ZSCALER AND RUBRIK DEPLOYMENT GUIDE

JULY 2025, VERSION 1.4

BUSINESS DEVELOPMENT GUIDE

Contents

Terms and Acronyms

The following table defines the acronyms used in this deployment guide. When applicable, a Request for Change (RFC) is included in the Definition column for your reference.

Acronym	Definition
CA	Central Authority (Zscaler)
CSV	Comma-Separated Values
DHCP	Dynamic Host Configuration Protocol
DLP	Data Loss Prevention
DNS	Domain Name Service
DPD	Dead Peer Detection (RFC 3706)
DR	Disaster Recovery
FQDN	Fully Qualified Doman Name
GLBA	Gramm-Leach-Bliley Act
GRE	Generic Routing Encapsulation (RFC2890)
HIPAA	Health Insurance Portability and Accountability Act of 1996
IaC	Infrastructure as Code
ICMP	Internet Control Message Protocol
IKE	Internet Key Exchange (RFC2409)
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security (RFC2411)
ITSM	IT Service Management
NAS	Network-Attached Storage
NTP	Network Time Protocol
OVA	Open Virtual Appliance
PAC	Programmable Automation Controller
PCI	Payment Card Industry
PFS	Perfect Forward Secrecy
PSK	Pre-Shared Key
RBS	Rubrik Backup Service
rCDM	Rubrick Cloud Data Management
RPO	Recovery Point Objective
SDD	Sensitive Data Discovery
SSH	Secure Shell
SSHD	Secure Shell Daemon
SSL	Secure Socket Layer (RFC6101)
TLS	Transport Layer Security
VDI	Virtual Desktop Infrastructure
XFF	X-Forwarded-For (RFC7239)
ZCP	Zscaler Cloud Protection (Zscaler)
ZDX	Zscaler Digital Experience (Zscaler)
ZIA	Zscaler Internet Access (Zscaler)
ZPA	Zscaler Private Access (Zscaler)

Trademark Notice

About This Document

The following sections describe the organizations and requirements of this deployment guide.

Zscaler Overview

Zscaler (NASDAQ: ZS) enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) services create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler delivers its services 100% in the cloud and offers the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions can't match. Used in more than 185 countries, Zscaler operates a massive, global cloud security platform that protects thousands of enterprises and government agencies from cyberattacks and data loss. For more information, see Zscaler's website.

Rubrik Overview

Rubrik is a cybersecurity company and our mission is to secure the world's data. Rubrik pioneered Zero Trust Data Security to help organizations achieve business resilience against cyberattacks, malicious insiders, and operational disruptions. Rubrik Security Cloud, built with a zero trust design and powered by machine learning, delivers complete cyber resilience in a single platform across enterprise, cloud, and SaaS. Rubrik's platform automates data policy management and enforcement, safeguards sensitive data, delivers data threat analytics and response, and orchestrates rapid cyber and operational recovery. To learn more, refer to Rubrik's website.

Audience

This guide is for network administrators, endpoint / IT administrators, data protection and security analysts responsible for deploying, monitoring, and managing enterprise security systems. For additional product and company resources, refer to:

- Zscaler Resources
- Rubrik Resources
- Appendix A: Requesting Zscaler Support

Software Versions

This document was authored using ZIA v6.2 and Rubrik Security Cloud.

Request for Comments

- For prospects and customers: Zscaler values reader opinions and experiences. Contact partner-doc-support@zscaler.com to offer feedback or corrections for this guide.
- For Zscaler employees: Contact z-bd-sa@zscaler.com to reach the team that validated and authored the integrations in this document.

Zscaler and Rubrik Introduction

The following are overviews of the Zscaler and Rubrik applications described in this deployment guide.

⚠ If you are using this guide to implement a solution at a government agency, some of the content might be different for your deployment. Efforts are made throughout the guide to note where government agencies might need different parameters or input. If you have questions, contact your Zscaler Account team.

ZIA Overview

ZIA is a secure internet and web gateway delivered as a service from the cloud. Think of it as a secure internet on-ramp—all you do is make Zscaler your next hop to the internet via one of the following methods:

- Setting up a tunnel (GRE or IPSec) to the closest Zscaler data center (for offices).
- Forwarding traffic via the lightweight Zscaler Client Connector or PAC file (for mobile employees).

No matter where users connect—a coffee shop in Milan, a hotel in Hong Kong, or a VDI instance in South Korea—they get identical protection. ZIA sits between your users and the internet and inspects every transaction inline across multiple security techniques (even within SSL).

You get full protection from web and internet threats. The Zscaler cloud platform supports Cloud Firewall, IPS, Sandboxing, DLP, and Isolation, allowing you to start with the services you need now and activate others as your needs grow.

ZPA Overview

ZPA is a cloud service that provides secure remote access to internal applications running on a cloud or data center using a zero trust framework. With ZPA, applications are never exposed to the internet, making them completely invisible to unauthorized users. The service enables the applications to connect to users via inside-out connectivity rather than extending the network to them.

ZPA provides a simple, secure, and effective way to access internal applications. Access is based on policies created by the IT administrator within the ZPA Admin Portal and hosted within the Zscaler cloud. On each user device, software called Zscaler Client Connector is installed. Zscaler Client Connector ensures the user's device posture and extends a secure microtunnel out to the Zscaler cloud when a user attempts to access an internal application.

Zscaler Resources

The following table contains links to Zscaler resources based on general topic areas.

Name and Link	Description
ZIA Help Portal	Help articles for ZIA.
Adding SaaS Application Tenants	Help article on using Zscaler API for visibility and security for sanctioned SaaS applications used in your organization.
About SaaS Application Tenants	Help article on adding SaaS applications to Zscaler.
SaaS Security API DLP Policy	Help article on creating rules to discover and protect sensitive data at rest in sanctioned SaaS applications.
About Data Loss Prevention	Help article on DLP.
About DLP Dictionaries	Help article on DLP dictionaries.

Name and Link	Description
About Custom DLP Engines	Help article on DLP engines.
SaaS Security Insights	Help article providing SaaS security information.
Zscaler Training and Certification	Training designed to help you maximize Zscaler products.
Submit a Zscaler Support Ticket	Zscaler Support portal for submitting requests and issues.

The following table contains links to Zscaler resources for government agencies.

Name and Link	Description
ZIA Help Portal	Help articles for ZIA.
Adding SaaS Application Tenants	Help article on using Zscaler API for visibility and security for sanctioned SaaS applications used in your organization.
About SaaS Application Tenants	Help article on adding SaaS applications to Zscaler.
SaaS Security API DLP Policy	Help article on creating rules to discover and protect sensitive data at rest in sanctioned SaaS applications.
About Data Loss Prevention	Help article on DLP.
About DLP Dictionaries	Help article on DLP dictionaries.
About Custom DLP Engines	Help article on DLP engines.
SaaS Security Insights	Help article providing SaaS security information.
Zscaler Training and Certification	Training designed to help you maximize Zscaler products.
Submit a Zscaler Support Ticket	Zscaler Support portal for submitting requests and issues.

Rubrik Security Cloud Overview

The Rubrik platform provides the following benefits:

- Backup and Recovery: Modernize and automate data protection. Deliver instant recoveries at scale, slash operational costs, and safeguard data from ransomware.
- Ransomware Recovery: With backups that can't be encrypted or deleted, recover quickly to the most recent clean state with added impact analysis.
- Data Security Posture: Proactively identify and monitor sensitive data exposure and use intelligent insights to mitigate risks to this data.
- Data Threat Analytics: Continuously monitor for threats to your data, including ransomware, data destruction, and indicators of compromise.
- Database Backup: Deliver the simplicity, operational efficiency, cloud mobility, and security needed to confidently protect your organization’s most vital resource.
- VM Backup: Rubrik delivers backup, replication, DR, archival, and analytics for the hypervisor of your choice – VMware vSphere (ESXi), Microsoft Hyper-V, and Nutanix AHV.
- NAS: NAS Cloud Direct allows you to efficiently store massive unstructured datasets elsewhere on-premises or in the cloud to unlock cost savings and high performance at scale.
- Rubrik Cloud Vault: Extend Rubrik Zero Trust Data Security to the cloud for isolated, off site archival of immutable data.
- Cloud Archival: Scalable, automated data archival that helps you facilitate compliance with the most complex enterprise and regulatory requirements.
- Cloud-Native Protection: Rubrik provides a secure software platform to mitigate data loss with granular recovery and seamless management across multiple cloud environments.

- Kubernetes: Protect, organize, and manage your Kubernetes environment from a single SaaS console and forget job-centric protection and slow, tedious restores.
- Continuous Data Protection: Rubrik's Continuous Data Protection (CDP) delivers near-zero RPOs to minimize data loss.
- Sensitive Data Monitoring: Accelerate regulatory compliance in a centralized platform that protects, manages, and monitors all your data.
- Remote and Branch Office: Extend data protection and management to virtualized and physical remote and branch office environments.
- Replication and DR: Minimize disruption during system or site failures to meet aggressive recovery objectives and maintain data availability.
- Drop server: Specific to the Zscaler integration, the drop server is a virtual machine running the Rubrik Backup Service, or a NAS share registered in Rubrik Security Cloud. This is the location to which sensitive files are recovered for indexing by the Zscaler Indexer appliance.

Rubrik Resources

The following table contains links to Rubrik support resources.

Name and Link	Description
Rubrik University	Several instructor-led virtual learning events and free eLearning resources.
Rubrik Security Cloud API	Rubrik Security Cloud API Integration documents.
Rubrik Virtual Demos	One-hour Rubrik live virtual demos.
Rubrik Explore	Guided, click-through lab demos.

Rubrik and Zscaler Data Loss Prevention Integration

The Rubrik and Zscaler Data Loss Prevention (DLP) integration automatically sends sensitive files found by Sensitive Data Discovery and backed up by Rubrik to Zscaler's service for DLP.

Zscaler's implementation detects and prevents sensitive file exfiltration that has been identified *sensitive* by the Rubrik solution.

There are three core parts to the integration:

- Zscaler DLP configuration
- Zscaler and Rubrik Integration configuration
- Rubrik Sensitive Data Discovery policy enablement

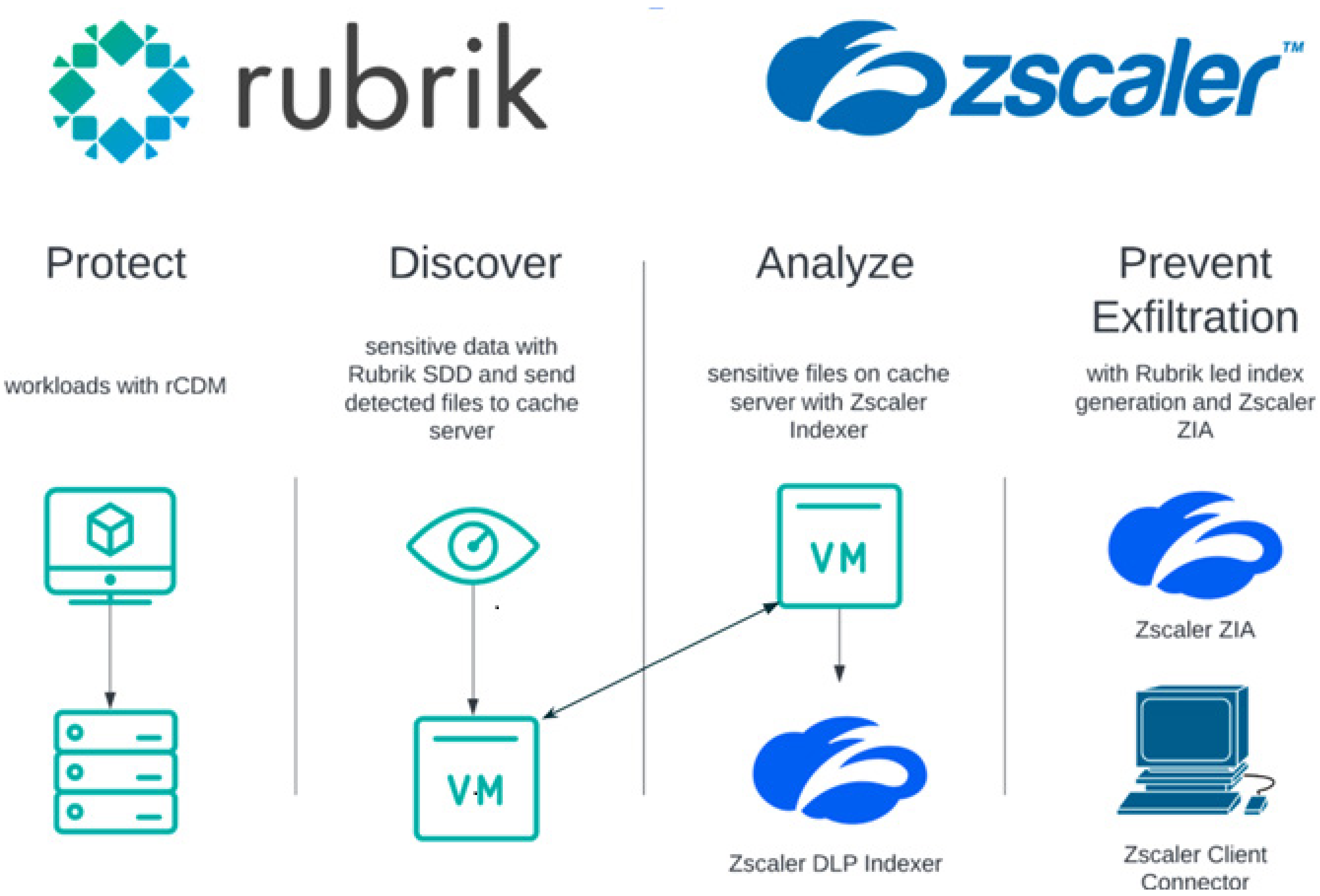

rubrik
zscaler™
Protect
workloads with rCDM
Discover
sensitive data with Rubrik SDD and send detected files to cache server
VM
Analyze
sensitive files on cache server with Zscaler Indexer
VM
Zscaler DLP Indexer
Prevent Exfiltration
with Rubrik led index generation and Zscaler ZIA
Zscaler ZIA
Zscaler Client Connector

Figure 1. Zscaler solutions for Rubrik

Zscaler DLP Configuration

You must deploy an OVA into the environment that processes files and sends the metadata or hash up to the ZIA Admin Portal that enforces DLP.

Since files must be placed into a configured location by the index server, ensure that the target location is a snappable configured on Rubrik Backup Service (RBS). Refer to the Rubrik User Guide for installing RBS to a VM or host. Note that TCP ports 12800 and 12801 on the drop server must be open to traffic from all nodes in the Rubrik Secure Vault cluster. For more information about RBS, including supported operating systems, refer to the Rubrik documentation.

The overall process uses a file recovery workflow to export the files detected by Sensitive Data Monitoring, and then places those files into the index location for Zscaler.

After these files are in the index location, the Zscaler Indexer indexes the files, and sends metadata and hashes up to ZIA so that DLP is enforced for these sensitive files. Zscaler requires that the server that houses exported files for indexing has SSHD installed.

Configure Zscaler Integration in Rubrik Security Cloud

To add the integration:

1. In the Rubrik Data Protection dashboard, go to **Apps** and click **Settings**.

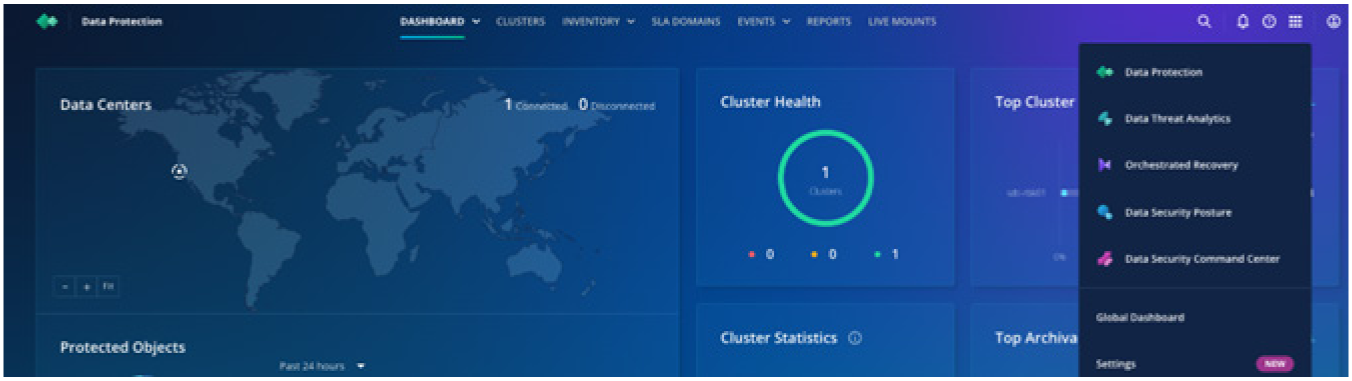
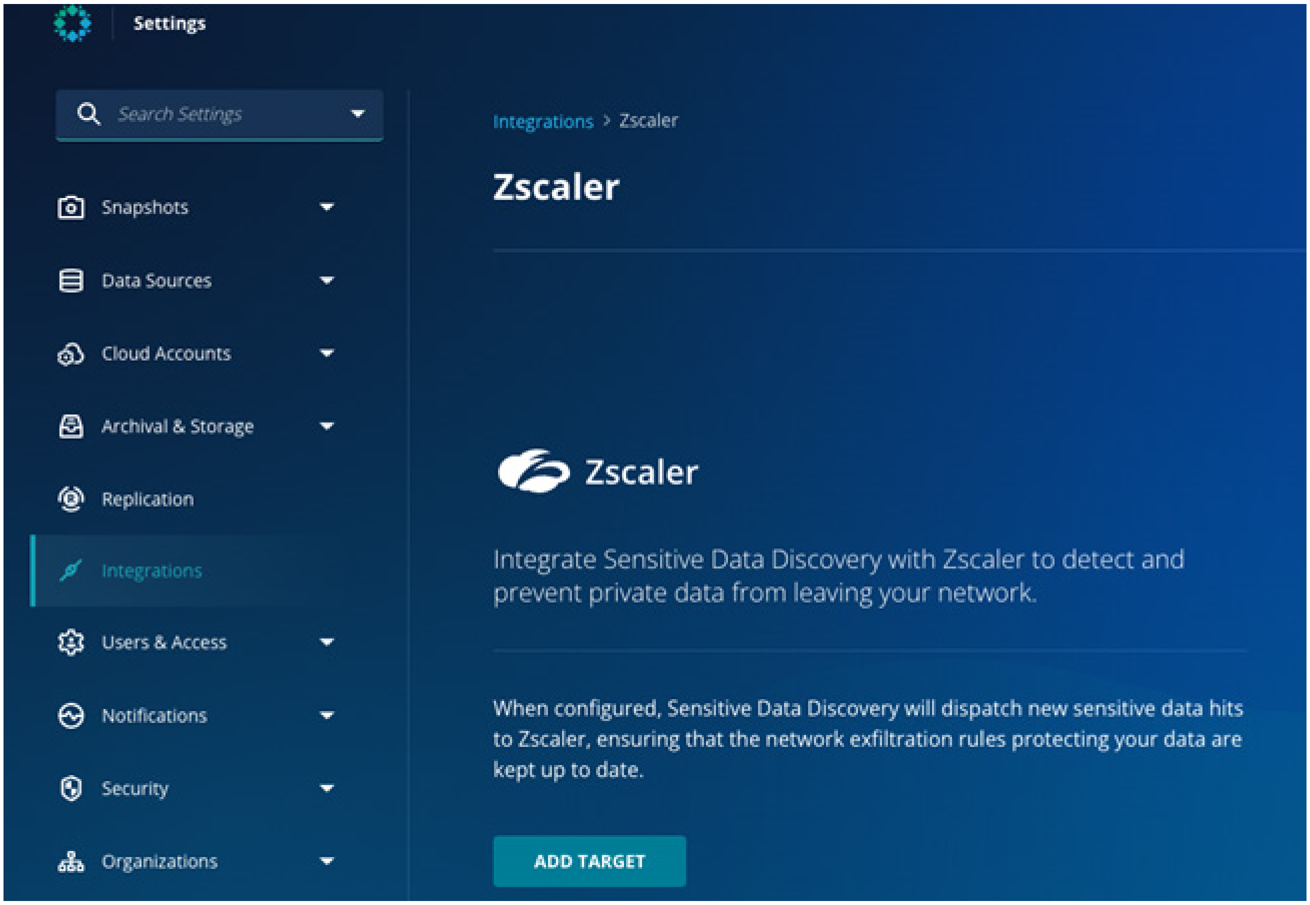


Figure 2. Rubrik Data Protection dashboard

2. In the **Settings** window, click **Integrations** and **Add Target**.

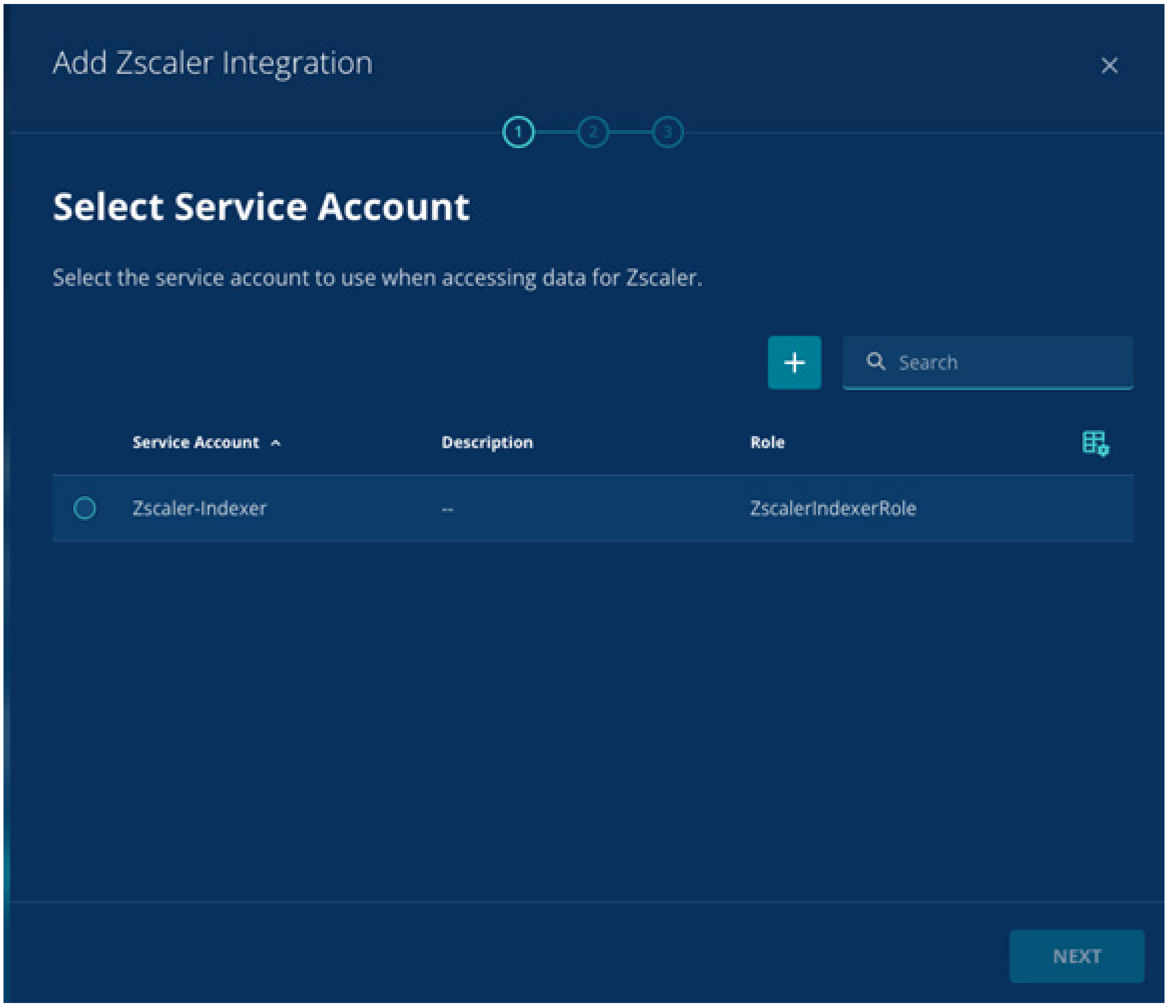


Integrate Sensitive Data Discovery with Zscaler to detect and prevent private data from leaving your network.

When configured, Sensitive Data Discovery will dispatch new sensitive data hits to Zscaler, ensuring that the network exfiltration rules protecting your data are kept up to date.

Figure 3. Rubrik Integration Settings

3. The **Select Service Account** window is displayed. Select the **Add** (+) icon to create a new Service Account. For more information about Service Accounts, refer to the Rubrik Security Cloud documentation.



Add Zscaler Integration

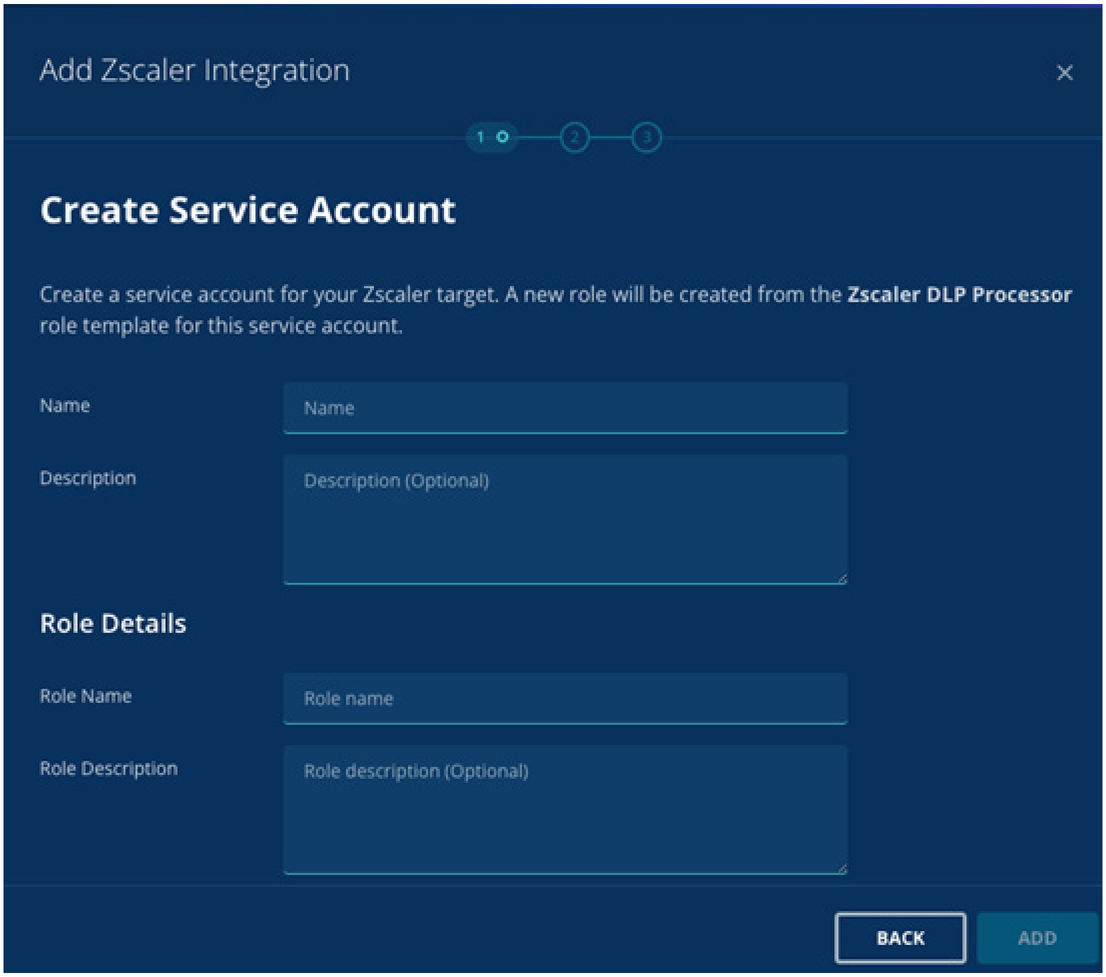
Select Service Account

Select the service account to use when accessing data for Zscaler.

	Service Account ^	Description	Role
○	Zscaler-Indexer	--	ZscalerIndexerRole

Figure 4. Rubrik Select Service Account

4. The **Create Service Account** window is displayed. Create a service account that the DLP Indexer uses and map it to a role.
5. Click **Add**.



Add Zscaler Integration

Create Service Account

Create a service account for your Zscaler target. A new role will be created from the **Zscaler DLP Processor** role template for this service account.

Name: Name

Description: Description (Optional)

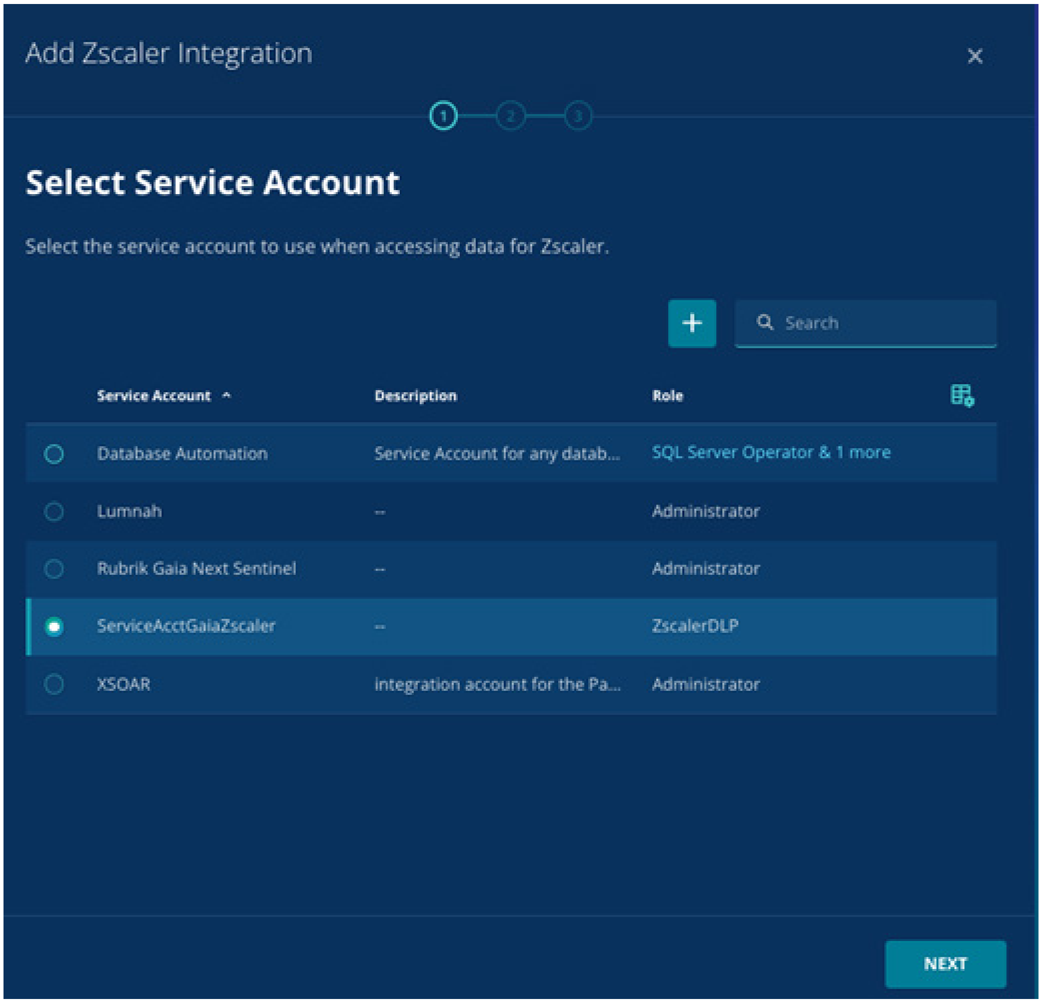
Role Details

Role Name: Role name

Role Description: Role description (Optional)

Figure 5. Rubrik Create Service Account

6. Select the previously created Service.
7. Click **Next**.



Add Zscaler Integration

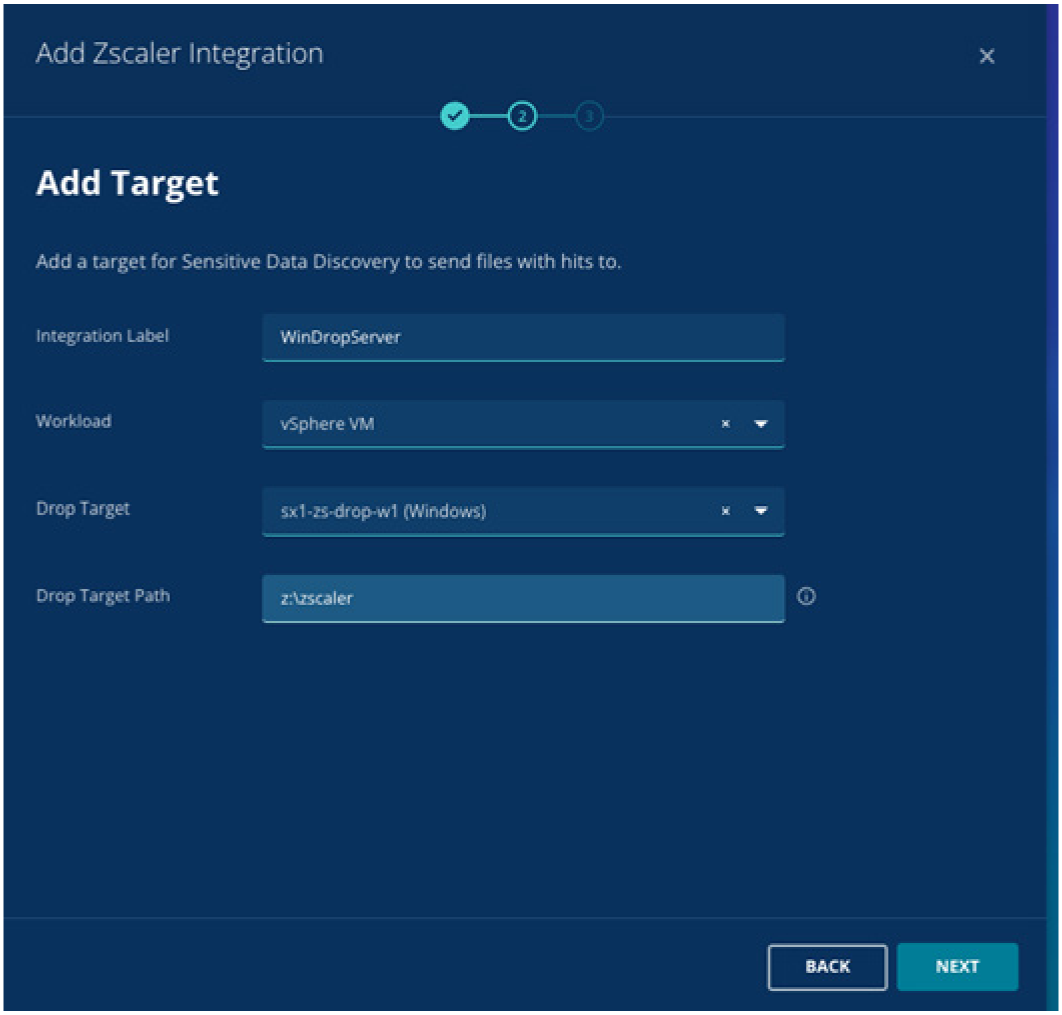
Select Service Account

Select the service account to use when accessing data for Zscaler.

	Service Account	Description	Role
○	Database Automation	Service Account for any datab...	SQL Server Operator & 1 more
○	Lumnah	--	Administrator
○	Rubrik Gaia Next Sentinel	--	Administrator
●	ServiceAcctGaiaZscaler	--	ZscalerDLP
○	XSOAR	integration account for the Pa...	Administrator

Figure 6. Rubrik Select Service Account

8. In the **Add Zscaler Integration** window:
   a. Enter the **Name** for the **Integration Label**.
   b. Select **Workload** (**vSphere VM** or **NAS Share**).
   c. Select **Drop Target** for the selected drop server. Only virtual machines with RBS installed and registered are selectable. If your drop target of choice is grayed out, verify that RBS is installed, running, and registered to Rubrik Security Cloud.
   d. Select the **Drop Target Path** that is used in the Zscaler indexer configuration. This is the path in-guest, so make sure to use the relevant path format (\ for Windows guests, / for Linux guests). When Rubrik Security Cloud detects sensitive data in your backups, these files are restored to this drop target.
9. Confirm the integration values are correct and click **Next**.



Add Zscaler Integration

Add Target

Add a target for Sensitive Data Discovery to send files with hits to.

Integration Label: WinDropServer

Workload: vSphere VM

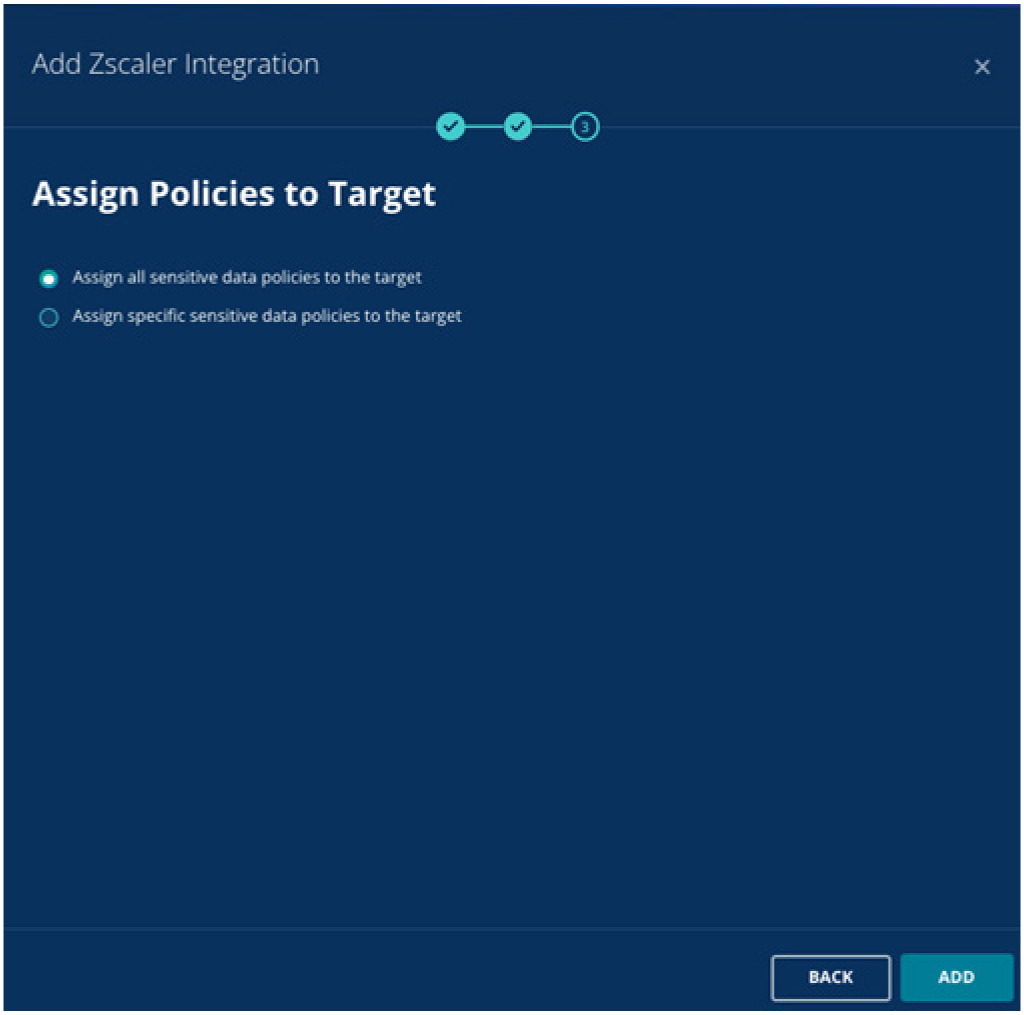
Drop Target: sx1-zs-drop-w1 (Windows)

Drop Target Path: z:\zscaler

Figure 7. Rubrik Add Target

10. The **Assign Policies to Targe**t window is displayed. Select and assign all sensitive data policies to the target or assign specific data policies to the target. For amplifying information on Rubrik Sensitive Data policies, refer to the [Rubrik Analyzer's Guide](#).

11. Select **Add**.



Add Zscaler Integration

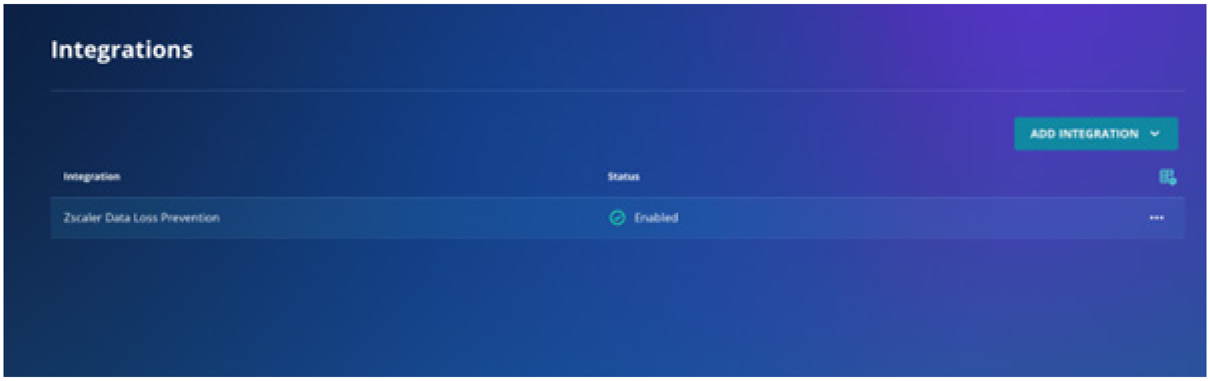
Assign Policies to Target

● Assign all sensitive data policies to the target
○ Assign specific sensitive data policies to the target

Figure 8. Rubrik Assign Policy to Target

Rubrik allows the use of either prebuilt data classification analyzers and policies. To learn more, refer to the [Rubrik documentation](#).

The Integrations screen displays the configured integration as Enabled.



Integrations

Integration	Status
Zscaler Data Loss Prevention	Enabled

Figure 9. Rubrik Integration Enabled

After the policy is enabled for Zscaler integration, the sensitive files are discovered by the Rubrik policy, a job runs over a 24-hour period and starts placing files into the configured target location. Rubrik uses a forever incremental approach to backups, and so any new or changed files are analyzed for sensitive data on each new backup going forward.

Zscaler DLP Indexed Document Match

Zscaler's Indexed Document Match (IDM) templates fingerprint which critical documents contain sensitive data in your organization. By fingerprinting and indexing your documents, you can create a document repository that the Zscaler service uses to identify completely or partially matching documents when evaluating outbound traffic with the DLP policy.

Creating an IDM template requires the Zscaler's Index Tool, which uploads and fingerprints your documents. You can upload text-based files and non-text-based documents (e.g., binary files). After an IDM template is created, you can then apply the template to a custom DLP dictionary. When adding the template to the dictionary, you must choose the match accuracy level for the template. Match accuracy is the level of accuracy (i.e., the percentage of similarity) that a document must meet to count as a match for an indexed document.

Configuring the Index Tool with VMware

New or clean deployment of the Index Tool requires a VM image running on Zscaler OS version 24 or later.

The following sections describe configuring the Index Tool with VMware.

Since the Index Tool provides access to highly sensitive information, ensure that everyone who has access to it is authorized and authenticated.

Index Tool VM Specifications and Sizing Guidelines

If your index templates include less than 300 million records, Zscaler recommends the following configuration:

- Hypervisor: VMware ESX/ESXi version 6.0 or later.
- CPUs: 4 CPUs. Zscaler requires 4 CPUs because the CPUs ensure that hash generation performance is not impacted.
- RAM: 16 GB
- Disk: 600 GB
- VM Network: 1 Virtual NIC

If your index templates include more than 300 million records, Zscaler recommends the following configuration:

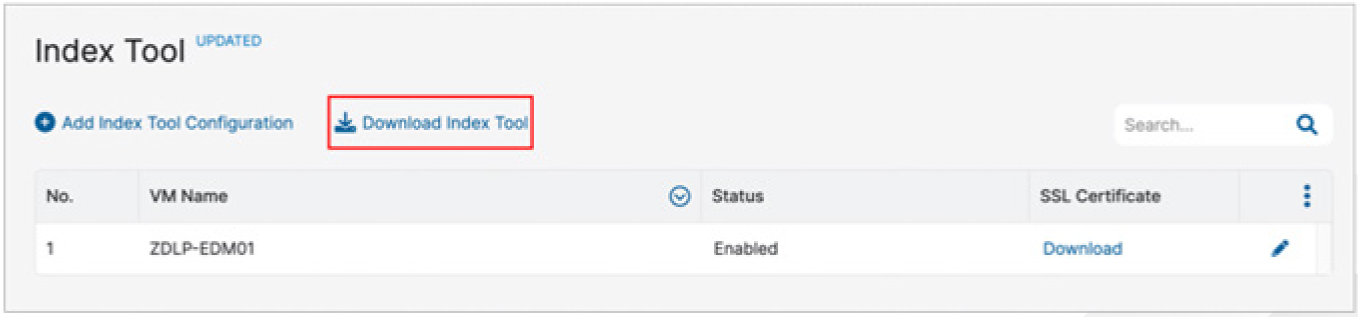
- Hypervisor: VMware ESX/ESXi version 6.0 or later.
- CPUs: 4 CPUs. Zscaler requires 4 CPUs because the CPUs ensure that hash generation performance is not impacted.
- RAM: 64 GB
- Disk: 1 TB
- VM Network: 1 Virtual NIC

Download the Index Tool Image

You must download the Index Tool VM before you configure it.

If your index templates include less than 300 million records, you can download the Index Tool VM image from the ZIA Admin Portal. To download the Index Tool VM:

1. Go to **Administration** > **Index Tool**.
2. Click **Download Index Tool**.



Index Tool UPDATED

No.	VM Name	Status	SSL Certificate
1	ZDLP-EDM01	Enabled	Download

Figure 10. Zscaler Index Tool download page

Adding an Index Tool Configuration

To add an Index Tool configuration:

1. Go to **Administration** > **Index Tool**.
2. Click **Add Index Tool Configuration**. The **Add Index Tool Configuration** window is displayed.
3. In the **Add Index Tool Configuration** window:
    a. **VM Name:** Enter a unique name for the virtual machine (VM).
    b. **Status**: Make sure that the VM is **Enabled**.

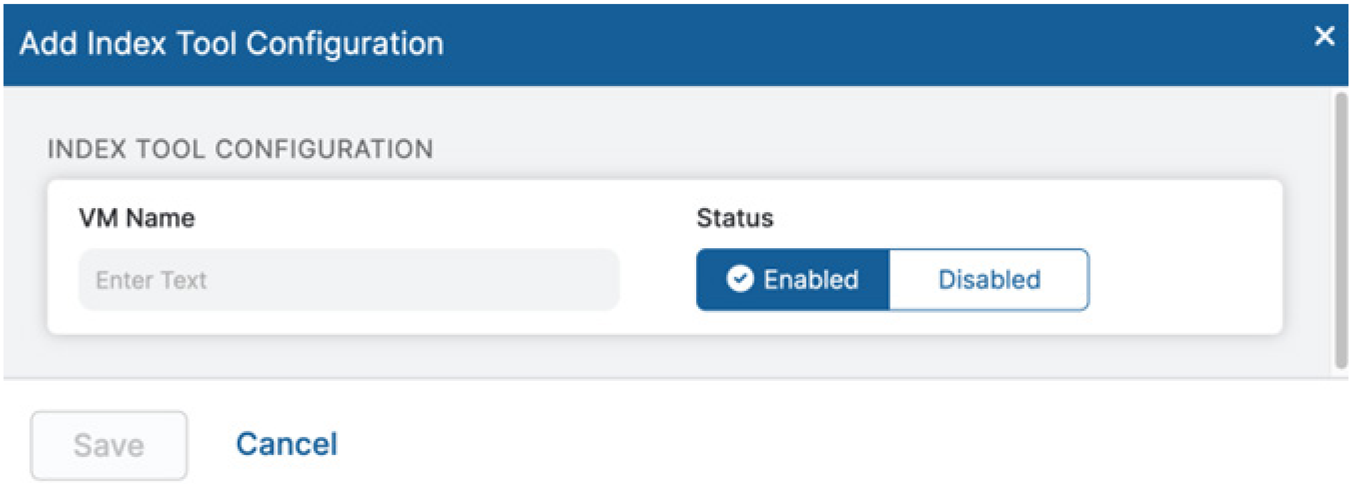


Figure 11. Zscaler Index Tool configuration

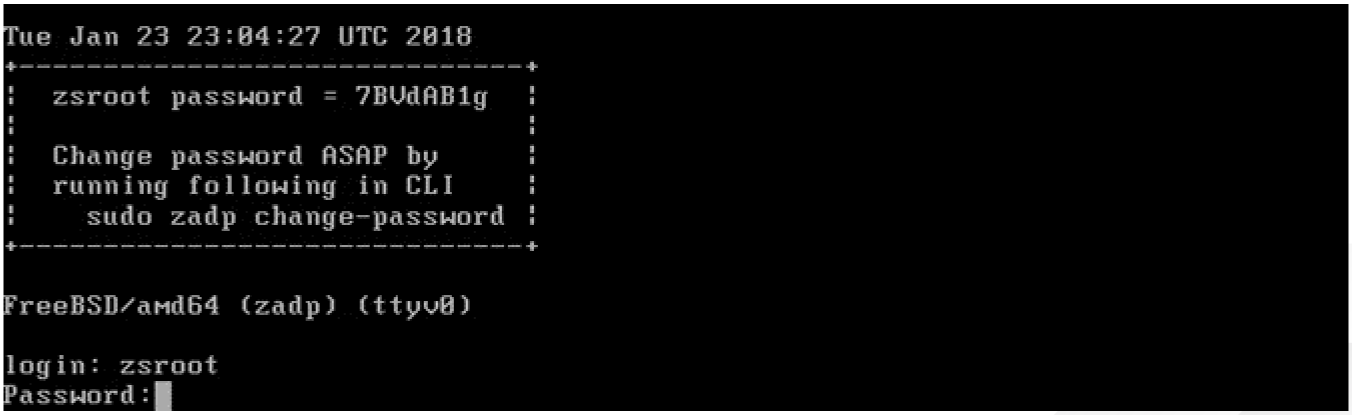
4. Click **Save** and activate the change (government agencies, see activate the change).

After you save the SSL Certificate for the configuration, you can download it from the Index Tool page or from the Edit Index Tool Configuration window.

Configuring the Index Tool VM (VMWare)

To configure the Index Tool VM:

1. Make sure you have added an Index Tool Configuration. You need this configuration to complete the VM setup.
2. In ESX/ESXi, install the Index Tool VM image you downloaded previously.
3. Boot up the VM and log in as user `zsroot`. The initial root password for this user is randomly generated.



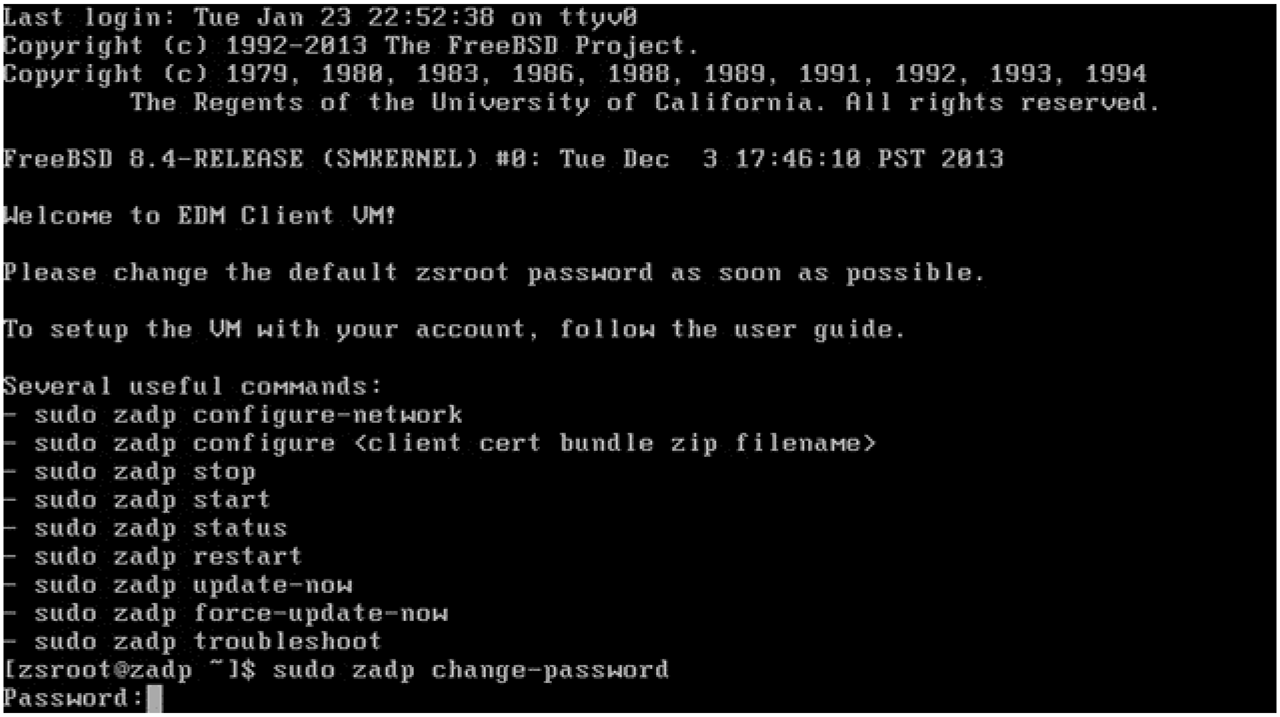
```
Tue Jan 23 23:04:27 UTC 2018
+------------------------------+
|  zsroot password = 7BVdAB1g  |
|                              |
|  Change password ASAP by     |
|  running following in CLI    |
|    sudo zadp change-password |
+------------------------------+

FreeBSD/amd64 (zadp) (ttyv0)

login: zsroot
Password:
```

Figure 12. Zscaler Index Tool - CLI

4. To change the root password:
   a. Enter the following command:

      ```
      sudo zadp change-password
      ```

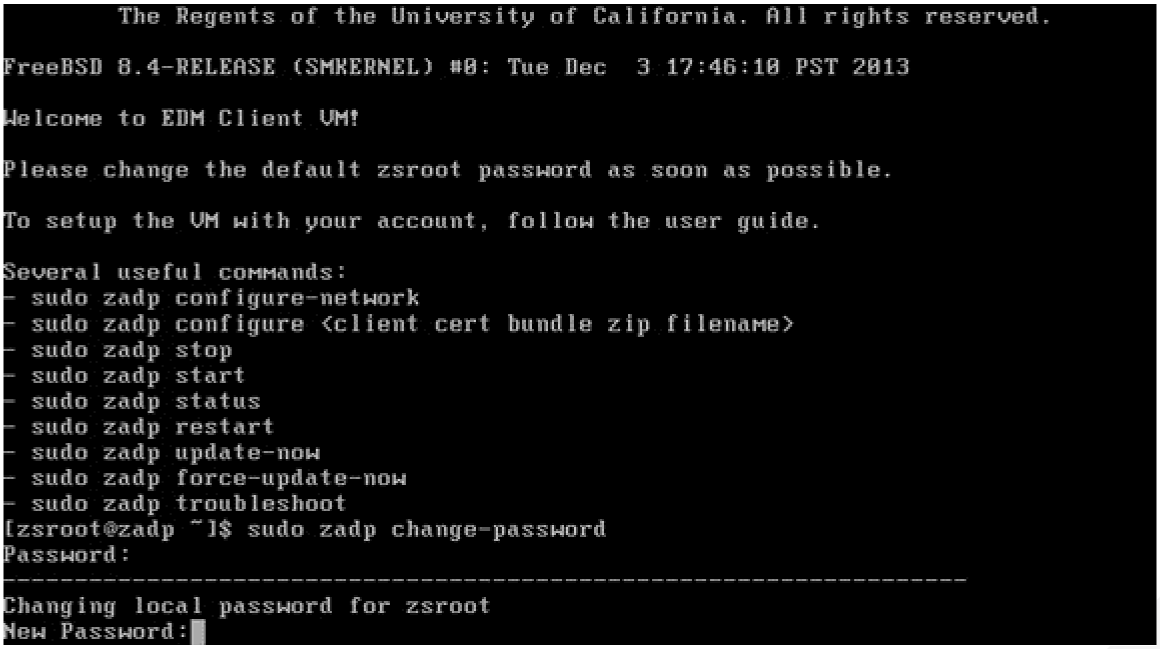
   b. Enter the initial root password that was randomly generated for you.



```
Last login: Tue Jan 23 22:52:38 on ttyv0
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
        The Regents of the University of California. All rights reserved.

FreeBSD 8.4-RELEASE (SMKERNEL) #0: Tue Dec  3 17:46:10 PST 2013

Welcome to EDM Client VM!

Please change the default zsroot password as soon as possible.

To setup the VM with your account, follow the user guide.

Several useful commands:
- sudo zadp configure-network
- sudo zadp configure <client cert bundle zip filename>
- sudo zadp stop
- sudo zadp start
- sudo zadp status
- sudo zadp restart
- sudo zadp update-now
- sudo zadp force-update-now
- sudo zadp troubleshoot
[zsroot@zadp ~]$ sudo zadp change-password
Password:
```

Figure 13. Zscaler Index Tool – CLI

   c. Enter the new root password.



```
        The Regents of the University of California. All rights reserved.

FreeBSD 8.4-RELEASE (SMKERNEL) #0: Tue Dec  3 17:46:10 PST 2013

Welcome to EDM Client VM!

Please change the default zsroot password as soon as possible.

To setup the VM with your account, follow the user guide.

Several useful commands:
- sudo zadp configure-network
- sudo zadp configure <client cert bundle zip filename>
- sudo zadp stop
- sudo zadp start
- sudo zadp status
- sudo zadp restart
- sudo zadp update-now
- sudo zadp force-update-now
- sudo zadp troubleshoot
[zsroot@zadp ~]$ sudo zadp change-password
Password:
---------------------------------------------------------------------
Changing local password for zsroot
New Password:
```

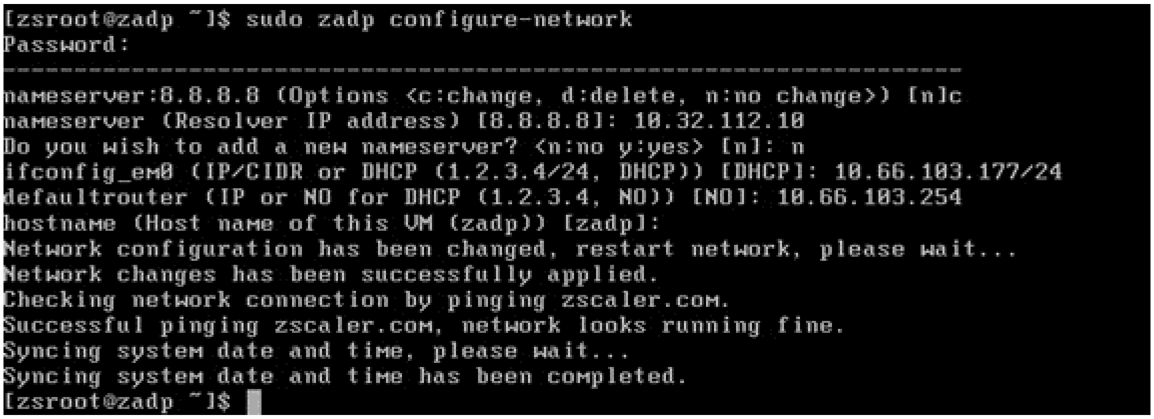
Figure 14. Zscaler Index Tool – Password Reset

   d. Re-enter the new root password. After changing the password, you must log in to `zsroot` again using the new password.

5. (Optional) By default, the VM starts using DHCP to obtain the IP address and default router information. If there's no DHCP server available, you can configure it manually:
   a. Enter the following command:

   ```
   sudo zadp configure-network
   ```

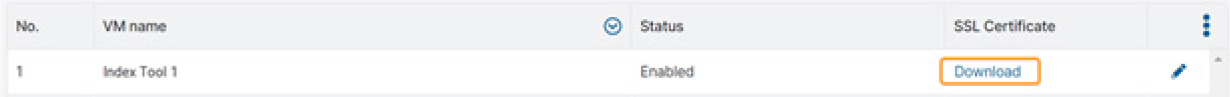
   b. For nameserver, enter `c` to change the IP address and press `Enter`.
   c. Enter the IP address and press `Enter`.
   d. If you want to add a new nameserver, enter `y`, otherwise enter `n`, and press `Enter`. The VM restarts the network and checks the connection.



```
[zsroot@zadp ~]$ sudo zadp configure-network
Password:
------------------------------------------------------------------
nameserver:8.8.8.8 (Options <c:change, d:delete, n:no change>) [n]c
nameserver (Resolver IP address) [8.8.8.8]: 10.32.112.10
Do you wish to add a new nameserver? <n:no y:yes> [n]: n
ifconfig_em0 (IP/CIDR or DHCP (1.2.3.4/24, DHCP)) [DHCP]: 10.66.103.177/24
defaultrouter (IP or NO for DHCP (1.2.3.4, NO)) [NO]: 10.66.103.254
hostname (Host name of this VM (zadp)) [zadp]:
Network configuration has been changed, restart network, please wait...
Network changes has been successfully applied.
Checking network connection by pinging zscaler.com.
Successful pinging zscaler.com, network looks running fine.
Syncing system date and time, please wait...
Syncing system date and time has been completed.
[zsroot@zadp ~]$ 
```

Figure 15. Zscaler Index Tool – System Network Configuration

6. Return to the ZIA Admin Portal and go to **Administration** > **Index Tool**.
7. Locate the Index Tool Configuration you added previously, and under the **SSL Certificate** column, click **Download**.



No.	VM name	Status	SSL Certificate
1	Index Tool 1	Enabled	Download

Figure 16. SSL Certificate

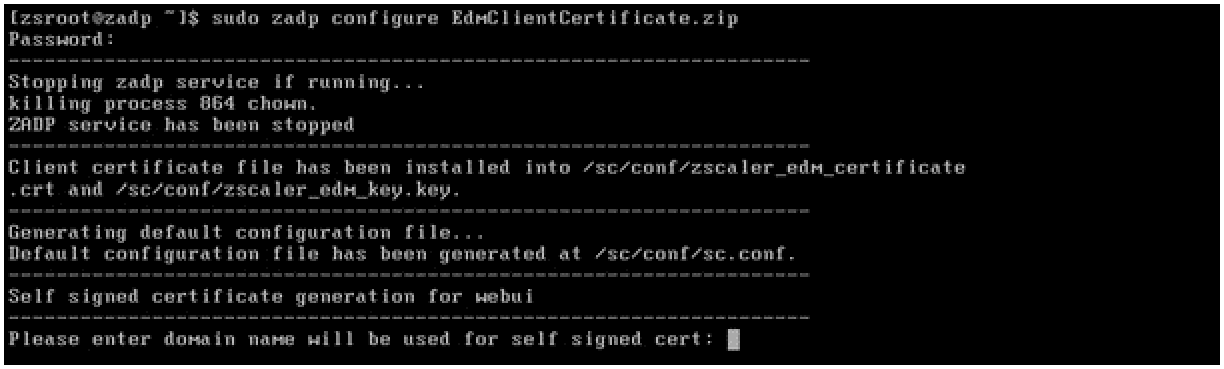
8. Copy the SSL client certificate.zip file to the VM and install it:
   a. This example uses `scp` to copy the file (for example, `scp EdmClientCertificate.zip zsroot@10.66.108.100:~/`):

   ```
   scp <SSL_certificate_zip_filename> zsroot@<vm_ip>:~/
   ```

   b. Enter the following command to install the SSL certificate (for example, `sudo zadp configure EdmClientCertificate.zip`):

   ```
   sudo zadp configure <SSL_certificate_zip_filename>
   ```

   c. Enter the domain name used for the Index Tool's fully qualified domain name (FQDN). For example, if the Index Tool is reachable from indextool.mycompany.com, then the domain name entered here would be `mycompany.com`. The self-signed certificate is generated for *.mycompany.com.



```
[zsroot@zadp ~]$ sudo zadp configure EdmClientCertificate.zip
Password:
--------------------------------------------------------------------------
Stopping zadp service if running...
killing process 864 chown.
ZADP service has been stopped
--------------------------------------------------------------------------
Client certificate file has been installed into /sc/conf/zscaler_edm_certificate
.crt and /sc/conf/zscaler_edm_key.key.
--------------------------------------------------------------------------
Generating default configuration file...
Default configuration file has been generated at /sc/conf/sc.conf.
--------------------------------------------------------------------------
Self signed certificate generation for webui
--------------------------------------------------------------------------
Please enter domain name will be used for self signed cert: █
```

Figure 17. Zscaler Index Tool – Install SSL Certificate

d. Enter a passphrase, then re-enter the passphrase to confirm it. You are prompted to enter the full path name to the text file where the passphrase is stored. You can also press `Enter` twice to accept the default location and file `/home/zsroot/zscaler_zadp_webui_certificate_pass.txt`.

   If the service was configured properly, the service:

   - Checks if the network is configured correctly.
   - Installs the SSL client certificate you specified.
   - Generates a self-signed SSL server certificate.
   - Downloads the latest install package.
   - Starts the service.

9. (Optional) If you need to install a self-signed or custom SSL server certificate:

   a. Enter the following command to install the server certificate:

   ```
   sudo zadp install-server-cert
   ```

   b. Type the full path to the PEM-formatted certificate file.

   c. Enter the following command to restart the Index Tool service:

   ```
   sudo zadp restart
   ```

Go to `https://<IP Address of the Index Tool VM>` to access the Index Tool. After the Index Tool service has started, you can log in with your ZIA Admin Portal login credentials and create Index Templates to use when creating DLP dictionaries.

To learn more, see Creating an Exact Data Match Template and Creating an Indexed Document Match Template (government agencies, see Creating an Exact Data Match Template and Creating an Indexed Document Match Template).

Updating the Index Tool VM

If you successfully configured the Index Tool, the service automatically downloads the latest install package before it starts. To manually update the service:

1. Enter the following command to stop the service:

   ```
   sudo zadp stop
   ```

2. Enter the following command to install the update:

   ```
   sudo zadp update-now
   ```

3. Enter the following command to start the service:

   ```
   sudo zadp start
   ```

Running the Index Tool VM in Explicit Proxy Mode

You can run the tool in explicit proxy mode. To do this:

1. Log in to the VM as user `zsroot`.
2. Enter the following command:

   ```
   sudo zadp configure-network
   ```

3. For **Do you require a proxy server configuration?**, enter `y` and press `Enter`.
4. For **proxyserver**, enter the IP address of your proxy server (e.g., `proxy.zscaler.net`) and press `Enter`.
5. For **proxyport**, enter your proxy port number (e.g., `9443`) and press `Enter`. The VM then tests the connection and when this is successful, the configuration is complete.

To remove the explicit proxy configuration:

1. Enter the following command:

   ```
   sudo zadp configure-network
   ```

2. For **Do you require proxy server configuration?**, enter `n` and press `Enter`.
3. For **Do you want to delete current proxy configuration?**, enter `y` and press `Enter`.

Requirements for Explicit Proxy Mode

If you're using explicit proxy mode, DNS and NTP connections are not tunneled. You need an internal DNS server to run in this mode. The Index Tool needs to have DNS resolution for the current Zscaler Central Authority (CA) IP, update server, and the NTP server. The Index Tool host also needs to query a DNS server to resolve the following settings:

- smcacluster.<Zscaler Cloud Name>
- update1.<Zscaler Cloud Name>
- update2.<Zscaler Cloud Name>
- zdistribute.<Zscaler Cloud Name>
- The NTP server. By default, the Index Tool VM has the following FQDNs for NTP servers configured:
  - 0.freebsd.pool.ntp.org
  - 1.freebsd.pool.ntp.org
  - 2.freebsd.pool.ntp.org

You can override these FQDNs to your internal IP address in your DNS server configuration or using other methods.

In addition, since the proxy configuration doesn't allow authentication, you must configure the proxy server to allow specific IP/MAC addresses without user and password authentication.

The proxy server must also allow SSL bypass for communication from the VM to a specific set of IP addresses. These IPs are listed at `config.zscaler.com/<Zscaler Cloud Name>.net/edm`. You can find your cloud name in the URL that your admins use to log in to the Zscaler service. For example, if an organization logs in to admin.zscalertwo.net, then that organization's cloud name is zscalertwo. You would go to `config.zscaler.com/zscalertwo.net`. To learn more, see What Is My Cloud Name for ZIA (government agencies, see What Is My Cloud Name for ZIA).

Index Tool VM Commands

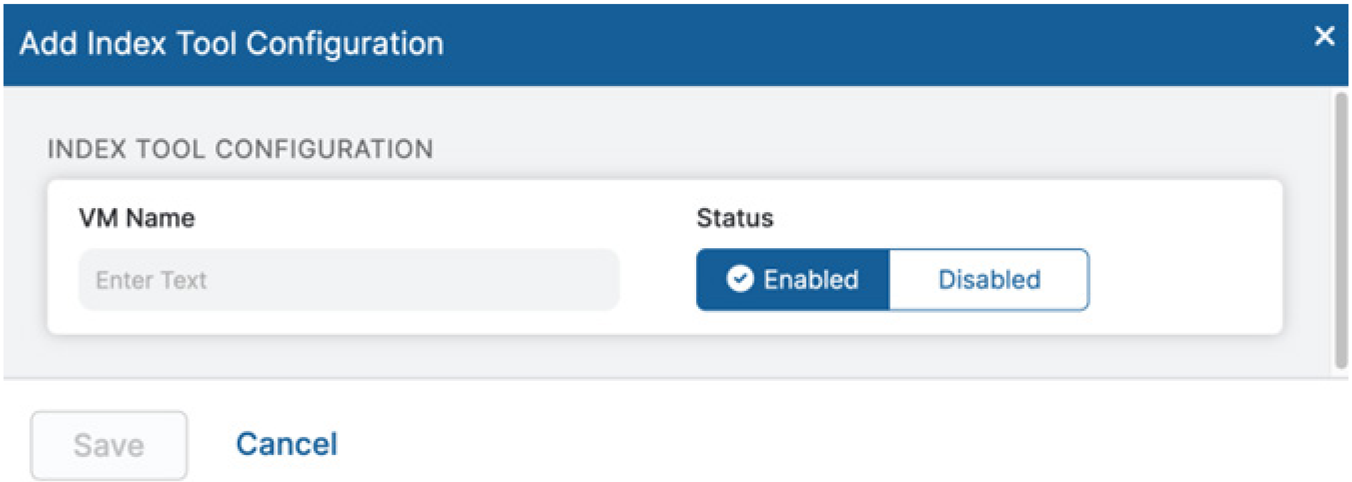
You can enter the following commands to configure, update, and troubleshoot your VM.

Command	Description
`sudo zadp stop`	Stops the Index Tool service.
`sudo zadp start`	Starts the Index Tool service.
`sudo zadp restart`	Restarts the Index Tool service.
`sudo zadp status`	Displays whether the Index Tool service is running or stopped.
`sudo zadp update-now`	Updates the Index Tool service. The service must be stopped before you can run this command.
`sudo zadp force-update-now`	Forces the Index Tool service to update to the latest version regardless of what version is on the VM. The service is automatically stopped before the update begins.
`sudo zadp troubleshoot`	Runs a series of checks to help troubleshoot issues, such as checking the installed certificates, the cloud server configuration, all services, and whether or not an update is needed.

Adding an Index Tool Configuration

To add an Index Tool Configuration:

1. Go to **Administration** > **Index Tool**.
2. Click **Add Index Tool Configuration**. The **Add Index Tool Configuration** window is displayed.
3. In the **Add Index Tool Configuration** window:
   a. **VM Name**: Enter a unique name for the virtual machine (VM).
   b. **Status**: Make sure that the VM is **Enabled**.



Add Index Tool Configuration

INDEX TOOL CONFIGURATION

VM Name: Enter Text

Status: Enabled

Figure 18. Zscaler Index Tool – Index Tool

4. Click **Save** and activate the change (government agencies, see activate the change).

After you save the SSL Certificate for the configuration, you can download it from the Index Tool page or from the Edit Index Tool Configuration window.

Creating an Indexed Document Match Template

Using the Index Tool, you can create, modify, or delete an Indexed Document Match (IDM) index template.

You can create up to 64 IDM templates for your organization. The largest file you can upload to an IDM template is 400 MB. You can index up to 100 GB of files for your organization.

The Zscaler Indexer supports SSH-based protocols only, it does not support SMB or NFS mounts.

Creating an IDM Template

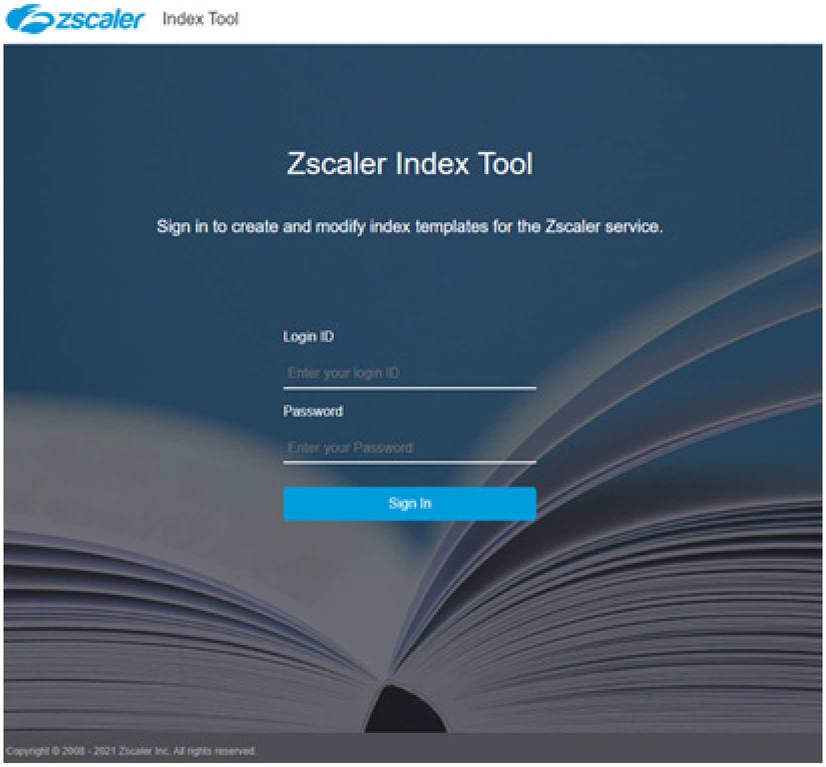
You can create manual or scheduled IDM templates.

The integration with Rubrik platform is focused on Scheduled IDM Templates and does not support the Manual IDM Template method.

- Scheduled IDM Templates: A scheduled IDM template allows you to set up an SSH connection and schedule updates between the template and your organization's storage server for the critical documents.
- Manual IDM Templates: A manual IDM template allows you to manually upload your organization's critical documents.

To create a Scheduled IDM template:

1. Go to `https://<IP Address of the Index Tool VM>` to access the Index Tool. Log in to the Index Tool with your ZIA Admin Portal login credentials.



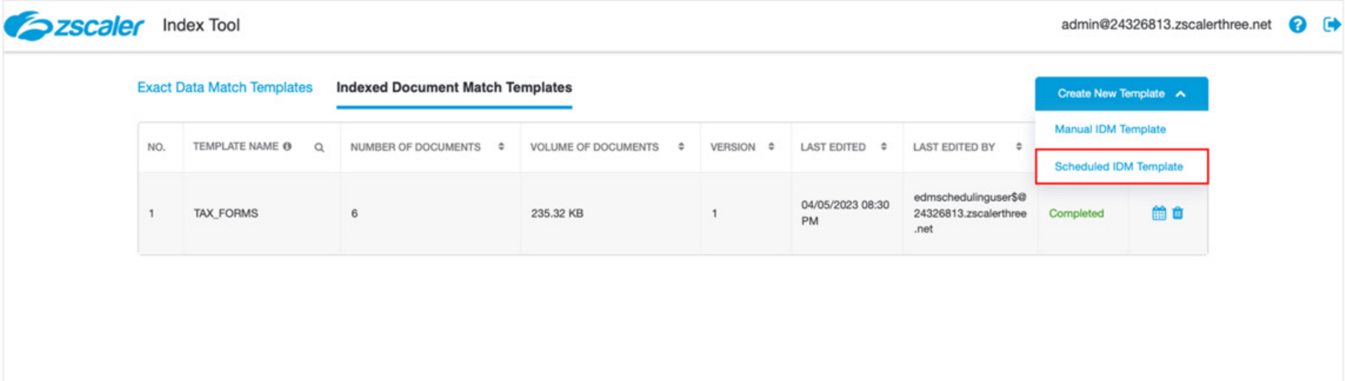
Zscaler Index Tool

Sign in to create and modify index templates for the Zscaler service.

Copyright © 2008 - 2021 Zscaler Inc. All rights reserved.

Figure 19. Login to Index Tool - WebUI

2. Click **Indexed Document Match Templates**.
3. In the **Indexed Document Match Templates** dashboard, click **Create New Template** and then select **Scheduled IDM Template**.



Index Tool

admin@24326813.zscalerthree.net

Exact Data Match Templates | Indexed Document Match Templates

Create New Template
- Manual IDM Template
- Scheduled IDM Template

NO.	TEMPLATE NAME	NUMBER OF DOCUMENTS	VOLUME OF DOCUMENTS	VERSION	LAST EDITED	LAST EDITED BY		
1	TAX_FORMS	6	235.32 KB	1	04/05/2023 08:30 PM	edmschedulinguser$@24326813.zscalerthree.net	Completed	

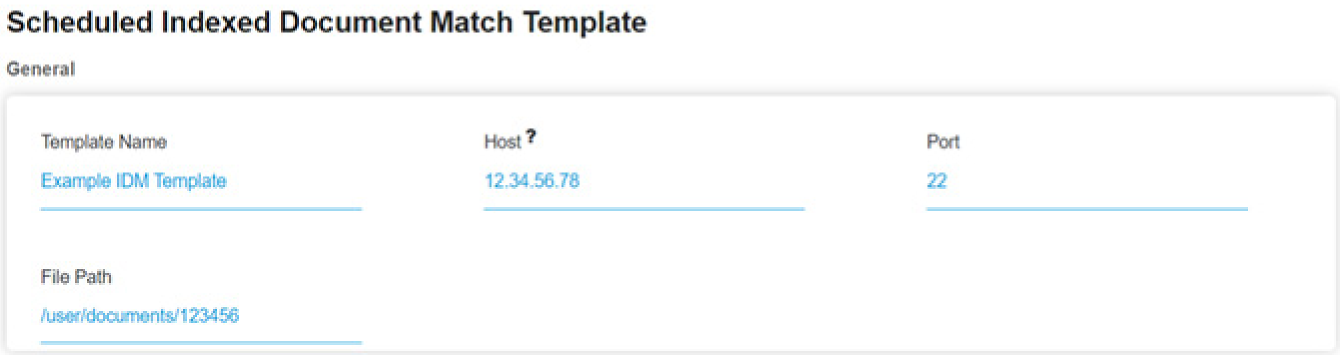
Figure 20. Scheduled IDM Template

Creating a Scheduled IDM Template

When you create a scheduled IDM template, you must set up an SSH connection between the template and your organization's document server. You must then schedule regular updates between the template and server.

In the Scheduled Indexed Document Match Template window:

1. Under **General**:
   a. Enter a **Template Name**. After the template is saved, this name appears in the Indexed Document Match page in the ZIA Admin Portal.
   b. For **Host**, enter the IP address or domain for the document server.
   c. Specify the **Port** for the document server.
   d. Specify the **File Path** for the directory where the documents are located in the document server.



Scheduled Indexed Document Match Template

General

Template Name: Example IDM Template

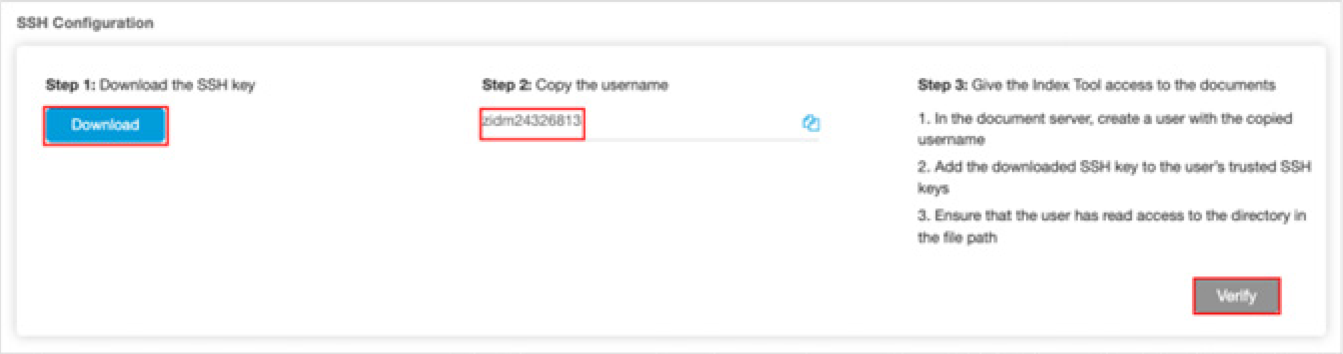
Host: 12.34.56.78

Port: 22

File Path: /user/documents/123456

Figure 21. Configure Scheduled Indexed Document Match Template

2. Under **SSH Configuration**:
   a. Click **Download** to download the SSH key.
   b. Copy the username. Use this username to create a user in your document server.
   c. Go to your document server and complete the following steps:
      i. Create a user with the username you copied from the Index Tool.
      ii. Add the downloaded SSH key to the user's trusted keys.
      iii. Ensure that the user has read access to the directory in the specified file path.
   d. Click **Verify** in the template to verify the SSH setup configuration. You cannot save the template until the setup is configured properly and verified.



SSH Configuration

Step 1: Download the SSH key

Step 2: Copy the username

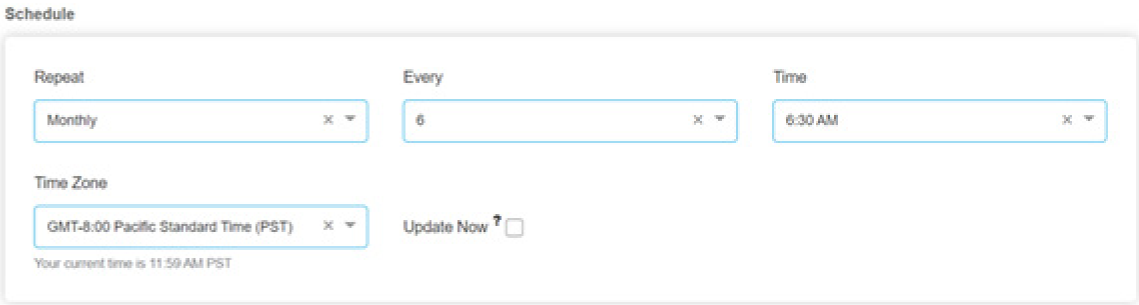
zidm24326813

Step 3: Give the Index Tool access to the documents

1. In the document server, create a user with the copied username
2. Add the downloaded SSH key to the user's trusted SSH keys
3. Ensure that the user has read access to the directory in the file path

Figure 22. SSH Configuration

3. Under **Schedule**:
   a. **Repeat**: Choose if the update repeats **Monthly**, **Weekly**, or **Daily**.
   b. **Every**: If you selected **Monthly** or **Weekly**, choose when in the selected period the update repeats. For example, if you selected Weekly, you can choose to have the update happen every Friday.
   c. **Time**: Select the time the schedule update happens.
   d. **Time Zone**: Select the time zone your update happens.
   e. **Update Now**: Select to immediately update the template.



Schedule

Repeat: Monthly

Every: 6

Time: 6:30 AM

Time Zone: GMT-8:00 Pacific Standard Time (PST)

Your current time is 11:59 AM PST

Update Now ? □

Figure 23. Configure Schedule

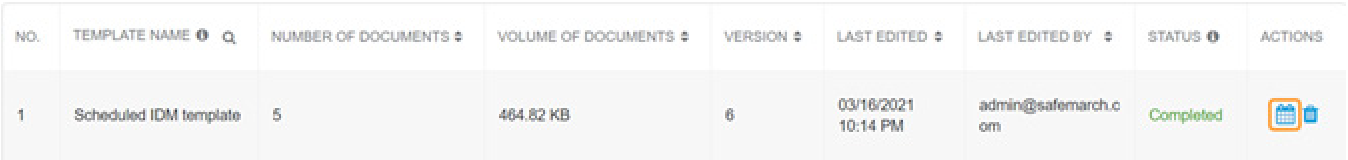
4. (Optional) Enter a **Description** for the template.
5. Click **Save**.

After saving the template, you are redirected to the **Indexed Document Match Template** dashboard, and the tool processes the template. If the template was created properly, `Completed` is shown in the **Status** column. If the template was created, but the documents weren't indexed yet, then `Created` is shown. If the template was not created properly, then `Error` is shown.

After an IDM template is created, it appears on the Indexed Document Match (government agencies, see Indexed Document Match) page of the ZIA Admin Portal, where you can view the template's details or delete it. You cannot change the template name after creation. To change the name, you must create a new template.

Modifying an IDM Template

To submit new documents or delete indexed documents for scheduled IDM templates, you must make the changes in the document server. The template updates at the scheduled time, or you can schedule an immediate update for the template in the Index Tool. To reschedule a scheduled template's update, click the **Calendar** icon in the **Actions** column.



NO.	TEMPLATE NAME	NUMBER OF DOCUMENTS	VOLUME OF DOCUMENTS	VERSION	LAST EDITED	LAST EDITED BY	STATUS	ACTIONS
1	Scheduled IDM template	5	464.82 KB	6	03/16/2021 10:14 PM	admin@safemarch.com	Completed	

Figure 24. Reschedule a scheduled template

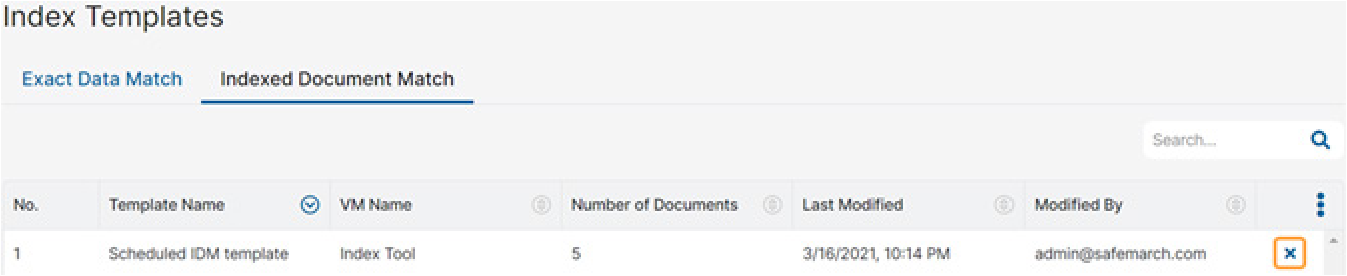
Deleting an IDM Template

To delete a scheduled IDM template:

1. Log in to the Index Tool.
2. In the **Indexed Document Match Templates** dashboard, locate the template you want to remove. In the **Template Name** column, you can click the **Search** icon to search for a specific template.
3. In the **Actions** column, click the **Delete** icon.
4. In the confirmation window that appears, click **Delete**.

You can also delete the IDM template from the ZIA Admin Portal:

1. Go to **Administration** > **Index Templates**.
2. In the **Indexed Document Match** tab, locate the template you want to remove.
3. Click **Delete**.



Index Templates

No.	Template Name	VM Name	Number of Documents	Last Modified	Modified By	
1	Scheduled IDM template	Index Tool	5	3/16/2021, 10:14 PM	admin@safemarch.com	✕

Figure 25. Index Templates

4. Click **OK**.

Defining IDM Match Accuracy for Custom DLP Dictionaries

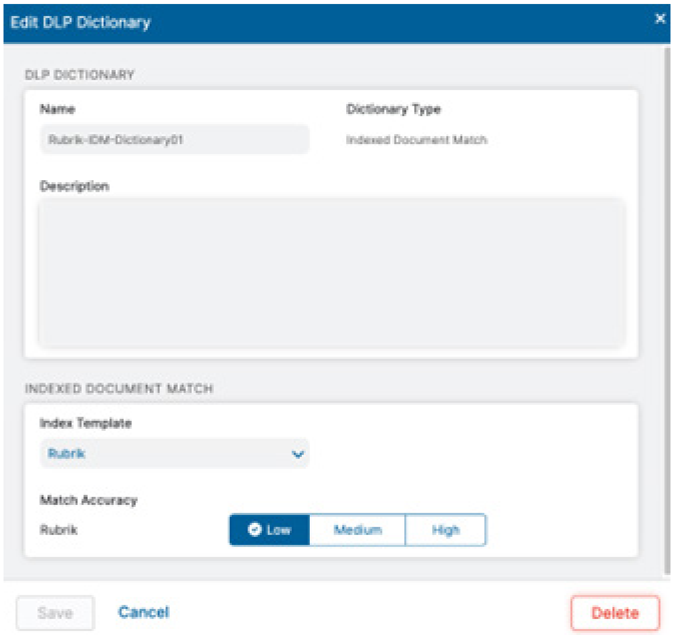
You can add Indexed Document Match (IDM) templates to custom DLP dictionaries that represent critical documents that you want to protect in your organization. When adding an IDM template, you must also choose the match accuracy level for the template in the dictionary. To learn more, see Creating an Indexed Document Match Template and Adding Custom DLP Dictionaries (government agencies, see Creating an Indexed Document Match Template and Adding Custom DLP Dictionaries).

To add an IDM template:

1. Go to **Administration** > **DLP Dictionaries & Engines**.
2. In the **DLP Dictionaries** tab, click **Add DLP Dictionary** or click the **Edit** icon for an existing dictionary. The **Add/Edit DLP Dictionary** window appears.

3. In the **Add/Edit DLP Dictionary** window:
    a. From **Dictionary Type**, choose **Indexed Document Match**.
    b. From the **Index Template**, select the IDM templates you want to use for the dictionary.
    c. Choose the **Match Accuracy** for the IDM templates you selected. This is the level of accuracy (i.e., the percentage of similarity) that a user-uploaded document must meet to count as a match for an indexed document.

        - **Low**: Zscaler detects a low-accuracy match when one of the following occurs:
            - A user-uploaded document matches at least 40% of an indexed document.
            - An indexed document matches at least 70% of a user-uploaded document.
        - **Medium**: Zscaler detects a medium-accuracy match when one of the following occurs:
            - A user-uploaded document matches at least 70% of an indexed document.
            - An indexed document matches at least 90% of a user-uploaded document.
        - **High**: Zscaler detects a high-accuracy match when a user-uploaded document matches at least 90% of an indexed document.



Edit DLP Dictionary

DLP DICTIONARY

Name: Rubrik-IDM-Dictionary01

Dictionary Type: Indexed Document Match

Description:

INDEXED DOCUMENT MATCH

Index Template: Rubrik

Match Accuracy

Rubrik: ● Low | Medium | High

Figure 26. DLP Dictionary

4. Click **Save** and activate the change (government agencies, see activate the change).

Understanding DLP Engine

A DLP engine is a collection of one or more DLP dictionaries. The Zscaler service provides predefined DLP engines and supports custom DLP engines:

- Predefined DLP Engines: The Zscaler service provides five predefined engines (HIPAA, GLBA, PCI, Offensive Language, and Self-Harm & Cyberbullying). These engines contain default DLP dictionaries. For example, the PCI engine contains the Credit Cards and Social Security Number dictionaries. You can also edit predefined engines. To learn more, see Editing Predefined DLP Engines (government agencies, see Editing Predefined DLP Engines).

  The Rubrik data protection integration leverages both Zscaler's Custom DLP Dictionary in combination with Custom DLP Dictionaries.

- Custom DLP Engines: You can create custom DLP engines to detect content that is relevant to your organization. You can create a maximum of 47 custom DLP engines. To learn more, see Adding Custom DLP Engines (government agencies, see Adding Custom DLP Engines).

Adding Custom DLP Engines

Adding a custom DLP engine is one of the tasks you can complete when configuring DLP policy rules (government agencies, see DLP policy rules). To learn more about the ranges and limitations for custom DLP engines, see Ranges & Limitations (government agencies, see Ranges & Limitations).

To add a custom DLP engine:

1. Go to **Administration** > **DLP Dictionaries & Engines**.
2. In the **DLP Engines** tab, click **Add DLP Engine**. The **Add DLP Engine** window is displayed.
3. In the **Add DLP Engine** window, enter the **Name** for the custom DLP engine.
4. For **Engine Builder**, add operators and DLP dictionaries to build an expression (government agencies, see build an expression). You can see your expression in the **Expression Preview**.

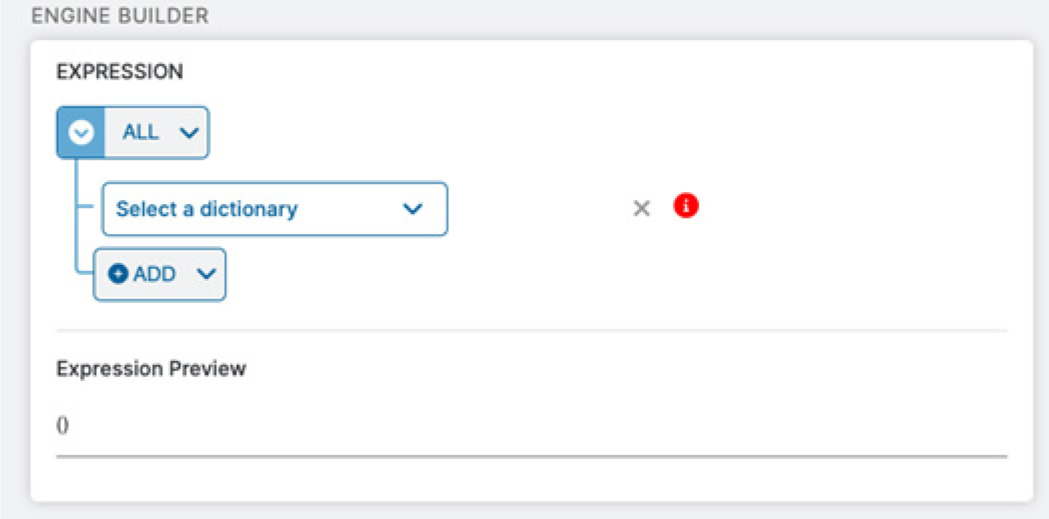
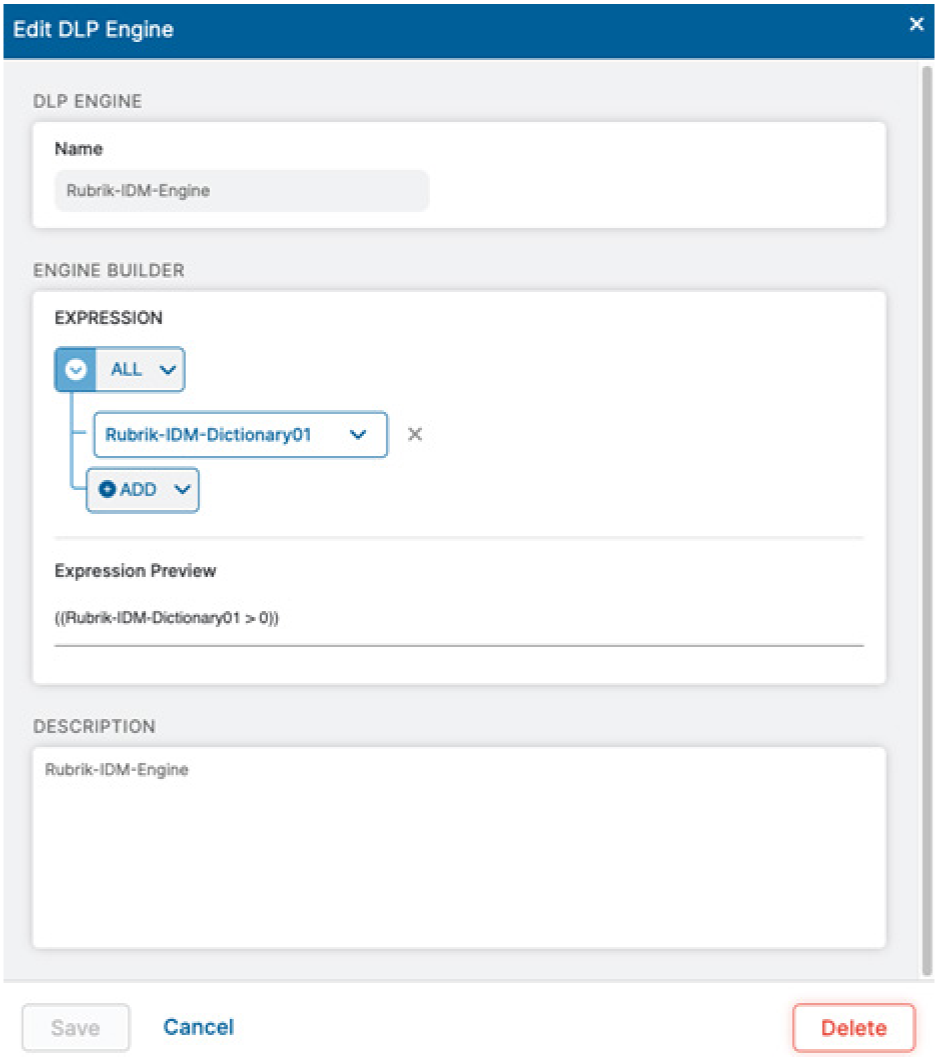


Figure 27. DLP Engine

5. Under **Expression**:
    a. Click **Add** to add a **Dictionary** or a **Subexpression**. Click the **Remove** icon (X) to delete dictionaries or subexpressions. If you click **Dictionary**, you must select the custom DLP dictionary that contains the Index template associated with the Rubrik tenant. Certain dictionaries require you to set a value for the match count (government agencies, see match count). You can enter any value less than 1,000.



Edit DLP Engine

DLP ENGINE

Name: Rubrik-IDM-Engine

ENGINE BUILDER

EXPRESSION

ALL

Rubrik-IDM-Dictionary01

Expression Preview

((Rubrik-IDM-Dictionary01 > 0))

DESCRIPTION

Rubrik-IDM-Engine

Figure 28. Rubrik Indexed DLP Engine

For the root subexpression, only the All (AND) and Any (OR) operators are allowed.

    b. Continue adding dictionaries and operators to the expression as needed. At each level, you can create up to 4 subexpressions, use up to 4 operators, and add up to 16 dictionaries per operator.

6. (Optional) For the **Description**, enter any additional notes or information. The description cannot exceed 255 characters.
7. Click **Save** and activate the change (government agencies, see activate the change).

Configuring DLP Policy Rules with Content Inspection

You can use Zscaler's DLP engines to detect data, allow, or block transactions, and notify your organization's auditor when a user's transaction triggers a DLP rule. If your organization has a third-party DLP solution, Zscaler can forward information about transactions that trigger DLP policy to your third-party solution via secure Internet Content Adaptation Protocol (ICAP). However, Zscaler does not take ICAP responses from your DLP solution.

Zscaler only monitors or blocks content according to the policy you configure, then forwards information about transactions so that your organization can take necessary remediation steps.

> The Zscaler DLP engines support files up to 400 MB and can scan the first 100 MB of the extracted text. The maximum size also applies to files extracted from archive files.

To configure a DLP policy rule with content inspection make sure you have completed the previous steps:

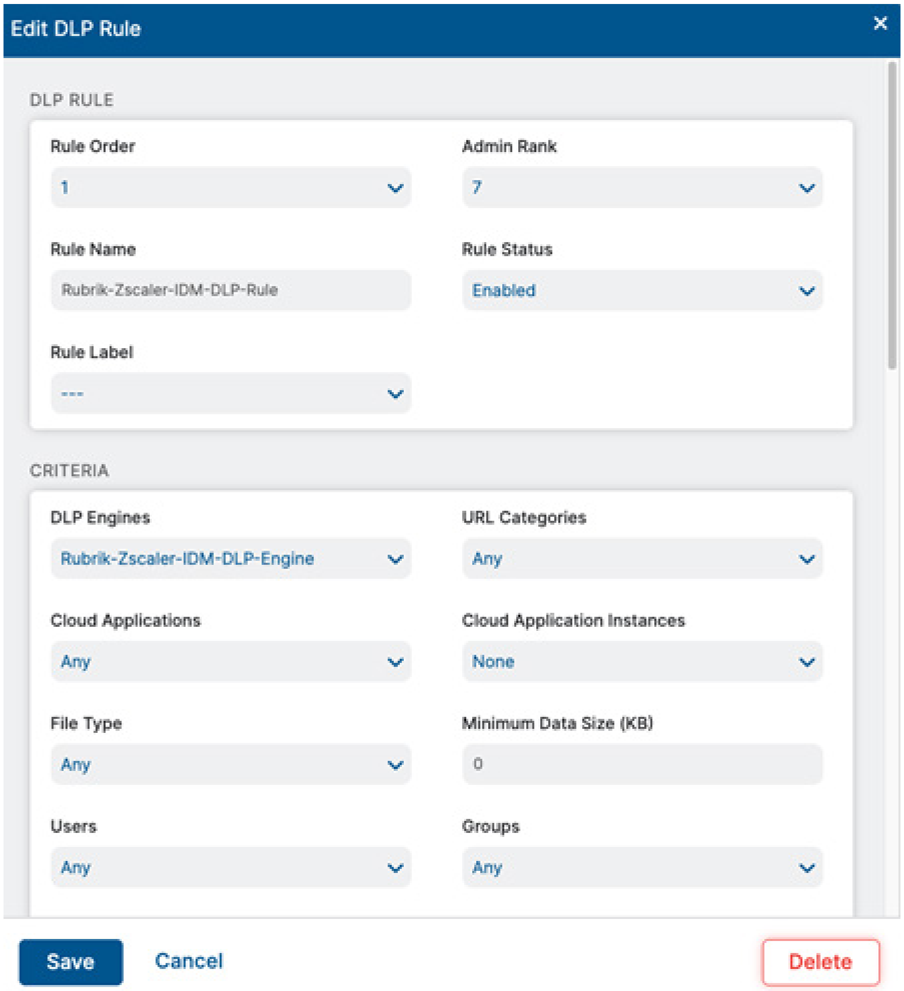
- Defining IDM Match Accuracy for Custom DLP Dictionaries
- Adding Custom DLP Engines

Defining DLP Inline Policy Rules

To create a DLP inline policy to inspect traffic matching the DLP engine associated with the DLP Dictionary containing the Indexed Documents delivered by Rubrik:

1. Go to **Policy** > **Data Loss Prevention**.
2. Click **Add** and select **Rule With Content Inspection**.

3. In the **Add DLP Rule** window, enter the following DLP Rule attributes:
   a. **Rule Order**: Policy rules are evaluated in ascending numerical order (Rule 1 before Rule 2, etc.), and the Rule Order reflects this rule's place in the order. You can change the value, but if you've enabled Admin Ranking, then the assigned **Admin Rank** determines the Rule Order values you can select.
   b. **Admin Rank**: Enter a value from 0–7 (0 is the highest rank). Your assigned admin rank determines the values you can select. You cannot select a rank that is higher than your own. The rule's Admin Rank determines the value you can select in Rule Order, so that a rule with a higher Admin Rank always precedes a rule with a lower Admin Rank.
   c. **Rule Name**: Enter a unique name for the DLP rule or use the default name.
   d. **Rule Status**: An enabled rule is actively enforced. A disabled rule is not actively enforced but does not lose its place in the Rule Order, the service skips it and moves to the next rule.
   e. **Rule Label**: Select a rule label to associate it with the rule.
   f. **DLP Engines**: Select the Rubrik DLP Engine created in the section Adding Custom DLP Engines.



Rule Order: 1
Admin Rank: 7
Rule Name: Rubrik-Zscaler-IDM-DLP-Rule
Rule Status: Enabled
Rule Label: ---

DLP Engines: Rubrik-Zscaler-IDM-DLP-Engine
URL Categories: Any
Cloud Applications: Any
Cloud Application Instances: None
File Type: Any
Minimum Data Size (KB): 0
Users: Any
Groups: Any

Figure 29. DLP Inline Policy

You can choose up to 4 DLP Engines per inline policy.

If your organization requires notification alerts sent to an auditor's mailbox or other automated system for analysis or Incident creation, you can configure an email notification for the rule.

If you do not select an auditor and notification template, a notification is not sent for this rule.

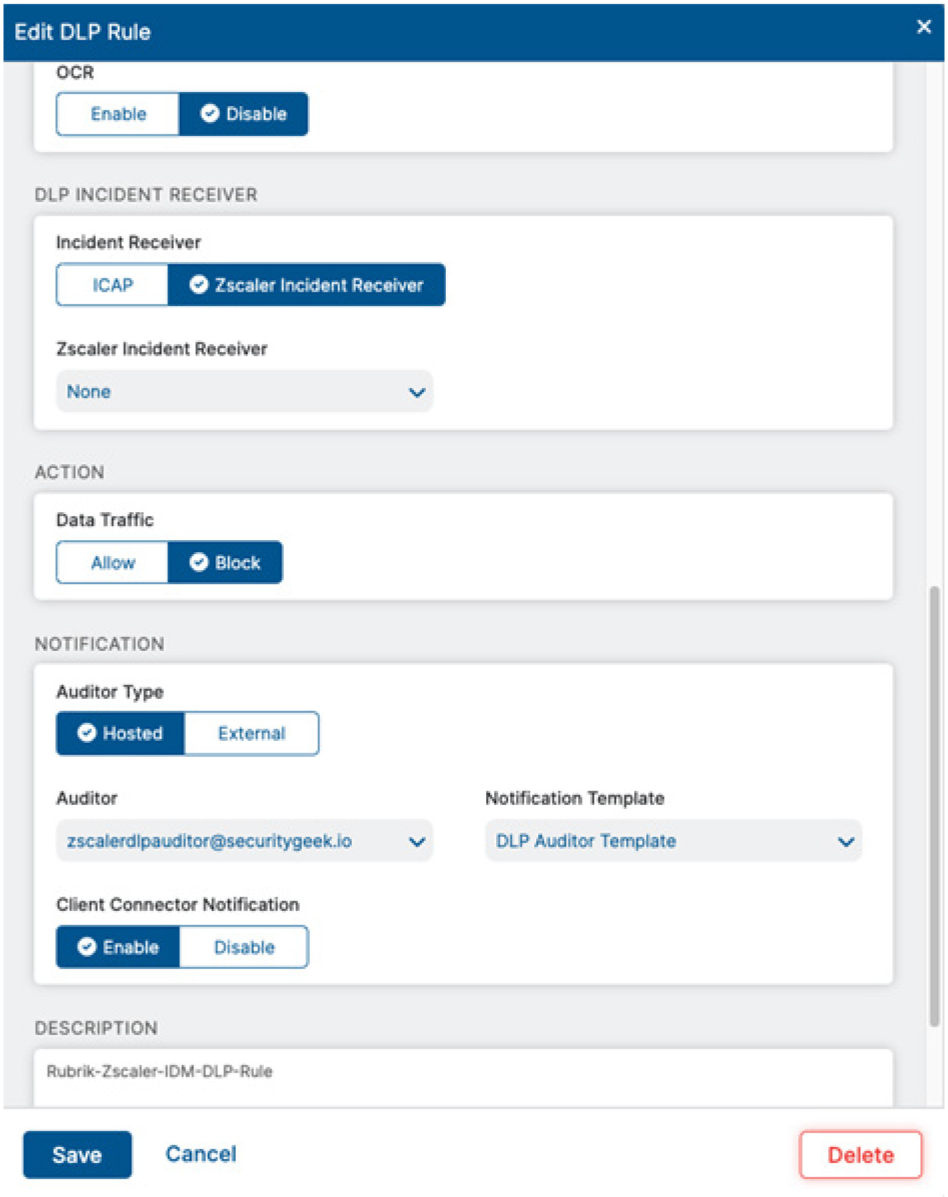
4. For **Auditor Type**, select whether the auditor is from a **Hosted** database or is **External** to your organization.
5. Select the **Auditor**:
    a. If the auditor is from a hosted database, select or search for the auditor.
    b. If the auditor is external, enter the auditor's email address.
    c. Select a **Notification Template** if you configure one. To learn more, see Configuring DLP Notification Templates (government agencies, see Configuring DLP Notification Templates). You can also search for a notification template or click the **Add** icon to add a new notification template.
    d. **OCR**: Enable this option to allow Zscaler's DLP engines to scan images in files. If this option is disabled, the DLP rule doesn't apply to image files.

To enable this option for your organization, contact your Zscaler Account team.

    e. **Inspect Downloads**: Enable this option to allow DLP inspection for content downloaded from specific cloud apps. If this option is enabled, you must also choose **Any** for **URL Categories** and at least one cloud app for **Cloud Application**. If disabled, the DLP rule only applies to content being sent to cloud apps.

6. (Optional) For **DLP Incident Receiver**, complete one of the following tasks:
    a. If you don't have a third-party DLP solution or don't want to forward content, leave the **Zscaler Incident Receiver** or **ICAP Receiver** field as **None**.
    b. If you want to forward the transactions captured by this policy rule to an on-premises DLP incident receiver:
        - For **Incident Receiver**, select whether the DLP incident receiver is an ICAP receiver or a Zscaler Incident Receiver.
        - Select the applicable **ICAP Receiver** or **Zscaler Incident Receiver** from the drop-down menu. You must configure your ICAP receivers or Zscaler Incident Receivers (government agencies, see ICAP receivers or Zscaler Incident Receivers) in order to complete this step.

7. Select the **Action** for the rule. You can **Allow** or **Block** transactions that match the rule. If you select **Allow**, the service allows and logs the transaction. If you select **Block**, the service blocks and logs the transaction.
8. (Optional) Configure **Client Connector Notification**. You can **Enable** or **Disable** Client Connector notifications for the rule when violations occur. The field is only available if you enable the **Web DLP Violations** option for your organization on the **End User Notifications** page in the ZIA Admin Portal and you select the **Action** as **Block** for the rule. To learn more, see Understanding Browser-Based End User Notifications (government agencies, see Understanding Browser-Based End User Notifications)
9. Click **Save** and activate the change (government agencies, see activate the change).



Edit DLP Rule

OCR: Enable | ☑ Disable

DLP INCIDENT RECEIVER

Incident Receiver: ICAP | ☑ Zscaler Incident Receiver

Zscaler Incident Receiver: None

ACTION

Data Traffic: Allow | ☑ Block

NOTIFICATION

Auditor Type: ☑ Hosted | External

Auditor: zscalerdlpauditor@securitygeek.io

Notification Template: DLP Auditor Template

Client Connector Notification: ☑ Enable | Disable

DESCRIPTION

Rubrik-Zscaler-IDM-DLP-Rule

Figure 30. DLP Inline Policy

For example, if a policy rule using predefined Zscaler DLP engines is configured (as shown in the following image), the Zscaler service blocks all the files that:

- Contain medical information
- Are over 1,000 KB in size
- Are being sent by users in the Operations group through Gmail

The Zscaler service sends an email notification regarding the policy violation to your organization's auditor but doesn't forward information to an incident receiver.

Analyzing Zscaler DLP Engine Logs

After the Zscaler DLP Inline policy is enabled, the Zscaler engines are triggered any time a violation is identified.

To visualize the DLP inline policy logs:

1. Go to **Analytics** > **Web Insights**.

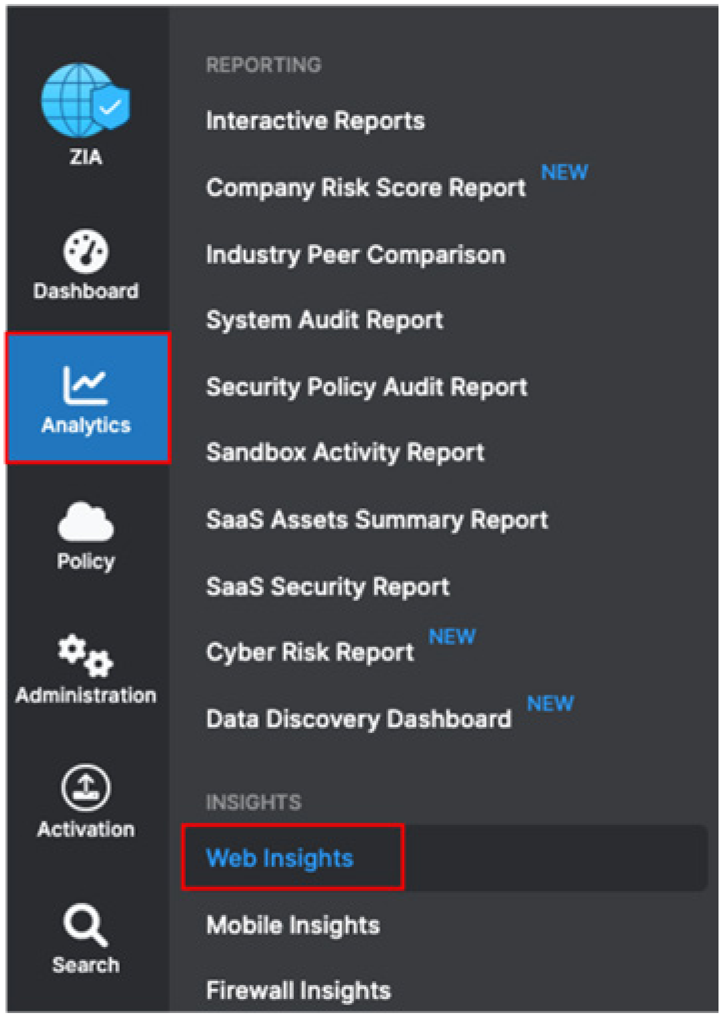
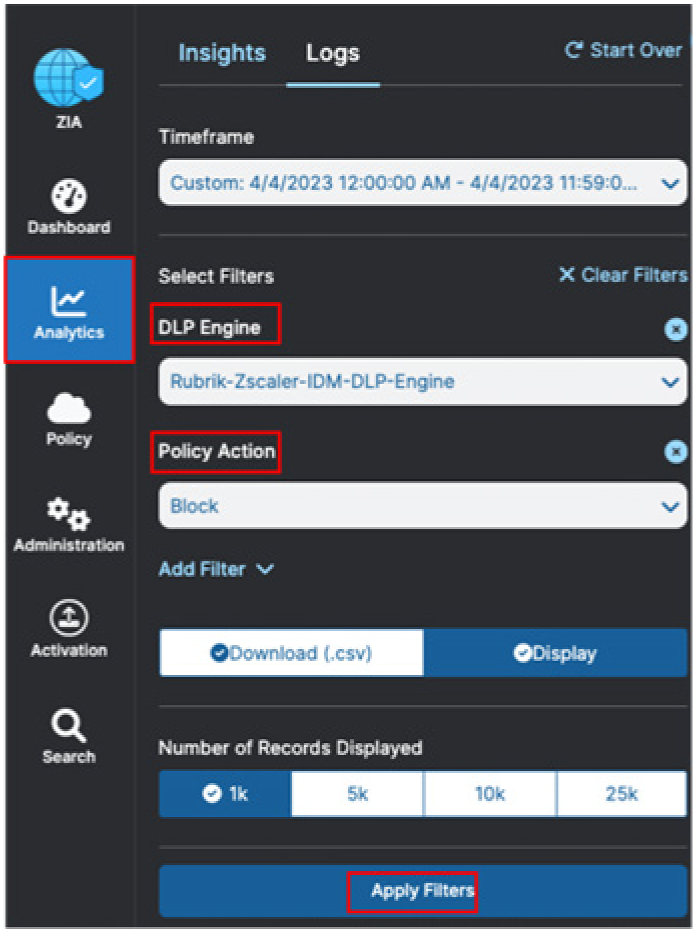


Figure 31. ZIA Web Insights

2. Filter the logs based on the specific DLP engines (i.e., **Rubrik-Zscaler-IDM-DLP-Engine**):
   a. Select the **Timeframe** for which to filter logs.
   b. Choose **Select Filters**.
   c. Select **DLP Engine**.
   d. Select the **DLP Engine** name created in the previous sections (e.g., **Rubrik-Zscaler-IDM-DLP-Engine**).
   e. Select **Add Filter** again.
   f. Select **Policy Action**.
   g. Select **Block**.
   h. Select **Apply Filters**.


Timeframe: Custom: 4/4/2023 12:00:00 AM - 4/4/2023 11:59:0...

Select Filters

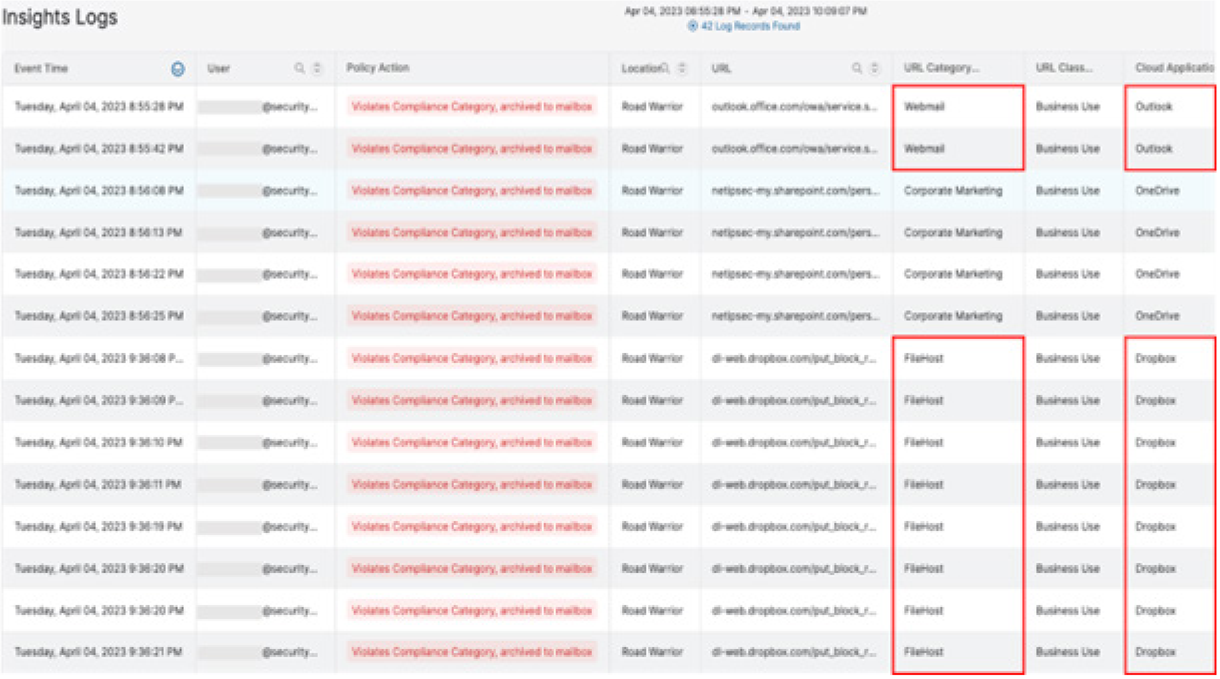
DLP Engine: Rubrik-Zscaler-IDM-DLP-Engine

Policy Action: Block

Number of Records Displayed: ● 1k

Figure 32. ZIA Log Filter

With the log filters applied, ZIA lists all the logs matching the selected criteria. If one or more violations is detected, it displays several types of information related to the violation such as: User, Policy Action, URL Category, Cloud Application.



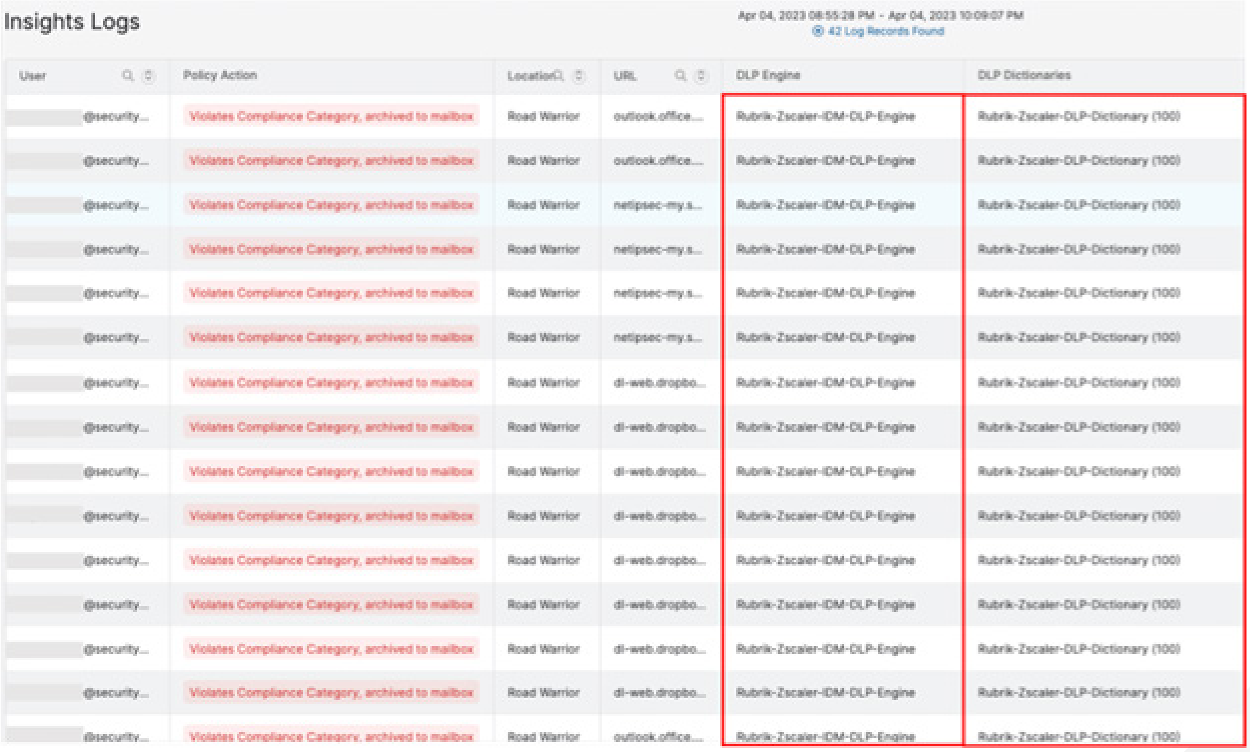
Insights Logs

Apr 04, 2023 08:55:28 PM - Apr 04, 2023 10:09:07 PM
42 Log Records Found

Event Time	User	Policy Action	Location	URL	URL Category...	URL Class...	Cloud Applicatio
Tuesday, April 04, 2023 8:55:28 PM	[redacted]@security...	Violates Compliance Category, archived to mailbox	Road Warrior	outlook.office.com/owa/service.s...	Webmail	Business Use	Outlook
Tuesday, April 04, 2023 8:55:42 PM	[redacted]@security...	Violates Compliance Category, archived to mailbox	Road Warrior	outlook.office.com/owa/service.s...	Webmail	Business Use	Outlook
Tuesday, April 04, 2023 8:56:08 PM	[redacted]@security...	Violates Compliance Category, archived to mailbox	Road Warrior	netipsec-my.sharepoint.com/pers...	Corporate Marketing	Business Use	OneDrive
Tuesday, April 04, 2023 8:56:13 PM	[redacted]@security...	Violates Compliance Category, archived to mailbox	Road Warrior	netipsec-my.sharepoint.com/pers...	Corporate Marketing	Business Use	OneDrive
Tuesday, April 04, 2023 8:56:22 PM	[redacted]@security...	Violates Compliance Category, archived to mailbox	Road Warrior	netipsec-my.sharepoint.com/pers...	Corporate Marketing	Business Use	OneDrive
Tuesday, April 04, 2023 8:56:25 PM	[redacted]@security...	Violates Compliance Category, archived to mailbox	Road Warrior	netipsec-my.sharepoint.com/pers...	Corporate Marketing	Business Use	OneDrive
Tuesday, April 04, 2023 9:36:08 P...	[redacted]@security...	Violates Compliance Category, archived to mailbox	Road Warrior	dl-web.dropbox.com/put_block_r...	FileHost	Business Use	Dropbox
Tuesday, April 04, 2023 9:36:09 P...	[redacted]@security...	Violates Compliance Category, archived to mailbox	Road Warrior	dl-web.dropbox.com/put_block_r...	FileHost	Business Use	Dropbox
Tuesday, April 04, 2023 9:36:10 PM	[redacted]@security...	Violates Compliance Category, archived to mailbox	Road Warrior	dl-web.dropbox.com/put_block_r...	FileHost	Business Use	Dropbox
Tuesday, April 04, 2023 9:36:11 PM	[redacted]@security...	Violates Compliance Category, archived to mailbox	Road Warrior	dl-web.dropbox.com/put_block_r...	FileHost	Business Use	Dropbox
Tuesday, April 04, 2023 9:36:19 PM	[redacted]@security...	Violates Compliance Category, archived to mailbox	Road Warrior	dl-web.dropbox.com/put_block_r...	FileHost	Business Use	Dropbox
Tuesday, April 04, 2023 9:36:20 PM	[redacted]@security...	Violates Compliance Category, archived to mailbox	Road Warrior	dl-web.dropbox.com/put_block_r...	FileHost	Business Use	Dropbox
Tuesday, April 04, 2023 9:36:20 PM	[redacted]@security...	Violates Compliance Category, archived to mailbox	Road Warrior	dl-web.dropbox.com/put_block_r...	FileHost	Business Use	Dropbox
Tuesday, April 04, 2023 9:36:21 PM	[redacted]@security...	Violates Compliance Category, archived to mailbox	Road Warrior	dl-web.dropbox.com/put_block_r...	FileHost	Business Use	Dropbox

Figure 33. ZIA Data Protection Insight Logs

In addition to User, Policy Action, URL Category, and Cloud Application, Zscaler also lists the DLP Engine (name) and DLP Dictionary that triggered the policy action.



Insights Logs

Apr 04, 2023 08:55:28 PM - Apr 04, 2023 10:09:07 PM
42 Log Records Found

User	Policy Action	Location	URL	DLP Engine	DLP Dictionaries
[redacted]@security...	Violates Compliance Category, archived to mailbox	Road Warrior	outlook.office...	Rubrik-Zscaler-IDM-DLP-Engine	Rubrik-Zscaler-DLP-Dictionary (100)
[redacted]@security...	Violates Compliance Category, archived to mailbox	Road Warrior	outlook.office...	Rubrik-Zscaler-IDM-DLP-Engine	Rubrik-Zscaler-DLP-Dictionary (100)
[redacted]@security...	Violates Compliance Category, archived to mailbox	Road Warrior	netipsec-my.s...	Rubrik-Zscaler-IDM-DLP-Engine	Rubrik-Zscaler-DLP-Dictionary (100)
[redacted]@security...	Violates Compliance Category, archived to mailbox	Road Warrior	netipsec-my.s...	Rubrik-Zscaler-IDM-DLP-Engine	Rubrik-Zscaler-DLP-Dictionary (100)
[redacted]@security...	Violates Compliance Category, archived to mailbox	Road Warrior	netipsec-my.s...	Rubrik-Zscaler-IDM-DLP-Engine	Rubrik-Zscaler-DLP-Dictionary (100)
[redacted]@security...	Violates Compliance Category, archived to mailbox	Road Warrior	netipsec-my.s...	Rubrik-Zscaler-IDM-DLP-Engine	Rubrik-Zscaler-DLP-Dictionary (100)
[redacted]@security...	Violates Compliance Category, archived to mailbox	Road Warrior	dl-web.dropbo...	Rubrik-Zscaler-IDM-DLP-Engine	Rubrik-Zscaler-DLP-Dictionary (100)
[redacted]@security...	Violates Compliance Category, archived to mailbox	Road Warrior	dl-web.dropbo...	Rubrik-Zscaler-IDM-DLP-Engine	Rubrik-Zscaler-DLP-Dictionary (100)
[redacted]@security...	Violates Compliance Category, archived to mailbox	Road Warrior	dl-web.dropbo...	Rubrik-Zscaler-IDM-DLP-Engine	Rubrik-Zscaler-DLP-Dictionary (100)
[redacted]@security...	Violates Compliance Category, archived to mailbox	Road Warrior	dl-web.dropbo...	Rubrik-Zscaler-IDM-DLP-Engine	Rubrik-Zscaler-DLP-Dictionary (100)
[redacted]@security...	Violates Compliance Category, archived to mailbox	Road Warrior	dl-web.dropbo...	Rubrik-Zscaler-IDM-DLP-Engine	Rubrik-Zscaler-DLP-Dictionary (100)
[redacted]@security...	Violates Compliance Category, archived to mailbox	Road Warrior	dl-web.dropbo...	Rubrik-Zscaler-IDM-DLP-Engine	Rubrik-Zscaler-DLP-Dictionary (100)
[redacted]@security...	Violates Compliance Category, archived to mailbox	Road Warrior	dl-web.dropbo...	Rubrik-Zscaler-IDM-DLP-Engine	Rubrik-Zscaler-DLP-Dictionary (100)
[redacted]@security...	Violates Compliance Category, archived to mailbox	Road Warrior	dl-web.dropbo...	Rubrik-Zscaler-IDM-DLP-Engine	Rubrik-Zscaler-DLP-Dictionary (100)
[redacted]@security...	Violates Compliance Category, archived to mailbox	Road Warrior	outlook.office...	Rubrik-Zscaler-IDM-DLP-Engine	Rubrik-Zscaler-DLP-Dictionary (100)

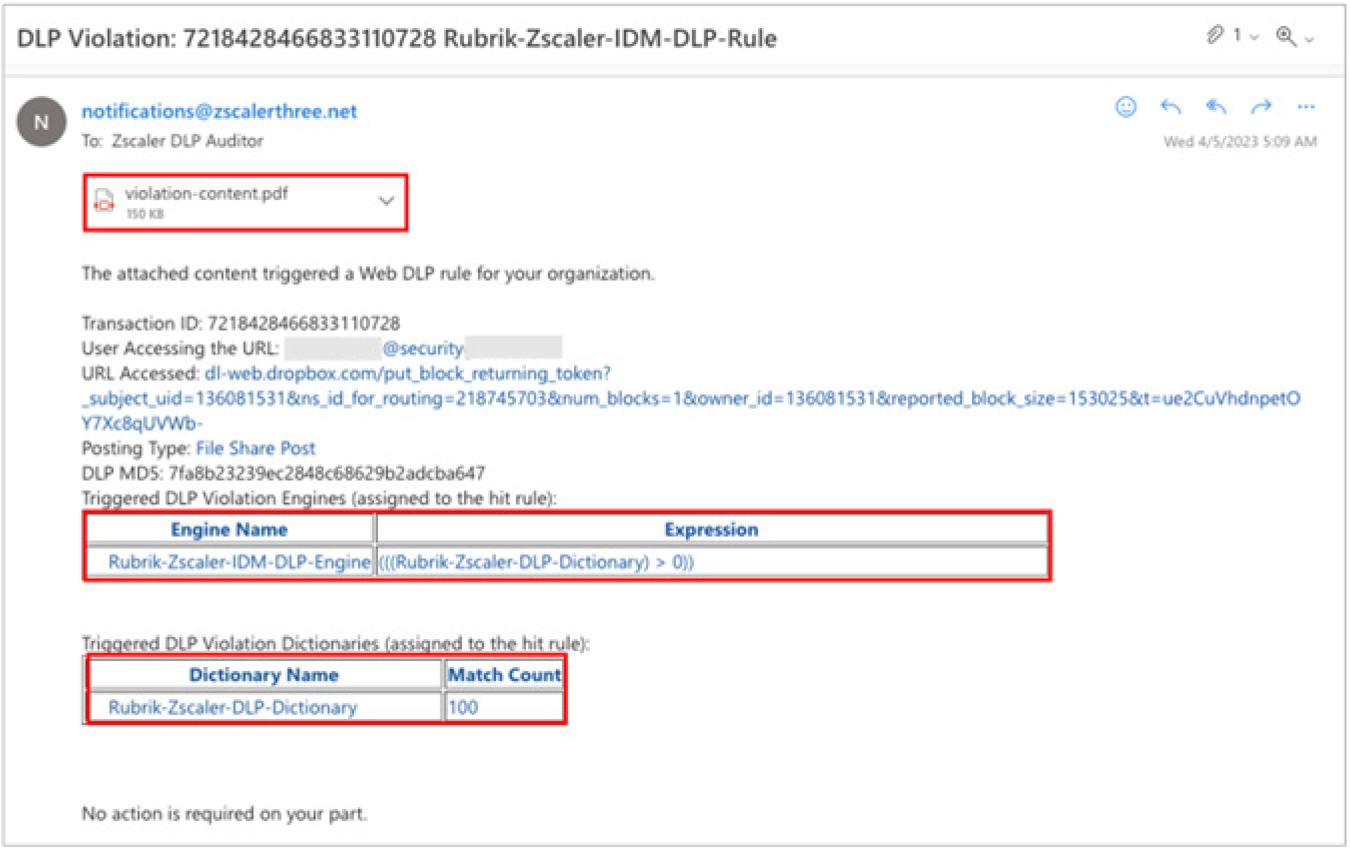
Figure 34. ZIA DLP Engine and Dictionary Logs

Zscaler DLP Auditor Notification

If you've configured the DLP inline policy to receive email-based notifications, for each violation logged by Zscaler, the system automatically sends an email to notify the compliance auditors about those violations.

A Zscaler DLP notification template contains:

- An attachment containing the content that triggered the potential violation.
- The DLP Engine name.
- The DLP Dictionary.



DLP Violation: 7218428466833110728 Rubrik-Zscaler-IDM-DLP-Rule

notifications@zscalerthree.net
To: Zscaler DLP Auditor

Wed 4/5/2023 5:09 AM

violation-content.pdf
150 KB

The attached content triggered a Web DLP rule for your organization.

Transaction ID: 7218428466833110728
User Accessing the URL: [redacted] @security [redacted]
URL Accessed: dl-web.dropbox.com/put_block_returning_token?_subject_uid=136081531&ns_id_for_routing=218745703&num_blocks=1&owner_id=136081531&reported_block_size=153025&t=ue2CuVhdnpetOY7Xc8qUVWb-
Posting Type: File Share Post
DLP MD5: 7fa8b23239ec2848c68629b2adcba647
Triggered DLP Violation Engines (assigned to the hit rule):

Engine Name	Expression
Rubrik-Zscaler-IDM-DLP-Engine	(((Rubrik-Zscaler-DLP-Dictionary) > 0))

Triggered DLP Violation Dictionaries (assigned to the hit rule):

Dictionary Name	Match Count
Rubrik-Zscaler-DLP-Dictionary	100

No action is required on your part.

Figure 35. ZIA DLP Email Notification

Although Zscaler supports sending email notifications from the Zscaler DLP engine to an ITSM-based system such as ServiceNow, this approach is not covered in this deployment guide due to high customization requirements that might not be applicable to every organization.

Zscaler Data Discovery Dashboard

Zscaler offers a detailed view of potential DLP violations via its Data Discovery Dashboard.

To visualize the Data Discovery Dashboard:

1. Go to **Analytics** > **Data Discovery Dashboard**. In this dashboard, you can apply several filters to obtain high-level visibility of the potential DLP violations that have occurred over time up to 90 days.

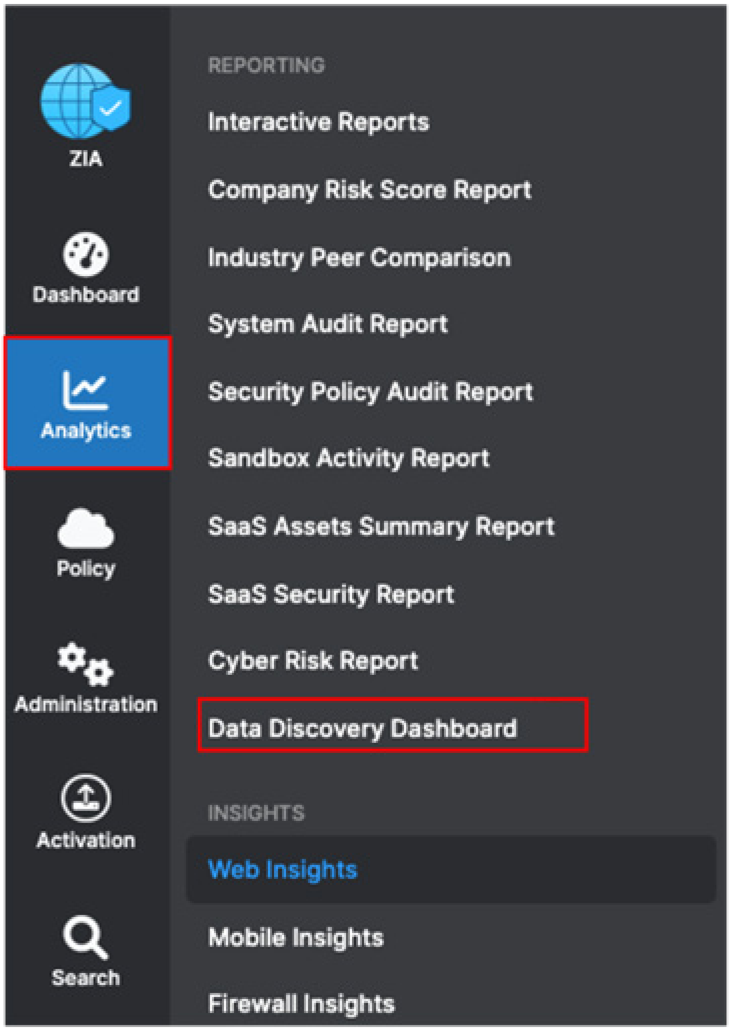
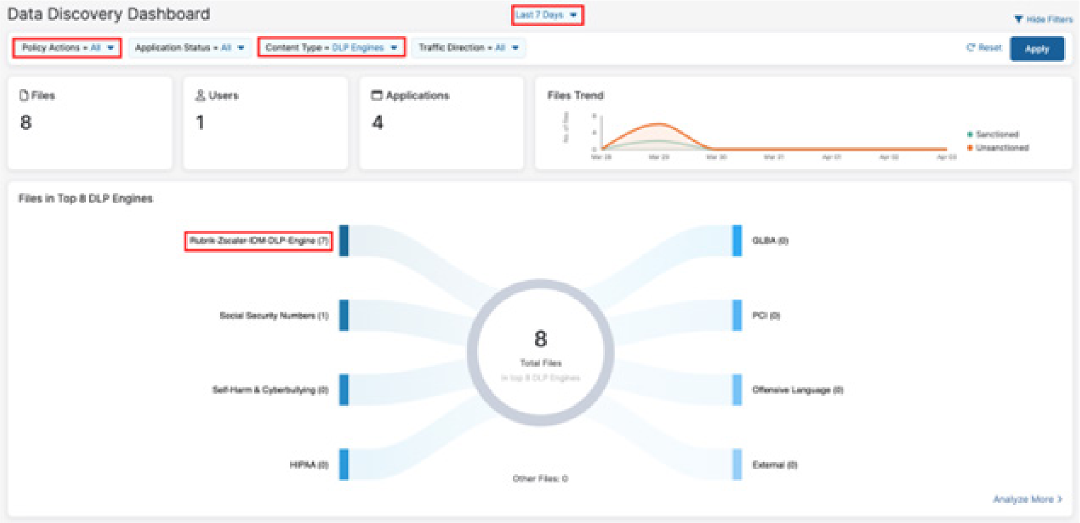


Figure 36. Data Discovery Dashboard

2. In the **Files in Top Eight DLP Engines**, find the engine to see its violation details (i.e., Rubrik-Zscaler-IDM-DLP-Engine).



Policy Actions = All
Application Status = All
Content Type = DLP Engines
Traffic Direction = All

Figure 37. ZIA DLP Data Discovery Dashboard

3. In the **Data Discovery Dashboard**, visualize the potential violations originated from files restored by Rubrik based on a graphical timeline.

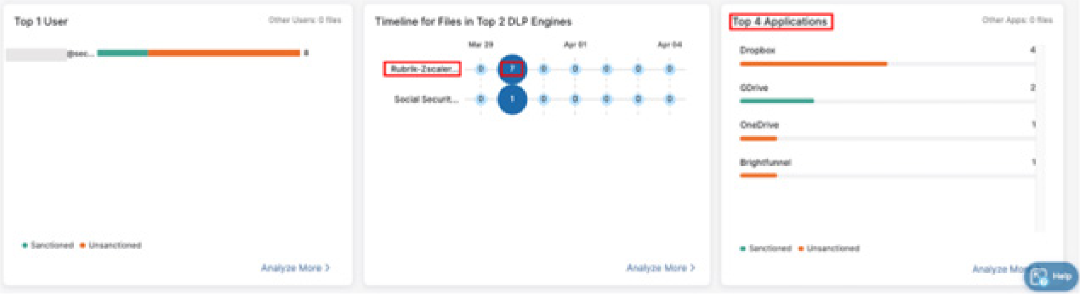
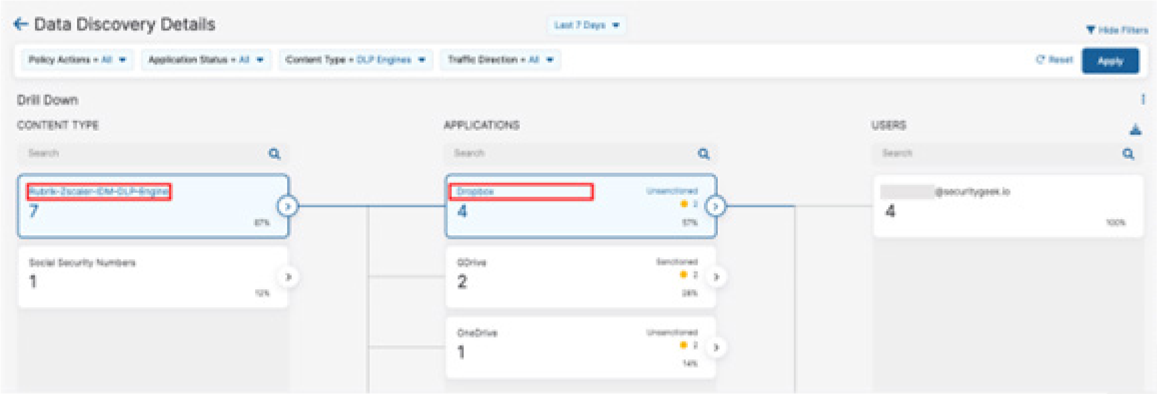


Figure 38. ZIA DLP Data Discovery Dashboard

4. In the **Files in Top Eight DLP Engines**, select the engine name for which you want to see the details.
5. The **Data Discovery Details** displays several associations.
    a. **Content Type**: DLP Engine triggered.
    b. **Applications**: Cloud applications that triggered the DLP Engine.
    c. **Users**: The users who have potentially violated a DLP inline policy.



Policy Actions = All
Application Status = All
Content Type = DLP Engines
Traffic Direction = All

Figure 39. Data Discovery Details

Considerations for a Windows Drop Server

When using a Windows-based drop server, the following considerations apply:

- It might be required that the local user created (the one with the username starting `zidm`) for the integration is a member of the Administrators group, otherwise if the source sensitive data has an ACL configured to block inheritance, the Indexer is unable to access these files on recovery, and so they aren't indexed.
- Due to the way that the native WIndows SFTP server responds to directory listing requests, there must be two subfolders in the specified path (at the same level, not one nested in the other). If these two subfolders do not exist, the Indexer setup fails to validate. Excluded these two folders from any cleanup scripts used, because if removed, the indexing process fails.
- If the sshd_config file uses chroot to specify the path that the zidm user is restricted to, the path specified in the IDM template should be /.
- If chroot is not specified for the zidm user, the full path should be specified, using UNIX style slashes (i.e., /Z:/sensitive_data/).

Best Practice for Securing Your Drop Server

The following section helps you set up the security functionality within your drop server.

Zscaler recommends using a supported and licensed OS that can run current updates for security patching. Since this server handles sensitive information, control and monitor access to it with the least privilege necessary. Ensure that everyone who has access to it is authorized and authenticated.

The examples used are not exhaustive. Zscaler recommends consulting your internal information security for recommendations, best practices, and considerations for your environment.

Microsoft Windows 11 Example

Securing a Windows 11 virtual appliance involves a variety of measures to protect against security threats. The following is a step-by-step guide to help you harden your system and limit the local firewall.

1. Ensure that you have a clean installation of Windows 11. You can obtain a Windows 11 installation from Microsoft or a pre-configured virtual appliance image. After you have the image, create a new virtual machine on your cluster and install Windows 11.
2. After Windows 11 is installed, ensure that automatic updates are enabled. This ensures your system receives security patches and updates as they become available. Go to **Settings** > **Update & Security** > **Windows Update** and enable the **Automatically download updates** option.
3. Change the default Administrator account. By default, Windows 11 creates an Administrator account with a well-known username. Attackers can easily target this. To change the default Administrator account, create a new user account with administrative privileges and delete the original Administrator account.
4. Windows 11 includes built-in antivirus software called Windows Defender. Ensure that Windows Defender is enabled to protect against malware and other security threats. Go to **Settings** > **Update & Security** > **Windows Security** and enable the **Real-time protection** option.
5. Windows 11 also includes a built-in firewall that can help protect your system from unauthorized access. To enable the Windows Firewall, go to **Settings** > **Update & Security** > **Windows Security** > **Firewall & network protection** and enable the **Windows Firewall** option.
6. After the Windows Firewall is enabled, configure it to allow only necessary traffic to and from the virtual appliance. To do this, go to **Settings** > **Update & Security** > **Windows Security** > **Firewall & Network Protection** > **Advanced settings**. From there, you can create inbound and outbound rules to allow or block specific types of traffic. For example, if you want to allow SSH access only from the Indexer appliance.

7. In addition to Windows Defender, consider installing additional anti-malware software to provide an extra layer of protection. There are many third-party options available, such as Malwarebytes, Norton, or McAfee. Ensure that the software is updated regularly and that scans are run regularly.
8. Add any tooling recommended by your internal information security team for monitoring activity on the host and the ability to respond in the event of an attempted attack.

Ubuntu Linux Example

Similar to the Windows example, the following is a step-by-step guide to help you harden your Ubuntu virtual appliance. If you have a prebuilt image or virtual instance, the organization already has a secured configuration.

1. Before starting the hardening process, ensure that your Ubuntu virtual appliance is up-to-date. Open a terminal and run the following commands:

   ```
   sudo apt update
   
   sudo apt upgrade
   ```

   This updates the system with the latest security patches and bug fixes.
2. Identify and disable any unnecessary services running on your Ubuntu virtual appliance. Use the following command to list the active services:

   ```
   systemctl list-units --type=service --state=running
   ```

   Disable any services that are not required by running the command:

   ```
   sudo systemctl stop <service-name>
   
   sudo systemctl disable <service-name>
   ```
3. Enable and configure a firewall to control incoming and outgoing network traffic to the host. Ubuntu uses `ufw` (Uncomplicated Firewall) by default. Open a terminal and run the following commands:

   ```
   sudo ufw enable
   
   sudo ufw allow ssh
   
   sudo ufw default deny incoming
   
   sudo ufw default allow outgoing
   ```

   This enables the firewall and sets the default policies for incoming and outgoing traffic.
4. It's essential to secure SSH access to the virtual appliance. Edit the SSH configuration file by running the following command:

   ```
   sudo nano /etc/ssh/sshd_config
   ```

   Inside the file, make the following changes:

   - Set `PermitRootLogin` to `no` to prevent remote root login.
   - Change the default SSH port (optional but recommended).
   - Set `PasswordAuthentication` to `no` and use SSH key-based authentication.
   - Save the changes and restart the SSH service:

     ```
     sudo systemctl restart ssh
     ```

Appendix A: Requesting Zscaler Support

You might need Zscaler Support for provisioning certain services, or to help troubleshoot configuration and service issues. Zscaler Support is available 24/7/365.

1. To contact Zscaler Support, go to **Administration** > **Settings** > **Company Profile**.

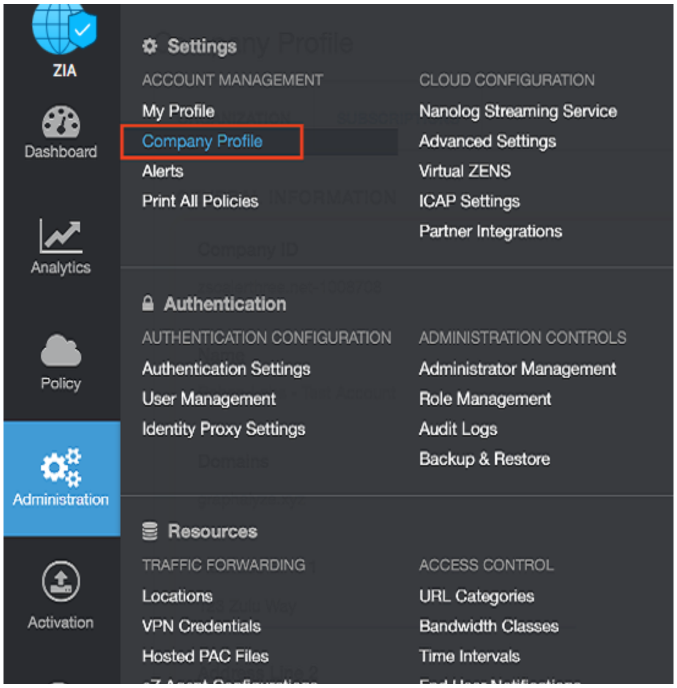
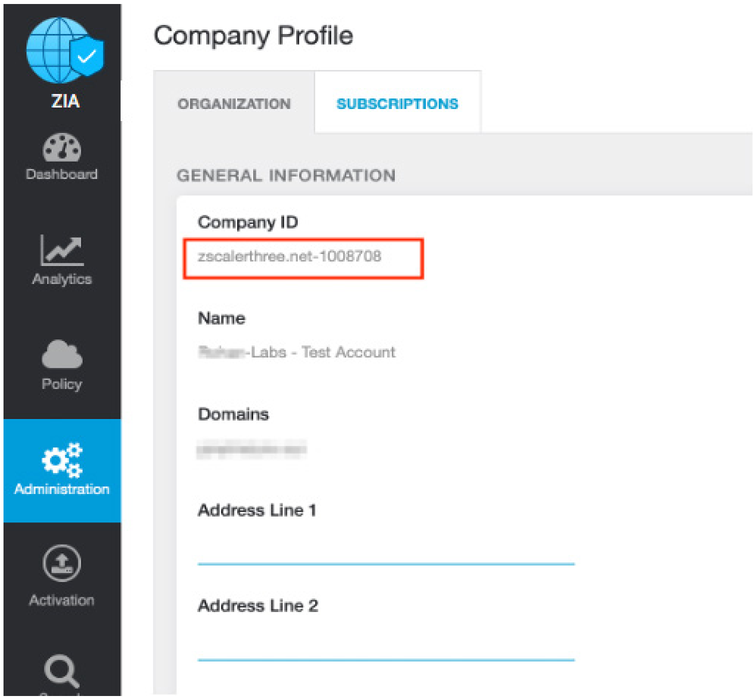


Figure 40. Collecting details to open support case with Zscaler TAC

2. Copy the Company ID.



Company Profile

GENERAL INFORMATION

Company ID
zscalerthree.net-1008708

Name
[redacted]-Labs - Test Account

Domains
[redacted]

Address Line 1

Address Line 2

Figure 41. Company ID

3. Now that you have your company ID, you can open a support ticket. Go to **Dashboard** > **Support** > **Submit a Ticket**.

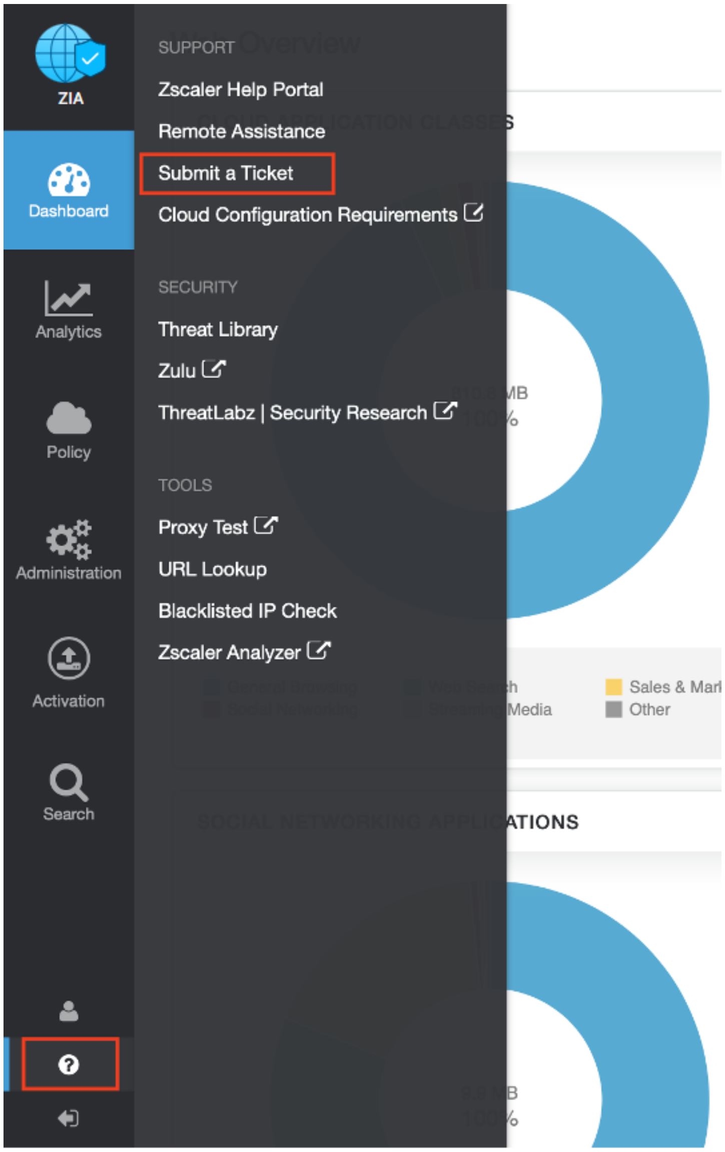


Figure 42. Submit a ticket