ZSCALER AND SAVIYNT CONNECTOR DEPLOYMENT GUIDE

NOVEMBER 2021, VERSION 1.1

BUSINESS DEVELOPMENT GUIDE

Contents

About This Document

The following sections describe Zscaler and the Zscaler partner.

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.

Saviynt Overview

Saviynt's cloud-architected identity and access governance platform helps modern enterprises scale cloud initiatives and solve the toughest security and compliance challenges in record time. The company brings together identity governance (IGA), granular application access, cloud security, and privileged access management (PAM) to secure the entire business ecosystem and provide a frictionless user experience. The world's largest brands trust Saviynt to accelerate business transformation, empower distributed workforces, and meet continuous compliance. To learn more, refer to Saviynt'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
- Saviynt Resources
- Appendix A: Requesting Zscaler Support

Software Versions

This document was authored using:

- Saviynt Enterprise Content Management (ECM) release version 6.0 and later.
- Zscaler release version 11.3 and later.

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 Saviynt Introduction

The following section describes the applications deployed in this 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 Representative.

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.

ZPA Overview

ZPA is a cloud service that provides secure remote access to internal applications running on 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	Definition
ZIA Help Portal	Help articles for ZIA.
ZPA Help Portal	Help articles for ZPA.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
ZPA Posture Profiles	Help link for how to configure ZPA posture profiles.
ZPA Access Policies	Help link for how to configure ZPA access policies with a set of configuration examples.
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.
ZPA Help Portal	Help articles for ZPA.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
ZPA Posture Profiles	Help link for how to configure ZPA posture profiles.
ZPA Access Policies	Help link for how to configure ZPA access policies with a set of configuration examples.
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.

Saviynt Security Overview

Saviynt Security combines SIEM threat detection features with endpoint prevention and response capabilities in one solution. These analytical and protection capabilities, leveraged by the speed and extensibility of Saviynt search, enable analysts to defend their organization from threats before damage and loss occur.

Saviynt Security provides the following security benefits and capabilities:

- A detection engine to identify attacks and system misconfigurations.
- A workspace for event triage and investigations.
- Interactive visualizations to investigate process relationships.
- Inbuilt case management with automated actions.
- Detection of signatureless attacks with prebuilt machine learning anomaly jobs and detection rules.

Saviynt Resources

The following table contains links to Saviynt support resources.

Name	Definition
Saviynt Enterprise Identity Cloud	Description of the Enterprise Identity Cloud (EIC) properties and value.
Saviynt Customer Support	Saviynt support portal for submitting requests and issues.
Saviynt Solution Guides	Solution guides help enterprises easily configure our products with their existing software solutions.

Zscaler Connector Guide

This guide describes the Zscaler connector used to integrate Saviynt EIC with ZPA and ZIA.

Introduction

Zscaler is the creator of the Zero Trust Exchange platform that transforms and empowers an anywhere-workforce seamlessly and securely by embracing a Zero Trust mindset. At a high-level, Zscaler comprises of elements such as users, groups, and policies.

The Zscaler connector creates an integration with ZPA and ZIA applications to manage Zscaler users and gain visibility of their groups and user-group memberships from EIC.

This guide provides information about using the Zscaler (SCIM-based) connector for performing operations listed in the Supported Features section.

Supported Features

The Zscaler connector supports the following features:

Import				Provisioning		
Zscaler Object	**EIC Object**	**Full Import**	**Incremental Import**	**Lifecycle Management**	**Add or Remove Access**	**Additional Configurations**
Users	Accounts	Yes	No	Support for creating and removing accounts		
Groups	Groups	Yes	No	N/A	Support for adding and removing group members	Groups

The features listed above are currently supported in EIC. Any new enhancements are communicated via the Release Notes.

Understanding the Integration Between Saviynt and Zscaler

You must integrate the EIC and the collaboration platform hosted by the target application (Zscaler, in this case) to execute import, provisioning, and deprovisioning tasks. The following components are involved in the integration:

- **Zscaler**: Zscaler is the target application for which EIC manages the identity lifecycle. Zscaler integrates with EIC through the connector to import, manage accounts, and access data.
- **Objects**: Objects are imported as entitlement types into EIC.
- **Security System**: The security system represents the connection between EIC and the target application.
  - The security system is an endpoint that is the target application for which you want EIC to manage the identity repository.
  - The security system provides application instance abstraction from connectivity, including high-level metadata. You can select one connection for importing data from the target application and another connection for provisioning data to the target application. For more information about creating a security system, see Creating a Security System.
- **Endpoint**: An endpoint is an instance of an application within the context of a security system.
  - Endpoints are the target applications that the connector imports or exports data and performs provisioning or deprovisioning of identity objects such as users, accounts, and entitlements.
  - You must create an endpoint after creating the security system. You can associate a single security system with multiple endpoints if the deployment involves modeling of multiple isolated virtual applications (based on sets of specific entitlements according to certain categories) within a single application instance.
- **Connector**: A connector is a software component that enables communication between the EIC and the target application. It provides a simplified integration mechanism where in some instances you only need to create a connection with minimal connectivity information for your target application. The REST Connector is used for importing, provisioning, and accessing accounts through the SCIM APIs. For more information about creating a connection, see Creating a Connection.
- **Job Scheduler**: The job scheduler is a software component that executes a job based on the configured schedule to perform import or provisioning operations from EIC. When a provisioning job is triggered, it creates provisioning tasks in EIC. When these tasks are completed, the provisioning action is performed on the target application through the configured connector. If you want to instantly provision requests for completing the tasks without running the provisioning job, you must enable Instant Provisioning at the security system level and the Instant Provisioning Tasks global configuration. For more information about the jobs used by the connectors in the Zscaler integration, see Using the Zscaler Connector.

Connector Architecture

The EIC uses a REST connection to integrate with Zscaler and import data, as well as for provisioning and deprovisioning tasks. The REST connection uses the System for Cross-domain Identity Management (SCIM) protocol to communicate with Zscaler's SCIM interface.

The following diagram illustrates the connector architecture and communication with the target application.

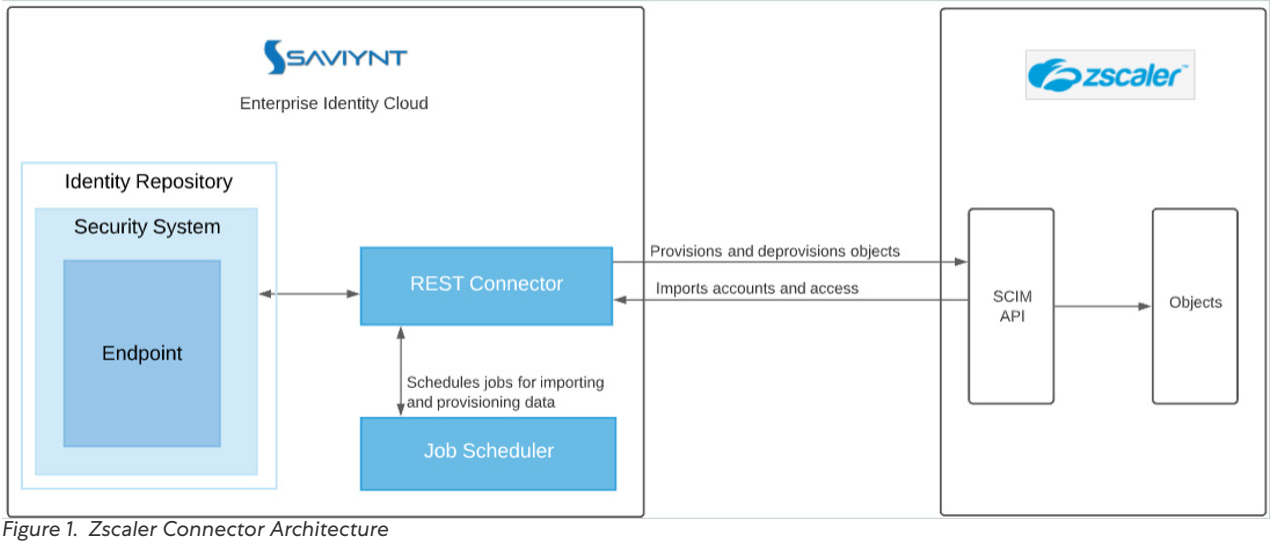

Figure 1. Zscaler Connector Architecture

Configuring a Connection

The connector configuration parameters use an access token and URL for its initial authentication to ZPA and ZIA applications, and to authorize subsequent calls for performing additional transactions.

Prerequisites

- Generate the access token and the URL for ZPA application. To learn more, see the Generating Access Token and URL for the ZPA Application.
- Generate the access token and the URL for ZIA application. To learn more, see the Generating Access Token and URL for the ZIA Application.

Generating Access Token and URL for the ZPA Application

Perform the following steps to generate an access token and URL for the ZPA application:

1. Log in to ZPA Admin Portal using administrator credentials.
2. Go to **Administration** > **IdP Configuration**.

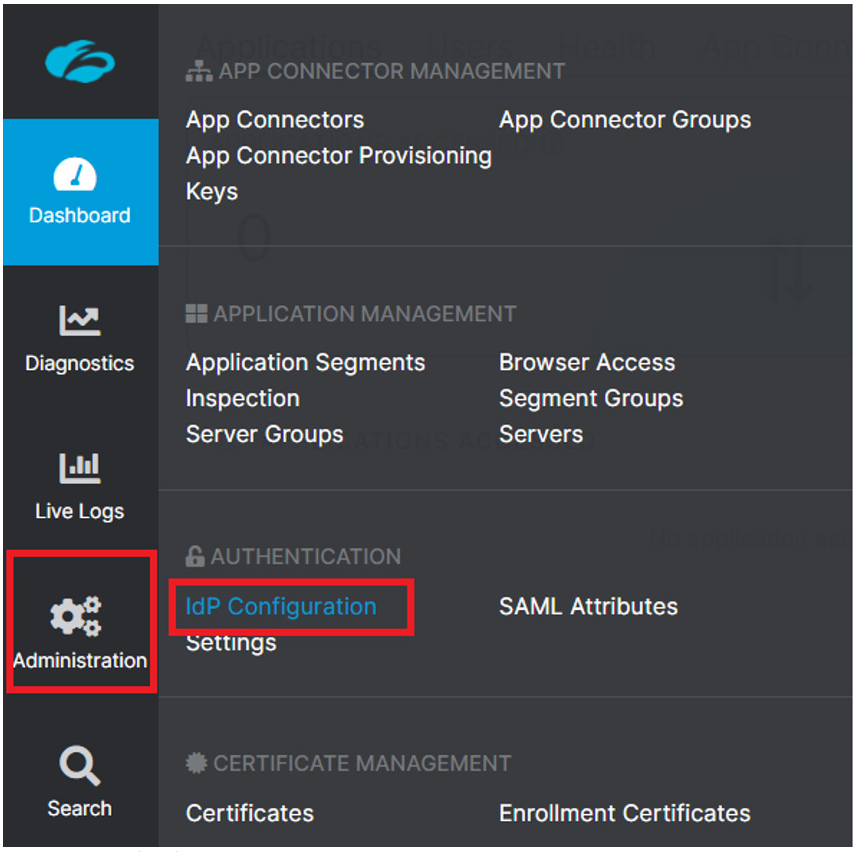

Figure 2. IdP Configuration in the ZPA Admin Portal

3. Specify the IdP Configuration details. The SCIM Configuration page displays the endpoint URL and the access token.

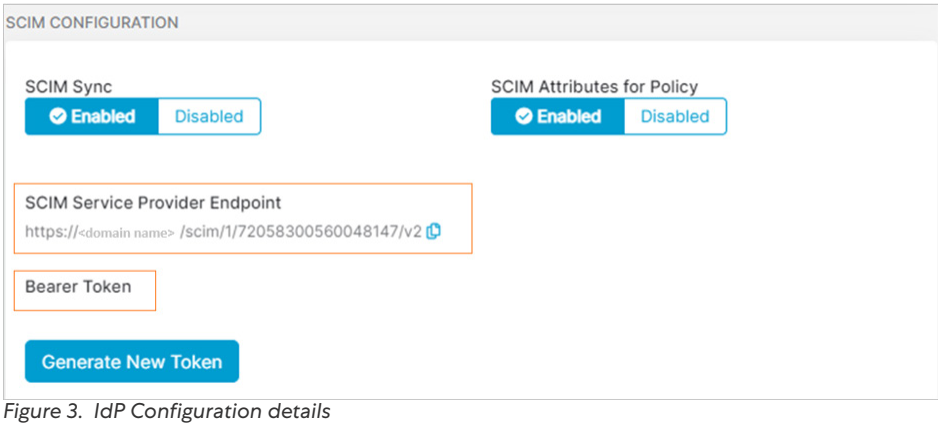

Figure 3. IdP Configuration details

In the figure, 72058300560048147 is the ZPA account number.

Generating Access Token and URL for the ZIA Application

Perform the following steps to generate an access token and URL for the ZIA application:

1. Log in to ZIA Admin Portal using administrator credentials.
2. Go to **Administration** > **Authentication Settings**.

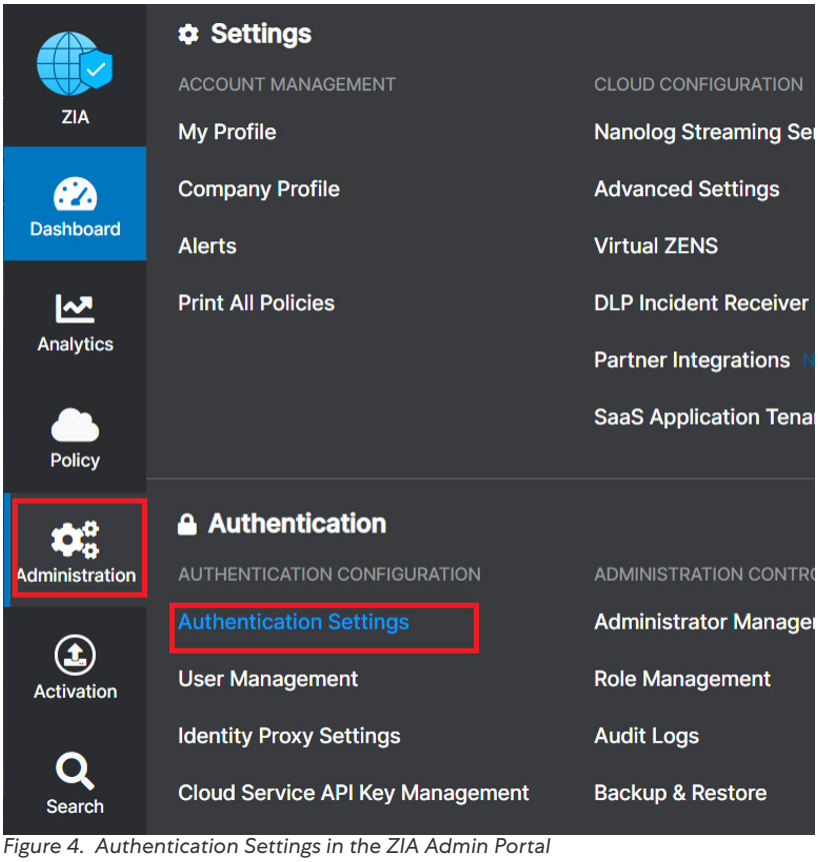

Figure 4. Authentication Settings in the ZIA Admin Portal

3. In the Authentication Settings page, click **Add IdP**.

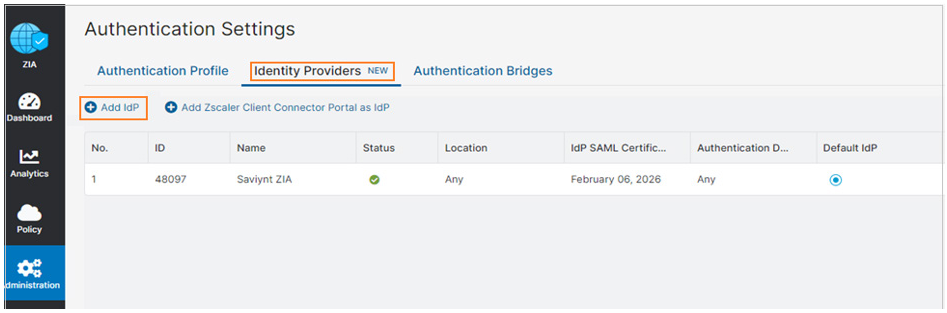

Figure 5. Add IdP

4. Specify the IdP Configuration details. The SCIM Configuration page displays the endpoint URL and the access token.

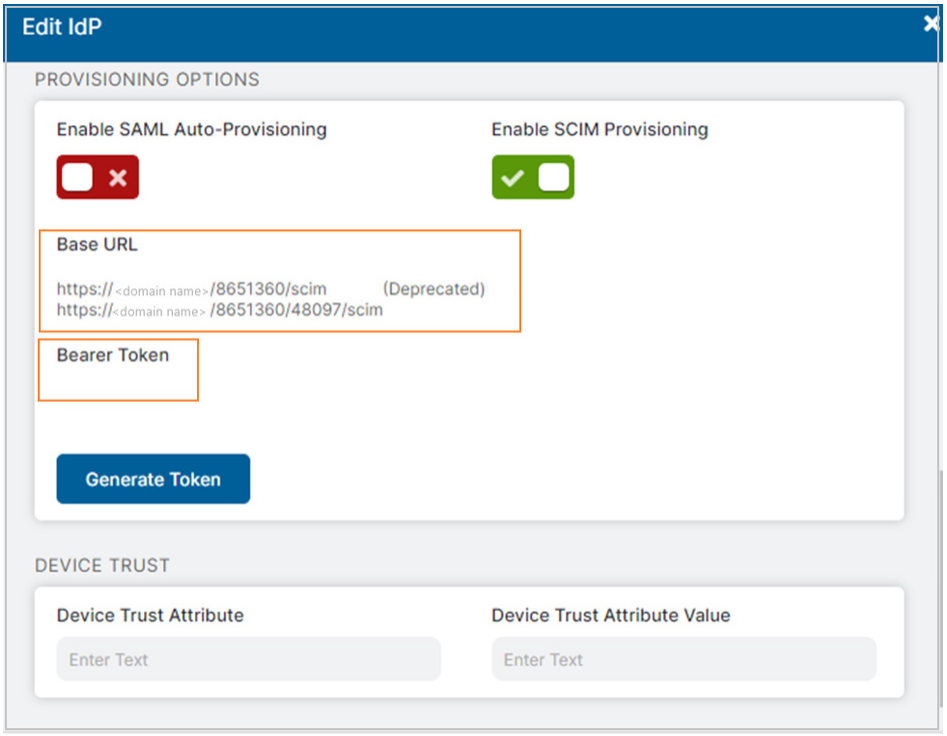

Figure 6. IdP Configuration page

In the figure, 8651360/48097 is the ZIA account number.

Creating a Connection

A connection refers to the configuration setup for connecting EIC to target applications.

Understanding the Configuration Parameters

When creating a connection, you must specify connection parameters that the connector uses to connect with the target application, define the type of operations to perform, the target application objects against which those operations are performed, and the frequency of performing them. In addition, you can view and edit attribute mappings between the EIC and the target application, predefined correlation rules, and provisioning and import jobs.

Configuration Parameters for Account and Access Import

The connector uses the following parameters for creating a connection and for importing account and access from the target application.

Connection Parameters

Connection Name

- **Description**: Specify the name to identify the connection.
- **Mandatory**: Yes

Connection Description

- **Description**: Specify the description for the connection.
- **Mandatory**: No

Connection Type

- **Description**: Select the connection type as REST.
- **Mandatory**: Yes

Default SAV Role

- **Description**: Specify this parameter to assign the SAV role for the connection. The SAV role is a role in EIC that assigns specific access to users. This parameter is valid only for importing users. Sample value: User assigned with the ROLE_ADMIN role, has access to all the sections of EIC.
- **Mandatory**: No

Email Template

- **Description**: Specify this parameter to select an email template for sending notifications. Email templates provide immediate trigger of emails to a user. Each email informs the user about the action performed. If critical, the email informs the user to take immediate action.
- **Mandatory**: No

ConnectionJSON

- **Description**: Specify this parameter to create a connection.
- **Mandatory**: Yes
- **Example Configuration**: Use the following format to connect to the ZPA application:

Modify the base URL to reflect your Zscaler tenant.

```
{
  "authentications": {
    "acctAuth": {
      "authType": "oauth2",
      "httpHeaders": {
        "contentType": "application/json"
      },
      "authError": [
        "InvalidAuthenticationToken",
        "AuthenticationFailed"
      ],
```



```
        "url": "https://<domain name>/scim/1/72058300560048147/v2",
        "httpMethod": "POST",
        "httpContentType": "application/json",
        "errorPath": "error.code",
        "maxRefreshTryCount": 5,
        "tokenResponsePath": "access_token",
        "tokenType": "Bearer",
        "authHeaderName": "Authorization",
        "accessToken": "<access token>",
        "httpParams": "[object Object]",
        "retryFailureStatusCode": []
      }
    }
  }
```

Use the following format to connect to the ZIA application:

Modify the base URL to reflect your Zscaler tenant.

```
{
  "authentications": {
    "acctAuth": {
      "authType": "oauth2",
      "httpHeaders": {
        "contentType": "application/json"
      },
      "authError": [
        "InvalidAuthenticationToken",
        "AuthenticationFailed"
      ],
```



```
        "url": "https://<domain name>/8651360/48097/scim",
        "httpMethod": "POST",
        "httpContentType": "application/json",
        "errorPath": "error.code",
        "maxRefreshTryCount": 5,
        "tokenResponsePath": "access_token",
        "tokenType": "Bearer",
        "authHeaderName": "Authorization",
        "accessToken": "<access token>",
        "httpParams": "[object Object]",
        "retryFailureStatusCode": []
      }
    }
  }
```

For more information on attribute descriptions in this parameter, see REST Connector Guide.

Import Parameters

ImportAccountEntJSON

- **Description**: Specify this parameter to map attributes of Zscaler application to attributes of EIC for account and entitlement import.
- **Mandatory**: Yes
- **Example Configuration**: Use the following format to import accounts and entitlements using the ZPA application:

Modify the base URL to reflect your Zscaler tenant.

```
{
"accountParams": {
"processingType":"SequentialAndIterative",
"connection": "acctAuth",
"createUsers": true,
"call": {
```



```
"call1": {
"http": {
"url": "https://<domain name>/scim/1/72058300560048147/v2/Users",
"basicUrl": "<domain name>",
"hostUrl": "/72058300560048128/scim/Users",
"httpContentType": "application/json",
"httpMethod": "GET",
"httpHeaders": {
        "Authorization": "${access_token}",
        "Accept": "application/json"
      }
},
"listField": "Resources",
"keyField": "name",
"colsToPropsMap": {
"accountID": "id~#~char",
"name": "userName~#~char",
"displayName": "displayName~#~char",
"customproperty1": "id~#~char",
"customproperty2": "department~#~char"
}}}
},
"entitlementParams": {
"processingType":"SequentialAndIterative",
"connection": "acctAuth",
"entTypes": {
"Entitlement": {
"call": {
"call1": {
"connection": "restconnectorscim",
```



```
"http": {
"url": "https://<domain name>/scim/1/72058300560048147/v2/Groups",
"basicUrl": "<domain name>",
"hostUrl": "/72058300560048128/scim/Groups",
"httpContentType": "application/json",
"httpMethod": "GET",
"httpHeaders": {
        "Authorization": "${access_token}",
        "Accept": "application/json"
      }
},
"listField": "Resources",
"keyField": "entitlementID",
"colsToPropsMap": {
"entitlementID": "id~#~char",
"entitlement_value": "displayName~#~char",
"customproperty1": "id~#~char",
"acctEntMappingInfoColumnFromEnt": "STORE#ACC#ENT#MAPPINGINFO~#~char"
}
}},
"acctEntMappings": {
"listField": "members",
"idPath": "value",
"keyField": "entitlementID"
}
}}},
    "acctEntParams": {
        "processingType": "entToAcctMapping"
    }
}
```


Use the following format to import accounts and entitlements using the ZIA application:

Modify the base URL to reflect your Zscaler tenant.

```
{
"accountParams": {
"processingType":"SequentialAndIterative",
"connection": "acctAuth",
"createUsers": true,
"call": {
"call1": {
"http": {
"url": "https://<domain name>/8651360/48097/scim/Users",
"basicUrl": "<domain name>",
"hostUrl": "/8651360/48097/scim/Users",
"httpContentType": "application/json",
"httpMethod": "GET",
"httpHeaders": {
        "Authorization": "${access_token}",
        "Accept": "application/json"
      }
},
"listField": "Resources",
"keyField": "name",
"colsToPropsMap": {
"accountID": "id~#~char",
"name": "userName~#~char",
"displayName": "displayName~#~char",
"customproperty1": "id~#~char",
"customproperty2": "department~#~char"
```



```
}}}
},
"entitlementParams": {
"processingType":"SequentialAndIterative",
"connection": "acctAuth",
"entTypes": {
"Entitlement": {
"call": {
"call1": {
"connection": "restconnectorscim",
"http": {
"url": "https://<domain name>/8651360/48097/scim/Groups",
"basicUrl": "<domain name>",
"hostUrl": "/8651360/48097/scim/Groups",
"httpContentType": "application/json",
"httpMethod": "GET",
"httpHeaders": {
        "Authorization": "${access_token}",
        "Accept": "application/json"
      }
},
"listField": "Resources",
"keyField": "entitlementID",
"colsToPropsMap": {
"entitlementID": "id~#~char",
"entitlement_value": "displayName~#~char",
"customproperty1": "id~#~char",
"acctEntMappingInfoColumnFromEnt": "STORE#ACC#ENT#MAPPINGINFO~#~char"
}
}},
```



```
"acctEntMappings": {
"listField": "members",
"idPath": "value",
"keyField": "entitlementID"
}
}}},
    "acctEntParams": {
        "processingType": "entToAcctMapping"
    }
}
```

For more information on attribute descriptions in this parameter, see REST Connector Guide.

CreateAccountJSON

- **Description**: Specify this parameter to create an account in the target application.
- **Mandatory**: Yes
- **Binding Variables**: The supported binding variables are:
  - ServiceAccountOwnerMap
  - endpoints
  - accountName
  - userManager
  - approvers
  - arsTasks/task
  - managerAccount
  - password
  - requestid
  - esponse
  - connection
  - userAccount
- **Example Configuration**: Use the following format to create accounts using the ZPA application:

Modify the base URL to reflect your Zscaler tenant.

```
{
  "accountIdPath": "Entitlement.message.id",
  "responseColsToPropsMap": {
```



```
    "name": "Entitlement.message.userName~#~char",
    "displayName": "Entitlement.message.displayName~#~char"
  },
  "call": [
    {
      "name": "Entitlement",
      "connection": "acctAuth",
      "url": "https://<domain name>/scim/1/72058300560048147/v2/Users",
      "httpMethod": "POST",
      "httpParams": "{\"schemas\":[\"urn:ietf:params:scim:schemas:core:2.0:User\",\"urn:ietf:params:scim:schemas:extension:enterprise:2.0:User\"],\"userName\":\"${user.email}\",\"displayName\":\"${user.username}\",\"urn:ietf:params:scim:schemas:extension:enterprise:2.0:User\" : {\"department\":\"Saviynt Global\"}}",
      "httpHeaders": {
        "Authorization": "${access_token}",
        "Accept": "application/json"
      },
      "httpContentType": "application/json",
      "successResponses": {
        "statusCode": [201]
      }
    }
  ]
}
```

Use the following format to create accounts using the ZIA application:

Modify the base URL to reflect your Zscaler tenant.

```
 {
"accountIdPath": "Entitlement.message.id",
"responseColsToPropsMap": {
```



```
"name": "Entitlement.message.userName~#~char",

"displayName": "Entitlement.message.displayName~#~char"

},

  "call": [

    {

      "name": "Entitlement",

      "connection": "acctAuth",

      "url": "https://<domain name>/8651360/48097/scim/Users",

      "httpMethod": "POST",

      "httpParams": "{\"schemas\":[\"urn:ietf:params:scim:schemas:core:2.0:User\",\"urn:ietf:params:scim:schemas:extension:enterprise:2.0:User\"],\"userName\":\"${user.email}\",\"displayName\":\"${user.username}\",\"urn:ietf:params:scim:schemas:extension:enterprise:2.0:User\" : {\"department\":\"Saviynt Global\"}}",

      "httpHeaders": {

        "Authorization": "${access_token}",

        "Accept": "application/json"

      },

      "httpContentType": "application/json",

      "successResponses": {

        "statusCode": [

          201

        ]

      }

    }

  ]

}
```

For more information on attribute descriptions in this parameter, see REST Connector Guide.

AddAccessJSON

- **Description**: Specify this parameter to add access to an account.
- **Mandatory**: Yes
- **Binding Variables**: The supported bindings are:
  - ServiceAccountOwnerMap
  - endpoints
  - userManager
  - approvers
  - arsTasks/task
  - managerAccount
  - requestid
  - response
  - connection
  - userAccount
  - requestAccessAttributes/reqAttrs
  - businessJustification
  - user
  - account
  - entitlementValue
- **Example Configuration**: Use the following format to add access using the ZPA application:

Modify the base URL to reflect your Zscaler tenant.

```
{
  "call": [
    {
      "name": "Entitlement",
      "connection": "acctAuth",
      "url": "https://<domain name>/scim/1/72058300560048147/v2/
Groups/${entitlementValue.entitlementID}",
      "httpMethod": "PATCH",
      "httpParams": "{\"schemas\": [\"urn:ietf:params:scim:api:messages:2.0:Pa-
tchOp\"],\"Operations\": [{\"op\": \"add\",\"value\":{\"members\":[{\"display\":
\"${account.name}\",\"value\": \"${account.accountID}\"}]}}]}",
      "httpHeaders": {
```



```
        "Authorization": "${access_token}",
        "Accept": "application/json"
      },
      "httpContentType": "application/json",
      "successResponses": {
        "statusCode": [204, 200, 201]
      }
    }
  ]
}
```

Use the following format to add access using the ZIA application:

Modify the base URL to reflect your Zscaler tenant.

```
{
  "call": [
    {
      "name": "Entitlement",
      "connection": "acctAuth",
      "url": "https://<domain name>/8651360/48097/scim/Groups/${entitlementValue.
entitlementID}",
      "httpMethod": "PATCH",
      "httpParams": "{\"schemas\": [\"urn:ietf:params:scim:api:messages:2.0:Pa-
tchOp\"],\"Operations\": [{\"op\": \"add\",\"value\":{\"members\":[{\"display\":
\"${account.name}\",\"value\": \"${account.accountID}\"}]}}]}",
      "httpHeaders": {
        "Authorization": "${access_token}",
        "Accept": "application/json"
      },
      "httpContentType": "application/json",
      "successResponses": {
        "statusCode": [
```



```
            204,
            200,
            201
          ]
        }
      }
    ]
  }
```

For more information on attribute descriptions in this parameter, see [REST Connector Guide](#).

RemoveAccessJSON

- **Description**: Specify this parameter to remove access from an account.
- **Mandatory**: Yes
- **Binding Variables**: The supported bindings are:
  - ServiceAccountOwnerMap
  - endpoints
  - userManager
  - approvers
  - arsTasks/task
  - managerAccount
  - requestid
  - response
  - connection
  - userAccount
  - requestAccessAttributes/reqAttrs
  - businessJustification
  - user
  - account
  - entitlementValue
  - account_entitlements

- **Example Configuration**: Use the following format to remove access using the ZPA application:

Modify the base URL to reflect your Zscaler tenant.

```
{
  "call": [
    {
      "name": "Entitlement",
      "connection": "acctAuth",
      "url": "https://<domain name>/scim/1/72058300560048147/v2/
Groups/${entitlementValue.entitlementID}",
      "httpMethod": "PATCH",
      "httpParams": "{\"schemas\": [\"urn:ietf:params:scim:api:messages:2.0:Pa-
tchOp\"],\"Operations\": [{\"op\": \"remove\",\"path\":\"members[value eq \\\"${ac-
count.accountID}\\\"]\"}]}",
      "httpHeaders": {
        "Authorization": "${access_token}",
        "Accept": "application/json"
      },
      "httpContentType": "application/json",
      "successResponses": {
        "statusCode": [204, 200, 201]
      }
    }
  ]
}
```


Use the following format to remove access using the ZIA application:

Modify the base URL to reflect your Zscaler tenant.

```
{
  "call": [
    {
      "name": "Entitlement",
      "connection": "acctAuth",
      "url": "https://<domain name>/8651360/48097/scim/Groups/${entitlementValue.
entitlementID}",
      "httpMethod": "PATCH",
      "httpParams": "{\"schemas\": [\"urn:ietf:params:scim:api:messages:2.0:Pa-
tchOp\"],\"Operations\": [{\"op\": \"remove\",\"path\":\"members[value eq \\\"${ac-
count.accountID}\\\"]\"}]}",
      "httpHeaders": {
        "Authorization": "${access_token}",
        "Accept": "application/json"
      },
      "httpContentType": "application/json",
      "successResponses": {
        "statusCode": [
          204,
          200,
          201
        ]
      }
    }
  ]
}
```

For more information on attribute descriptions in this parameter, see [REST Connector Guide](#).

RemoveAccountJSON

- **Description**: Specify this parameter to remove the account.
- **Mandatory**: Yes
- **Binding Variables**: The supported bindings are:
  - ServiceAccountOwnerMap
  - endpoints
  - userManager
  - approvers
  - arsTasks/task
  - managerAccount
  - requestid
  - response
  - connection
  - userAccount
  - businessJustification
  - user
  - accounts

- **Example Configuration**: Use the following format to remove accounts using the ZPA application:

Modify the base URL to reflect your Zscaler tenant.

```
{
  "call": [
    {
      "name": "Call1",
      "connection": "acctAuth",
      "url": "https://<domain name>/scim/1/72058300560048147/v2/Users/${account.
accountID}",
      "httpMethod": "DELETE",
      "httpHeaders": {
        "Authorization": "${access_token}",
        "Accept": "application/json"
      },
      "httpContentType": "application/json",
      "successResponses": {
        "statusCode": [200, 201, 204]
      }
    }
  ]
}
```


Use the following format to remove accounts using the ZIA application:

```
{
  "call": [
    {
      "name": "Call1",
      "connection": "acctAuth",
      "url": "https://<domain name>/8651360/48097/scim/Users/${account.accountID}",
      "httpMethod": "DELETE",
      "httpHeaders": {
        "Authorization": "${access_token}",
        "Accept": "application/json"
      },
      "httpContentType": "application/json",
      "successResponses": {
        "statusCode": [
          200,
          201,
          204
        ]
      }
    }
  ]
}
```

For more information on attribute descriptions in this parameter, see REST Connector Guide.

Creating a Security System

The security system represents the connection between the EIC and the target application. For more information on creating a security system, see Saviynt's documentation section Creating a Security System.

Using the Zscaler Connector

You can use the Zscaler connector for performing import and provisioning operations after configuring it to meet your requirements.

Guidelines for Using the Connector

You must apply the following guidelines for configuring import:

- Run account import before running the access import.
- Map all Zscaler attributes to the EIC account attributes using `ImportAccountEntJSON`.

Use Java ternary operators if you want to add conditions in the provisioning parameters.

Configuring Import Operations

- Full account import: When configuring the connection for the first time, perform a full import of all existing accounts from the target application to the EIC. To perform a full import, the invoke API gets a response from the target application and maps the attributes in the target application with attributes in the EIC. As part of this process, the deleted accounts are also identified and marked as suspended from import service.
- Full Access import: When configuring the connection for the first time, perform a full import of all existing access from the target application to the EIC. To perform a full import, the invoke API gets a response from the target application and maps the attributes in the target application with attributes in the EIC. As part of this process, the deleted entitlements are also identified and marked as inactive.

The reconciliation jobs are automatically created in the EIC after you create a connection for Zscaler. For more information about creating jobs, see Data Jobs.

Importing Accounts and Accesses

You must import accounts after the users are available in the EIC.

To import accounts:

1. Specify the connection and import parameters. For more information, see the Configuration Parameters for Account and Access Import section in Creating a Connection.

Ensure that you select the REST connection type.

2. Configure the Application Data Import (Single Threaded) job to import accounts and access. For more information, see Data Jobs.

Configuring Provisioning and Deprovisioning

Provisioning is automatically enabled when a connection is configured. For detailed information about performing provisioning tasks, see Access Request System.

To provision objects to the target application:

1. Specify the connection and provisioning parameters. For more information, see the Configuration Parameters for Provisioning section in Creating a Connection.

Ensure that you select the REST connection type.

2. Configure the Provisioning job (WSRETRY). For more information, see Provisioning Jobs.

When a provisioning job is triggered, it creates provisioning tasks in EIC. When these tasks are completed, the provisioning action is performed on the target application through the connector.

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.

To contact Zscaler Support:

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

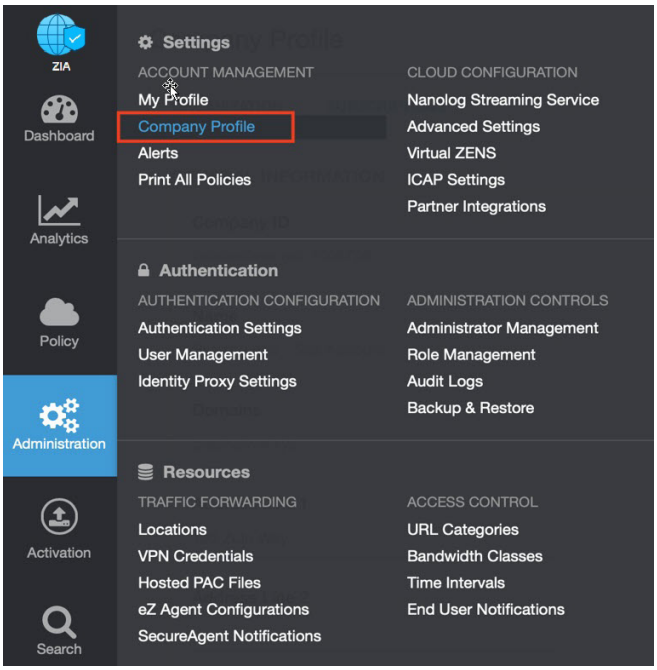

Figure 7. Collecting details to open support case with Zscaler TAC

2. Copy your Company ID.

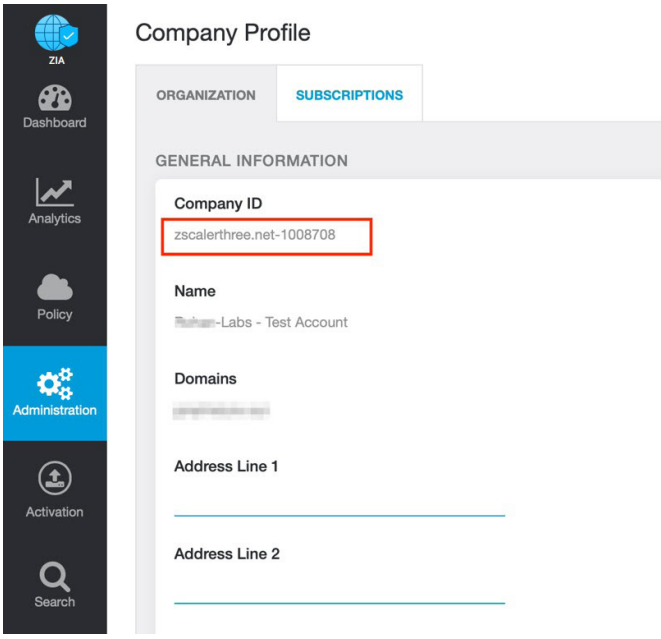

Figure 8. Company ID

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

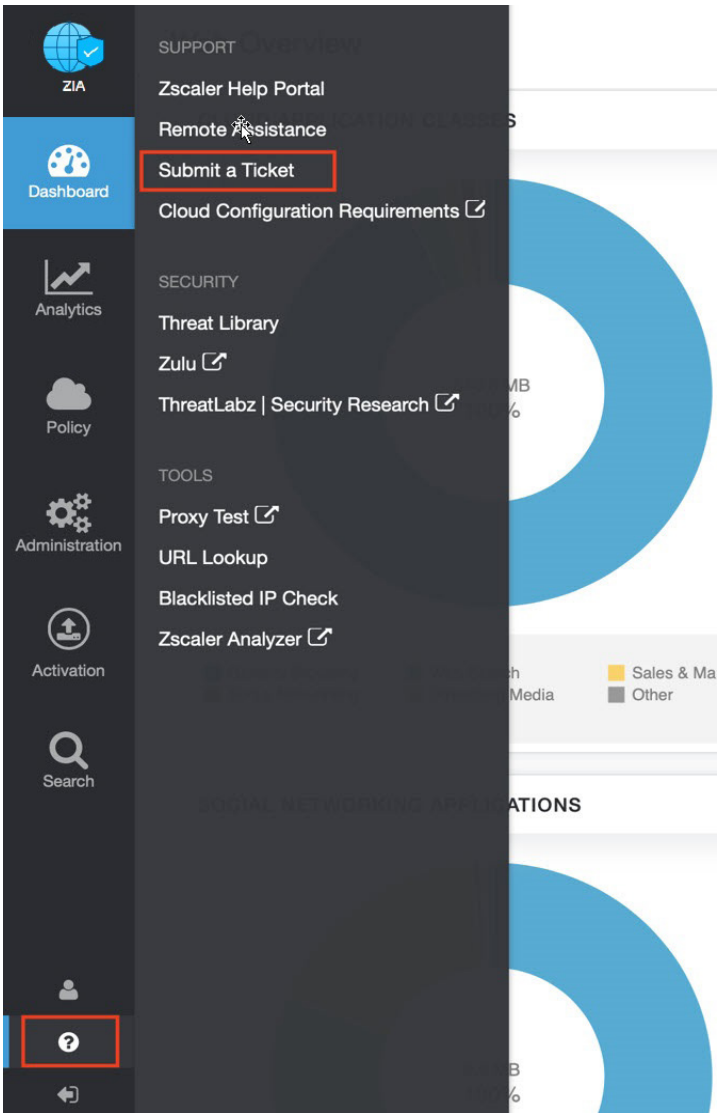

Figure 9. Submit a Ticket

