ZSCALER AND EGNYTE DEPLOYMENT GUIDE

SEPTEMBER 2024, VERSION 1.0

BUSINESS DEVELOPMENT GUIDE

Contents

Terms and Acronyms

The following table defines 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
DLP	Data Loss Prevention
DNS	Domain Name Service
DPD	Dead Peer Detection (RFC 3706)
GRE	Generic Routing Encapsulation (RFC2890)
ICMP	Internet Control Message Protocol
IdP	Identity Provider
IKE	Internet Key Exchange (RFC2409)
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security (RFC2411)
PFS	Perfect Forward Secrecy
PSK	Pre-Shared Key
SaaS	Software as a Service
SSL	Secure Socket Layer (RFC6101)
TLS	Transport Layer Security
VDI	Virtual Desktop Infrastructure
XFF	X-Forwarded-For (RFC7239)
ZPC	Zscaler Posture Control (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. Its flagship 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. To learn more, see Zscaler's website.

Egnyte Overview

Egnyte combines the power of cloud content management, data security, and AI into one intelligent content platform. More than 22,000 customers trust Egnyte to improve employee productivity, automate business processes, and safeguard critical data, in addition to offering specialized content intelligence and automation solutions across industries, including architecture, engineering, and construction (AEC), life sciences, and financial services. To learn more, refer to Egnyte's website.

Audience

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

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

Software Versions

This document was authored using the latest version of Zscaler software.

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 Egnyte Introduction

Overviews of the Zscaler and Egnyte applications are described in this section.

⚠ 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 ZIA as a secure internet on-ramp—just 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 our 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.

Zscaler Resources

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

Name	Definition
ZIA Help Portal	Help articles for ZIA.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
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	Definition
ZIA Help Portal	Help articles for ZIA.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
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.

Egnyte Secure and Govern Overview

Egnyte provides the only unified cloud content governance solution for collaboration, data security, compliance, and threat prevention for multi-cloud businesses. Organizations trust Egnyte to reduce risks and IT complexity, prevent ransomware and IP theft, and boost employee productivity on any app, any cloud, anywhere.

Egnyte Secure and Govern provides organizations with a platform for identifying, classifying, managing, sharing, and securing sensitive data. You can store data in Egnyte applications for full control, in existing third-party applications like Box, OneDrive, SharePoint, and Gmail, or in a combination of Egnyte and third-party applications. Users can access data through existing third-party apps and cloud services and Egnyte's web, desktop, mobile, and tablet apps.

Egnyte Resources

The following table contains links to Egnyte support resources.

Name	Definition
Egnyte Helpdesk	Help articles for Egnyte.
Egnyte University	Egnyte learning resources.
Microsoft Information Protection	Sensitivity label creation.

Customer Challenge: Data Exfiltration at the Endpoint

Egnyte Secure and Govern provides content safeguards to prevent data from unauthorized access and accidental sharing for data in Egnyte cloud. After the data is downloaded to endpoints (user laptops and mobile devices), Egnyte detects unusual activity and potential data exfiltration attempts. However, Egnyte cannot prevent end users from copying files to external storage or uploading files to non-authorized clouds.

Egnyte is partnering with Zscaler to provide customers with in-line, preventive controls at the endpoint, as shown in the following figure.

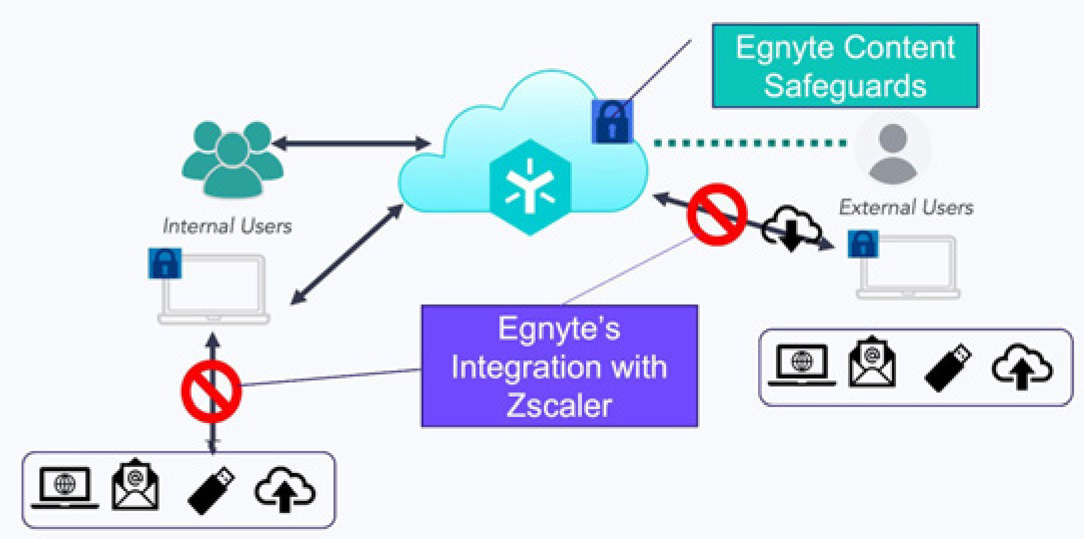


Figure 1. Zscaler and Egnyte architecture

Egnyte and Zscaler Integrated Solution for Data Exfiltration Prevention

Egnyte's integration with Microsoft Information Protection (MIP) sensitivity labels and Zscaler enables dynamic policy application based on real-time data sensitivity analysis, keeping your data governance practices current with the latest regulatory standards. By applying classification labels to files according to sensitivity levels, regulatory requirements, and business policies, Egnyte and Zscaler integrated solution not only protects data but also automates workflows to enforce preventive security policies. The integration includes the following steps (also illustrated in the following diagram):

1. Importing Microsoft MIP sensitivity label definitions into Egnyte.
2. Applying MIP labels to documents and files stored in the Egnyte cloud based on data classification and categorization.
3. Defining Zscaler ZIA DLP and Data Protection policies based on MIP labels.
4. Zscaler ZIA and Data Protection modules enforcing DLP policies for web and email traffic and on endpoints.

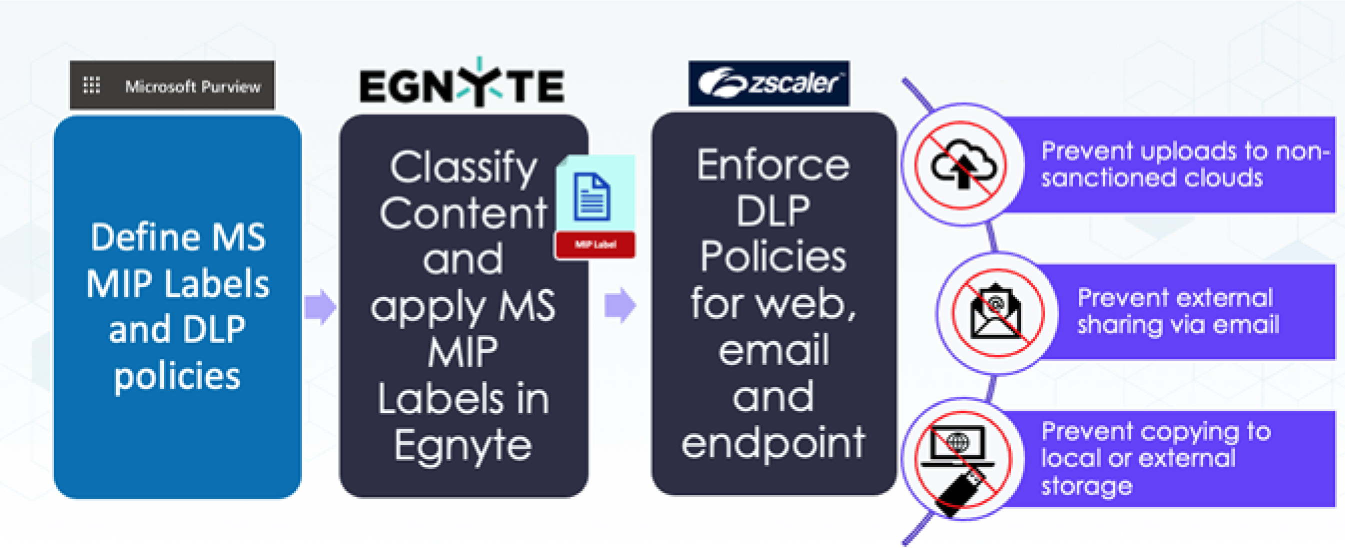

Microsoft Purview
Define MS MIP Labels and DLP policies
EGNYTE
Classify Content and apply MS MIP Labels in Egnyte
MIP Label
zscaler
Enforce DLP Policies for web, email and endpoint
Prevent uploads to non-sanctioned clouds
Prevent external sharing via email
Prevent copying to local or external storage

Figure 2. High-level Zscaler-Egnyte conceptual diagram

Egnyte Configuration Steps

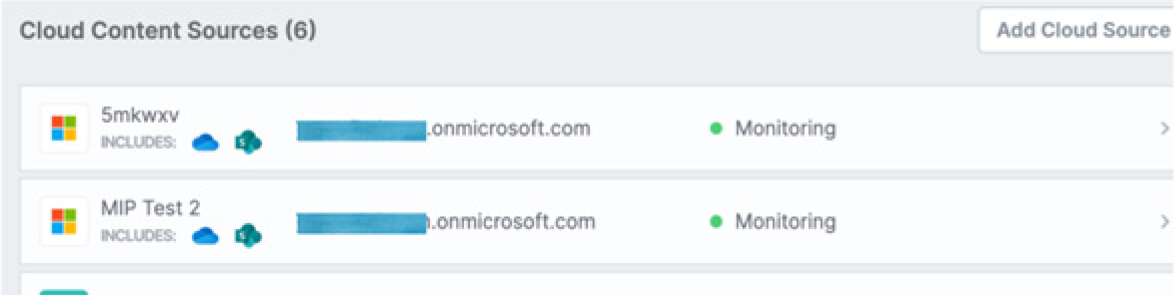
The configuration in Egnyte consists of the following steps:

1. Importing MS MIP label definitions from customers Microsoft M365 tenant.
2. Mapping MIP labels to Egnyte classification policies.
3. Add Microsoft 365 as a content source or reconfigure an existing Microsoft 365 integration to enable Microsoft Purview Labels (MIP Labels) in the Egnyte Secure and Govern Admin Portal to retrieve the MIP labels from Microsoft. After the MIP labels are imported in the Egnyte, they are assigned to any of the content classification policies that were already created (built-in and/or custom). Detailed instructions are provided next:
   - Importing the MIP Labels
   - Configuring MIP Labels

Importing the MIP Labels

To import the MIP labels:

1. Log in to the Egnyte domain and go to **Secure and Govern** > **Settings** > **Content Sources**.
2. Click Add Cloud Source.



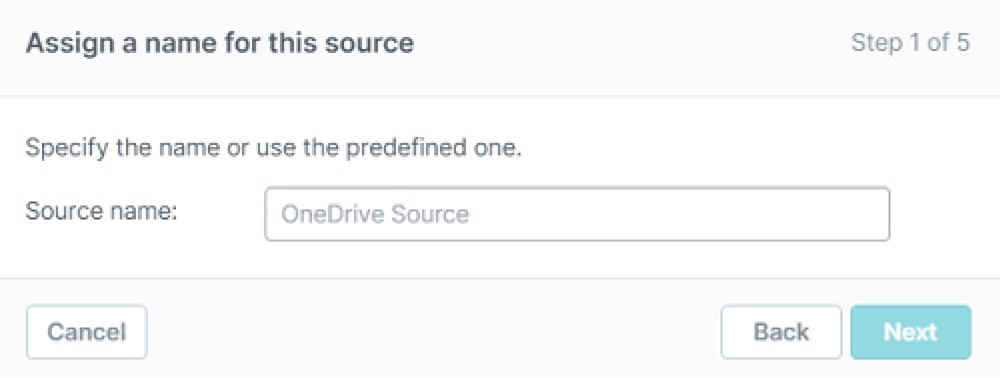
Cloud Content Sources (6)

5mkwxv INCLUDES: [redacted].onmicrosoft.com ● Monitoring

MIP Test 2 INCLUDES: [redacted].onmicrosoft.com ● Monitoring

Figure 3. Egynte Add Cloud Source

3. Choose Microsoft as the source to integrate with Microsoft Purview (aka Microsoft Sensitivity Information Protection) and click **Next**.
4. Enter a source name or use the default option and click **Next**.



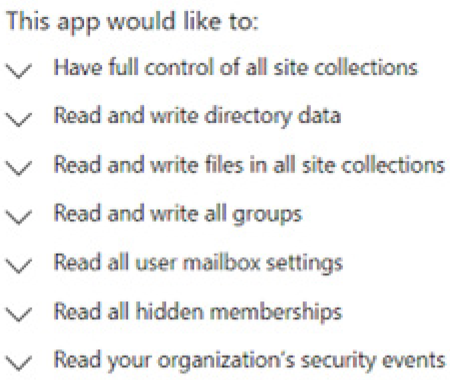
Assign a name for this source — Step 1 of 5

Specify the name or use the predefined one.

Source name: OneDrive Source

Figure 4. Egynte Assign Name for Source Instance

5. Log in with Global Admin credentials provided by Microsoft and complete the next steps. Accept the Permissions requested. To learn more, refer to Add Count Content Source.

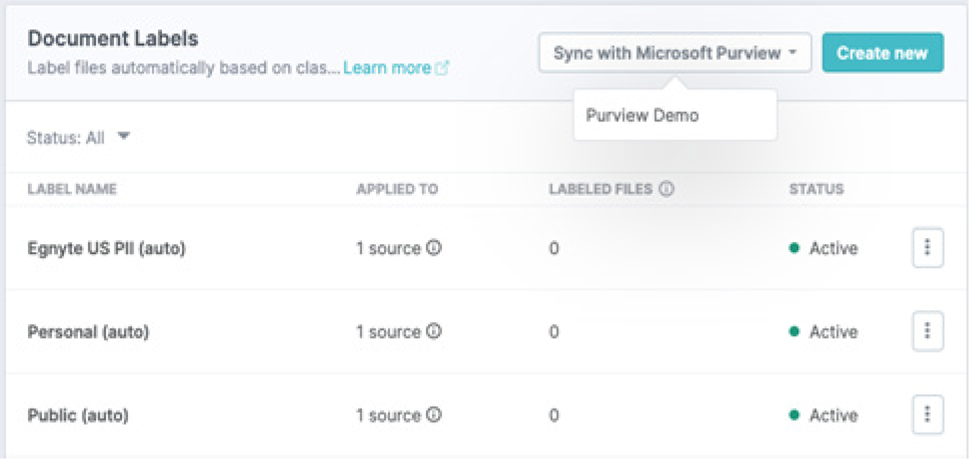


This app would like to:

- Have full control of all site collections
- Read and write directory data
- Read and write files in all site collections
- Read and write all groups
- Read all user mailbox settings
- Read all hidden memberships
- Read your organization's security events

Figure 5. Microsoft Permissions Requested example

6. After the successful integration of Microsoft as cloud source addition, Purview labels are imported. To learn more, refer to [Add Cloud Content Sources](#).
7. Microsoft Purview labels are imported and are visible under **Secure and Govern** > **Settings** > **Document Label**. To learn more, refer to [Egnyte Document Labeling](#).



Document Labels

Label files automatically based on clas... Learn more

LABEL NAME	APPLIED TO	LABELED FILES	STATUS
Egnyte US PII (auto)	1 source	0	● Active
Personal (auto)	1 source	0	● Active
Public (auto)	1 source	0	● Active

Figure 6. Egnyte Document Labels Example

Configure the Microsoft Purview Labels

To configure the Microsoft Purview labels:

1. Select the required label from **Secure & Govern** > **Settings**.

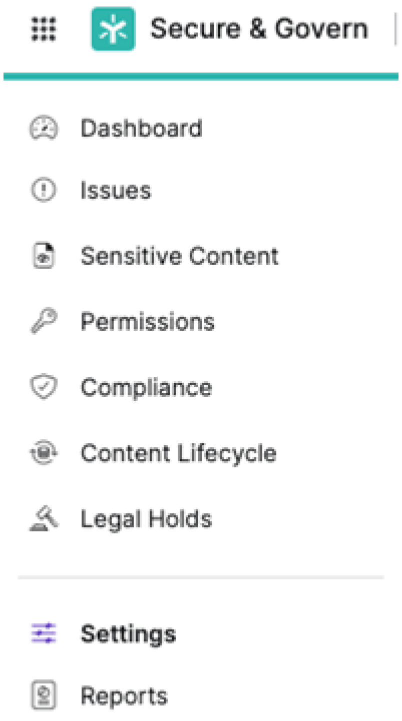
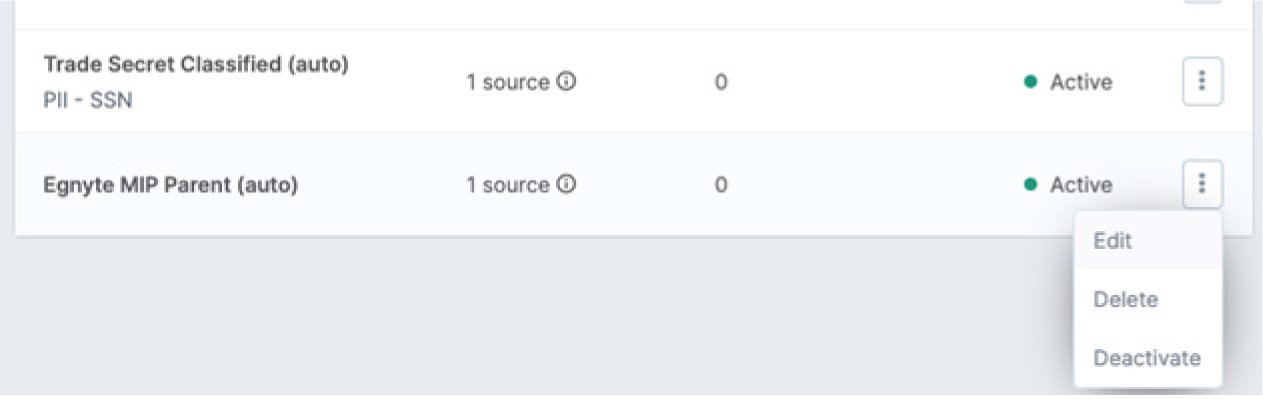


Figure 7. Labels

2. Go to **Document Labels** and click **Edit** from the options available.



Trade Secret Classified (auto) PII - SSN	1 source ⓘ	0	● Active	⋮
Egnyte MIP Parent (auto)	1 source ⓘ	0	● Active	⋮

Figure 8. Egnyte Document Labels Edits

3. Assign the required Content Classification Policies that applies to this label, click **Add and Save**. To learn more, refer to [Egnyte Content Classification](#).

One policy can have only one label at any given time, but you can assign one label to multiple policies.

ZIA Data Label Configuration

Egnyte Data Labels use MIP sensitivity labels, which you can use to identify and protect files with sensitive content. These MIP labels are maintained by Microsoft and, through the addition of a MIP Account in the ZIA Admin Portal, these labels can be retrieved from Egnyte and used when defining a DLP policy in the ZIA Admin Portal.

Egnyte MIP labels provide the following benefits and enable you to:

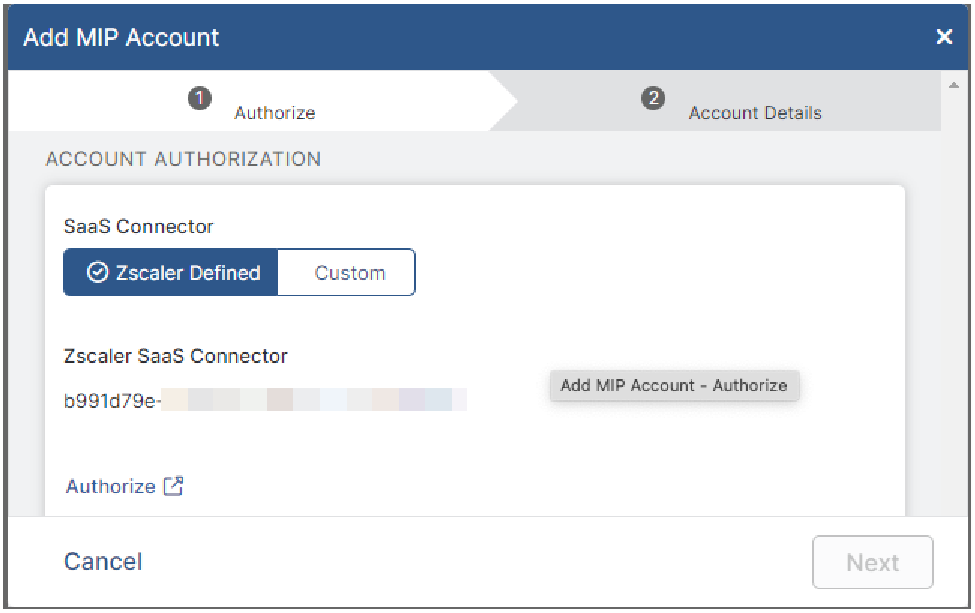
- Prevent exfiltration of files tagged with MIP labels through inline web DLP policies. With the inline web DLP policy, the service can detect files tagged with these sensitivity labels when evaluating transactions.
- Auto-classify sensitive files using Zscaler SaaS Security API policies.

Add an MIP account in the ZIA Admin Portal to enable the scan and retrieval of the MIP labels from Microsoft to the ZIA Admin Portal. After the MIP account has been successfully validated, the service scans and retrieves the MIP labels from Microsoft for the MIP account in the ZIA Admin Portal.

For the service to scan and retrieve the MIP labels from Microsoft, you must change the status on the MIP account from Validation Successful to Active using the Edit MIP Account window. To stop the scan and retrieval of these MIP labels from Microsoft, change the status of the MIP account to Tenant Inactive.

To add an MIP account:

1. Go to **Administration** > **Labels and Tags**.
2. In the **Microsoft Information Protection (MIP) Labels** tab, click **Add MIP Account**. The **Add MIP Account** window appears.

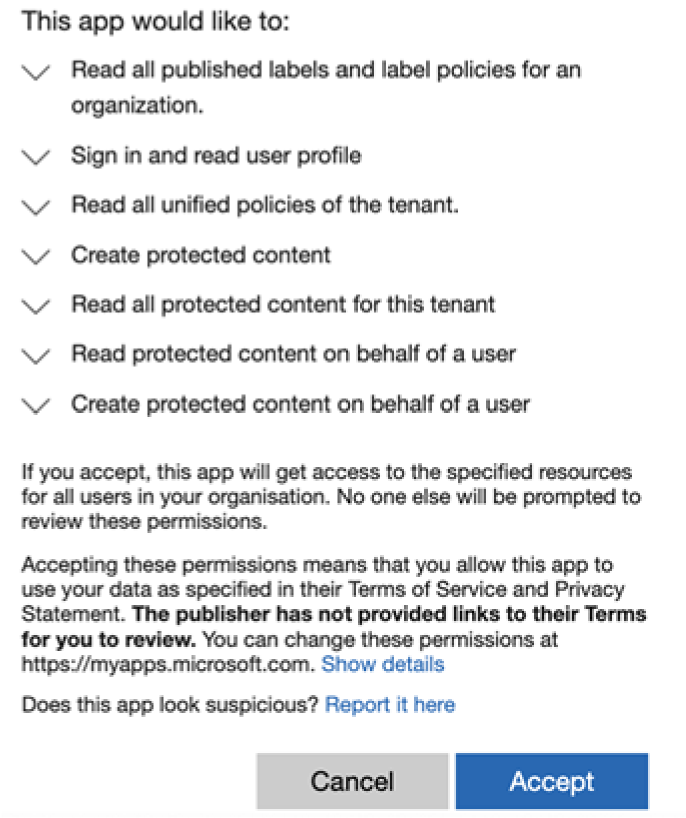


SaaS Connector: ● Zscaler Defined ○ Custom

Zscaler SaaS Connector
b991d79e-[redacted]

Figure 9. Add MIP Account

3. In the **Add MIP Account** window, select a **SaaS Connector** option. A Zscaler-defined connector grants the Zscaler service full administrator privileges to the application. A custom connector grants only necessary permissions.
   a. **Zscaler Defined**:
      i. Click **Authorize**. The **Microsoft Portal** displays.
      ii. Choose an account and log in to the Microsoft Portal. A Microsoft window appears listing the permissions requested by the Zscaler service.



This app would like to:

- Read all published labels and label policies for an organization.
- Sign in and read user profile
- Read all unified policies of the tenant.
- Create protected content
- Read all protected content for this tenant
- Read protected content on behalf of a user
- Create protected content on behalf of a user

If you accept, this app will get access to the specified resources for all users in your organisation. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their Terms of Service and Privacy Statement. **The publisher has not provided links to their Terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

Figure 10. Microsoft Permissions Request

      iii. Review the required permissions for the ZIA service to access the Microsoft account and click Accept.
   b. **Custom**: To create a custom MIP connector, first configure permissions in Azure so that you can provide the Client ID, Client Secret, and Tenant ID for the MIP account in the ZIA Admin Portal. To learn more, see Authorizing a Custom Zscaler Connector for Microsoft Applications (government agencies, see Authorizing a Custom Zscaler Connector for Microsoft Applications).
4. In the **Add MIP Account** window, under **Account Name**, enter a name you want to associate with the Microsoft account. It must be unique.
5. Click **Save** and activate the change.

The MIP account is added to the ZIA Admin Portal. The MIP Account displays a status of **Validation Successful** if the account is authorized. It displays a status of **Validation Failed** if the account is not authorized. If the status on the MIP account is Validation Failed, you can try the authorization process again by clicking **Reauthorize** in the **Edit MIP Account** window.

ZIA DLP Policy Configuration

For DLP configuration, follow outlined configuration guidance. To learn more, see **About Data Loss Prevention** (government agencies, see **About Data Loss Prevention**).

Appendix A: Requesting Zscaler Support

If you need Zscaler Support to provision certain services or to help troubleshoot configuration and service issues, it is available 24/7/365.

To contact Zscaler Support:

1. Go to **Administration** > **Settings** > **Company Profile**.

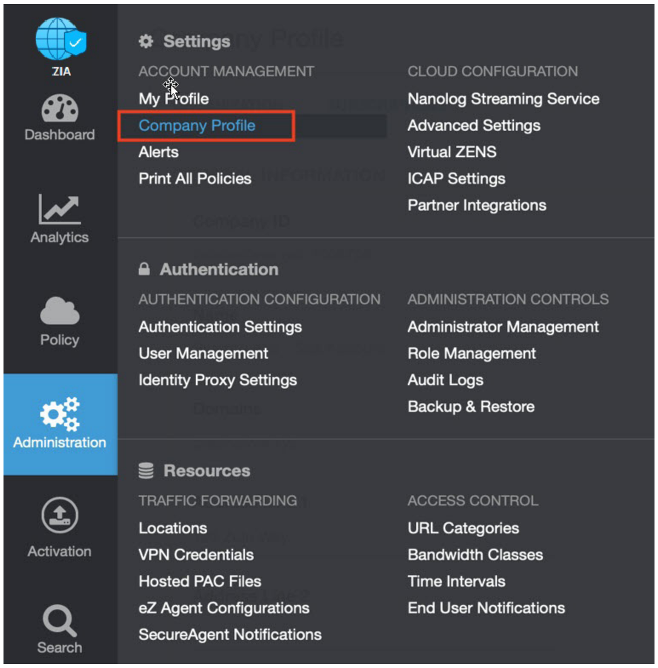
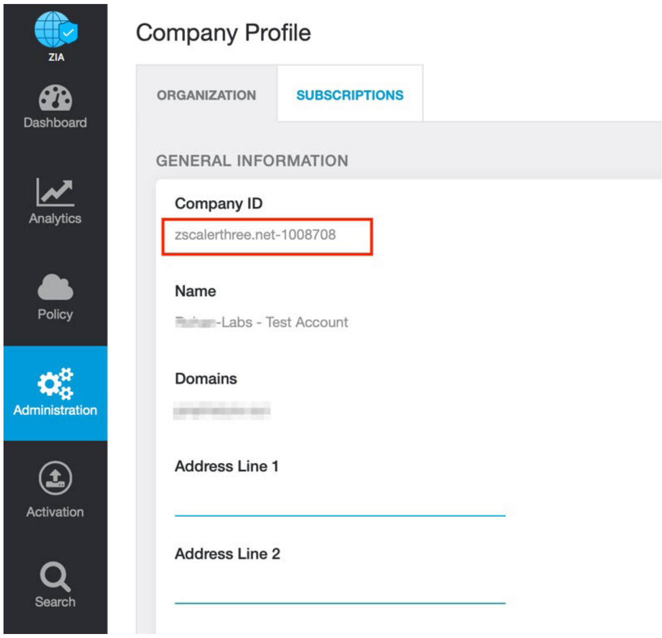


Figure 11. Collecting details to open support case with Zscaler TAC

2. Copy your **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 12. Company ID

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

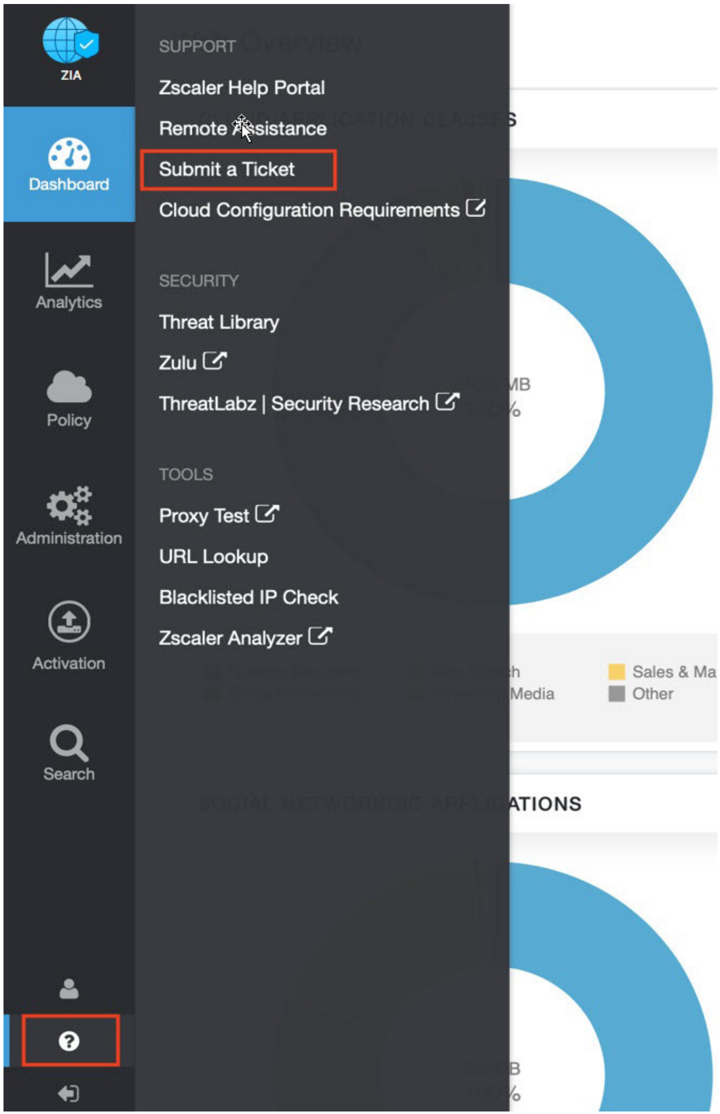


Figure 13. Submit a ticket