



ZSCALER AND SAILPOINT DEPLOYMENT GUIDE

Syncing Users and Groups from
Zscaler to Sailpoint

Contents

Terms and Acronyms	4
About This Document	5
Zscaler Overview	5
SailPoint Overview	5
Audience	5
Software Versions	5
Prerequisites	5
Request for Comments	6
Zscaler and SailPoint Introduction	7
ZIA Overview	7
ZPA Overview	7
Zscaler Resources	8
SailPoint IdentityIQ	8
SailPoint IdentityNow	8
SailPoint Resources	9
Configuring SailPoint IdentityIQ for ZIA	10
Create the Zscaler Application	10
Configuring Aggregation Tasks	19
Confirm Account Provisioning	27
Configuring SailPoint IdentityIQ for ZPA	32
Creating the Zscaler Application	32
Configuring Aggregation Tasks	41
Confirm Account Provisioning	48

Configuring SailPoint IdentityNow for ZIA	53
Creating the Zscaler Source	53
Additional Resources	56
Working with Connectors and Sources	56
Provisioning	56
Configuring SailPoint IdentityNow for ZPA	57
Creating the Zscaler Source	57
Additional Resources	60
Working with Connectors and Sources	60
Provisioning	60
Appendix A: Requesting Zscaler Support	61

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
DPD	Dead Peer Detection (RFC 3706)
GRE	Generic Routing Encapsulation (RFC2890)
IKE	Internet Key Exchange (RFC2409)
IPSec	Internet Protocol Security (RFC2411)
OAM	Operation, Administration, and Management
PFS	Perfect Forward Secrecy
SD-WAN	Software Defined Wide Area Network
SSL	Secure Socket Layer (RFC6101)
TLS	Transport Layer Security (RFC5246)
XFF	X-Forwarded-For (RFC7239)
ZIA	Zscaler Internet Access (Zscaler)
ZPA	Zscaler Private Access (Zscaler)

About This Document

This section describes the partners involved in the integration described in this 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. For more information on Zscaler, see [Zscaler's website](#).

SailPoint Overview

SailPoint (NYSE: [SAIL](#)) provides security software products and services. The company offers identity governance software that integrates role, access request, and compliance management solutions. SailPoint Technologies serves banks, property and casualty insurers, telecommunication providers, and healthcare sectors worldwide.

Audience

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

- [Zscaler Resources](#)
- [SailPoint Resources](#)
- [Appendix A: Requesting Zscaler Support](#)

Software Versions

This document was written using the latest version of Zscaler software and SailPoint IdentityIQ 8.0 and SailPoint IdentityNow.

Prerequisites

This guide provides GUI examples for configuring Zscaler Internet Access (ZIA) or Zscaler Private Access (ZPA) and SailPoint. All examples in this guide presume the reader has a basic comprehension of Identity and Access Management (IAM). All examples in this guide explain how to provision new service with Zscaler and with SailPoint. The prerequisites to use this guide are:

- ZPA and ZIA
 - A working instance of ZPA or ZIA (any cloud)
 - Administrator login credentials
- SailPoint
 - A working instance of SailPoint IdentityIQ with administrator login credentials, or
 - A working instance of SailPoint IdentityNow with administrator login credentials

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 SailPoint Introduction

This guide covers the specific use case of syncing users/groups from Zscaler to SailPoint via SCIM to provide visibility of identity and entitlements to an organization. For other use cases regarding SailPoint, consult Zscaler Professional Services.



This guide **does not** cover configuring SailPoint for user authentication and provisioning as with a traditional IdP. Zscaler currently does not support that integration use case.

The following are overviews of the Zscaler and SailPoint applications 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 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 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

Zscaler Private Access (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.
ZPA Help Portal	Help articles for ZPA.
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 based on general topic areas.

Name and Link	Description
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.
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.

SailPoint IdentityIQ

SailPoint IdentityIQ is an identity and access management (IAM) solution for enterprise customers that delivers automated access certifications, policy management, access request and provisioning, password management, and identity intelligence. IdentityIQ has a flexible connectivity model that simplifies the management of applications running on-premises or in the cloud.

SailPoint IdentityNow

SailPoint IdentityNow is a SaaS identity governance solution that allows you to control user access to all systems and applications, enhance audit response, and increase your operational efficiency.

It's delivered from the cloud as multi-tenant SaaS, so IdentityNow can be up and running quickly with no additional hardware or software to purchase, install, or maintain.

- Easy to deploy with rapid time to business value.
- Automatically delivers new features and enhancements.
- Scales up or down to meet your evolving needs.
- Can be managed by a business analyst, no identity expertise required.
- Simple, cloud software subscription model.
- Proven to reduce help desk calls by up to 90 percent.

SailPoint Resources

The following table contains links to SailPoint support resources.

Name and Link	Description
SailPoint Getting Started Guide	Help articles for using SailPoint software.
SailPoint Customer Service	Site for getting SailPoint support.
SailPoint Community	Site for accessing the SailPoint online technical community.
SailPoint Developer Community	Site for developer help and support.

Configuring SailPoint IdentityIQ for ZIA

The following describes how to configure SailPoint IdentityIQ for ZIA.

Create the Zscaler Application

The following describes how to create the Zscaler application:

1. From the **Applications** drop-down menu, select **Application Definition**.

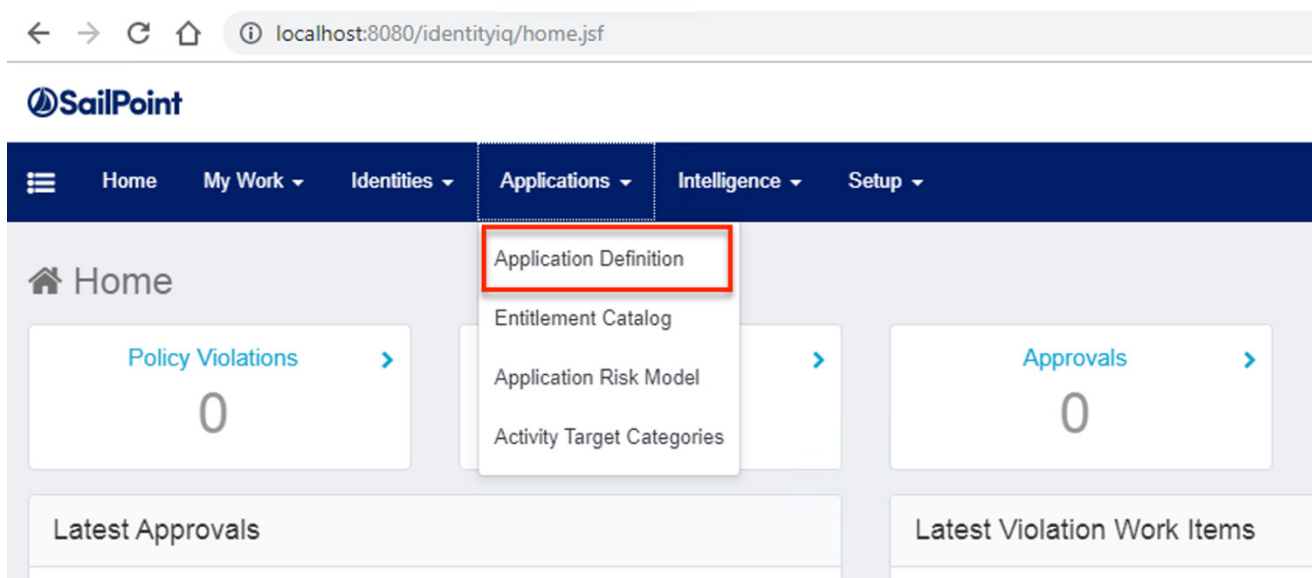


Figure 1. Create the Zscaler application definition

2. Click **Add New Application**.

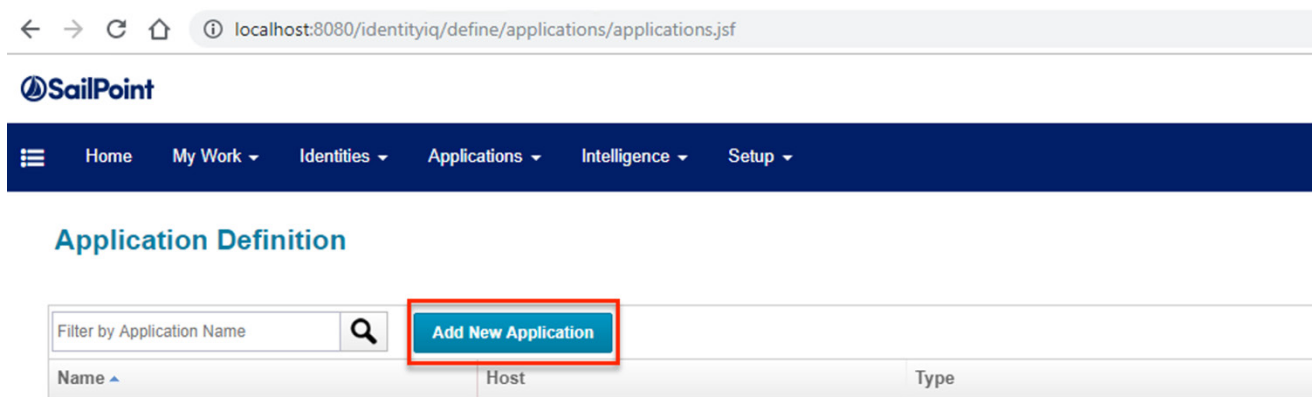


Figure 2. Add new application

3. Select **SCIM 2.0** from the **Application Type** drop-down menu to configure the application type.

The screenshot shows the SailPoint web interface for editing an application. The browser address bar displays `localhost:8080/identityiq/define/applications/application.jsf`. The page title is "Edit Application". The "Details" tab is active. The "Application Type" dropdown menu is open, showing a list of application types. "SCIM 2.0" is highlighted with a red box, and a red arrow points to it. Other application types in the list include RuleBasedFileParser, SAP - Direct, SAP GRC, SAP HANA Database, SAP HR/HCM, SAP Portal - UMWebService, SCIM, SOAPConnector, SQLloader, Salesforce, SecurityIQ, ServiceNow, Siebel, Solaris - Direct, SuccessFactors, SunOne - Direct, Sybase - Direct, Tenrox, and Top Secret LDAP. The "Extended Attributes" link is visible at the bottom of the dropdown. Other fields on the page include Name, Owner, Revoker, Proxy Application, Profile Class, and Scope, each with a dropdown menu or text input field. There are also checkboxes for Authoritative Application, Case Insensitive, Native Change Detection, and Maintenance Enabled.

Figure 3. Configure application type

4. Enter an application **Name**, and an application **Owner** for the ZIA application. For more information on how IdentityIQ uses these fields, refer to the [SailPoint product documentation](#).

The screenshot shows the 'Edit Application' page in the SailPoint IdentityIQ interface. The browser address bar shows 'localhost:8080/identityiq/define/applications/application.jsf'. The page has a dark blue header with the SailPoint logo and a navigation menu with items: Home, My Work, Identities, Applications, Intelligence, and Setup. Below the header, the page title is 'Edit Application'. A tabbed interface shows 'Details' as the active tab, with other tabs including Configuration, Correlation, Risk, Activity Data Sources, Rules, and Password Policy. The 'Details' tab contains several form fields. On the left, there is a section for 'Name' and 'Owner', both marked with an asterisk to indicate they are required fields. The 'Name' field contains 'Zscaler ZIA' and the 'Owner' field contains 'The Administrator'. Below these is the 'Application Type' dropdown, which is set to 'SCIM 2.0'. To the right of these fields are 'Revoker', 'Proxy Application', and 'Profile Class' dropdowns, all of which are currently empty. Below the 'Application Type' field is a 'Description' section with a rich text editor toolbar (bold, italic, underline, bulleted list, numbered list) and a language dropdown set to 'English (United States)'. The description area is empty, and a character count at the bottom indicates '7 of 1024 characters (including markup)'. On the right side of the page, there is a 'Scope' dropdown, which is also empty, followed by four checkboxes: 'Authoritative Application', 'Case Insensitive', 'Native Change Detection', and 'Maintenance Enabled', all of which are currently unchecked.

Figure 4. Log into Zscaler

5. Test the connection by entering the connection parameters specific to your ZIA SCIM server:
- Use the format `https://scim.zscalerbeta.net/<your_tenant_id>/scim` as the base URL.
 - Select **API Token** as the **Authentication Type**.
 - Enter the API token provided by your ZIA administrator.

6. Click **Test Connection** to ensure the parameters were entered correctly.

The screenshot shows the SailPoint IdentityIQ web interface. The browser address bar displays `localhost:8080/identityiq/define/applications/application.jsf`. The page title is "Edit Application". The navigation bar includes "Home", "My Work", "Identities", "Applications", "Intelligence", and "Setup". The "Configuration" tab is selected, showing sub-tabs for "Settings", "Schema", and "Provisioning Policies". The "SCIM Settings" section contains the following fields:

- Base URL: `https://scim.zscalerbeta.net/6120389/scim`
- Authentication Type: ☒ OAuth 2.0, ☒ API Token, ☐ Basic Authentication
- API Token: [Redacted]
- Account Filter: [Empty]
- Group Filter: [Empty]
- Role Filter: [Empty]
- Entitlement Filter: [Empty]
- Server Time Zone: [Empty]
- Explicit Attribute Request: ☐
- Accept Header: [Empty]
- Content-type Header: [Empty]

At the bottom left, a red box highlights the "Test Connection" button and the "Test Successful" status message.

Figure 5. Test connection

7. To configure the schema, go to the **Schema** sub-tab under the **Configuration** tab. Click **Discover Schema Attributes** in the **Object Type: account** section..

The screenshot shows the SailPoint web interface. The browser address bar displays `localhost:8080/identityiq/define/applications/application.jsf`. The SailPoint logo is in the top left. A navigation bar contains links: Home, My Work, Identities, Applications, Intelligence, and Setup. Below this is a section titled "Edit Application". A sub-navigation bar includes tabs: Details, Configuration, Correlation, Risk, Activity Data Sources, Rules, and Password Policy. Under the "Configuration" tab, there are sub-tabs: Settings, Schema (highlighted with a red box), and Provisioning Policies. The main content area is titled "Object Type: account". It has a "Details" section with fields for "Native Object Type" (User), "Identity Attribute" (id), "Display Attribute" (userName), and "Instance Attribute". There is also a "Remediation Modifiable" dropdown set to "Readonly". Below this is an "Attributes" section with a table header: Name, Description, Type, Properties. At the bottom of the "Attributes" section are three buttons: "Add New Schema Attribute", "Discover Schema Attributes" (highlighted with a red box), and "Delete Schema Attribute". A "Preview" button is located at the bottom left of the configuration area.

Figure 6. Schema Configuration

The ZIA user attributes are populated into the object.

Object Type: account

Details

Native Object Type:

Display Attribute:

Identity Attribute:

Instance Attribute:

Remediation Modifiable:

Attributes

	Name	Description	Type	Properties	
<input type="checkbox"/>	id	Unique Identifier for the SCIM Resource as defined by th	string ▼		Edit
<input type="checkbox"/>	externalId	A String that is an identifier for the resource as defined b	string ▼		Edit
<input type="checkbox"/>	userName	A service provider's unique identifier for the user, typicall	string ▼		Edit
<input type="checkbox"/>	name.familyName	The family name of the User, or last name in most West	string ▼		Edit
<input type="checkbox"/>	name.givenName	The given name of the User, or first name in most West	string ▼		Edit
<input type="checkbox"/>	displayName	The name of the User, suitable for displayto end-users.	string ▼		Edit
<input type="checkbox"/>	active	A Boolean value indicating the User's administrative stat	boolean ▼		Edit
<input type="checkbox"/>	groups	A list of groups to which the user belongs,either through	group ▼	Managed, Entitlement, Multi-Valued	Edit
<input type="checkbox"/>	department	department	string ▼		Edit

Figure 7. ZIA user attributes

8. Click **Discover Schema Attributes** in the **Object Type: group** section of the **Schema** sub-tab..

Object Type: group

Details

Native Object Type

Display Attribute

Identity Attribute

Instance Attribute

Description Attribute

Remediation Modifiable Readonly ▼

Attributes

Name Description Type Properties

Add New Schema Attribute **Discover Schema Attributes** Delete Schema Attribute

Preview

Figure 8. Discover schema attributes

9. Verify the ZIA group attributes populated in the group object.

Object Type: group

Details

Native Object Type

Display Attribute

Identity Attribute

Instance Attribute

Description Attribute

Remediation Modifiable Readonly ▼

Attributes

	Name	Description	Type	Properties	
<input type="checkbox"/>	id	Unique identifier for the SCIM Resource as defined by the	string ▼		⚙ Edit
<input type="checkbox"/>	externalid	A String that is an identifier for the resource as defined by the	string ▼		⚙ Edit
<input type="checkbox"/>	displayName	A human-readable name for the Group. REQUIRED.	string ▼		⚙ Edit
<input type="checkbox"/>	members	A list of members of the Group.	string ▼	Multi-Valued	⚙ Edit

Add New Schema Attribute Discover Schema Attributes Delete Schema Attribute

Preview

Figure 9. Verify attributes

10. Test the schema configuration by clicking **Preview** under each Object Type (account, group).

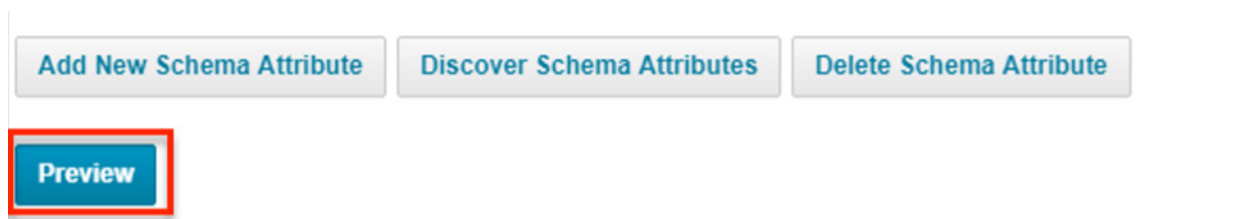


Figure 10. Test configuration

11. Click **Preview** to display the live data from the ZIA SCIM server connection (account preview shown).

userName	id	groups	externalId	name-family	name-givenN	displayName	active	department
adam.kenn...	7a736361-...					Adam Ken...	true	
admin@sa...	7a736361-...	7a736361-...				DEFAULT ...	true	Service Ad...
testy.test...	7a736361-...					Testy.Test...	true	Service Ad...

Figure 11. Preview Live Data

12. Configure provisioning plans. For this tutorial, an account creation plan is shown. First, click **Configuration > Provisioning Policies** in the application definition. Then click **Add Policy** next to the **Create** type in the **Object Type: account** section.

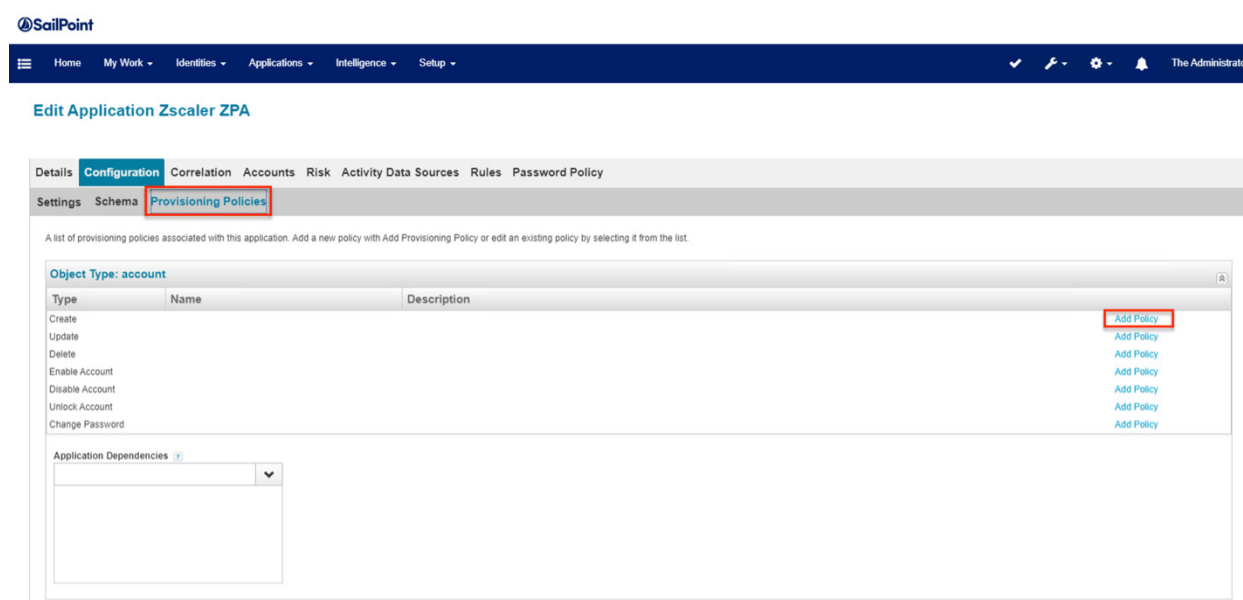


Figure 12. Configure provisioning plan

13. Click **Create Policy Form**.

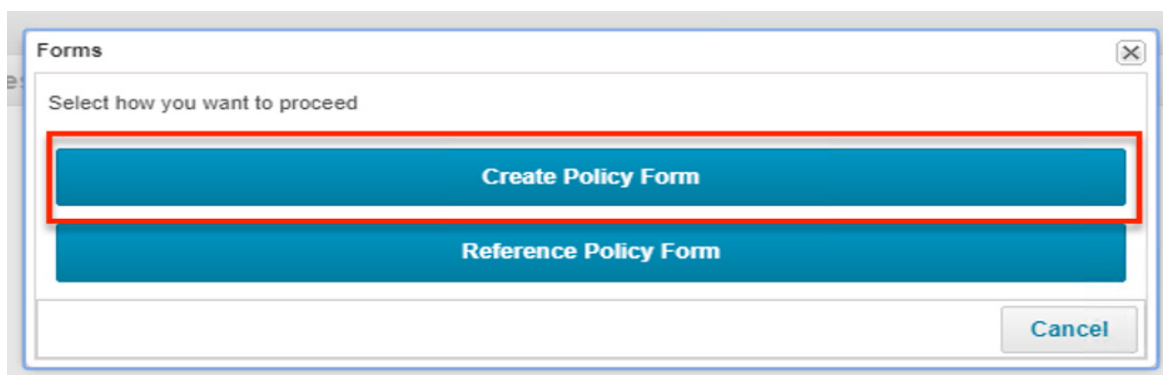


Figure 13. Create Policy Form

14. Configure the policy form for ZIA. For more information, refer to [SailPoint's provisioning documentation](#).

- Enter a name of the create account policy.
- (Optional) Enter a description.
- Add a section to the policy form. In this case, it was edited and named Required Attributes.
- Click the **Add (+)** icon next to the section to add a new field.
- For ZIA, new accounts require that a **Name** and **Display Name** are populated. Create a field for each of these.

For each field, make sure to select the **Required** checkbox under **Type Settings**.

Figure 14. Configure policy form for ZIA

15. Click **Save**.

- Verify that the new provisioning policy appears next to the **Create** type on the application definition.



Figure 15. Verify configuration policy

- Click **Save** at the bottom of the main application definition screen.

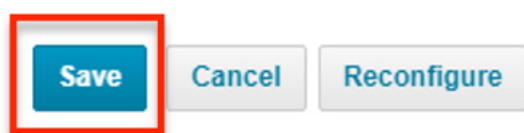


Figure 16. Save configuration policy

The new application is listed in the Application view of IdentityIQ.

Zscaler	https://scim.zscalerbeta.net/6120389/scim	SCIM 2.0	12/10/2019 11:57:47 am	account_group
---------	---	----------	------------------------	---------------

Figure 17. Verify new application

Configuring Aggregation Tasks

- From the **Setup** drop-down menu, select **Tasks**.

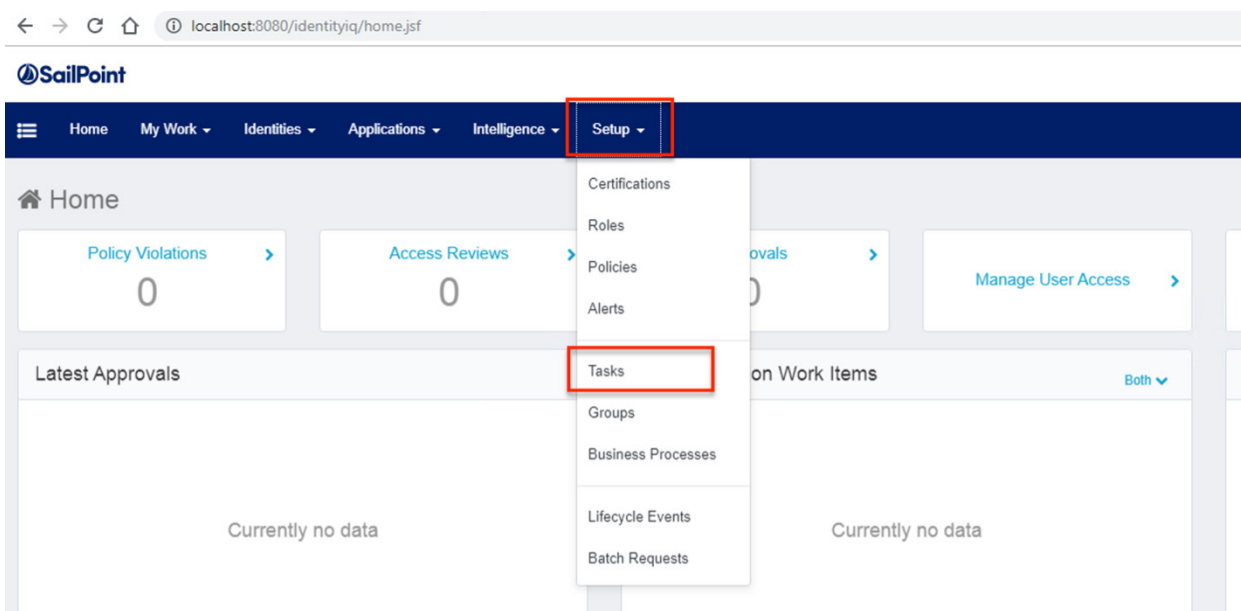


Figure 18. Configuring aggregation tasks

2. To create an account aggregation task, click **New Task** in the top-right of the window, and then select **Account Aggregation**.

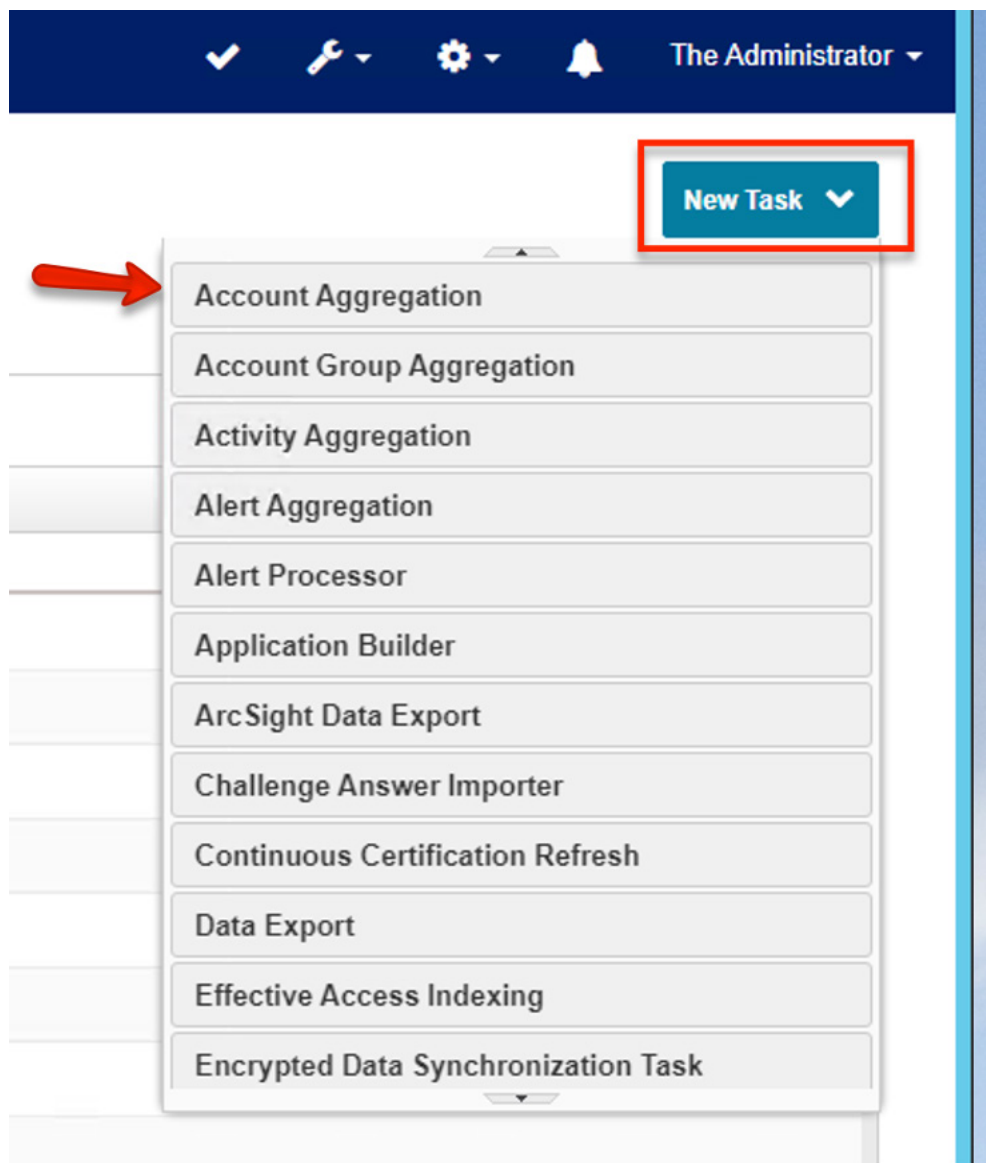


Figure 19. Create new task

3. Give the task a name, and make sure to select the previously-defined ZIA application from the **Select applications to scan** drop-down menu.

New Task

Standard Properties

*Indicates a required field

Name* Zscaler Account Aggregation Previous Result Action Delete

Description Task template for application account scanning.

Allow Concurrency ☐

Require Signoff ☐

Host

Number of Runs 0

Average Run Time 0:00:00

Reset Run Statistics

Email Task Alerts

Email Notification Disabled

Scope

Account Aggregation Options

Select applications to scan* Zscaler

Optionally select a rule to assign capabilities or perform other processing on new identities -- Select Rule --

Figure 20. Configure task settings

4. Click **Save and Execute** at the bottom of the task configuration page.



Figure 21. Save and Execute

5. Verify that the new task displays under the **Type: Account Aggregation** section of the task list. Click the **Task Results** tab.

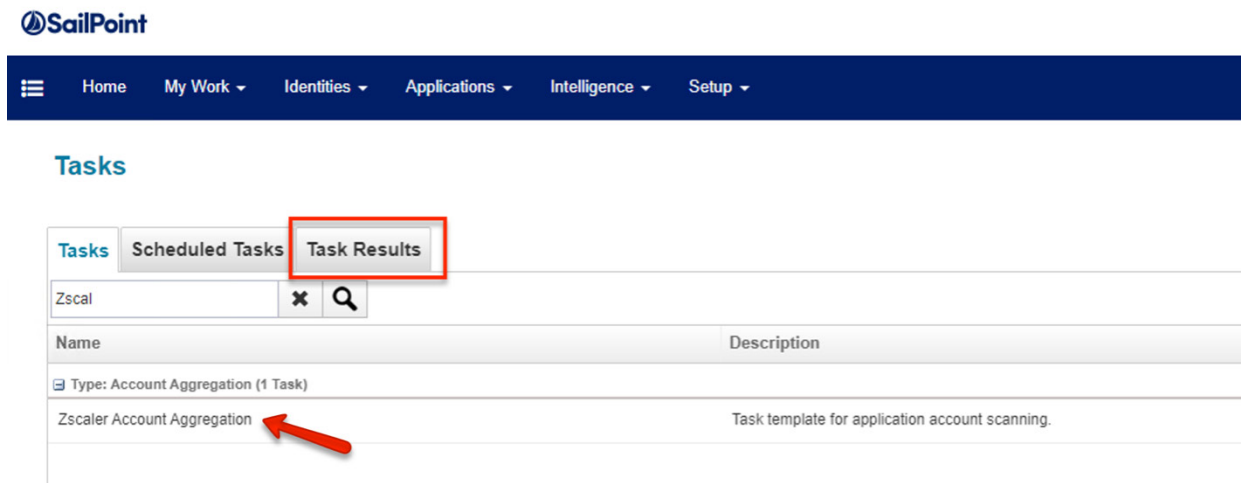


Figure 22. Verify account aggregation task

6. Confirm that the account aggregation completed.

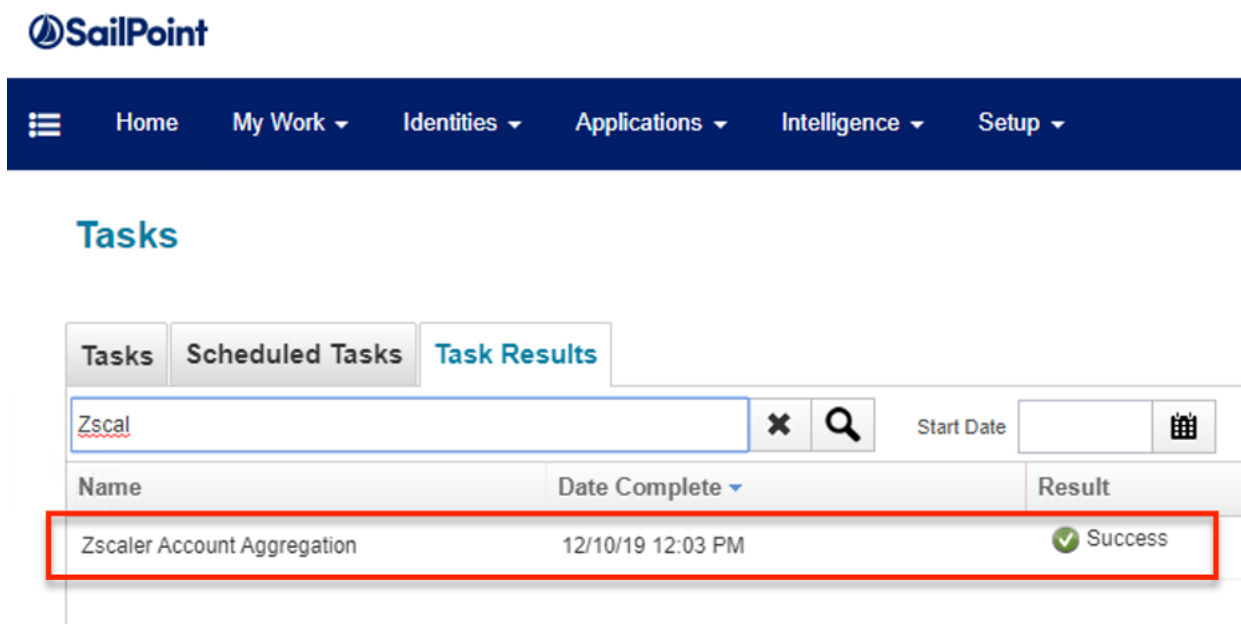


Figure 23. Config account aggregation task completion

7. View the task execution details by clicking the successful task.

The screenshot displays the SailPoint interface with a navigation bar at the top containing 'Home', 'My Work', 'Identities', 'Applications', 'Intelligence', and 'Setup'. The main heading is 'Task Result'. Below it, a 'Details' section contains two tables. The first table lists task metadata, and the second table lists execution attributes. A red box highlights the 'Zscaler Account Aggregation Attributes' table.

Details	
Name	Zscaler Account Aggregation
Type	Account Aggregation
Description	Task template for application account scanning.
Run Time	0:00:02
Run Time Change	0%
Status	Success
Started By	The Administrator
Started	12/10/19 12:03:57 PM
Completed	12/10/19 12:03:59 PM
Average Run Time	0:00:02
Host	ad-resource
Progress	Completed

[Return to Tasks](#)

Zscaler Account Aggregation Attributes	
Attribute	Value
Applications scanned	Zscaler
Accounts scanned	3
Accounts optimized	3

Figure 24. View task execution details

8. Return to the main tasks window to create a group aggregation task. Click **New Task**, and then select **Account Group Aggregation**.

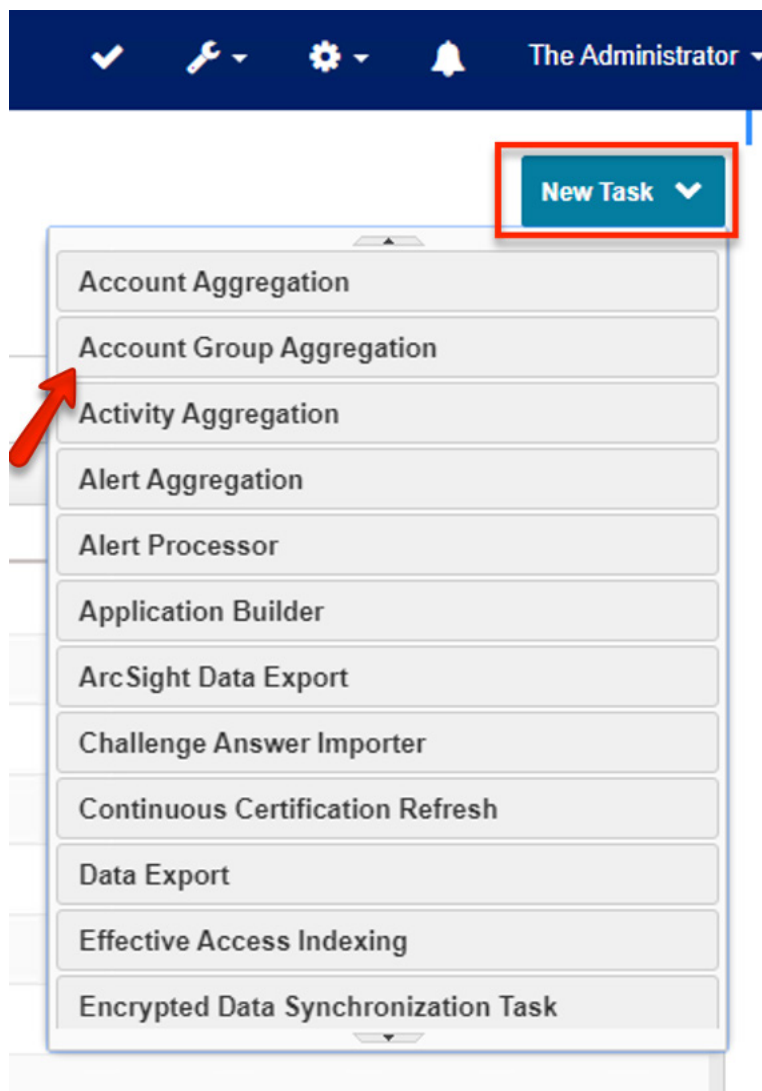


Figure 25. Create group aggregation task

9. Like the account aggregation, give the group aggregation a name and select the ZIA application from the **Select applications to scan** drop-down menu.

SailPoint

Home My Work Identities Applications Intelligence Setup

New Task

Standard Properties

*Indicates a required field.

Name* Zscaler Group Aggregation

Description Task template for application group scanning.

Allow Concurrency ☐

Require Signoff ☐

Host

Number of Runs 0

Average Run Time 0:00:00

Reset Run Statistics

Email Task Alerts

Email Notification Disabled

Scope

Account Group Aggregation Options

Select applications to scan*

Zscaler

Figure 26. Link account aggregation

10. Click **Save and Execute**.

Save Save and Execute Cancel Refresh

Figure 27. Save and Execute

11. Confirm the group aggregation was successful by switching to the **Task Results** tab.


Tasks Scheduled Tasks Task Results		
Zscaler		
Start Date		
Name	Date Complete	Result
Zscaler Group Aggregation	12/10/19 12:07 PM	✓ Success
Zscaler Account Aggregation	12/10/19 12:03 PM	✓ Success

Figure 28. Confirm group aggregation

12. View a detailed summary of the task by clicking the task.

Task Result

Details

Name	Zscaler Group Aggregation	Started By	The Administrator
Type	Account Group Aggregation	Started	12/10/19 12:07:12 PM
Description	Task template for application group scanning.	Completed	12/10/19 12:07:15 PM
Run Time	0:00:02	Average Run Time	0:00:00
Run Time Change	0%	Host	ad-resource
Status	 Success	Progress	Completed

Return to Tasks

Zscaler Group Aggregation Attributes

Attribute	Value
Applications scanned	Zscaler
Groups scanned	2
Groups created	2

Zscaler Attributes

group	
Application Objects scanned	2
Application Objects created	2

Figure 29. View task detailed summary

Confirm Account Provisioning

Confirm that the account provisioning was accurately set up.

1. Click the menu in the top left of any screen in IdentityIQ. Go to **Manage User Access > Manage Accounts**.

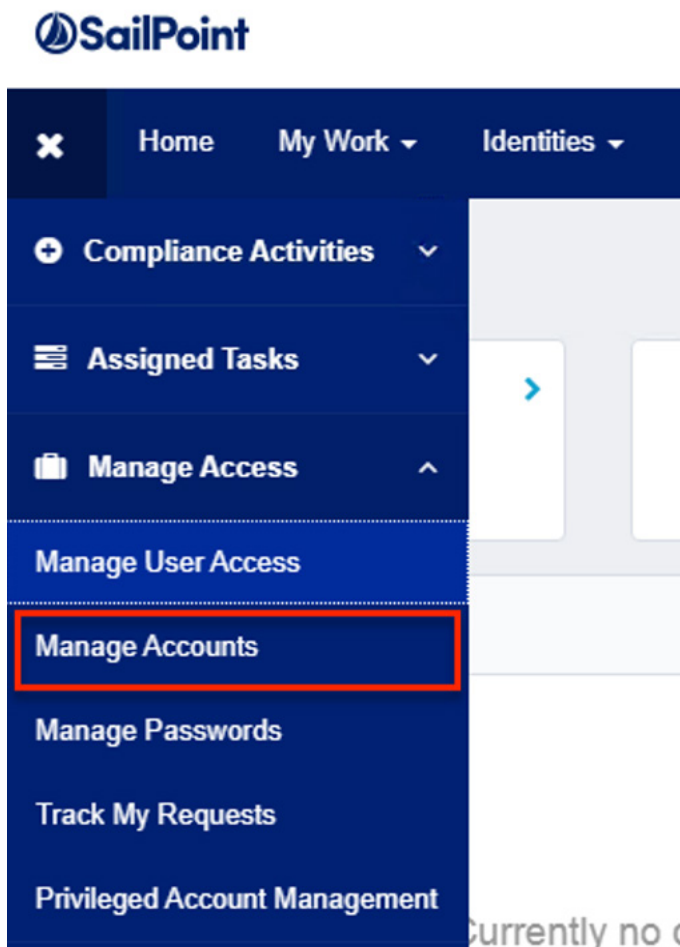


Figure 30. Navigate to Manage Accounts

- Find the identity for which you are creating a new ZIA account. Click **Manage** for that user's tile.

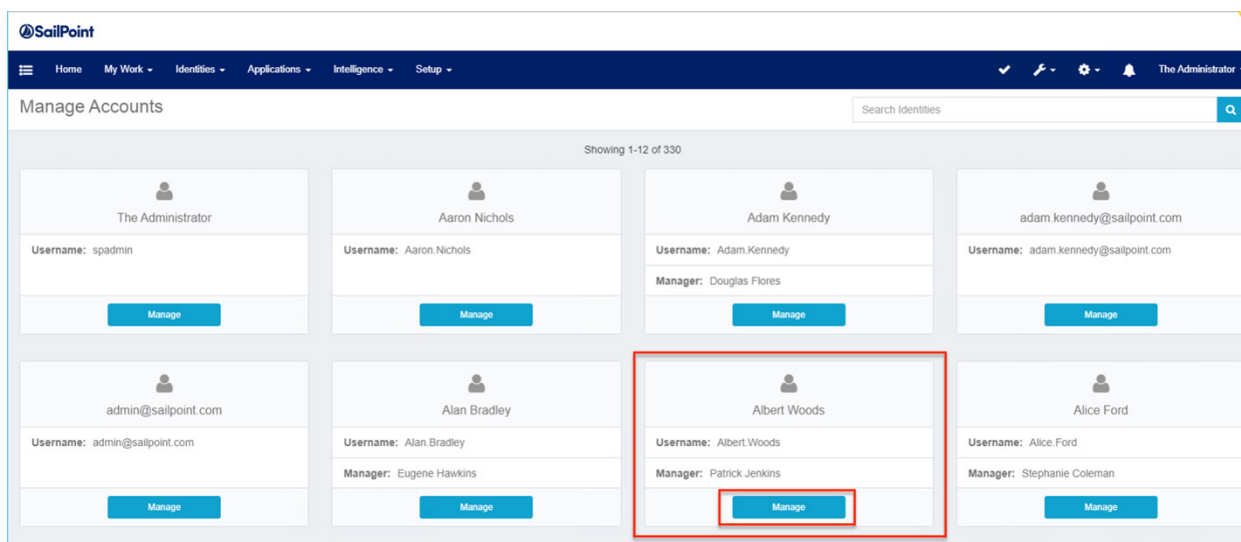


Figure 31. Manage ZIA user

- Click **Request Account**, which displays the identities currently-provisioned application accounts.

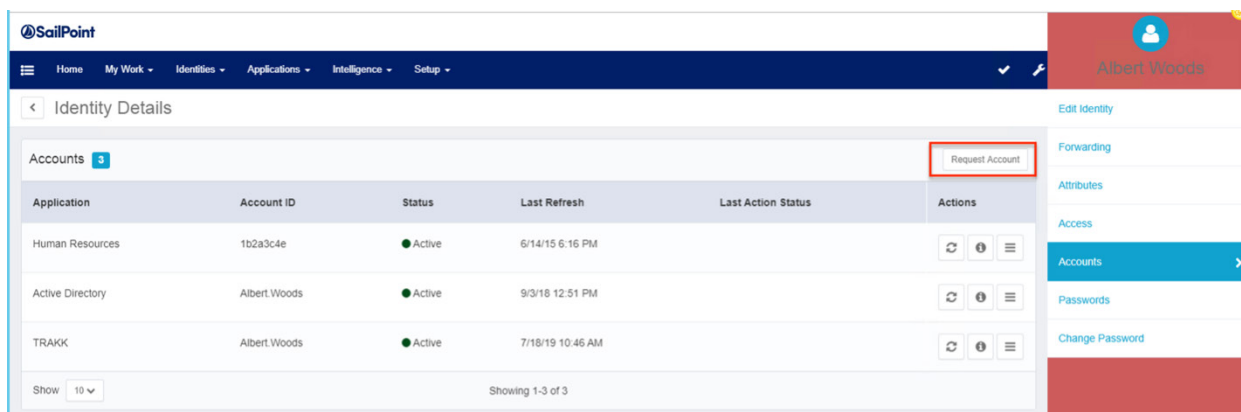
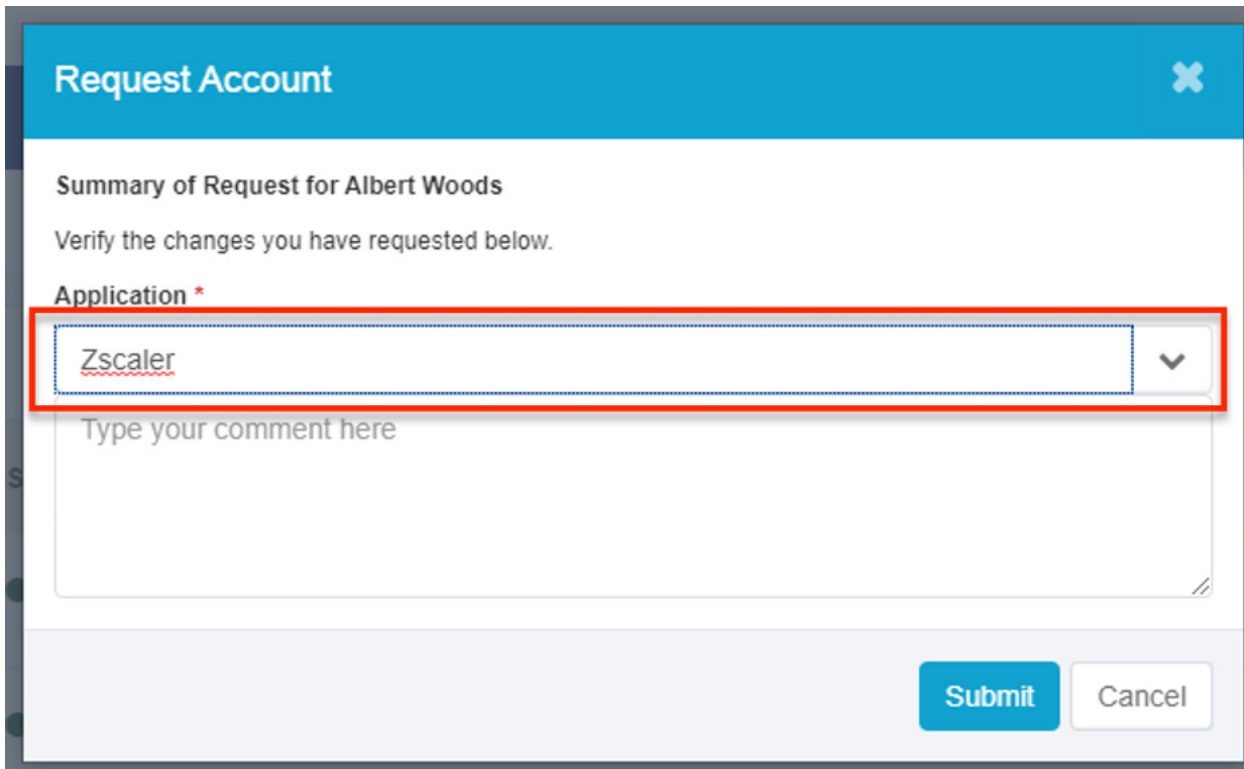


Figure 32. Request ZIA user

4. Select the ZIA application from the **Application** drop-down menu.

A screenshot of a 'Request Account' dialog box. The title bar is blue with the text 'Request Account' and a close button. Below the title bar, the text 'Summary of Request for Albert Woods' is displayed, followed by 'Verify the changes you have requested below.' The 'Application' field is a dropdown menu with 'Zscaler' selected and is highlighted with a red border. Below this is a text area with the placeholder 'Type your comment here'. At the bottom right, there are 'Submit' and 'Cancel' buttons.

Request Account

Summary of Request for Albert Woods

Verify the changes you have requested below.

Application *

Zscaler

Type your comment here

Submit Cancel

Figure 33. Request ZIA application

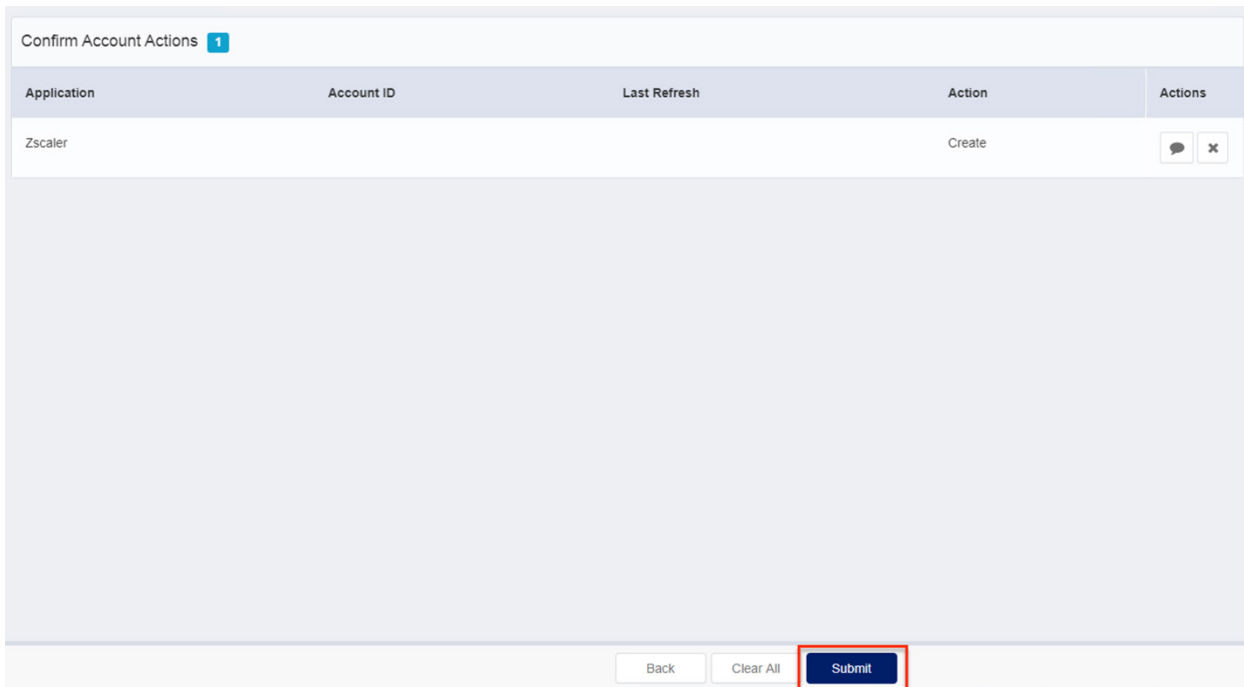
5. Click **Confirm**.

A screenshot showing two buttons: 'Clear All' and 'Confirm'. The 'Confirm' button is dark blue with white text and is highlighted with a red border.



Clear All Confirm

Figure 34. Confirm ZIA application

6. Submit the user request by clicking **Submit**.



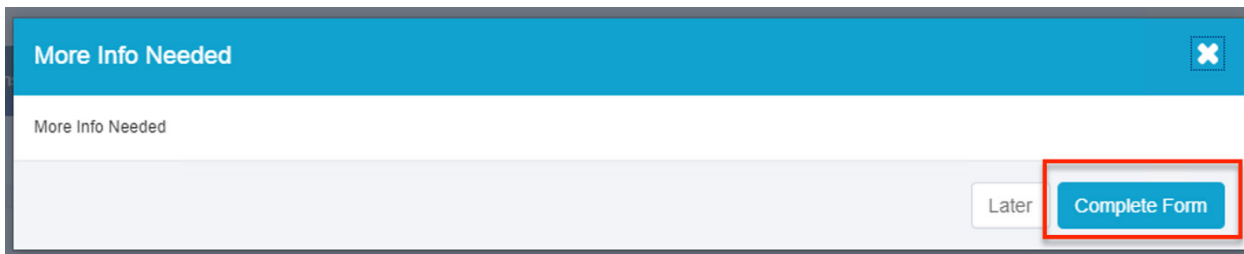
The image shows a 'Confirm Account Actions' dialog box with a blue header bar containing the title and a notification icon. Below the header is a table with five columns: Application, Account ID, Last Refresh, Action, and Actions. The table contains one row for 'Zscaler' with the action 'Create'. To the right of the 'Create' action are two icons: a speech bubble and a close button. At the bottom of the dialog are three buttons: 'Back', 'Clear All', and 'Submit'. The 'Submit' button is highlighted with a red rectangle.

Application	Account ID	Last Refresh	Action	Actions
Zscaler			Create	 

Back Clear All **Submit**

Figure 35. Submit user request

7. Since the create provisioning policy had several required fields (**userName**, **displayName**), IdentityIQ prompts the requester with a form to provide those values. Click **Complete Form**.



The image shows a 'More Info Needed' dialog box with a blue header bar containing the title and a close button. Below the header is a white area with the text 'More Info Needed'. At the bottom right of the dialog are two buttons: 'Later' and 'Complete Form'. The 'Complete Form' button is highlighted with a red rectangle.

More Info Needed

Later **Complete Form**

Figure 36. Enter in user required fields

8. Fill in the **User Name**. The user name must be in the format of a valid email address. Click **Ok**.

Complete Work Item

Request provisioning form for Albert.Woods

Please supply initial values for account attributes in the forms below.

Request Information

Requester
The Administrator

Target Identity

First Name
Albert

Last Name
Woods

Account ID
Albert Woods

Assigned Roles
All Users, Inventory Analyst

Zscaler

User Name *

albert.woods@sailpoint.com

Username must be a valid email address

Cancel Ok

Figure 37. Verify user email address

9. To confirm if the account was correctly provisioned, run another account aggregation for the ZIA application. Otherwise, confirm directly in ZIA.

Attributes				
Attribute	Value			
Applications scanned	Zscaler			
Accounts scanned	4			
Accounts optimized	3			
Identities updated	1			

Application	Account	Action	Identity	Attribute
Zscaler	7a736361-6c65-7200-7363-696d0060484f	CorrelateManual	Albert.Woods	undetermined

Figure 38. Confirm account provisioning

Configuring SailPoint IdentityIQ for ZPA

The following section reviews how to configure SailPoint IdentityIQ for ZPA.

Creating the Zscaler Application

The following describes how to create the Zscaler application:

1. From the **Applications** drop-down menu, select **Application Definition**.

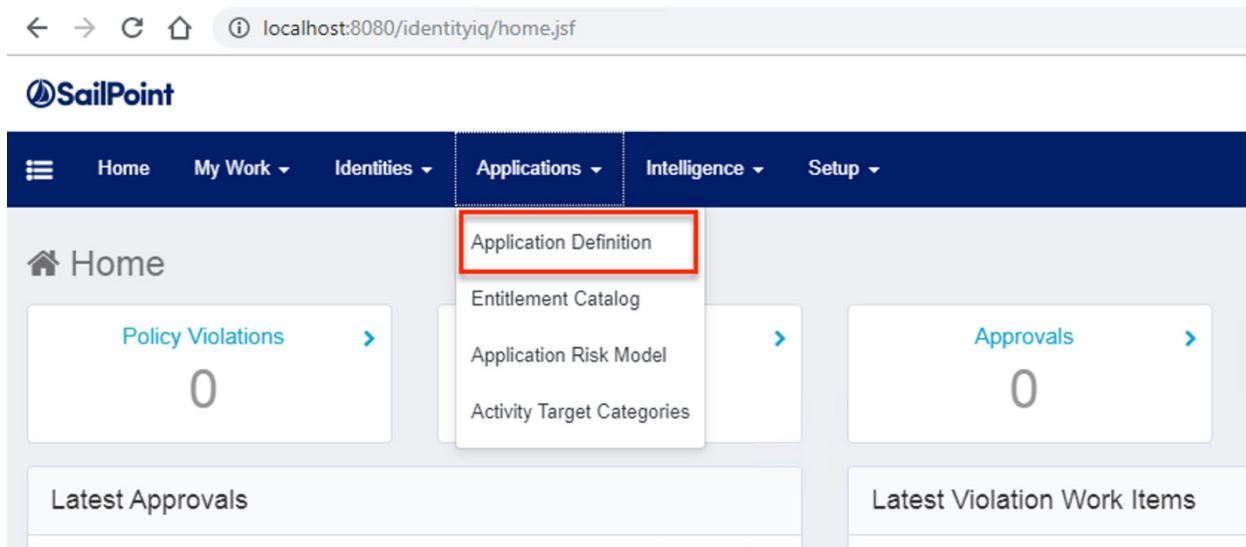


Figure 39. Create the Zscaler application definition

2. Click **Add New Application**.

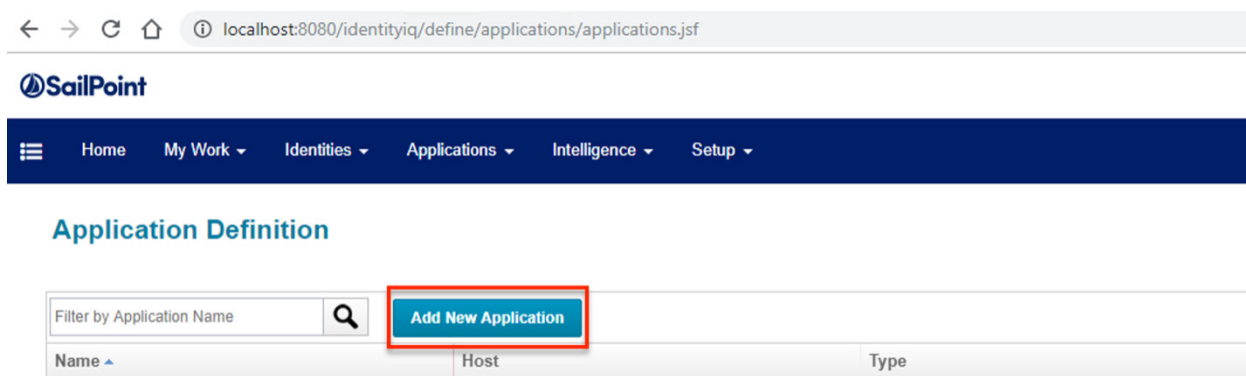


Figure 40. Add new application

3. To set the application type, select **SCIM 2.0** from the **Application Type** drop-down menu.

The screenshot shows the SailPoint web interface for editing an application. The browser address bar displays `localhost:8080/identityiq/define/applications/application.jsf`. The top navigation bar includes links for Home, My Work, Identities, Applications, Intelligence, and Setup. The main heading is "Edit Application".

The "Details" tab is active, showing a form with the following fields:

- Name**: A text input field.
- Owner**: A dropdown menu.
- Application Type**: A dropdown menu with a red arrow pointing to it. The dropdown is open, showing a list of application types. "SCIM 2.0" is highlighted with a red box.
- Revoker**: A dropdown menu.
- Proxy Application**: A dropdown menu.
- Profile Class**: A text input field.
- Scope**: A dropdown menu.
- Extended Attributes**: A section with checkboxes for "Authoritative Application", "Case Insensitive", "Native Change Detection", and "Maintenance Enabled".

The "Application Type" dropdown menu is open, showing a list of application types. "SCIM 2.0" is highlighted with a red box. A red arrow points to the dropdown menu.

Figure 41. Configure application type

4. Create a Zscaler application by entering an application name and an application owner for the ZPA application. For more information on how IdentityIQ uses these fields, refer to the [SailPoint Product Documentation](#).

localhost:8080/identityiq/define/applications/application.jsf

SailPoint

Home My Work Identities Applications Intelligence Setup

Edit Application

Details Configuration Correlation Risk Activity Data Sources Rules Password Policy

*Indicates a required field.

*Name [?](#)

Zscaler ZPA

*Owner [?](#)

The Administrator

*Application Type [?](#)

SCIM 2.0

Description [?](#)

B **I** **U** **English (United States)**

7 of 1024 characters (including markup)

Revoker [?](#)

Proxy Application [?](#)

Profile Class [?](#)

Scope [?](#)

☐ Authoritative Application [?](#)

☐ Case Insensitive [?](#)

☐ Native Change Detection [?](#)

☐ Maintenance Enabled [?](#)

Figure 42. Log into Zscaler

5. Test the connection by entering the connection parameters specific to your ZPA SCIM server:
- Use `https://scim.zscalerbeta.net/<your_tenant_id>/scim` as the base URL to the SCIM server.
 - Select **API Token** as the **Authentication Type**.
 - Enter the API token provided by your ZPA administrator.

6. Click **Test Connection** to ensure the parameters were entered correctly.

The screenshot shows the SailPoint IdentityIQ web interface. The browser address bar displays `localhost:8080/identityiq/define/applications/application.jsf`. The page title is "SailPoint". The navigation bar includes links for Home, My Work, Identities, Applications, Intelligence, and Setup. The main content area is titled "Edit Application". Below this, there are tabs for Details, Configuration (selected), Correlation, Risk, Activity Data Sources, Rules, and Password Policy. Under the Configuration tab, there are sub-tabs for Settings, Schema, and Provisioning Policies. The "SCIM Settings" section contains the following fields:

- Base URL *** (1): `https://scim.zscalerbeta.net/6120389/scim`
- Authentication Type** (2): ☒ OAuth 2.0, ☒ API Token, ☐ Basic Authentication
- API Token *** (3): [Redacted]
- Account Filter**: [Empty]
- Group Filter**: [Empty]
- Role Filter**: [Empty]
- Entitlement Filter**: [Empty]
- Server Time Zone**: [Empty]
- Explicit Attribute Request**: ☐
- Accept Header**: [Empty]
- Content-type Header**: [Empty]

At the bottom left, there is a "Test Connection" button and a "Test Successful" status message, both highlighted by a red box.

Figure 43. Test connection

7. Go to **Configuration > Schema** to set the schema configuration. Click **Discover Schema Attributes** under the **Object Type: account** section.

localhost:8080/identityiq/define/applications/application.jsf

SailPoint

Home My Work Identities Applications Intelligence Setup

Edit Application

Details **Configuration** Correlation Risk Activity Data Sources Rules Password Policy

Settings **Schema** Provisioning Policies

Object Type: account

Details

Native Object Type: User

Identity Attribute: id

Display Attribute: userName

Instance Attribute:

Remediation Modifiable: Readonly

Attributes

Name	Description	Type	Properties
------	-------------	------	------------

Add New Schema Attribute **Discover Schema Attributes** Delete Schema Attribute

Preview

Figure 44. Schema configuration

8. Review the populated ZPA attributes for a user.

Object Type: account

Details

Native Object Type:

Display Attribute:

Identity Attribute:

Instance Attribute:

Remediation Modifiable:

Attributes

	Name	Description	Type	Properties	
<input type="checkbox"/>	id	Unique Identifier for the SCIM Resource as defined by tr	string ▼		Edit
<input type="checkbox"/>	externalId	A String that is an identifier for the resource as defined b	string ▼		Edit
<input type="checkbox"/>	userName	A service provider's unique identifier for the user, typicall	string ▼		Edit
<input type="checkbox"/>	name.familyName	The family name of the User, or last name in most West	string ▼		Edit
<input type="checkbox"/>	name.givenName	The given name of the User, or first name in most West	string ▼		Edit
<input type="checkbox"/>	displayName	The name of the User, suitable for displayto end-users.	string ▼		Edit
<input type="checkbox"/>	active	A Boolean value indicating the User's administrative stat	boolean ▼		Edit
<input type="checkbox"/>	groups	A list of groups to which the user belongs,either through	group ▼	Managed, Entitlement, Multi-Valued	Edit
<input type="checkbox"/>	department	department	string ▼		Edit

Figure 45. ZPA user attributes

9. Click **Discover Schema Attributes** under the **Object Type: group** section of the Schema sub-tab.

Object Type: group

Details

Native Object Type

Identity Attribute

Description Attribute

Display Attribute

Instance Attribute

Remediation Modifiable
 Readonly ▼

Attributes

Name	Description	Type	Properties
Add New Schema Attribute Discover Schema Attributes Delete Schema Attribute			

[Preview](#)

Figure 46. Discover schema attributes

10. Verify that the attributes for the ZPA group were populated.

Object Type: group

Details

Native Object Type
 Group

Identity Attribute
 id

Description Attribute

Display Attribute

Instance Attribute

Remediation Modifiable
 Readonly ▼

Attributes

Name	Description	Type	Properties
<input type="checkbox"/> id	Unique identifier for the SCIM Resource as defined by the	string ▼	Edit
<input type="checkbox"/> externalid	A String that is an identifier for the resource as defined by the	string ▼	Edit
<input type="checkbox"/> displayName	A human-readable name for the Group. REQUIRED.	string ▼	Edit
<input type="checkbox"/> members	A list of members of the Group.	string ▼	Multi-Valued Edit

[Add New Schema Attribute](#) [Discover Schema Attributes](#) [Delete Schema Attribute](#)

[Preview](#)

Figure 47. Verify attributes

11. Test the configuration. Click **Preview** under each Object Type (account, group).

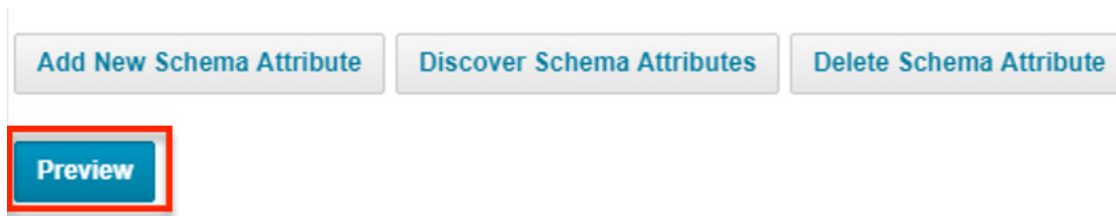


Figure 48. Test configuration

12. Review the live data from the ZPA SCIM server connection (account preview shown).

userName	id	groups	externalId	name-family	name-givenN	displayName	active	department
adam.kenn...	7a736361-...					Adam Ken...	true	
admin@sa...	7a736361-...	7a736361-...				DEFAULT ...	true	Service Ad...
testy.test...	7a736361-...					Testy.Test...	true	Service Ad...

Figure 49. Preview live data

13. Configure provisioning plans. This tutorial shows an account creation plan. First, click the **Configuration** > **Provisioning Policies** sub-tab in the application definition.
14. Click **Add Policy** next to the **Create** type in the **Object Type: account** section.

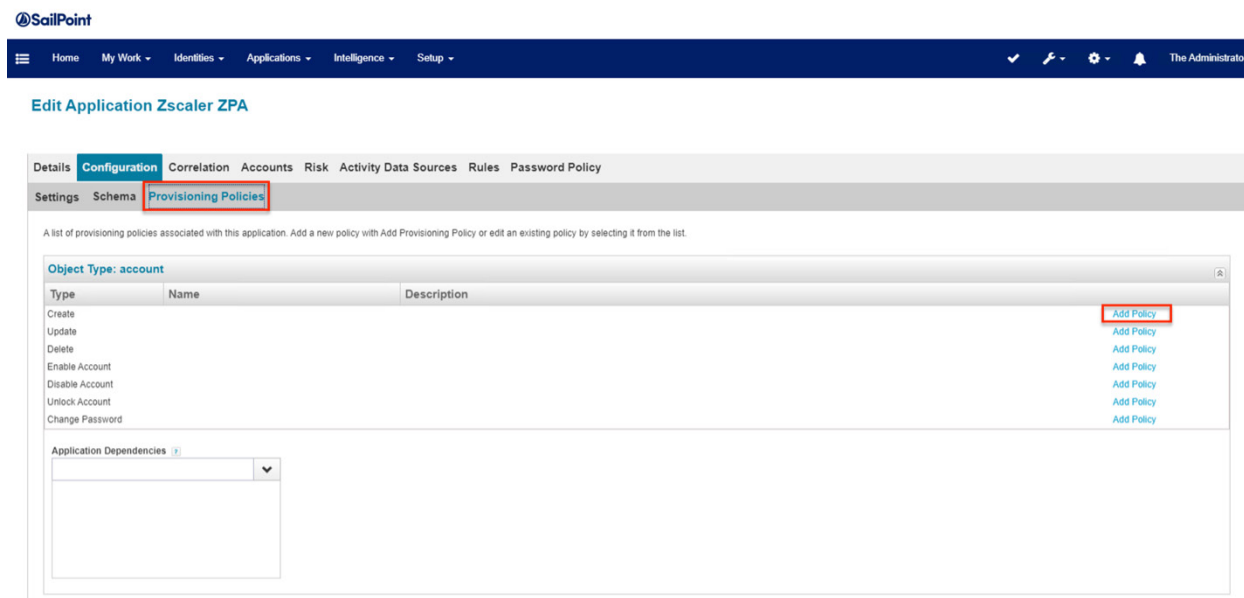


Figure 50. Configure provisioning plan

15. Click **Create Policy Form**.

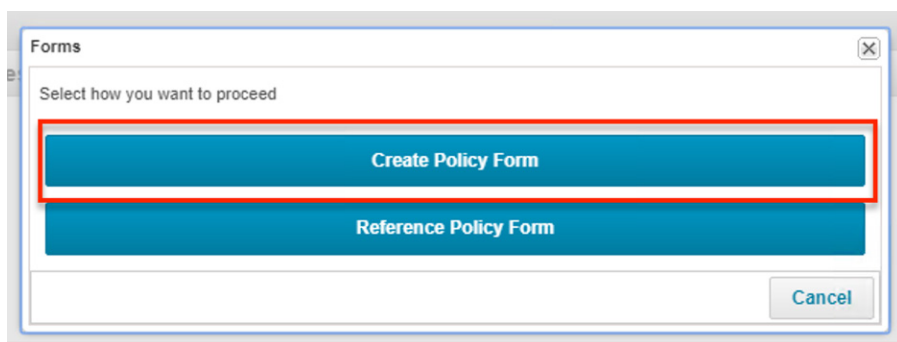


Figure 51. Create policy form

16. Configure the policy form for ZPA. For more information, refer to [SailPoint's provisioning documentation](#):

- a. Enter a name of the create account policy.
- b. (Optional) Enter a description.
- c. Add a section to the policy form. In this case, it was edited and named **Required Attributes**.
- d. Click the **Add (+)** icon next to the section to add a new field.
- e. For ZPA, new accounts require that a **Name and Display Name** are populated. Create a field for each of these.
- f. For each field, make sure to select the **Required** checkbox under **Type Settings**.
- g. When completed, click **Save**.

Figure 52. Configure policy form for ZPA

- Verify that the new provisioning policy appears next to the **Create** type on the application definition.



Figure 53. Verify configuration policy

- Save the configuration policy. Click **Save**.

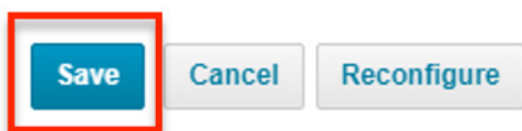


Figure 54. Save configuration policy

The new application is listed in the **Application** view of IdentityIQ.

Zscaler	https://scim.zscalerbeta.net/6120389/scim	SCIM 2.0	12/10/2019 11:57:47 am	account, group
---------	---	----------	------------------------	----------------

Figure 55. Verify new application

Configuring Aggregation Tasks

In this section, aggregation tasks for ZPA and SailPoint IdentityIQ are identified.

- From the **Setup** drop-down menu, select **Tasks**.

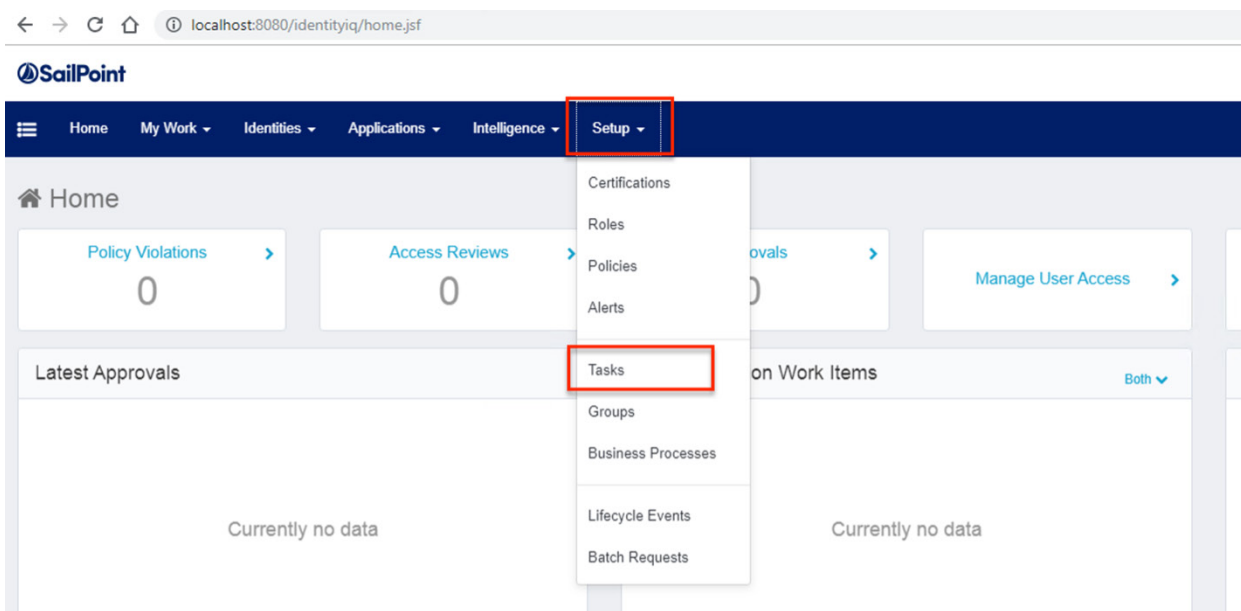


Figure 56. Configuring aggregation tasks

2. To create an account aggregation task, click **New Task**, and then select **Account Aggregation**.

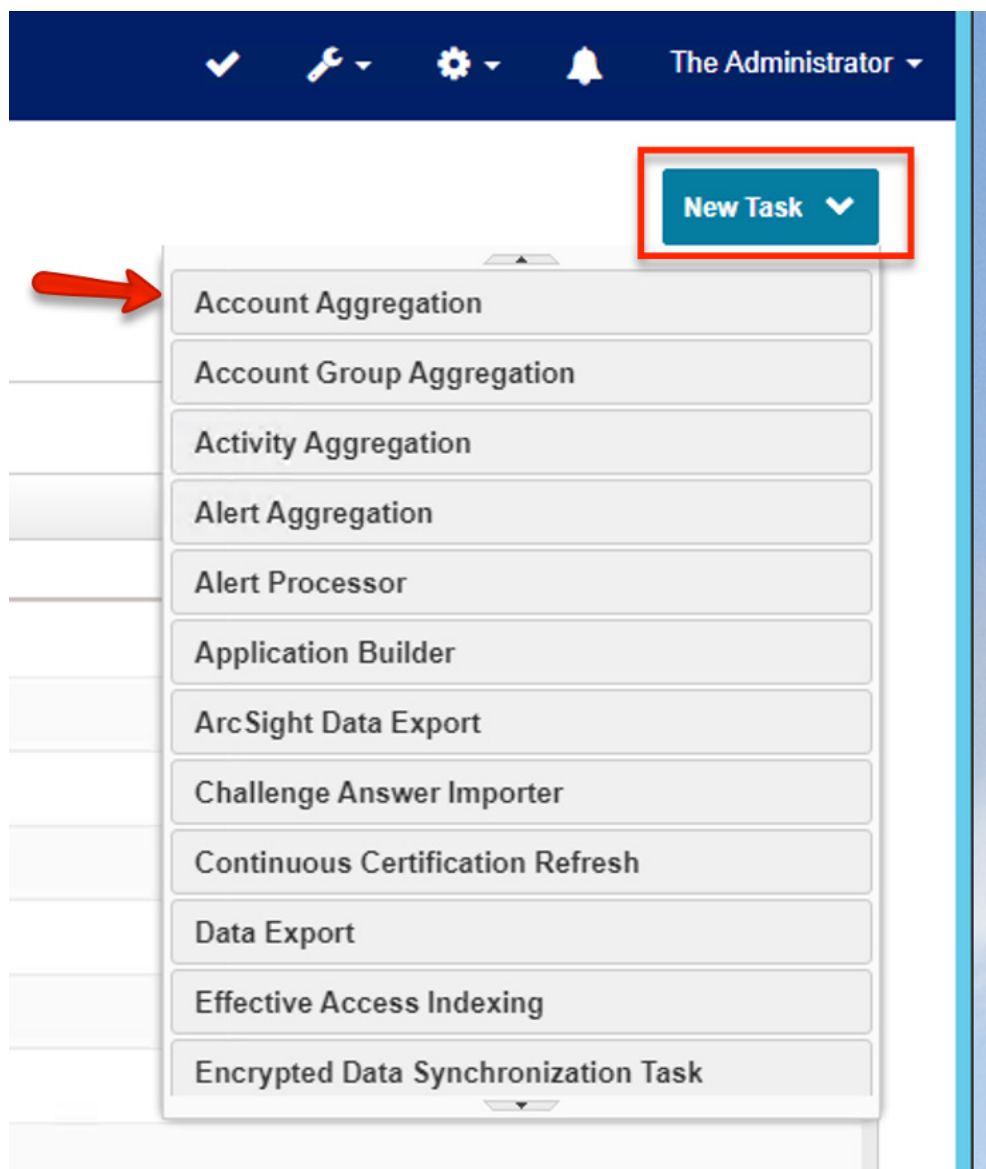


Figure 57. Create new task

3. Give the task a name, and make sure to select the previously-defined ZPA application from the **Select applications to scan** drop-down menu.

New Task

Standard Properties

*Indicates a required field

Name* Zscaler Account Aggregation

Previous Result Action Delete

Description Task template for application account scanning.

Allow Concurrency ☐

Require Signoff ☐

Host

Number of Runs 0

Average Run Time 0:00:00

Reset Run Statistics

Email Task Alerts

Email Notification Disabled

Scope

Account Aggregation Options

Select applications to scan* Zscaler

Optionally select a rule to assign capabilities or perform other processing on new identities -- Select Rule --

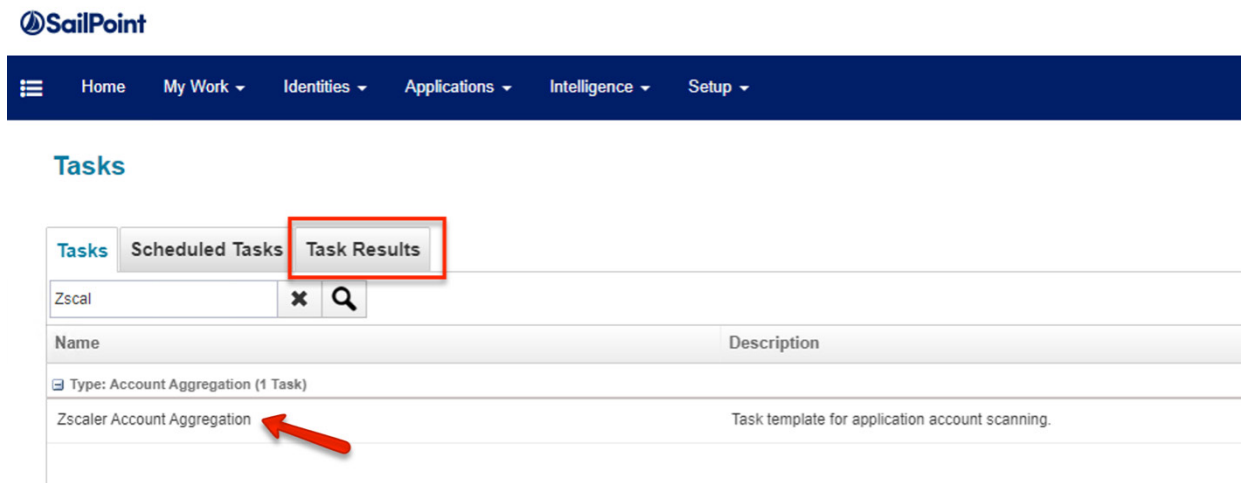
Figure 58. Configure task settings

4. Click **Save and Execute** at the bottom of the task configuration page.



Figure 59. Save and Execute

5. Verify that the new task is displayed under the **Type: Account Aggregation** section of the task list. Click the **Task Results** tab.

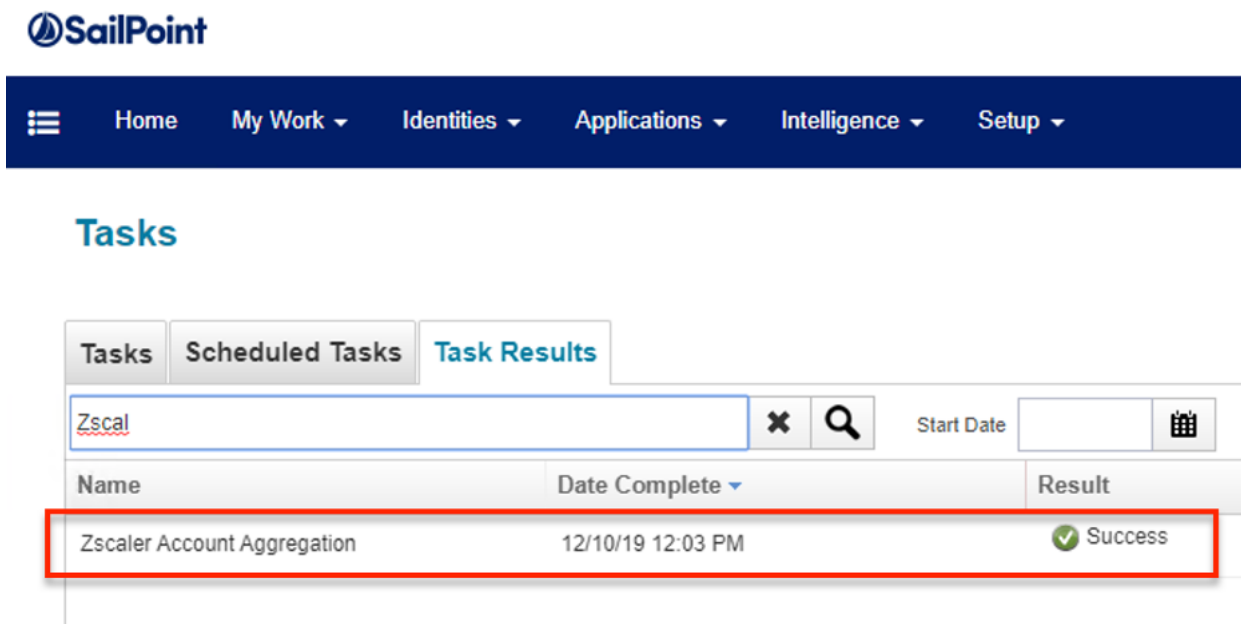


The screenshot shows the SailPoint interface with the 'Tasks' section. The 'Task Results' tab is selected and highlighted with a red box. Below the tabs, there is a search bar with 'Zscal' entered. A table lists tasks, with the first task being 'Zscaler Account Aggregation', which is pointed to by a red arrow. The task is categorized under 'Type: Account Aggregation (1 Task)'.

Name	Description
Type: Account Aggregation (1 Task)	
Zscaler Account Aggregation	Task template for application account scanning.

Figure 60. Verify account aggregation task

6. Confirm that the account aggregation completed.



The screenshot shows the 'Task Results' tab selected. The search bar contains 'Zscal'. A table displays the results of the task, with the first row highlighted by a red box. The row shows the task name 'Zscaler Account Aggregation', the completion date '12/10/19 12:03 PM', and the result 'Success' with a green checkmark icon.

Name	Date Complete	Result
Zscaler Account Aggregation	12/10/19 12:03 PM	✓ Success

Figure 61. Config account aggregation task completion

7. View task execution details by clicking the successful task.

The screenshot shows the SailPoint interface with a 'Task Result' page. The task is 'Zscaler Account Aggregation' and its status is 'Success'. A table below shows the task's attributes.

Zscaler Account Aggregation Attributes	
Attribute	Value
Applications scanned	Zscaler
Accounts scanned	3
Accounts optimized	3

Figure 62. View task execution details

8. Return to the main tasks window to create a group aggregation task. Click **New Task**, and then select **Account Group Aggregation**.

The screenshot shows the 'New Task' dropdown menu in the SailPoint interface. The 'Account Group Aggregation' option is highlighted with a red arrow.

- Account Aggregation
- Account Group Aggregation**
- Activity Aggregation
- Alert Aggregation
- Alert Processor
- Application Builder
- ArcSight Data Export
- Challenge Answer Importer
- Continuous Certification Refresh
- Data Export
- Effective Access Indexing
- Encrypted Data Synchronization Task

Figure 63. Create group aggregation task

9. Link the account aggregation, give the group aggregation a name, and select the ZPA application from the **Select applications to scan** drop-down menu.

The screenshot shows the SailPoint 'New Task' form. The 'Standard Properties' section includes a 'Name*' field (highlighted with a red box) containing 'Zscaler Group Aggregation', a 'Description' field with 'Task template for application group scanning.', and checkboxes for 'Allow Concurrency' and 'Require Signoff'. Below these are fields for 'Host', 'Number of Runs' (set to 0), and 'Average Run Time' (set to 0:00:00), along with a 'Reset Run Statistics' button. The 'Email Task Alerts' section has an 'Email Notification' dropdown set to 'Disabled' and a 'Scope' dropdown. The 'Account Group Aggregation Options' section features a 'Select applications to scan*' dropdown menu (highlighted with a red box) showing 'Zscaler' as the selected option.

Figure 64. Link account aggregation

10. Click **Save and Execute**.



Figure 65. Save and execute

11. Confirm the group aggregation was successful by switching to the **Task Results** tab.

Tasks Scheduled Tasks Task Results		
Zscaler		
Start Date		
Name	Date Complete	Result
Zscaler Group Aggregation	12/10/19 12:07 PM	✓ Success
Zscaler Account Aggregation	12/10/19 12:03 PM	✓ Success

Figure 66. Confirm group aggregation

12. View a detailed summary of the task by clicking the task.

Task Result

Details

Name	Zscaler Group Aggregation	Started By	The Administrator
Type	Account Group Aggregation	Started	12/10/19 12:07:12 PM
Description	Task template for application group scanning.	Completed	12/10/19 12:07:15 PM
Run Time	0:00:02	Average Run Time	0:00:00
Run Time Change	0%	Host	ad-resource
Status	<div><div></div>Success</div>	Progress	Completed

Return to Tasks

Zscaler Group Aggregation Attributes

Attribute	Value
Applications scanned	Zscaler
Groups scanned	2
Groups created	2

Zscaler Attributes

group	
Application Objects scanned	2
Application Objects created	2

Figure 67. View task detailed summary

Confirm Account Provisioning

Confirm the account provisioning in SailPoint and ZPA.

1. Click the menu in the top left of any screen in IdentityIQ. Go to **Manage User Access > Manage Accounts**.

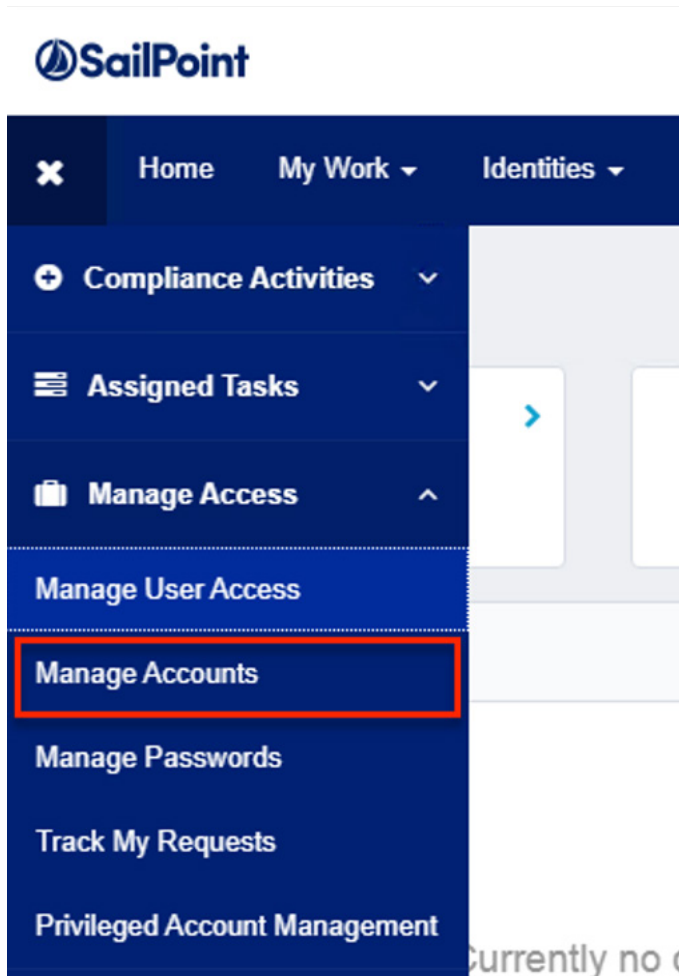


Figure 68. Navigate to Manage Accounts

- Find the identity for which you are creating a new ZPA account. Click **Manage** for that user's tile.

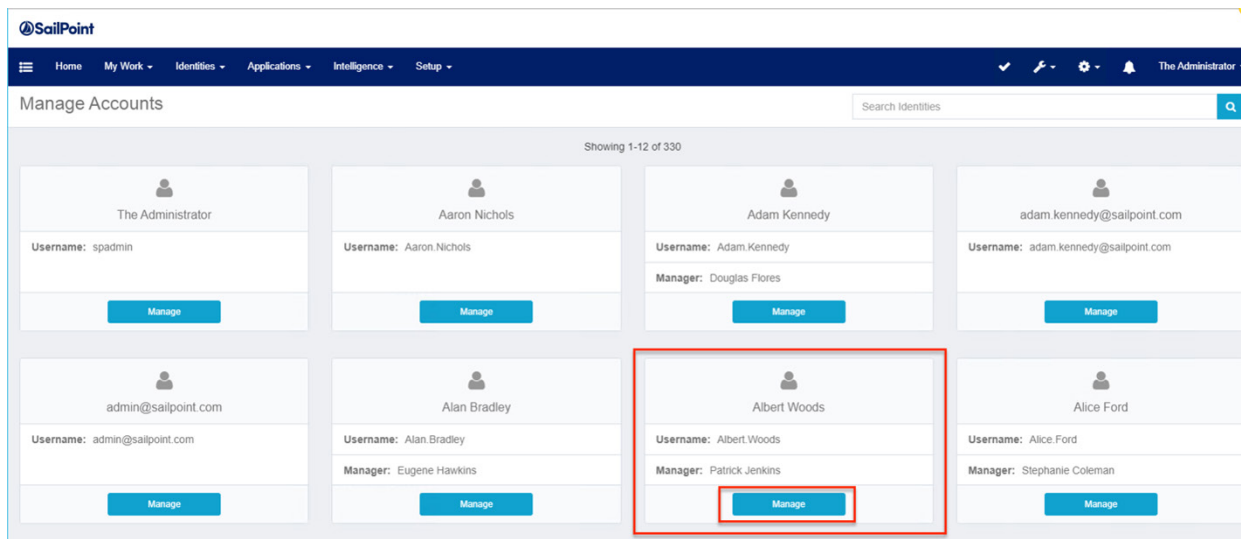


Figure 69. Manage ZPA user

- Click **Request Account**, which displays the identities currently-provisioned application accounts. Click **Request Account**.

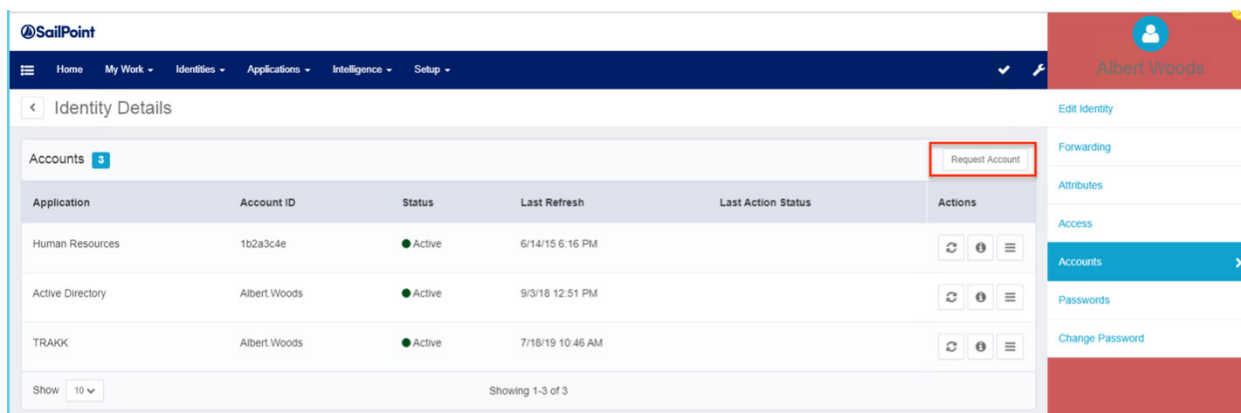


Figure 70. Request ZPA user

4. Select the ZPA application from the **Application** drop-down menu and click **Submit**.

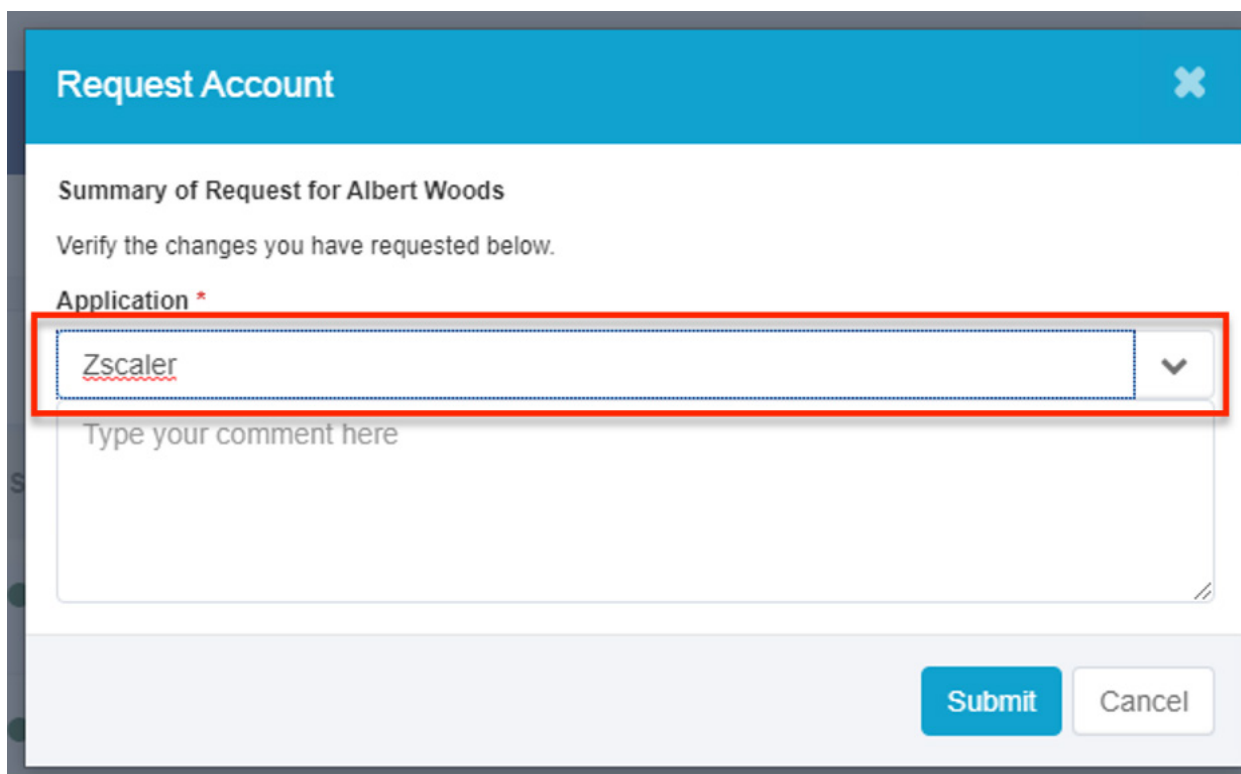


Figure 71. Request ZPA application

5. Click **Confirm**.

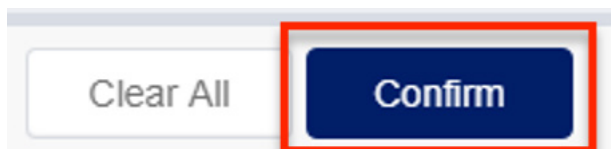


Figure 72. Confirm ZPA application

6. Submit a user request by clicking **Submit**.

Application	Account ID	Last Refresh	Action	Actions
Zscaler			Create	

Back Clear All **Submit**

Figure 73. Submit user request

7. Since the Create Provisioning policy had several required fields (**Name, Display Name**), IdentityIQ prompts the requester with a form to provide those values. Click **Complete Form**.

More Info Needed

More Info Needed

Later **Complete Form**

Figure 74. Enter user required fields

8. Fill in the **User Name**. The user name must be a valid email address. Click **Ok** to launch the request.

Complete Work Item

Request provisioning form for Albert.Woods

Please supply initial values for account attributes in the forms below.

Request Information

Requester
The Administrator

Target Identity

First Name: Albert, Last Name: Woods, Account ID: Albert Woods

Assigned Roles: All Users, Inventory Analyst

Zscaler

User Name *
albert.woods@sailpoint.com

Username must be a valid email address

Cancel Ok

Figure 75. Verify user email address

9. To confirm if the account was correctly provisioned, run another account aggregation for the ZPA application. Otherwise, confirm directly in ZPA.

Attributes				
Attribute	Value			
Applications scanned	Zscaler			
Accounts scanned	4			
Accounts optimized	3			
Identities updated	1			

Application	Account	Action	Identity	Attribute
Zscaler	7a736361-8c65-7200-7363-696d0060484f	CorrelateManual	Albert.Woods	undetermined

Figure 76. Confirm account provisioning

Configuring SailPoint IdentityNow for ZIA

In this section, you'll configure SailPoint IdentityNow for ZIA.

Creating the Zscaler Source

The following describes how to create the Zscaler source:

1. Log into IdentityNow as an administrator and go to the administrative dashboard. Define a new Source by selecting **Sources** from the **Connections** drop-down menu.

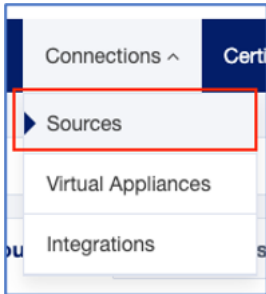


Figure 77. Navigating to sources page

2. Click **New**.

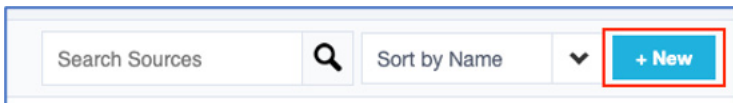


Figure 78. Creating new source

3. Select **SCIM 2.0** from the **Source Type** drop-down menu. Give the source a **Source Name**, a **Description**, and select **Direct Connection** as the **Connection Type**. Click **Continue**.

A screenshot of the 'Create New Source' form in the SailPoint IdentityNow administrative dashboard. The form contains the following fields: 'Source Type' (dropdown menu set to 'SCIM 2.0'), 'Source Name' (text input field containing 'ZIA Source'), 'Description' (text input field containing 'ZIA Source'), 'Source Owner' (dropdown menu set to 'Adam Creaney'), and 'Connection Type' (radio buttons for 'Direct Connection' and 'Flat File', with 'Direct Connection' selected). At the bottom right, there are 'Cancel' and 'Continue' buttons.

Figure 79. Source creation fields

4. Enter the connection parameters specific to your ZIA SCIM server:

- Select your virtual appliance from the drop-down menu.
- Provide any governance group selection (if applicable).

5. Click **Save**.

Base Configuration

The SCIM 2.0 source is a type of 'Direct Connection' source used to communicate between a source server and SailPoint. To configure a Direct Connection source, provide or select values for all required fields, including a source owner and virtual appliance cluster.

The source owner is responsible for administering, operating, and managing the source system. The virtual appliance (VA) is a Linux-based virtual machine that is deployed and configured to connect to sources and apps using APIs, connectors / integrations provided by SailPoint.

You can also optionally select a governance group to refine the scope of access requests for the members of the governance group.

[Learn more about governance groups](#)

Source Name *
ZIA

Source Description *
ZIA Test

Source Owner *
adam.creaney

Virtual Appliance Cluster *
ACLocal

Governance Group for Source Management

Save

Figure 80. Virtual application selection

6. Configure connection settings:

- Set the **Host URL** to the SCIM server in the format `https://scim.zscalerbeta.net/<your_tenant_id>/scim`.
- Select **API Token** as the **Authentication Type**.
- Enter the API token provided by your ZIA administrator in the **API token** field.

7. Click **Save**.

Connection Settings

To configure a direct connection between the source and managed system. **Basic Authentication, API Token, OAuth 2.0, and No Authentication** are supported as authentication types.

To establish a secure connection, you will need to provide the values for the **required/mandatory** fields on this page for the authentication.

Optional field **Additional Payload** for Password and JWT Grant Type, can be used in the systems where authentication may require **additional parameters** along with mandatory fields. You can provide those details in **JSON format**.

[Learn more about Connection Settings](#)

Connection Timeout (In minutes)
1

Host URL *
https://scim.zscalerbeta.net/6120389/scim

Authentication Type

☐ Basic Authentication

☐ OAuth 2.0

☒ API Token

☐ No Authentication

API Token *

Save

Figure 81. Host URL, Authentication Type, and API Token configuration

8. From the left-side navigation, select **Review and Test**. Then click **Test Connection** to verify connectivity to the Zscaler SCIM server.

Source Name: ZIA

Source Type: SCIM 2.0

Aggregation Settings

Filter Condition For Accounts	
Filter Condition For Groups	
Explicit Attribute Request	false
Delta Aggregation Mode	false
Page Size	50

Additional Settings

Content-type	
Accept	
No Authentication Headers	
OAuth Request Parameters	
Retryable Errors	
usePatch	
Skip Group Update	false

Buttons: Exit Configuration, Test Connection

Figure 82. Test connection successful

9. Click **Back** and then click **Go To Source Page** to continue configuration.

Are you sure you want to go back?

All your changes are saved, are you sure you want to leave edit mode?

Buttons: Return to Configuration, Go To Source Page

Figure 83. Return to source configuration page

10. From the left-side navigation, go to **Import Data > Account Schema**. From the **Options** drop-down menu, select **Discover Schema**.

Account Schema: ZIA

Search for an attribute

Options (dropdown menu open)

- Discover Schema (highlighted)
- Edit Schema

Attribute Name	Description	Type	Entitlement	Actions
id	Unique identifier for the SCIM Resource as defined...	string		
externalid	A String that is an identifier for the resource as def...	string		

Figure 84. Schema discovery

11. The attributes for a user in ZIA are populated. Flag the **id** attribute as **Account ID**. Flag the **userName** attribute as **Account Name**. Flag the **groups** attribute as **Entitlement** and **Multi-Valued**.

Account Schema: ZIA

Search for an attribute Options Add New Attribute

<input type="checkbox"/>	Attribute Name		Description	Type	Entitlement	Multi-Valued	Actions
<input type="checkbox"/>	id	Account ID	Unique identifier for the SCIM Resource as defined...	string			
<input type="checkbox"/>	externalid		A String that is an identifier for the resource as def...	string			
<input type="checkbox"/>	userName	Account Name	A service provider's unique identifier for the user, t...	string			
<input type="checkbox"/>	name.familyName		The family name of the User, or last name in most ...	string			
<input type="checkbox"/>	name.givenName		The given name of the User, or first name in most ...	string			
<input type="checkbox"/>	displayName		The name of the User, suitable for display	string			
<input type="checkbox"/>	active		A Boolean value indicating the User's administrati...	boolean			
<input type="checkbox"/>	groups		A list of groups to which the user belongs,	group	Entitlement	Multi-Valued	
<input type="checkbox"/>	department		department	string			

Figure 85. Flagging account id, userName, and groups attributes in schema

12. Set up account correlation. This is likely a mapping of the attribute that includes a username in Zscaler (email address) and the **Work Email** attribute of the identity. This might be different or require additional correlation depending on your organization.

Correlation Configuration

Identity Attribute	Operation	Account Attribute	
Work Email	Equals	userName	+ Add

Figure 86. Correlation definition

Source configuration is now complete.

Additional Resources

For additional information regarding standard IdentityNow and its configuration (such as Identity Profiles, source aggregation, and provisioning) refer to the following SailPoint community articles.

Working with Connectors and Sources

<https://community.sailpoint.com/t5/IdentityNow-Connectors/Guide-to-IdentityNow-Sources-and-Connectors/ta-p/73888>

Provisioning

- Populate the required attributes, **Name** and **Display Name**, to provision a new user account. The **username** must be a valid email format. Creation fails if these conditions are not met.
- https://documentation.sailpoint.com/saas/help/?_gl=1*u1djs1*_ga*OTQ1MzE3NzU5LjE2ODU1NjI4MDI.*_ga_SS72Z4HXJM*MTY4NTY0MjI3My42LjEuMTY4NTY0MjYzOC4zNS4wLjA.&_ga=2.33746017.130981577.1685562802-945317759.1685562802#_gl=1*I3gs0*_gcl_au*MTM5NTA5NzYyOC4xNjg1NTYyODAy

Configuring SailPoint IdentityNow for ZPA

This section shows you how to configure SailPoint IdentityNow for ZPA.

Creating the Zscaler Source

The following describes how to create the Zscaler source:

1. Log into IdentityNow as an administrator and go to the administrative dashboard. Define a new Source by selecting **Sources** from the **Connections** drop-down menu.

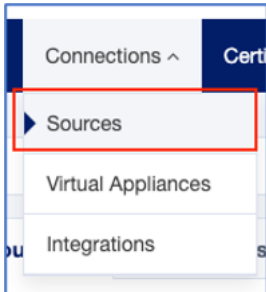


Figure 87. Navigating to Sources page

2. Click **New**.

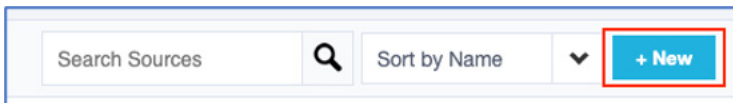


Figure 88. Creating new source

3. Select **SCIM 2.0** from the **Source Type** drop-down menu. Give the source a **Source Name**, a **Description**, and select **Direct Connection** as the **Connection Type**. Click **Continue**.

A screenshot of the 'Create New Source' form in the SailPoint IdentityNow administrative dashboard. The form contains the following fields: 'Source Type' (a dropdown menu with 'SCIM 2.0' selected), 'Source Name' (a text input field with 'ZPA Source' entered), 'Description' (a text input field with 'ZPA Source' entered), 'Source Owner' (a dropdown menu with 'Adam Creaney' selected), and 'Connection Type' (radio buttons for 'Direct Connection' and 'Flat File', with 'Direct Connection' selected). At the bottom of the form are 'Cancel' and 'Continue' buttons.

Figure 89. Source creation fields

4. Enter the Virtual Appliance information for the connection to the ZPA SCIM server:

- Select your virtual appliance from the drop-down menu.
- Provide any governance group selection (if applicable).
- Click **Save**.

Base Configuration

The SCIM 2.0 source is a type of 'Direct Connection' source used to communicate between a source server and SailPoint. To configure a Direct Connection source, provide or select values for all required fields, including a source owner and virtual appliance cluster.

The source owner is responsible for administering, operating, and managing the source system. The virtual appliance (VA) is a Linux-based virtual machine that is deployed and configured to connect to sources and apps using APIs, connectors / integrations provided by SailPoint.

You can also optionally select a governance group to refine the scope of access requests for the members of the governance group.

[Learn more about governance groups](#)

Source Name *
ZPA

Source Description *
Zscaler Private Access SCIM Test

Source Owner *
adam.creaney

Virtual Appliance Cluster *
ACLocal

Governance Group for Source Management

Save

Figure 90. Virtual application selection

5. Configure connection settings:

- Set the **Host URL** to the SCIM server and in the format `https://scim1.zpabeta.net/scim/1/<your_tenant_id>/v2`.
- Select **API Token** as the **Authentication Type**.
- Enter the API token provided by your ZPA administrator in the **API token** field.
- Click **Save**.

Connection Settings

To configure a direct connection between the source and managed system, **Basic Authentication, API Token, OAuth 2.0, and No Authentication** are supported as authentication types.

To establish a secure connection, you will need to provide the values for the **required/mandatory** fields on this page for the authentication.

Optional field **Additional Payload** for Password and JWT Grant Type, can be used in the systems where authentication may require **additional parameters** along with mandatory fields. You can provide those details in **JSON format**.

[Learn more about Connection Settings](#)

Connection Timeout (in minutes)
1

Host URL *
`https://scim1.zpabeta.net/scim/1/72057765836619787/v2`

Authentication Type

☐ Basic Authentication

☐ OAuth 2.0

☒ API Token

☐ No Authentication

API Token *

Save

Figure 91. Host URL, Authentication Type, and API Token configuration

6. From the left-side navigation, select **Review and Test**. Then click **Test Connection** to verify connectivity to the Zscaler SCIM server..

Figure 92. Test connection successful

7. Click **Back** and then click **Go To Source Page** to continue configuration.

Figure 93. Return to source configuration page

8. From the left-side navigation, select **Import Data > Account Schema**. From the **Options** drop-down menu, select **Discover Schema**.

Figure 94. Schema discovery

9. The attributes for a user in ZPA are populated. Flag the **id** attribute as **Account ID**. Flag the **userName** attribute as **Account Name**. Flag the **groups** attribute as **Entitlement** and **Multi-Valued**.

Account Schema: ZPA

Search for an attribute Options Add New Attribute

Attribute Name	Description	Type	Entitlement	Multi-Valued	Actions
<input type="checkbox"/> id	Unique identifier for the SCIM Resource as defined...	string	Account ID		
<input type="checkbox"/> externalId	A String that is an identifier for the resource as def...	string			
<input type="checkbox"/> userName	A service provider's unique identifier for the user, t...	string	Account Name		
<input type="checkbox"/> name.familyName	The family name of the User, or last name in most ...	string			
<input type="checkbox"/> name.givenName	The given name of the User, or first name in most ...	string			
<input type="checkbox"/> displayName	The name of the User, suitable for display	string			
<input type="checkbox"/> active	A Boolean value indicating the User's administrati...	boolean			
<input type="checkbox"/> groups	A list of groups to which the user belongs,	group	Entitlement	Multi-Valued	
<input type="checkbox"/> department	department	string			

Figure 95. Flagging account id, userName, and groups attributes in schema

10. Set up account correlation. This is likely a mapping of the attribute representing a username in Zscaler (email address) and **Work Email** attribute of the identity. This might be different and require additional correlation for your organization.

Correlation Configuration

Identity Attribute	Operation	Account Attribute	
Work Email	Equals	userName	+ Add

Figure 96. Correlation definition

Source configuration is now complete.

Additional Resources

For additional information regarding standard IdentityNow and its configuration, such as Identity Profiles, source aggregation, and provisioning, refer to the following SailPoint community articles.

Working with Connectors and Sources

<https://community.sailpoint.com/t5/IdentityNow-Connectors/Guide-to-IdentityNow-Sources-and-Connectors/ta-p/73888>

Provisioning

- Populate the required attributes, Name and Display Name, to provision a new user. The **username** must be a valid email format. Creation fails if these conditions are not met.
- https://documentation.sailpoint.com/saas/help/?_gl=1*u1djs1*_ga*OTQ1MzE3NzU5LjE2ODU1NjI4MDI.*_ga_SS72Z4HXJM*MTY4NTY0MjI3My42LjEuMTY4NTY0MjYzOC4zNS4wLjA.&_ga=2.33746017.130981577.1685562802-945317759.1685562802#_gl=1*I3gs0*_gcl_au*MTM5NTA5NzYyOC4xNjg1NTYyODA

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**.

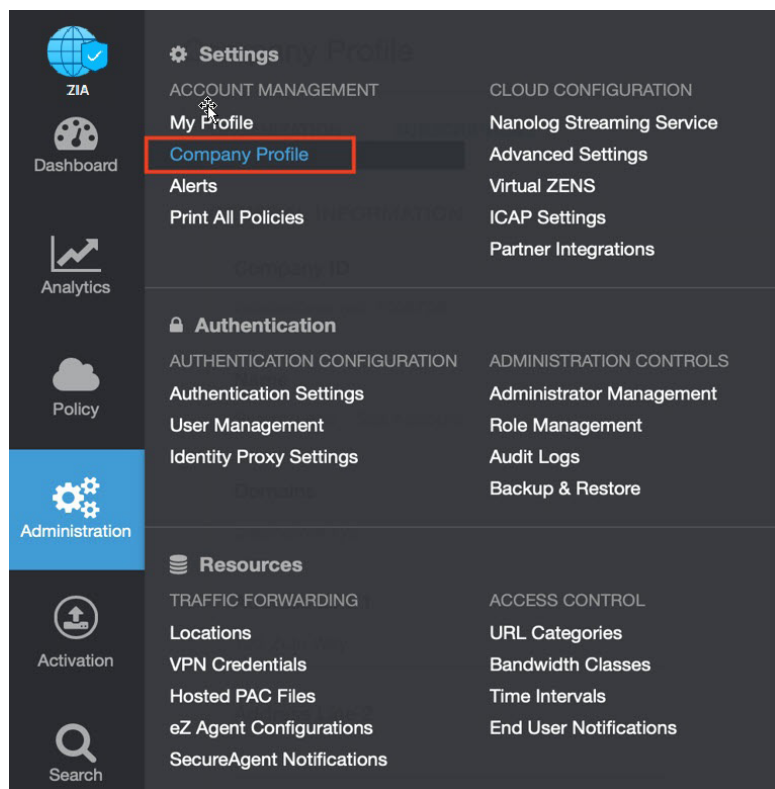


Figure 97. Collecting details to open support case with Zscaler TAC

2. Copy the Company ID, as shown below.

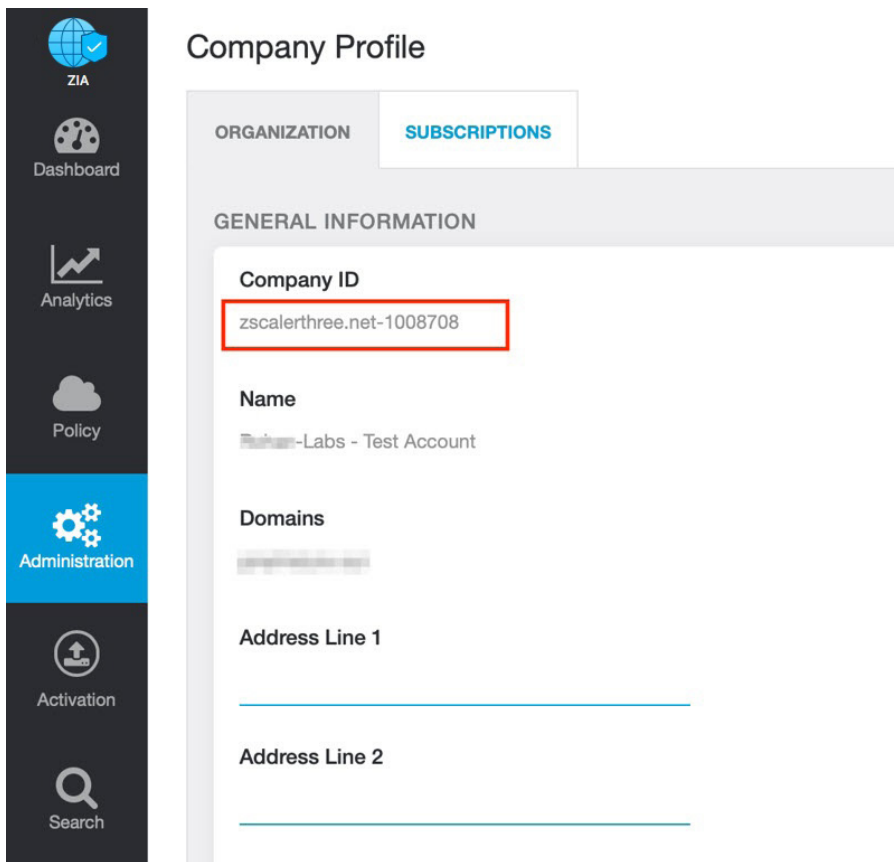


Figure 98. Company ID

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

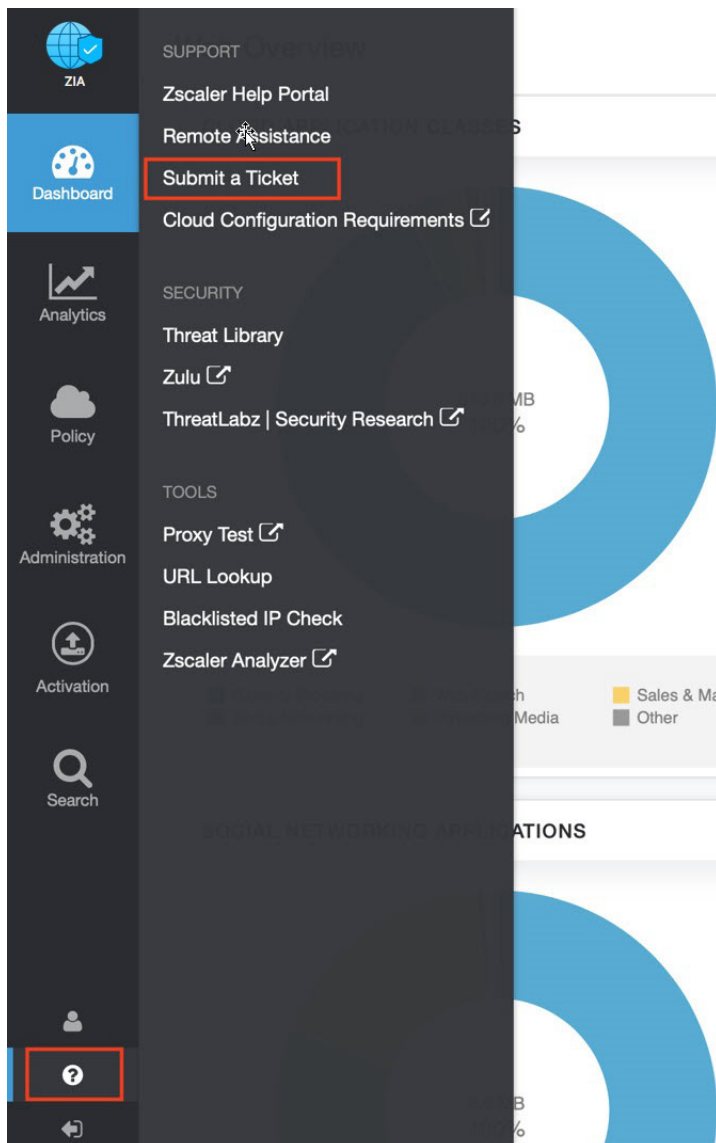


Figure 99. Submit a ticket