ZSCALER AND MIMECAST DEPLOYMENT GUIDE

OCTOBER 2025, VERSION 1.1

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)
EUN	End User Notification
GRE	Generic Routing Encapsulation (RFC2890)
ICMP	Internet Control Message Protocol
IdP	Identity Provider
IKE	Internet Key Exchange (RFC2409)
IOC	Indicator of Compromise
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)
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.

Mimecast Overview

Mimecast (NASDAQ: MIME) is a leading AI-powered, API-enabled connected Human Risk Management platform, purpose-built to protect organizations from the spectrum of cyber threats. Integrating cutting-edge technology with human-centric pathways, the Human Risk Management platform enhances visibility and provides strategic insight that enables decisive action and empowers businesses to protect their collaborative environments, safeguard their critical data, and actively engage employees in reducing risk and enhancing productivity. More than 42,000 businesses worldwide trust Mimecast to help them keep ahead of the ever-evolving threat landscape. From insider risk to external threats, with Mimecast, customers get more. More visibility. More insight. More agility. More security. To learn more, refer to Mimecast'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
- Mimecast 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 Mimecast Introduction

Overviews of the Zscaler and Mimecast 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.

Mimecast Threat Sharing Overview

Mimecast's URL Protection performs various checks against URLs within an email in transit or when a user attempts to click a link within an email. It can source the domain where the scan result is malicious.

Additionally, Mimecast's Impersonation Protection identifies domains used in a phishing attack where the sender's domain is like a domain within your Mimecast account or similar to a list of domains uploaded to the custom domain list.

In each of these cases, the integration can add the domain to a URL category in Zscaler, which you can use with a Zscaler URL and Cloud App Control policy.

Mimecast Resources

The following table contains links to Mimecast support resources.

Name	Definition
Mimecast Support Center	Access technical product, education, and support resources directly from the Mimecast Support Center.

ZIA and Mimecast Threat Share Integration

ZIA maintains a global database of malicious IPs, Domains, or URLs (i.e., IoCs) and blocks these threats inline in all ZIA customer tenants if pertinent security engines are enabled by ZIA admins. ZIA also maintains per-tenant custom URL lists. You can bring in your own custom threat feeds and populate these URL lists. You can then reference these custom URL lists in ZIA URL policies for granularly controlling end user access within that ZIA tenant.

Mimecast expands your defenses with real-time access to global IoCs delivered by Mimecast Threat Share. An existing Mimecast and ZIA customer can configure this integration to continually push high-value threats from Mimecast into a ZIA tenant.

This deployment guide describes how to configure the Zscaler and Mimecast integration. When configured, each integration configuration instance creates an associated URL category in Zscaler. This is used as the destination of any malicious domains sourced from Mimecast by this specific integration configuration instance. You can create up to 10 individual configurations, allowing different source and destination URL categories, each with its own policy application.

The following figure shows a conceptualization of the integration.

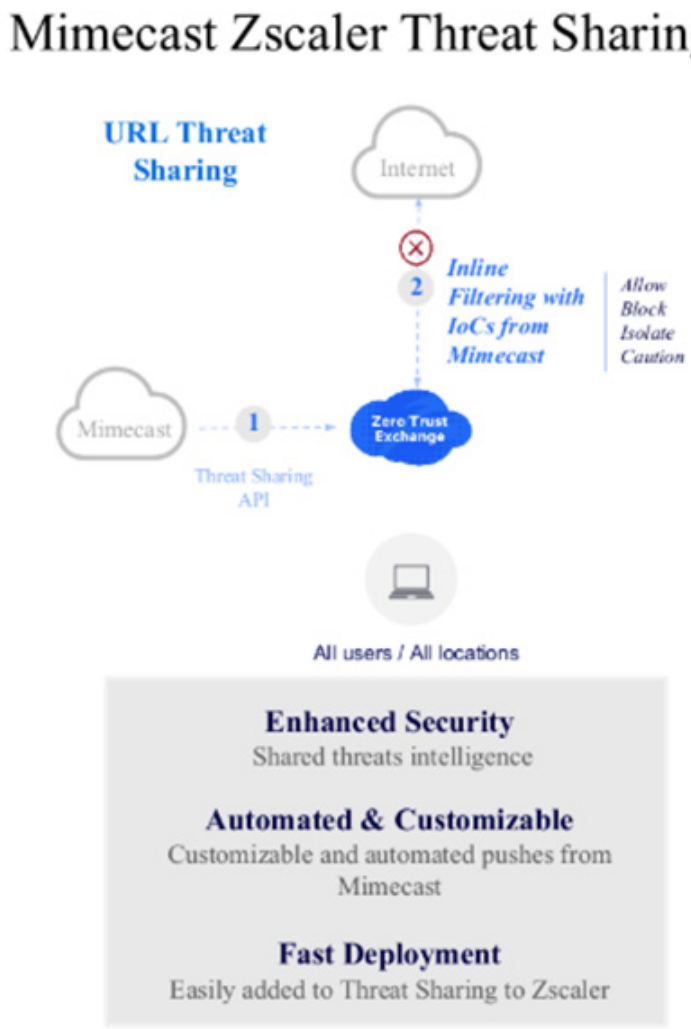

Figure 1. Mimecast and Zscaler threat sharing

Configuration Steps

The following sections describe how to configure ZIA.

Create an Administration Role

The purpose of the role is to limit the integration user's access to only a set of allowed actions:

- Create and manage custom URL categories.
- Create and manage IP and FQDN groups.

To create an administrator role:

1. Log in to the ZIA Admin Portal.
2. Go to **Administration** > **Role Management**.
3. Click **Add API Role**. The **Add API Role** window appears
4. In the **Add API Role** window:
   a. **Name**: Enter a name for the API role.
   b. **Permissions**: Permissions allow you to control a client application's access to the major API categories of the cloud service API. For each API role, you must select permissions. For the Mimecast integration, perform the following:
      - For **Policy Reporting**, select **None**.
      - For **Policy & Components**:
        - **Security**, select **None**.
        - **Access Control**, select **None** for both **Policy Control** and **Policy Components**.
        - **Data Protection**, select **None** for both **Policy Control** and **Policy Components**.
        - **Decryption**, select **None** for both **Policy Control** and **Policy Components**.
        - **URL Categories**, select **Full**.
        - **Shared Policy Components**, select **None**.
      - For **Cloud Configuration & Integration**:
        - **Integrations**, select **None**.
        - **Cloud Configuration**, select **None**.
      - For **Traffic Forwarding**:
        - **Traffic Forwarding**, select **None**.
        - **Traffic Forwarding Methods**, select **None**.
      - For **Administrative Controls**:
        - **Administrative Controls**, select **None**.
        - **Backup Controls**, select **None**.
      - For **Reporting Data**:
        - **Reporting Data**, select **None**.
      - For **Administrative Access**, select **None**.
5. Click **Save** and **Activate** the change.

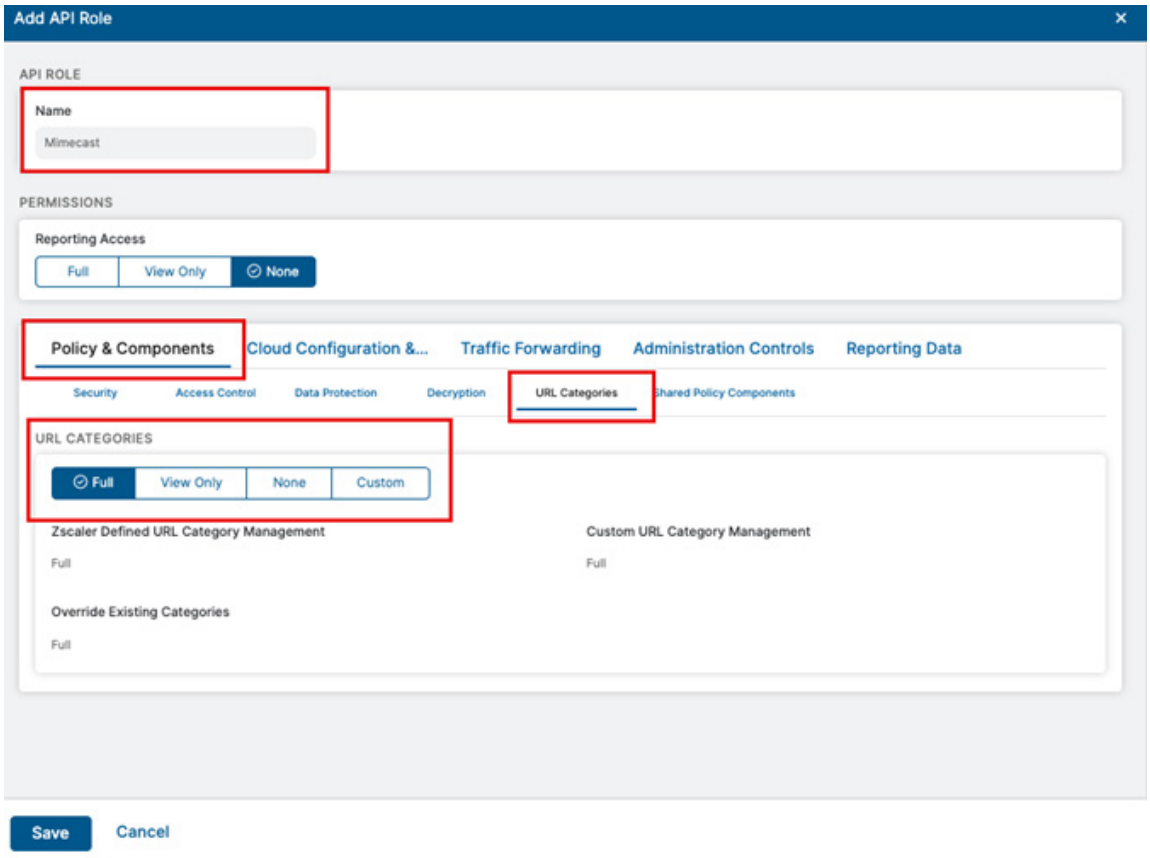

Figure 2. Zscaler Role for API

When managing OAuth 2.0 Authorization Servers, the Mimecast Zscaler threat sharing integration requires an OAuth 2.0 provider (e.g., Okta, Ping, or Microsoft Entra) to authorize client applications.

Follow the appropriate OAuth Provider Authorization Server configuration steps before proceeding to OAuth 2.0 Authorization.

For configuring the scope claim in the `<Zscaler Cloud Name>::<Org ID>::<API Role>;` format in the OAuth 2.0 provider application and copy this value. The Zscaler Cloud Name is located by going to **Administration** > **Company Profile** > **Company ID**.

You can add and manage your authorization servers from the OAuth 2.0 Authorization Servers page. You need an admin role with the API Key Management permission enabled to manage your authorization servers.

To learn more, see Securing ZIA APIs with OAuth 2.0 (government agencies, see Securing ZIA APIs with OAuth 2.0).

OAuth 2.0 Authorization

To enable OAuth 2.0 Authorization:

1. Go to **Administration** > **Cloud Service API Security**.
2. Click the **OAuth 2.0 Authorization Server** tab.
3. Click **Add Authorization Server**. The **Add Authorization Server** window appears.
4. In the **Add Authorization Server** window.
   a. **Enable**: Enable the authorization server configuration. The authorization server configuration must be enabled for JWT verification to occur. You can enable one authorization server at a time.
   b. **Name**: Enter a name for your authorization server configuration. The name can only contain alphanumeric characters without spaces and cannot exceed 64 characters.
   c. **Description**: Enter a description for the authorization server configuration. The description cannot exceed 256 characters.
   d. **OAuth 2.0 JWKS Location**: Enter the JSON Web Key Set (JWKS) endpoint that returns the public key set of the authorization server in the JWKS format. This public key set is fetched by the Zscaler service on a regular basis to cryptographically verify the authenticity of the JWT in API requests.
   e. **JWKS Server Certificate Validation**: If the authorization server uses an SSL certificate signed by an unrecognized Certificate Authority (CA) or has a root certificate issued by an unrecognized CA, an SSL handshake error occurs when the Zscaler service tries to establish an SSL connection with the JWKS endpoint. To avoid this error, you can disable the certificate validation using the **JWKS Server Certificate Validation** option or change the server certificate.
   f. **Audience URI**: (Optional) Enter the audience claim value that identifies the recipient of the JWT. If a value is specified for this field, requests are accepted only if the JWT contains a matching audience claim.
   g. **Issuer URI**: (Optional) Enter the issuer claim value that identifies the issuer of the JWT. If a value is specified for this field, requests are accepted only if the JWT contains a matching issuer claim.
   h. **Client ID**: (Optional) Enter the client ID of the client application that is requesting access to the ZIA API service. The client ID is issued by the authorization server at the time of client application registration and can be obtained from the OAuth 2.0 service console. If a value is specified for this field, requests are accepted only if the JWT contains a matching client_id claim. If multiple client applications need access to the cloud service API, leave this field blank.
5. Click **Save**.

Configure the Mimecast Threat Share Integration

To configure the Mimecast Threat Share integration:

1. Log in to the Mimecast Administration Console.
2. Go to **Integrations** > **Integrations Hub**.
3. Go to **Zscaler Managed by Mimecast SASE Threat Sharing**.
4. Review and click **I Accept**.

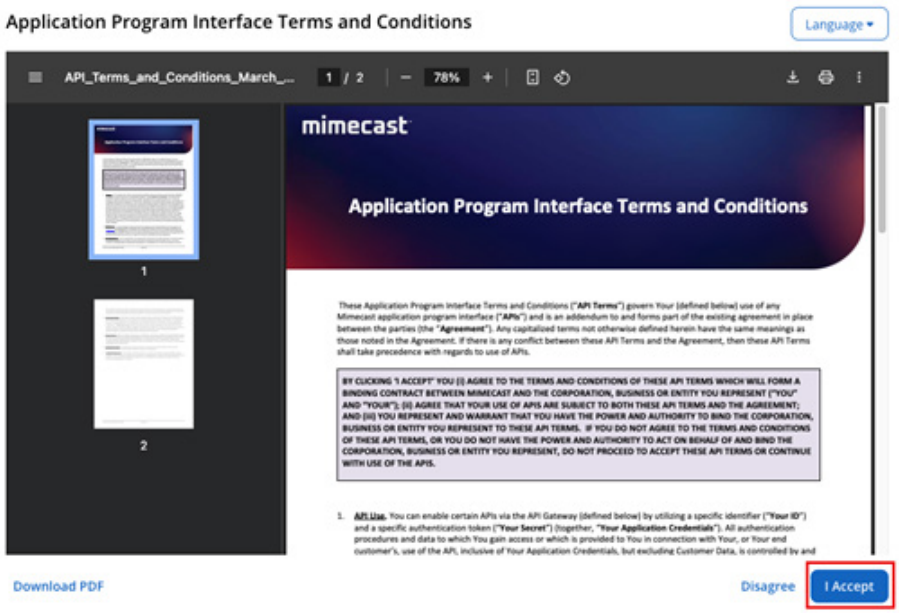

Figure 3. Mimecast Application Program Interface Terms and Condition

5. Enter an **Application Name** to differentiate multiple instances of the threat share integration.
6. Enter an application **Description**.

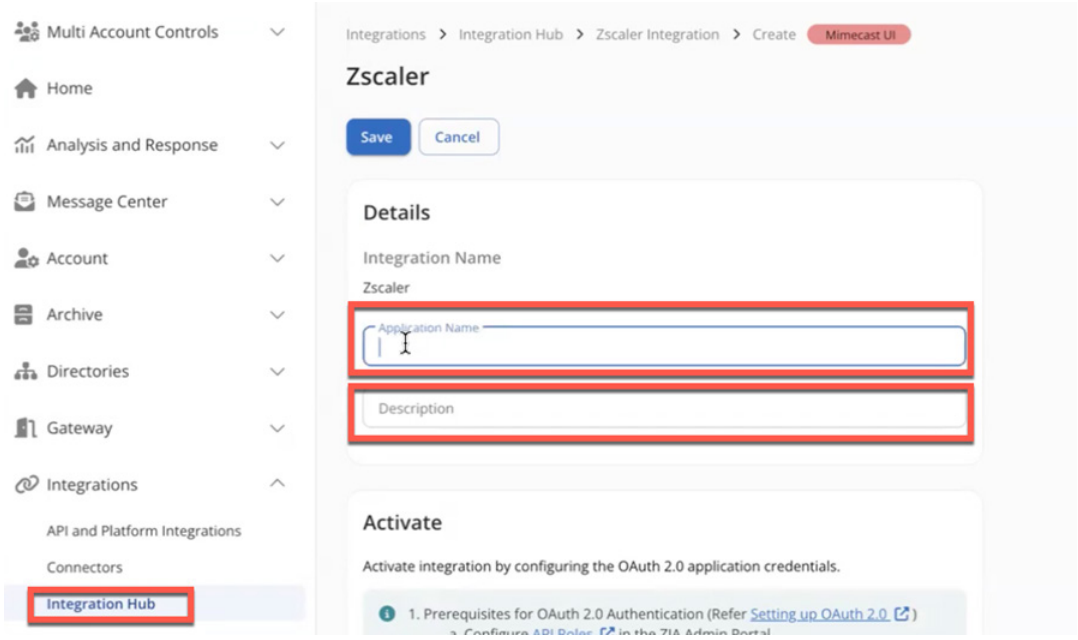

Figure 4. Zscaler integration details

7. **Zscaler Base URL**: Select the drop-down menu that represents the instance being configured.
8. In **Activate**, provide the following fields obtained from the ZIA Admin Portal in the previous steps:
    - **OAuth 2.0 Provider Token Endpoint**
    - **Client ID**
    - **Client Secret**
    - **Scope**

OAuth 2.0 Provider Token Endpoint, Client ID, Client Secret, and Scope are created during the OAuth server integration from the previous step.

9. **Fetch from Duration**: Select **Activate**, and select the period you want to go back in Mimecast logs to search for domains to add to the URL category that is created. By default, the integration starts by pulling domains from the past 24 hours of events in Mimecast.

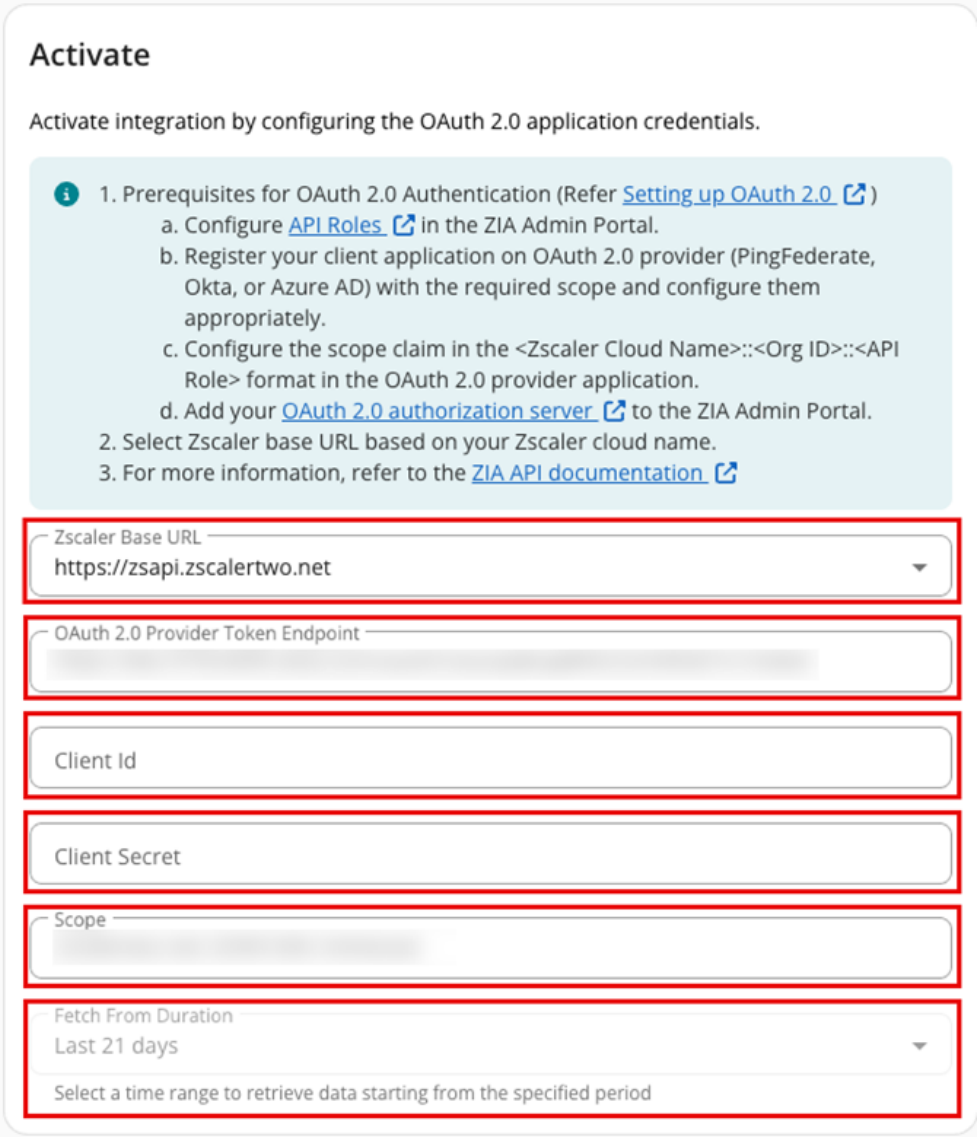

Figure 5. Zscaler Activate parameters

10. Under **Send from Mimecast**, select the sources to obtain domains from Mimecast:
    - **Malicious Domains**: These are domains sourced from Mimecast Impersonation Protection, where the domain similarity match was triggered.
    - **Malicious URLs**: Full malicious URLs from Mimecast URL Protection, where the scan result was malicious. This is more accurate, as it provides the full URL. However, this can cause the quota on the Zscaler side to fill up more quickly.
    - **Malicious Domains Extracted from URLs**: The domain only from Mimecast URL Protection, where the scan result was malicious. By default, Zscaler appends a wildcard to the end of the domain to capture any path. Malicious Domains Extracted from URLs can only be enabled if Malicious URLs is enabled.
11. **In Notification Configuration**, add email addresses followed by a comma to receive alerts should the integration encounter a permanent failure.
12. Review the information provided and click **Save** at the top of the form.
13. Wait approximately 30 seconds for the integration to create and populate the URL category in Zscaler.

Validate Custom URL Category

To validate customer URL categories:

1. In the ZIA Admin Portal, go to **Administration** > **Resources** > **URL Categories**.
2. Expand **User-Defined**, then verify the configuration name from the Mimecast configuration and number of Customer URLs has incremented.

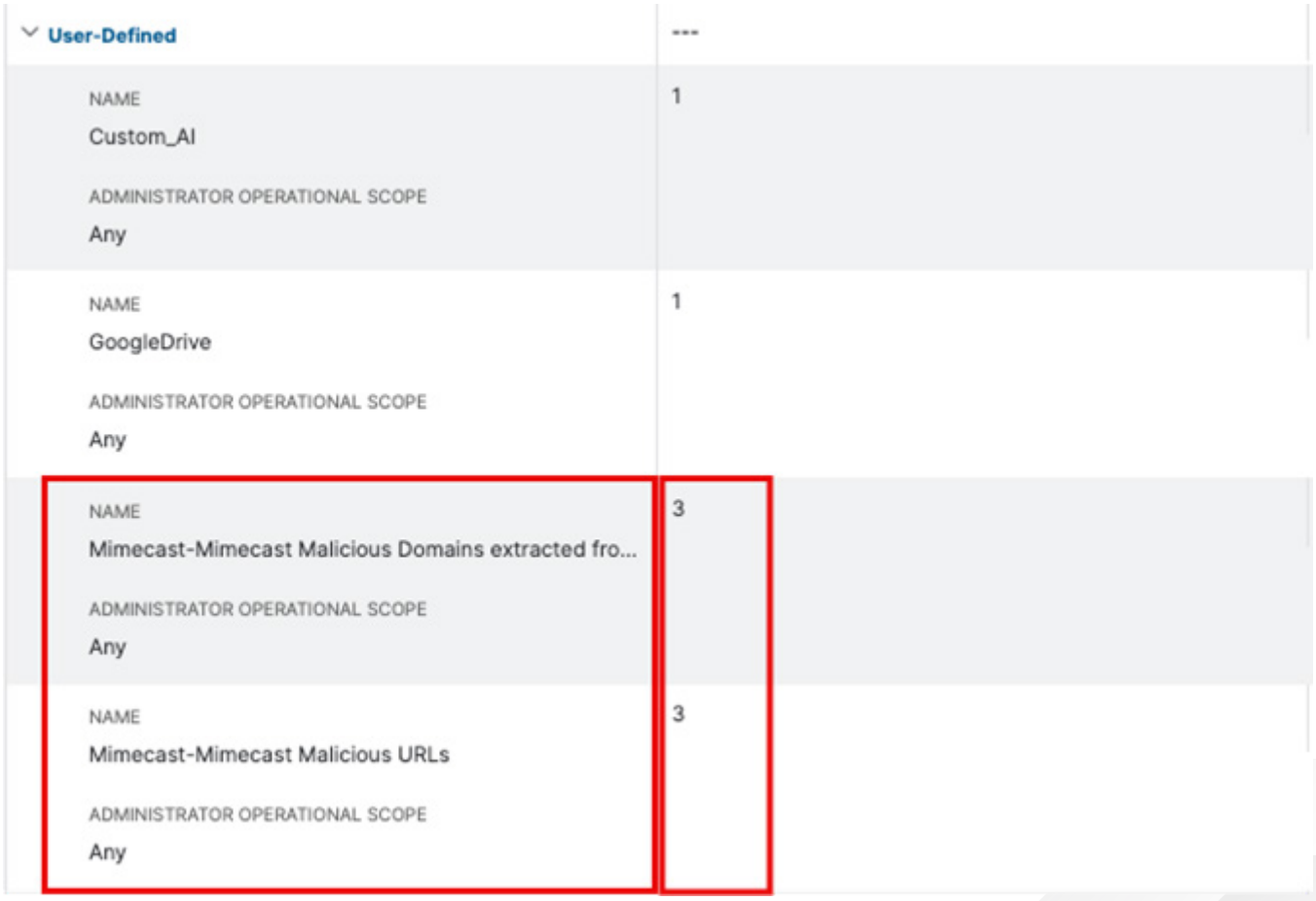

Figure 6. Zscaler Custom URLs

Configuring URL Filtering Policy

To add a URL Filtering rule for Mimecast Threat Sharing:

1. Go to **Policy** > **URL & Cloud App Control**.
2. Click **Add URL Filtering Rule**. You can also copy an existing rule by clicking **Duplicate**. The **Add URL Filtering Rule** window appears.
3. In the **Add URL Filtering Rule** window, enter the **URL Filtering Rule** attributes:
   a. **Rule Order**: Policy rules are evaluated in ascending numerical order (Rule 1 before Rule 2, and so on), and the rule order reflects this rule's place in the order. You can change the value, but if you've enabled admin rank, your assigned **admin rank** (government agencies, see **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** (government agencies, see **admin rank**) always precedes a rule with a lower admin rank.
   c. **Rule Name**: Enter a unique name for the 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. To learn more, see **About Rule Labels** (government agencies, see **About Rule Labels**).
4. Define the **Criteria**. You can either choose from the list or add an item:
   a. **Source IP Groups**: Select any number of **source IP groups** (government agencies, see **source IP groups**). You can also search for source IP groups or click **Add** to add a new source IP group. Selecting no value ignores this criterion in the policy evaluation.
   b. **URL Categories**: Select the **User-Defined Mimecast Category** created in the previous step.
   c. **Users**: Select up to 4 general or special **users** (government agencies, see **users**) or both. Select **General Users** for all authenticated users and **Special Users** for all unauthenticated users if you've enabled the **Policy for Unauthenticated Traffic** (government agencies, see **Policy for Unauthenticated Traffic**). You can search for users or click **Add** to add a new user. Selecting no value ignores this criterion in the policy evaluation.
   d. **Groups**: Select up to 8 groups. You can search for **groups** (government agencies, see **groups**) or click **Add** to add a new group. Selecting no value ignores this criterion in the policy evaluation.
   e. **Departments**: Select up to 8 **departments** (government agencies, see **departments**). If you've enabled the **Policy for Unauthenticated Traffic** (government agencies, see **Policy for Unauthenticated Traffic**), you can select **Special Departments** to apply this rule to all unauthenticated transactions. You can search for departments or click **Add** to add a new department. Selecting no value ignores this criterion in the policy evaluation.
   f. **User Risk Profile**: Select the user risk score levels to which the rule applies. Selecting no value ignores the criterion in the policy evaluation. Users are assigned a risk score based on their browsing activities. A range of risk scores is grouped as a risk score level.

      By default, the following user risk score levels are available:

      - **Low**: Level with user risk scores ranging from 0 to 29
      - **Medium**: Level with user risk scores ranging from 30 to 59
      - **High**: Level with user risk scores ranging from 60 to 79
      - **Critical**: Level with user risk scores ranging from 80 to 100

g. **Locations**: Select up to 8 **locations** (government agencies, see **locations**). You can also search for a location or click **Add** to add a new location. Selecting no value ignores the criterion in the policy evaluation.

h. **Location Groups**: Select up to 32 **location groups** (government agenices, see **location groups**). You can also search for a location group. Selecting no value ignores this criterion in the policy evaluation.

i. **Request Methods**: Select the required HTTP request methods for which you want to apply the rule. You can also search for a specific HTTP request method.

   The following HTTP request methods are available:

   - **OPTIONS**: Requests for information about communication options for the specified resource.
   - **GET**: Requests for and retrieves the specified resource from the server.
   - **HEAD**: Requests for and retrieves only the header information from the server. This is similar to the GET request but does not retrieve a response body from the server.
   - **POST**: Requests the specified resource to accept the data enclosed in the request message and process it according to the resource's semantics.
   - **PUT**: Requests the specified resource to create or replace the data enclosed in the request message.
   - **DELETE**: Requests the server to delete the specified resource.
   - **TRACE**: Requests a remote loop-back of the message along the path to the target resource. This method is useful for diagnostic purposes.
   - **CONNECT**: Requests an HTTP Proxy server to tunnel the TCP connection with the client.
   - **PROPFIND**: Requests for and retrieves the properties of the specified resource from the server.
   - **PROPPATCH**: Requests the specified resource to set or remove properties enclosed in the request message.
   - **COPY**: Requests the specified resource to create a duplicate of it.
   - **MOVE**: Requests the specified resource to move to the location enclosed in the request message.
   - **MKCOL**: Requests the specified resource to create a new collection (directory) at the location enclosed in the request message.
   - **LOCK**: Requests the server to lock the specified resource.
   - **UNLOCK**: Requests the server to unlock the specified resource.
   - **PATCH**: Requests the specified resource to apply partial modifications to it.
   - **OTHER**: All other request methods.

j. **Time**: Select **Always** to apply this rule to all **time intervals** (government agencies, see **time intervals**), or select up to two time intervals. You can also search for a time interval or click **Add** to add a new time interval.

k. **Protocols**: Select the protocols to which the rule applies. Selecting no value ignores this criterion in the policy evaluation.
   - **DNS Over HTTPS**: URLs that use DNS over HTTPS.
   - **FTP over HTTP**: URLs that use FTP over HTTP.
   - **HTTP**: URLs that use HTTP.
   - **HTTP Proxy**: URLs that use HTTP Proxy server when the client is configured in explicit proxy mode, which makes the HTTP CONNECT request to the proxy server to tunnel the TCP connections. The tunnel is typically set up when using TLS.
   - **HTTPS**: URLs that use HTTP encrypted by TLS/SSL.
   - **Native FTP**: URLs that use FTP.
   - **SSL**: URLs that use SSL encryption and haven't been decrypted. For example, URLs you've **exempted from SSL inspection** (government agencies, see **exempted from SSL inspection**).
   - **Tunnel**: Encrypted URLs that use an unidentified protocol. For example, URLs from tunneling applications such as Telnet or SSH that are encapsulated in HTTP or HTTPS.
   - **Tunnel SSL**: Undecodable protocol within an SSL connection.
   - **WebSocket**: URLs that use WebSocket.
   - **WebSocket SSL**: URLs that use WebSocket within an SSL connection.

l. **User Agent**: Select any number of user agents to which the rule applies. You can also search for an agent. Selecting no value ignores this criterion in the policy evaluation.

m. **Devices**: Select the **devices** (government agencies, see **devices**) to which the rule applies. You can also search for a device. Selecting no value ignores this criterion in the policy evaluation.

n. **Device Groups**: Select the **device groups** (government agencies, see **device groups**) to which the rule applies. For Zscaler Client Connector traffic, select the appropriate group based on the device platform. Select **Cloud Browser Isolation**, **IoT**, or **No Client Connector** to apply the rule to Isolation traffic, IoT traffic, or traffic that is not tunneled through Zscaler Client Connector, respectively. You can also search for a device group. Selecting no value ignores this criterion in the policy evaluation.

o. **Workload Groups**: Select up to 8 **workload groups** (government agencies, see **workload groups**) for which you want to apply the rule. You can also search for a workload group. Selecting no value ignores the criterion in the policy evaluation.

p. **Device Trust Level**: Select the device trust level values (**High Trust**, **Medium Trust**, **Low Trust**, or **Unknown**) to which the rule applies. While the High Trust, Medium Trust, or Low Trust evaluation is applicable only to Zscaler Client Connector traffic, Unknown evaluation applies to all traffic. Selecting no value ignores the criterion in the policy evaluation.

5. Define the **Rule Expiration**:
   a. **Enable Rule Expiration**: Enable this option to set a validity period for the rule:
      - **Start Date and Time**: Select a start date and time. The rule is valid starting on this date and time.
      - **End Date and Time**: Select an end date and time. The rule ceases to be valid on this date and time.
      - **Time Zone**: Select the time zone in which the rule is valid.
   b. You can use the rule expiration feature to temporarily allow or block access for a set period of time to a category if any configured rules block or allow access to it, respectively.
6. Select **Action** for the rule.

7. (Optional) Define the notification settings:
    a. **Browser Notification Template**: Select a browser-based EUN message from the drop-down menu to display the message on the browser when the user activity triggers the Cloud App Control Policy rule.
    b. **Description**: (Optional) Enter additional notes or information. The description cannot exceed 10,240 characters.
8. Click **Save** and **Activate Change**.

Troubleshooting

The following sections describe troubleshooting options.

Permanent Errors

A permanent error occurs when the integration is unable to proceed in sharing threats until manual intervention is performed. In the event of a permanent error, you see the status change in the Integration Hub and the recipients specified in the Notifications section of the setup receives an alert. While in a permanent error state, the integration doesn't attempt to share any threats until resolved.

Example reasons for a permanent error:

- Expired or rotated API keys in Zscaler.
- Quota exhaustion for URL categories in Zscaler.

To manually return an integration to normal state after resolving a permanent error, edit the specific integration, and click Save. If the resolution of an error state requires changes, make them at this time. Otherwise, you can click Save without changes. The integration attempts to resume and return to a normal state or go back into a permanent error state.

Temporary Errors

If the integration encounters a temporary error, such as unexpected responses when making API calls to Zscaler or a Mimecast service degradation, then no action is required, and the integration continues to attempt sharing threats until it automatically returns to a normal state or goes into a permanent error state. Temporary errors do not generate alert emails.

Threats Observed While in Error State

The integration uses timestamp bookmarking when sharing threats. If the integration goes into an error state, the timestamp bookmark does not advance. This allows for threats observed while in an error state to be shared when the integration returns to a normal state, as long as the integration is not in an error state for more than 30 days.

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**.

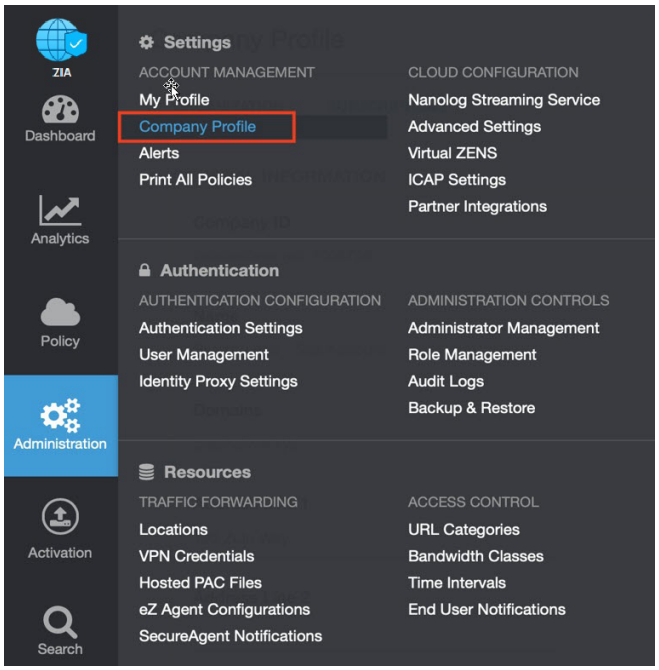

Figure 7. Collecting details to open support case with Zscaler TAC

2. Copy your **Company ID**.

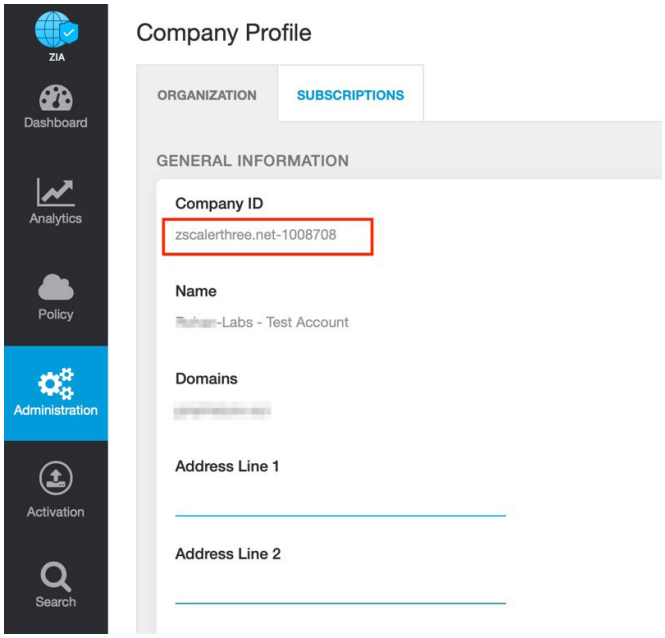

Figure 8. Company ID

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

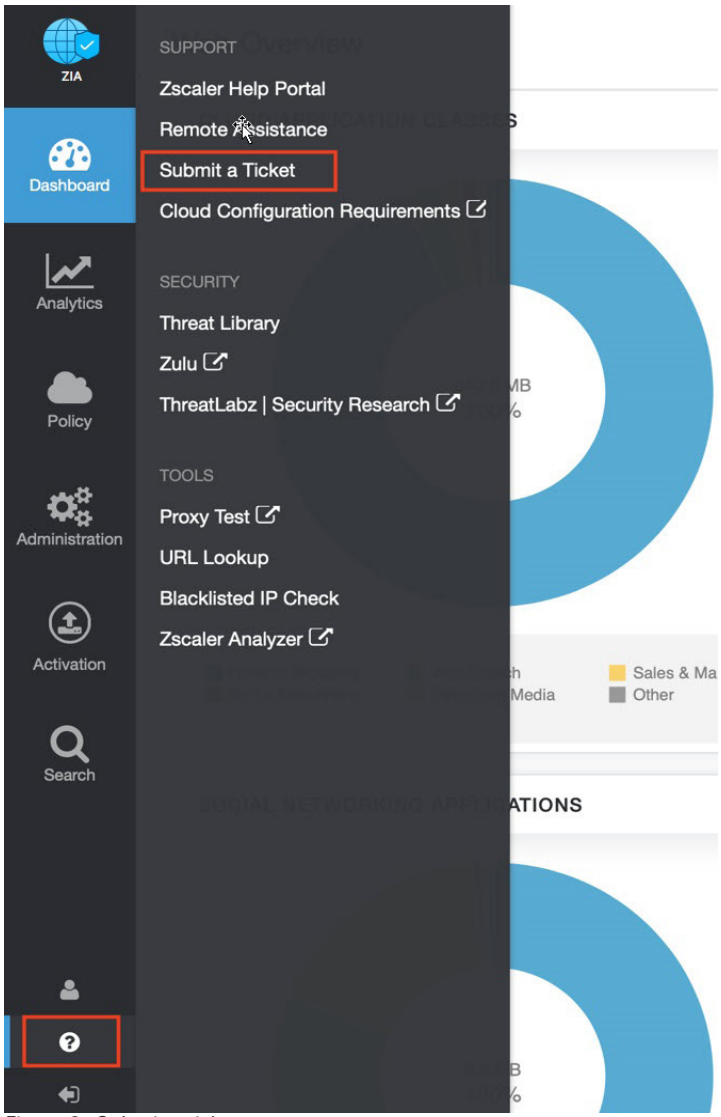

Figure 9. Submit a ticket

