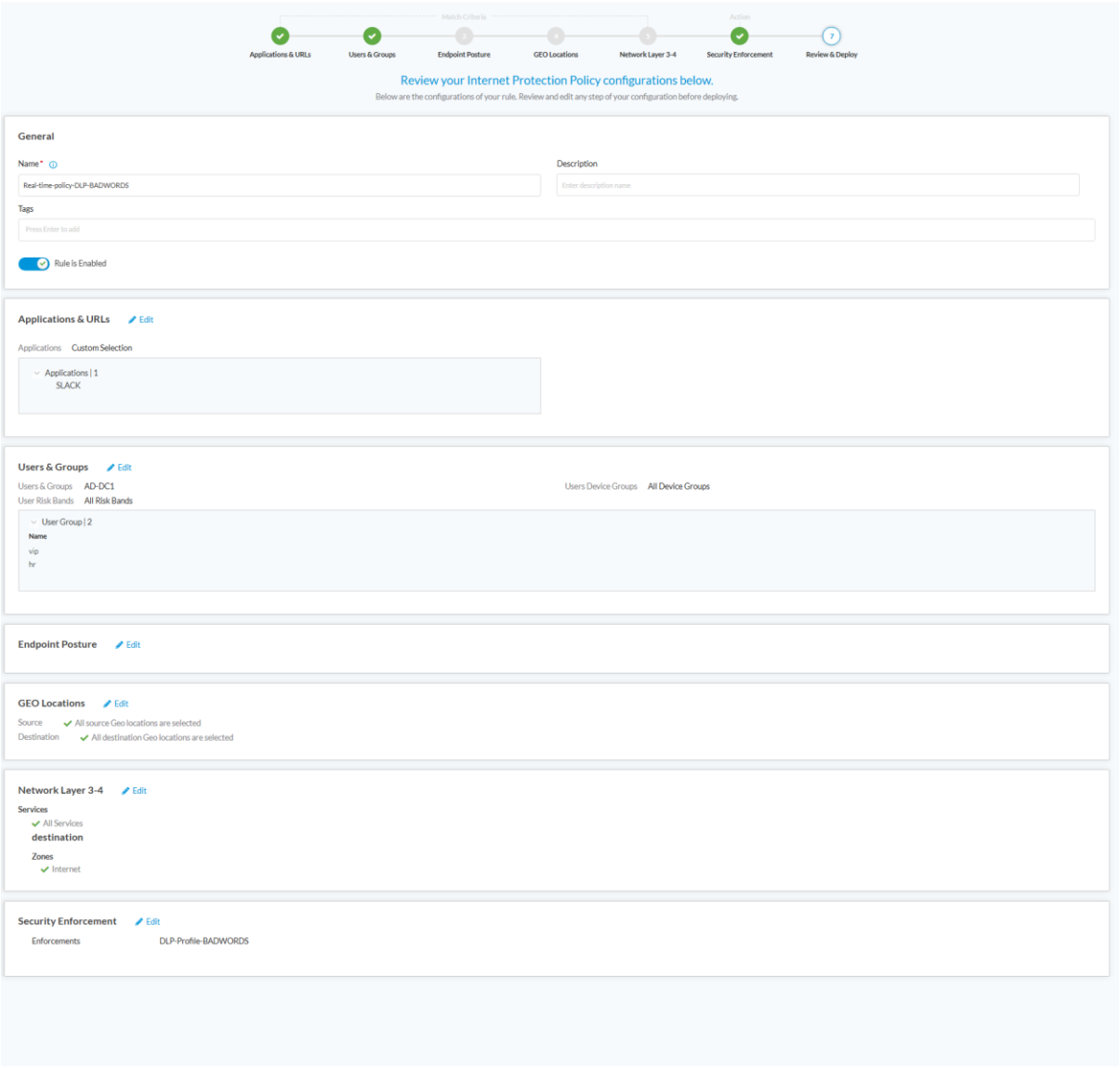
Endpoint Posture: You can apply Endpoint Information Profiles and Entity Risk Bands; however, in our case, leave the default settings to apply none and click **Next**.

Geolocation: You can filter by Source or Destination Geo Location. In our case, we leave the default setting to **All** and click **Next**.

Network Layer 3-4: You can filter by services (Layer 4) such as HTTP, HTTPS, DNS, ICMP, etc. You can also filter by Source & Destination (Layer 3). However, leave the default values and click **Next**.

Security Enforcement: Click on the **Security Profiles** option, then select **Data Loss Prevention**. Toggle the switch to enable it, then choose the profile named **DLP-Profile-BADWORDS**, which is the one we created. Click **Next**.

Review & Validate: Review the configuration (see image below), click **Save**, and select **add this rule at the top of the rule list**.

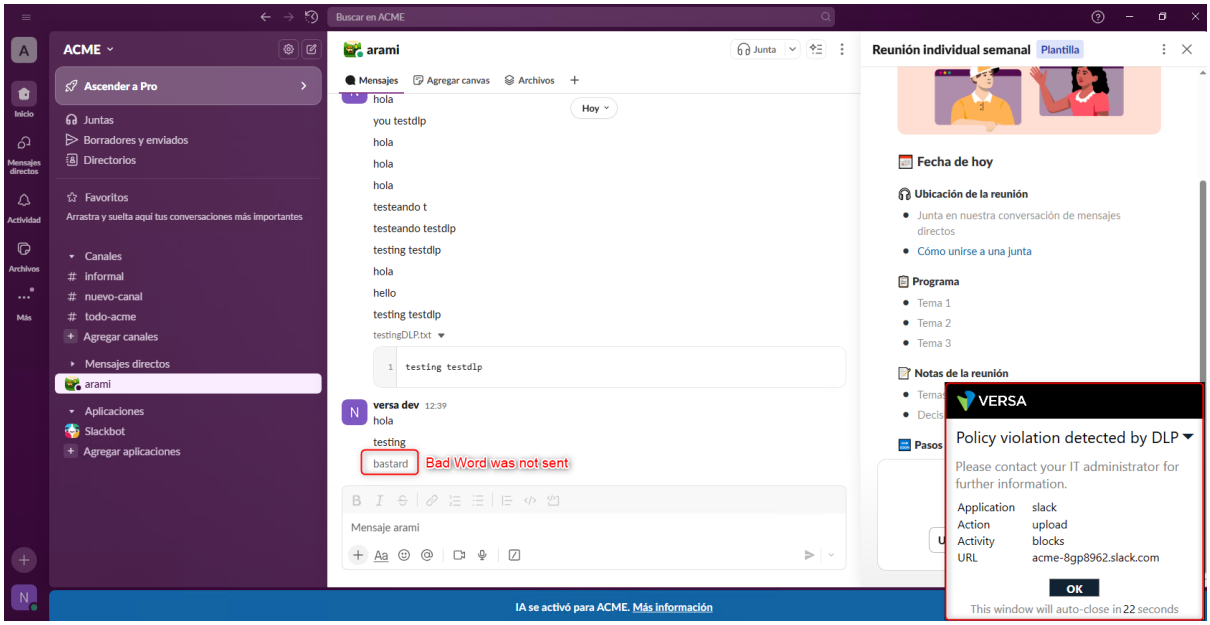


Finally, publish the changes applied in Concerto and proceed with the verifications.

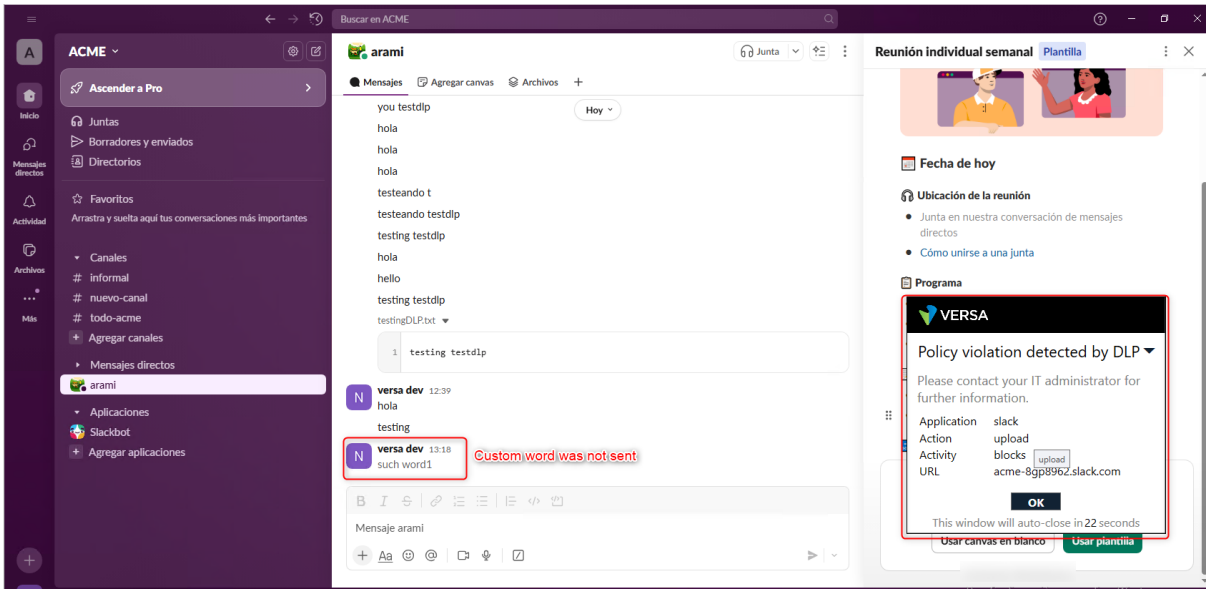
Step 4. Perform tests and validate the behaviour.

To perform the tests, we only need to send via Slack with the Versa SASE client enabled.

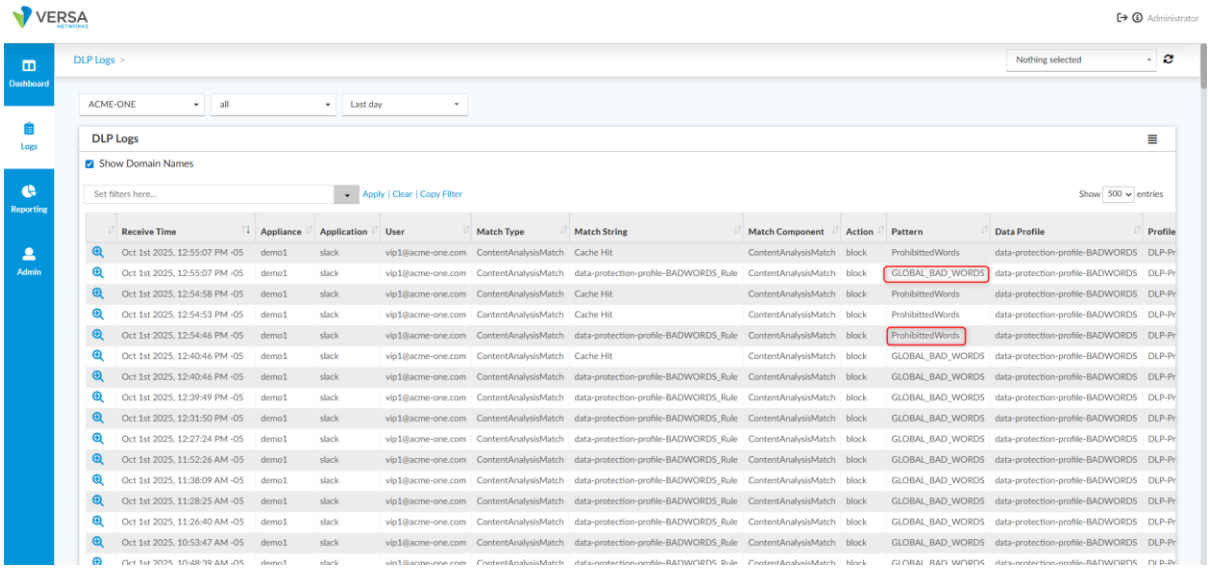
Slack Test using global bad word sample



Slack test using custom bad word sample.



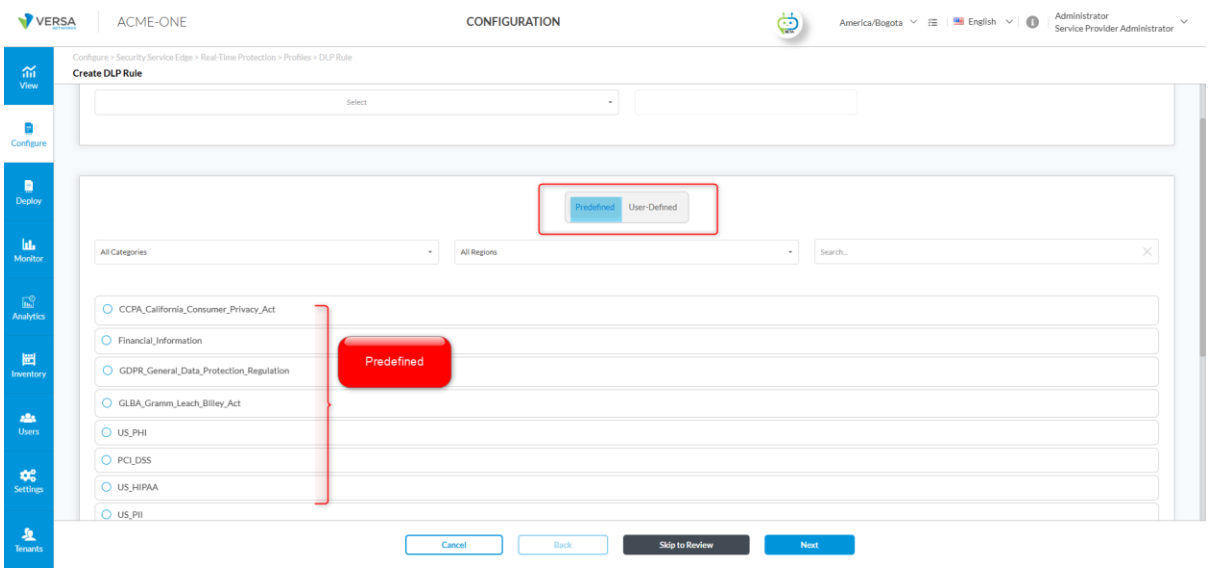
Logs from Analytics



Appendix A – DLP Rule Types

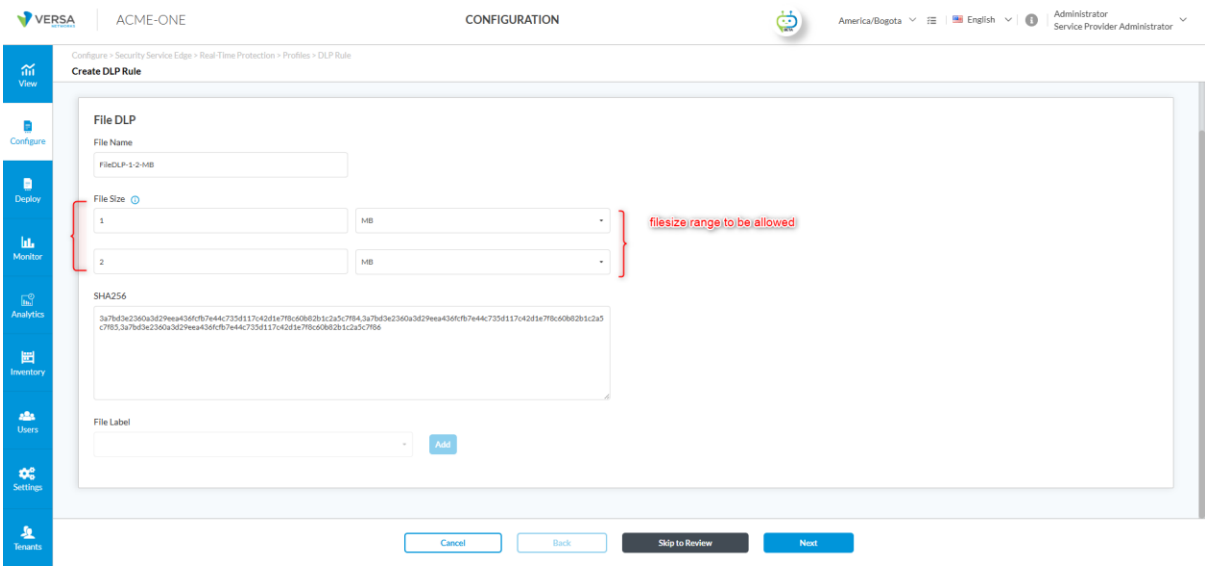
Content Analysis

Use many prefilters before actual data is scanned and analyzed. It helps to apply DLP policies on 'data in motion' effectively. Additionally, it can leverage either predefined or user-defined Data Protection Profiles, as shown in the image below.



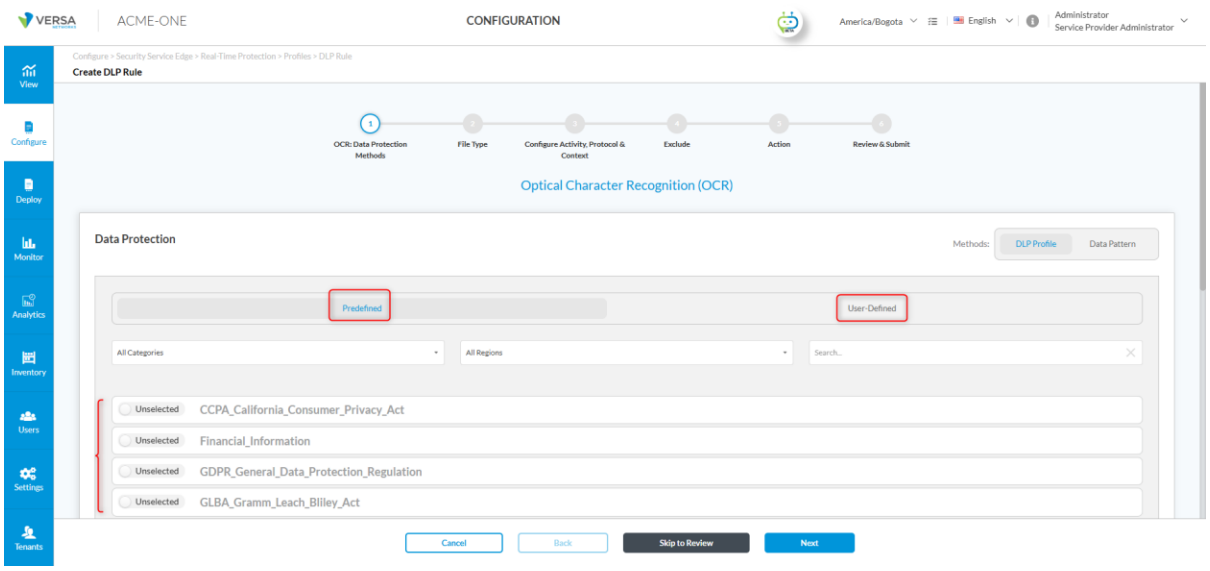
File DLP

File-based DLP provides protection based on the configured file attributes, as shown in the image below. Administrators can define rules such as file name (using specific patterns or values), file size (by setting minimum and maximum thresholds with actions applied outside the allowed range), and SHA256 hashes (to explicitly allow or block specific files). When multiple attributes are configured, they are evaluated using AND conditions, meaning that all specified criteria must be met simultaneously for the rule to apply. Alternatively, a single attribute can be used on its own—for example, configuring only the file size range, or only the SHA256 hash—by leaving the other fields blank. This flexibility allows organizations to fine-tune protection by combining general attributes with precise identifiers, or by focusing on a single attribute when needed.



Optical Character Recognition (OCR)

OCR technology converts images into text and applies DLP policies on the extracted text data. It requires connectivity to the Versa OCR Cloud Instance, which should be reviewed with the support team. Similar to Content Analysis, it can leverage either predefined or user-defined Data Protection Profiles, as shown in the image below.



Exact Data Match (EDM)

Versa's Data Loss Prevention (DLP) Exact Data Match (EDM) is an advanced security feature that detects and prevents data breaches by matching specific, sensitive data records against predefined datasets. Unlike traditional pattern-based detection, EDM allows organizations to upload structured data (such as customer records, financial information, or employee details) into a secure, hashed database. Versa DLP then scans network traffic for exact matches to these datasets, ensuring highly accurate data protection with minimal false positives.

A financial institution needs to prevent unauthorized transmission of customer account numbers and Social Security Numbers (SSNs). By using Versa's DLP EDM, they upload a securely hashed database of customer records. If an employee attempts to send an email or upload a file containing an exact match to this data, the system detects the violation and enforces security policies, such as blocking the transmission, alerting administrators, or requiring additional authorization.

This ensures compliance with regulations (e.g., PCI DSS, GDPR, HIPAA) and protects sensitive business and customer information from leaks or theft.

Document Fingerprinting

It converts a standard form into a sensitive information type, which you can use to define transport rules and DLP policies.

Appendix B – DLP Rule Actions

Allow: The content transfer is permitted without restriction. No enforcement action is taken.

Alert: The action is allowed, but an alert/notification is generated for visibility, monitoring, or further investigation.

Block: The content transfer is prevented. The user may receive a notification that the action was blocked depending on policy configuration.

Reject: The content transfer is actively denied, and the session is forcefully terminated. The browser typically shows a *"connection reset"* or similar error, and at the same time the endpoint client displays a popup notifying the user of the DLP violation.

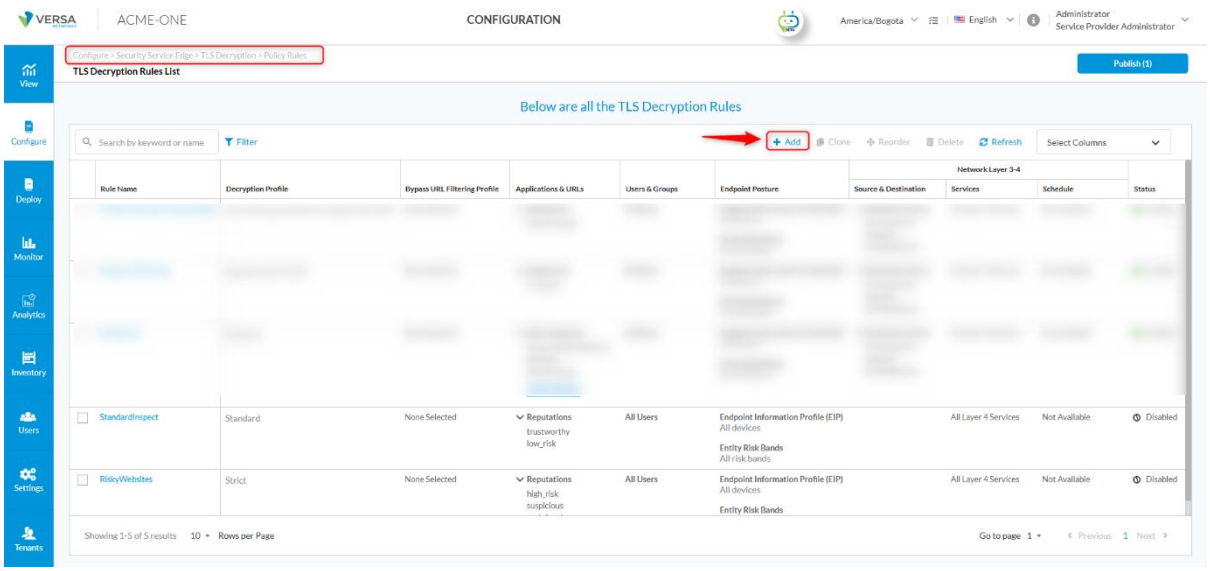
Quarantine: API-DP still in roadmap for 2025

Encrypt: API-DP still in roadmap for 2025

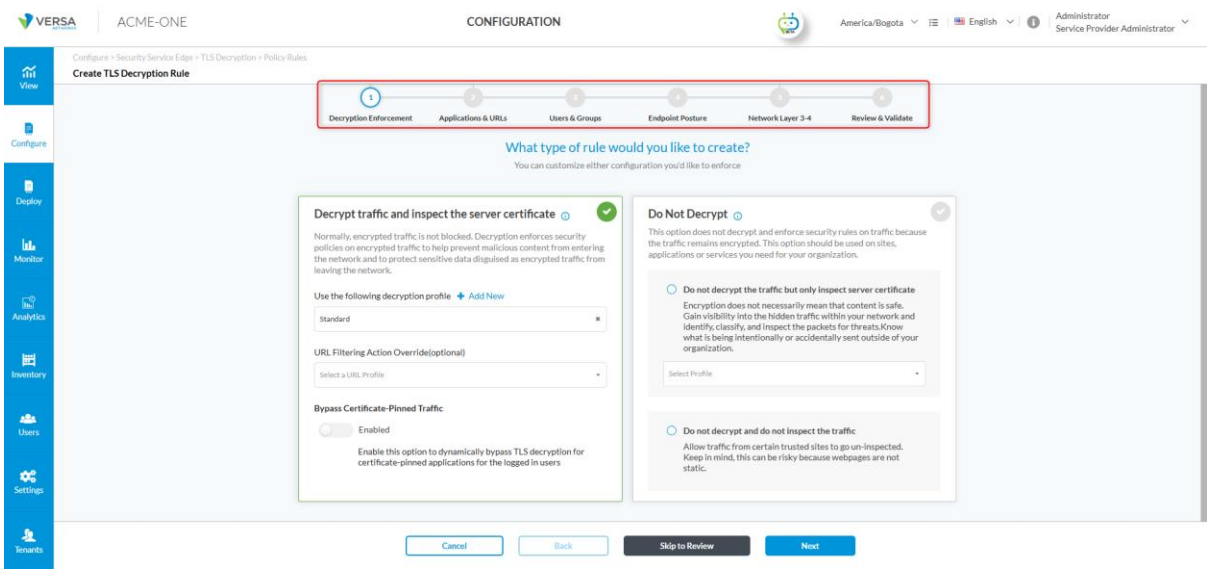
Legal Hold: API-DP still in roadmap for 2025

Appendix C – TLS Decryption Rule Configuration

Navigate to ***Configure*** > ***Security Service Edge*** > ***TLS Decryption*** > ***Policy Rules. Click + Add***, as shown in the image below.



Then complete the 6 steps shown in the following image.



Decryption Enforcement: Select the green checkmark (Decrypt traffic and inspect the server certificate) and under Use the following decryption profile, select Standard, then click Next.

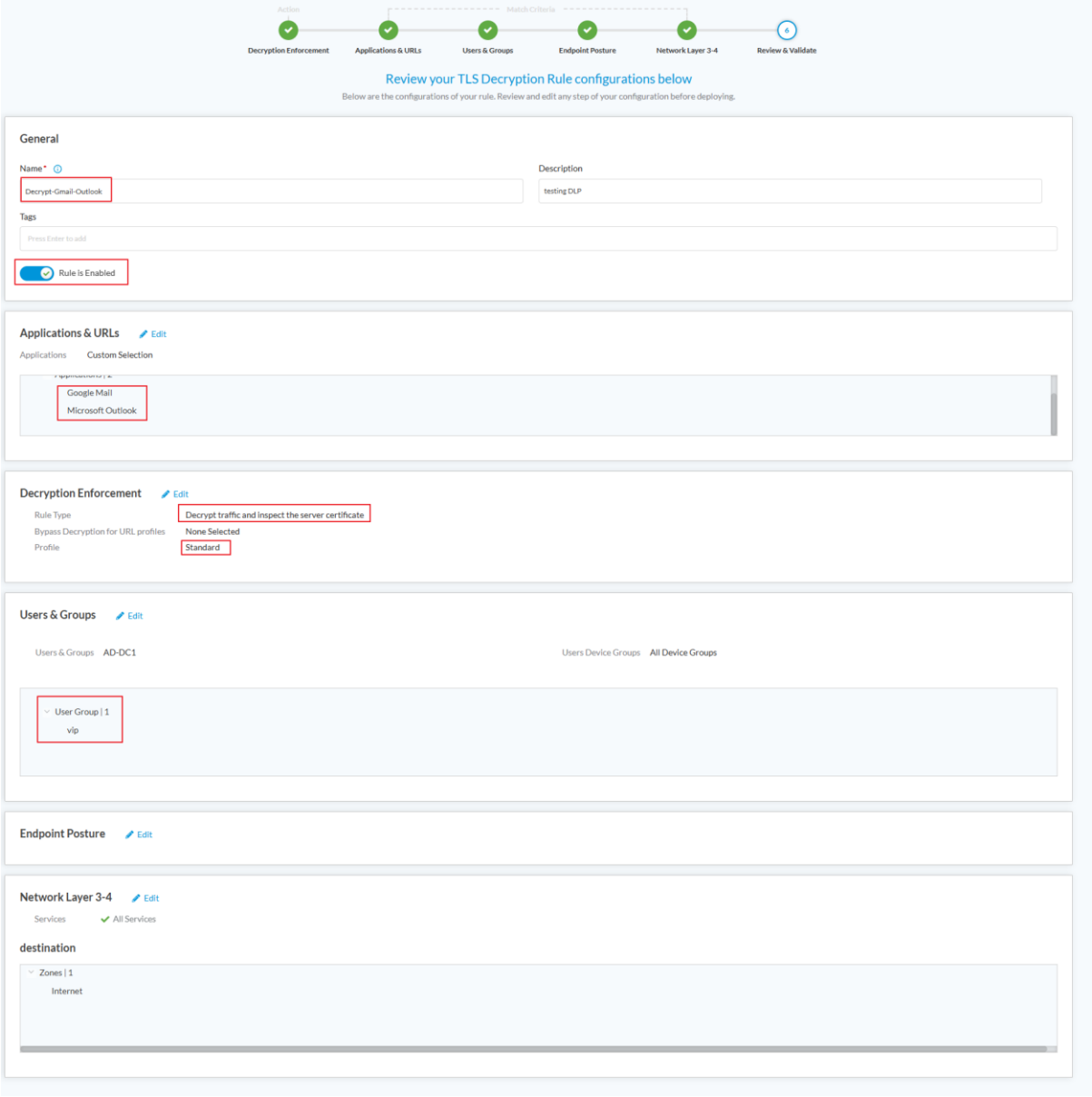
Applications & URLs: Click the Applications tab and in the search field add Gmail and Outlook, then click Next.

Users & Groups: Select your test group, then click Next. In our case, it can be the VIP group coming from our LDAP-AD.

Endpoint Posture: Leave the default values and click **Next**.

Network Layer 3-4: You can filter by services like **http**, **https**, **dns**, **icmp**, etc. However, leave the default values and click **Next**.

Review & Validate: Review the configuration (see image below), click **Save**, and select **add this rule at the top of the rule list**.



Appendix D – Incident_Report_Form_Filled.docx.

This section lists the sample data used in the testing of use case 2

Confidential Employee Incident Report Form

This form is intended for the reporting of workplace incidents and policy violations. All submissions are confidential and will be reviewed by the HR Compliance Department. Please complete all required sections. Additional evidence or extended narratives should be attached as separate documents. Do not exceed the provided space in each section.

Section 1 – Employee Information

Employee Name: John Doe

Department: IT Security

Position: Senior Security Analyst

Date of Incident: 09 / 12 / 2025

Section 2 – Type of Violation

Please check one or more categories that best describe the violation (mandatory selection):
[X] Confidentiality Breach
[ ] Code of Conduct
[ ] Workplace Harassment
[ ] Safety Violation
[ ] Other (please specify) _____

Section 3 – Description of Violation

Provide a concise summary of the violation in 3–4 sentences maximum. If additional details are needed, attach a supporting document.

Description:
On September 12th, 2025, an employee was observed uploading a confidential HR policy document to a personal Dropbox account. The file contained sensitive disciplinary procedures. The incident was detected by the DLP monitoring system and reported for investigation.

Section 4 – Witnesses

List up to 2 witnesses with name and department. Additional names must be attached separately.

1. Jane Smith – HR Department

2. Michael Brown – IT Department

Section 5 – Co-Workers Involved

List any co-workers directly involved in the incident. Specify their role or relation to the case.

1. Alice Johnson – Co-worker who shared the document link internally.

2. N/A

Section 6 – Acknowledgement

By signing this form, the reporting employee confirms that the information provided is accurate to the best of their knowledge. The HR Compliance Department will review the case and take the appropriate action as outlined in company policy.

Employee Signature: John Doe Date: 09 / 12 / 2025

About Versa

Versa, the global leader in SASE, enables organizations to create self-protecting networks that radically simplify and automate their network and security infrastructure. Powered by AI, the VersaONE Universal SASE Platform delivers converged SSE, SD-WAN, and SD-LAN solutions that protect data and defend against cyberthreats while delivering a superior digital experience. Thousands of customers globally, with hundreds of thousands of sites and millions of users, trust Versa with their mission critical networks and security. Versa is privately held and funded by investors such as Sequoia Capital, Mayfield, and BlackRock. For more information, visit https://www.versa-networks.com and follow Versa on LinkedIn and X (Twitter) @versanetworks.