



Zscaler and Sail Point Deployment Guide

July 2020

Version 1.0



Table of Contents

1 Zscaler and SailPoint	7
1.1 Prerequisites	7
2 Configuring SailPoint for ZIA	8
2.1 Creating the Zscaler Application	8
2.1.1 Add New Application	9
2.1.2 Configure Application Type	10
2.1.3 Creating the Zscaler Application	11
2.1.4 Test Connection	12
2.1.5 Schema Configuration	13
2.1.6 ZIA User Attributes	14
2.1.7 Discover Schema Attributes	15
2.1.8 Verify Attributes	16
2.1.9 Test Configuration	17
2.1.10 Preview Live Data	17
2.1.11 Configure Provisioning Plan	18
2.1.12 Create Policy Form	19
2.1.13 Configure Policy Form for ZIA	20
2.1.14 Verify Configuration Policy	21
2.1.15 Save Configuration Policy	21
2.1.16 Verify New Application	21
2.2 Configuring Aggregation Tasks	22
2.2.1 Create New Task	23
2.2.2 Configure Task Settings	24
2.2.3 Save and Execute Task	25
2.2.4 Verify Account Aggregation Task	25
2.2.5 Confirm Account Aggregation Task Completion	26
2.2.6 View Task Execution Details	27
2.2.7 Create Group Aggregation Task	28
2.2.8 Link Account Aggregation	29
2.2.9 Save and Execute	30
2.2.10 Confirm Group Aggregation	30
2.2.11 View Task Detailed Summary	31
2.3 Confirm Account Provisioning	32
2.3.1 Navigate to Manage Accounts	32
2.3.2 Manage ZIA User	33
2.3.3 Request ZIA User	34
2.3.4 Request ZIA Application	35
2.3.5 Confirm ZIA Application	36
2.3.6 Submit User Request	37
2.3.7 Enter in User Required Fields	38



2.3.8	Verify User Email Address	39
2.3.9	Confirm Account Provisioning	40
3	Configuring SailPoint for ZPA	41
3.1	Creating the Zscaler Application.....	41
3.1.1	Add New Application.....	42
3.1.2	Configure Application Type.....	43
3.1.3	Creating the Zscaler Application	44
3.1.4	Test Connection.....	45
3.1.5	Schema Configuration	46
3.1.6	ZIA User Attributes.....	47
3.1.7	Discover Schema Attributes.....	48
3.1.8	Verify Attributes.....	49
3.1.9	Test Configuration.....	50
3.1.10	Preview Live Data	50
3.1.11	Configure Provisioning Plan.....	51
3.1.12	Create Policy Form	52
3.1.13	Configure Policy Form for ZPA	53
3.1.14	Verify Configuration Policy.....	54
3.1.15	Save Configuration Policy.....	54
3.1.16	Verify New Application	54
3.2	Configuring Aggregation Tasks	55
3.2.1	Create New Task	56
3.2.2	Configure Task Settings.....	57
3.2.3	Save and Execute Task	58
3.2.4	Verify Account Aggregation Task.....	58
3.2.5	Confirm Account Aggregation Task Completion	59
3.2.6	View Task Execution Details.....	60
3.2.7	Create Group Aggregation Task	61
3.2.8	Link Account Aggregation	62
3.2.9	Save and Execute.....	63
3.2.10	Confirm Group Aggregation	63
3.2.11	View Task Detailed Summary.....	64
3.3	Confirm Account Provisioning	65
3.3.1	Navigate to Manage Accounts	65
3.3.2	Manage ZPA User	66
3.3.3	Request ZPA User	67
3.3.4	Request ZPA Application	68
3.3.5	Confirm ZPA Application	69
3.3.6	Submit User Request.....	69
3.3.7	Enter in User Required Fields.....	70
3.3.8	Verify User Email Address	71
3.3.9	Confirm Account Provisioning.....	72
4	Appendix A: Zscaler Resources	73
4.1	Zscaler IP Pages	73



5 Appendix B: SailPoint Resources 74



Terms and Acronyms

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



About This Document

Zscaler Overview

Zscaler enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship services, Zscaler Internet Access and Zscaler Private Access, create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler services are 100% cloud delivered and offer the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions are unable to 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, please visit www.zscaler.com or follow them on Twitter @zscaler.

SailPoint Overview

SailPoint Technologies, Inc. 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 written for network administrators, network analysts, and IT administrators responsible for deploying, monitoring and managing Enterprise branch network. For additional product and company resources, please refer to the Appendix section.

Software Revisions

This document was written using Zscaler Internet Access v6.0 and SailPoint.

Request for Comments

We value the opinions and experiences of our readers. To offer feedback or corrections for this guide, please contact us at partner-doc-support@zscaler.com.



1 Zscaler and SailPoint

1.1 Prerequisites

This guide will provide GUI examples for configuring Zscaler Internet Access (ZIA) 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 will explain how to provision new service with Zscaler and with SailPoint. The prerequisites to use this guide are:

Zscaler Internet Access (ZIA)

- A working instance of ZIA (any cloud)
- Administrator login credentials

SailPoint

- A working instance of Sail Point with administrator login credentials.



2 Configuring SailPoint for ZIA

2.1 Creating the Zscaler Application

Step 1: Define a new application by clicking the 'Application' -> 'Application Definition' navigation option

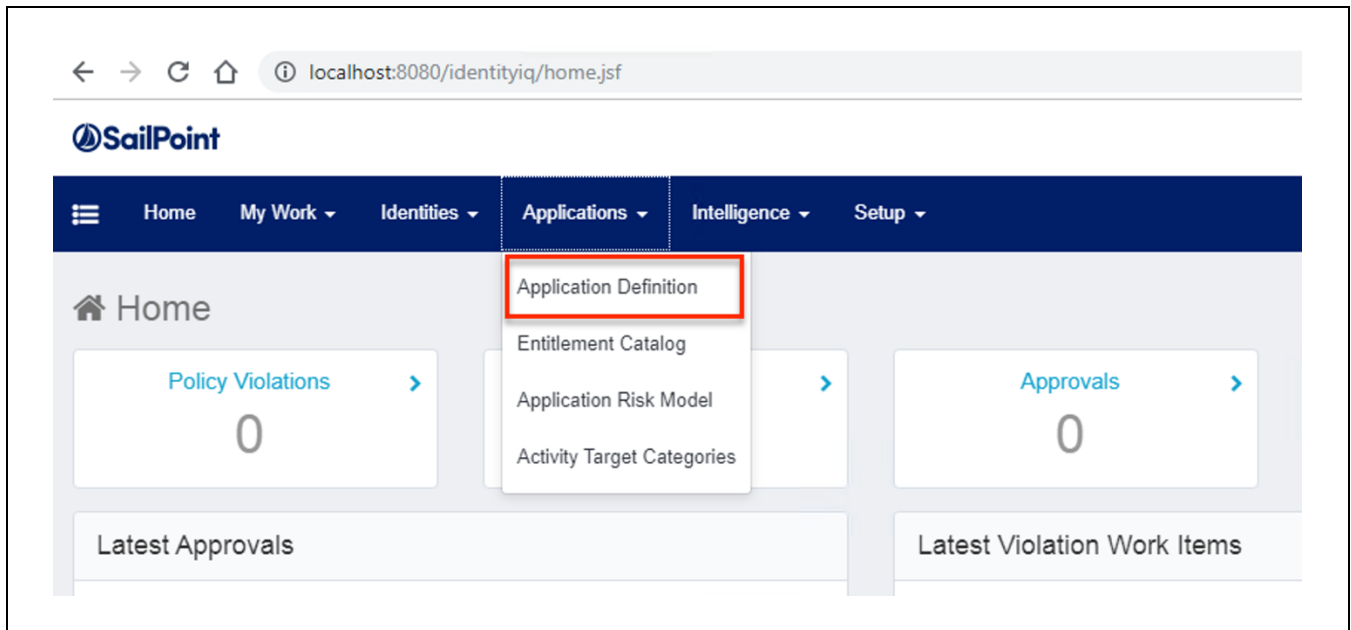


Figure 1: Create the Zscaler Application Definition



2.1.1 Add New Application

Step 2: Click the 'Add New Application' button

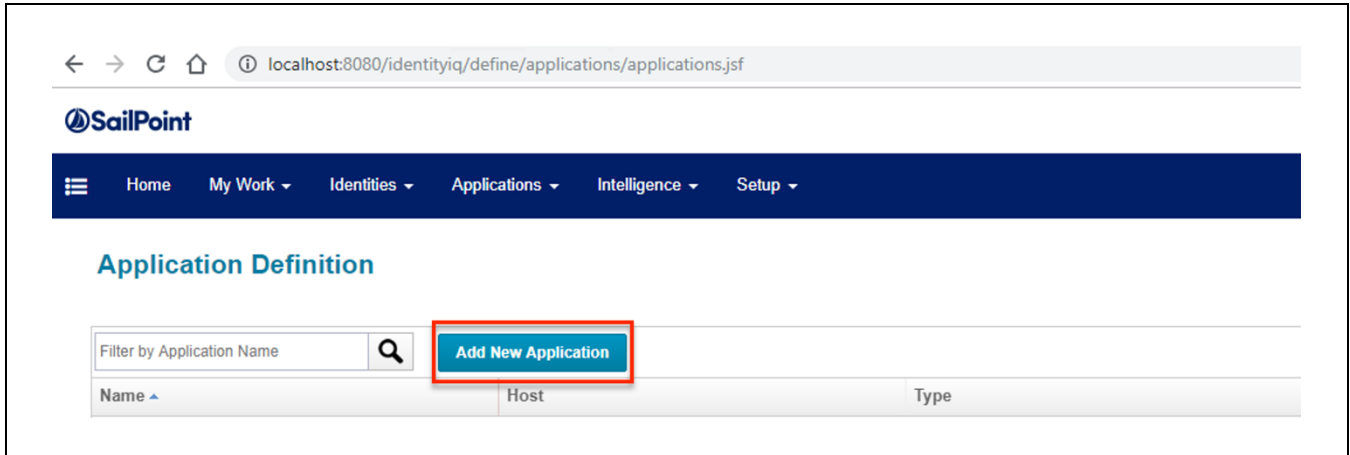


Figure 2: Add New Application



2.1.2 Configure Application Type

Step 3: Select 'SCIM 2.0' from the Application Type dropdown

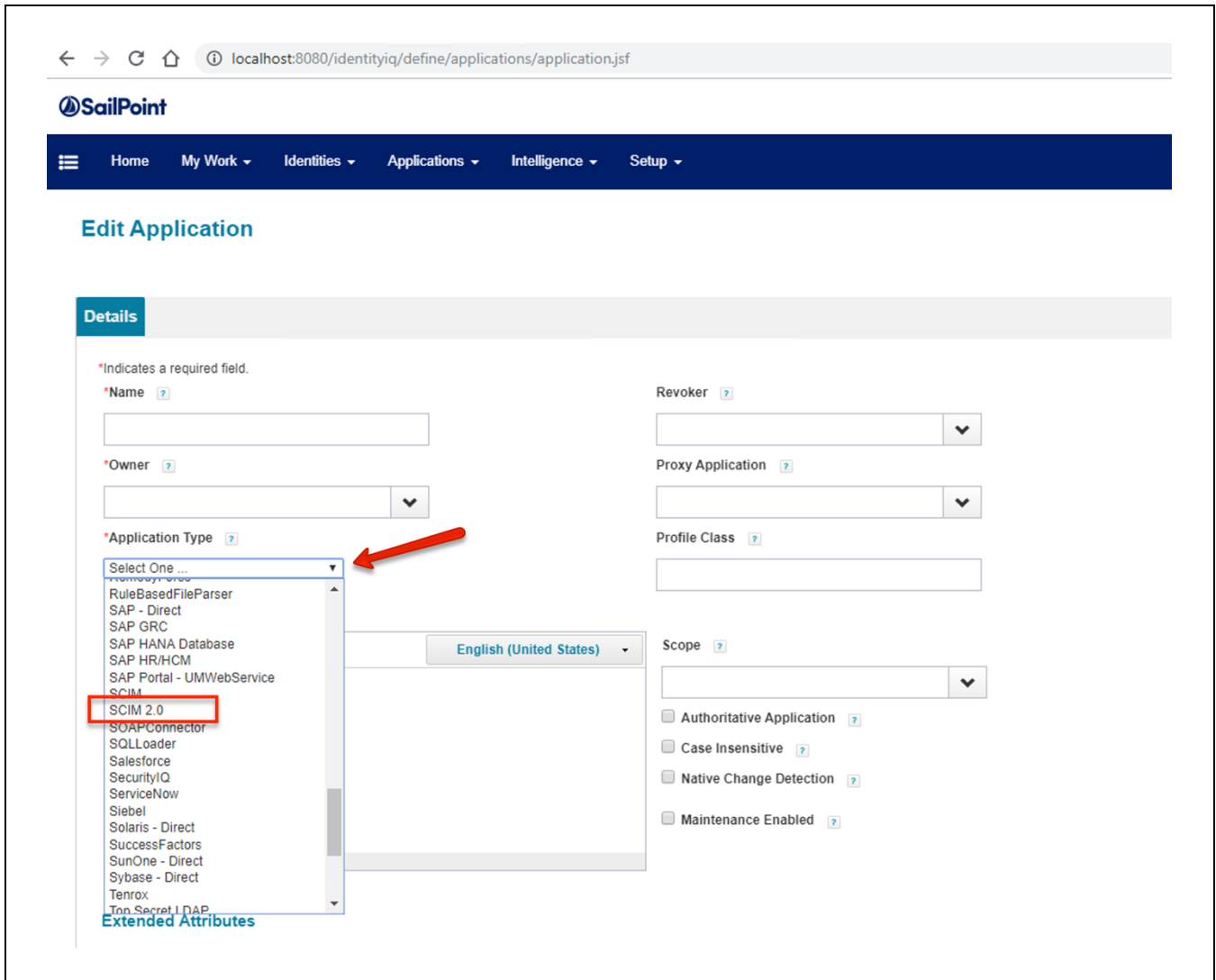


Figure 3: Configure Application Type



2.1.3 Creating the Zscaler Application

Step 4: Enter an application name, and an application owner for the Zscaler Internet Access application. For more information on how IdentityIQ uses these fields, refer to the SailPoint product documentation

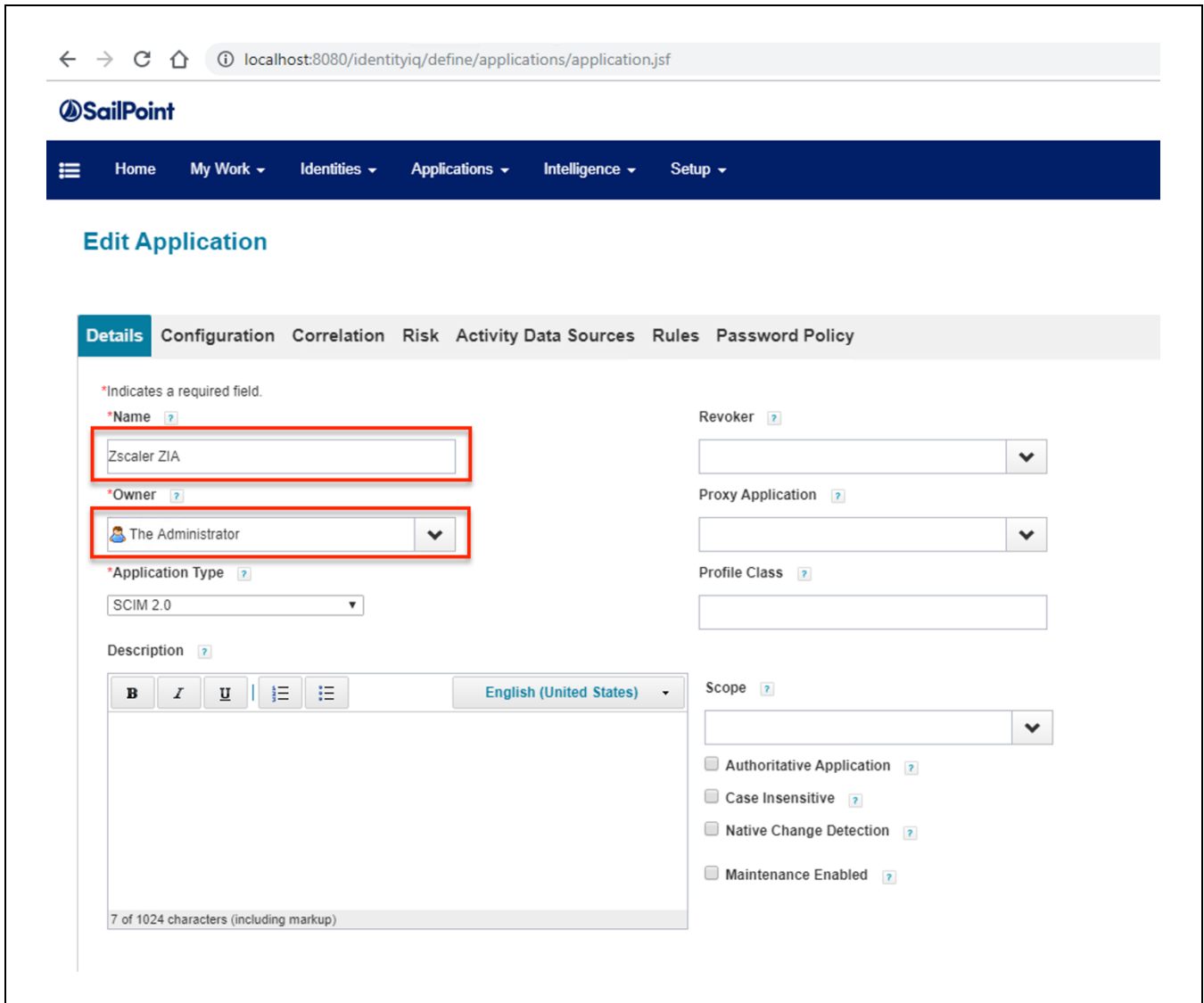


Figure 4: Log Into Zscaler



2.1.4 Test Connection

Step 5: Enter the connection parameters specific to your ZIA SCIM server.

1. The base url to the SCIM server should be of the format 'https://scim.zscalerbeta.net/<your_tenant_id>/scim
2. Select 'API Token' as the authentication type
3. Enter the API token provided by your ZIA administrator

Click the 'Test Connection' button to ensure the parameters were entered correctly

The screenshot shows the 'Edit Application' page in the SailPoint interface. The browser address bar displays 'localhost:8080/identityiq/define/applications/application.jsf'. The page title is 'SailPoint' and the navigation menu includes 'Home', 'My Work', 'Identities', 'Applications', 'Intelligence', and 'Setup'. The main content area is titled 'Edit Application' and has tabs for 'Details', 'Configuration', '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 is active and contains the following fields:

- Base URL ***: https://scim.zscalerbeta.net/6120389/scim (marked with a red circle 1)
- Authentication Type**: Radio buttons for OAuth 2.0, **API Token** (selected, marked with a red circle 2), and Basic Authentication.
- API Token ***: A masked input field (marked with a red circle 3).
- Account Filter**: Empty text input field.
- Group Filter**: Empty text input field.
- Role Filter**: Empty text input field.
- Entitlement Filter**: Empty text input field.
- Server Time Zone**: Empty text input field.
- Explicit Attribute Request**: A checkbox that is unchecked.
- Accept Header**: Empty text input field.
- Content-type Header**: Empty text input field.

At the bottom left, a 'Test Connection' button is highlighted with a red box, and a green checkmark indicates 'Test Successful'.

Figure 5: Test Connection



2.1.5 Schema Configuration

Step 6: Navigate to the 'Schema' sub-tab under the 'Configuration' tab. Click the 'Discover Schema Attributes' button under the 'Object Type: account' section.

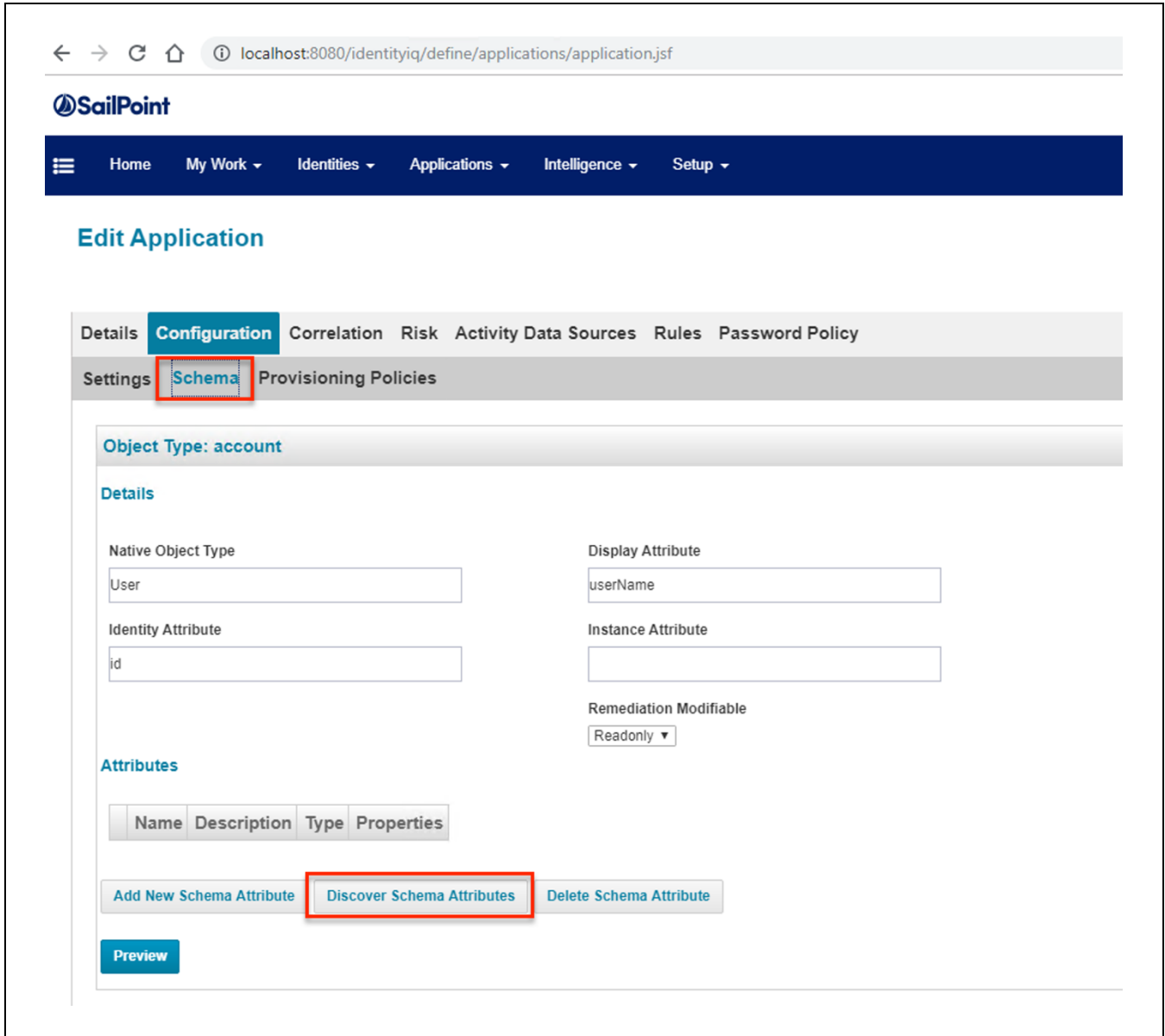


Figure 6: Schema Configuration



2.1.6 ZIA User Attributes

Step 7: The attributes for a user in ZIA will be populated

Object Type: account

Details

<p>Native Object Type <input type="text" value="User"/></p> <p>Identity Attribute <input type="text" value="id"/></p>	<p>Display Attribute <input type="text" value="userName"/></p> <p>Instance Attribute <input type="text"/></p> <p>Remediation Modifiable <input type="text" value="Readonly"/></p>
---	---

Attributes

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

Figure 7: ZIA User Attributes



2.1.7 Discover Schema Attributes

Step 8: Next, click the 'Discover Schema Attributes' under the 'Object Type: group' section of the schema sub-tab

The screenshot shows a web interface for configuring schema attributes. At the top, a header bar displays 'Object Type: group' in a blue font, which is highlighted with a red rectangular box. Below this header, the page is divided into two main sections: 'Details' and 'Attributes'.
The 'Details' section contains several input fields and a dropdown menu:

- 'Native Object Type': A text input field.
- 'Identity Attribute': A text input field.
- 'Description Attribute': A text input field.
- 'Display Attribute': A text input field.
- 'Instance Attribute': A text input field.
- 'Remediation Modifiable': A dropdown menu currently set to 'Readonly'.

The 'Attributes' section features a table with the following columns: 'Name', 'Description', 'Type', and 'Properties'. Below the table, there are three buttons: 'Add New Schema Attribute', 'Discover Schema Attributes' (highlighted with a red box), and 'Delete Schema Attribute'. At the bottom left of the form, there is a blue 'Preview' button.

Figure 8: Discover Schema Attributes



2.1.8 Verify Attributes

Step 9: The attributes for a group in ZIA will be populated

Object Type: group

Details

Native Object Type <input type="text" value="Group"/>	Display Attribute <input type="text"/>
Identity Attribute <input type="text" value="id"/>	Instance Attribute <input type="text"/>
Description Attribute <input type="text"/>	Remediation Modifiable <input type="button" value="Readonly"/>

Attributes

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

Figure 9: Verify Attributes



2.1.9 Test Configuration

Step 10: To test the configuration of the schemas, click the 'Preview' button under each one (account, group)

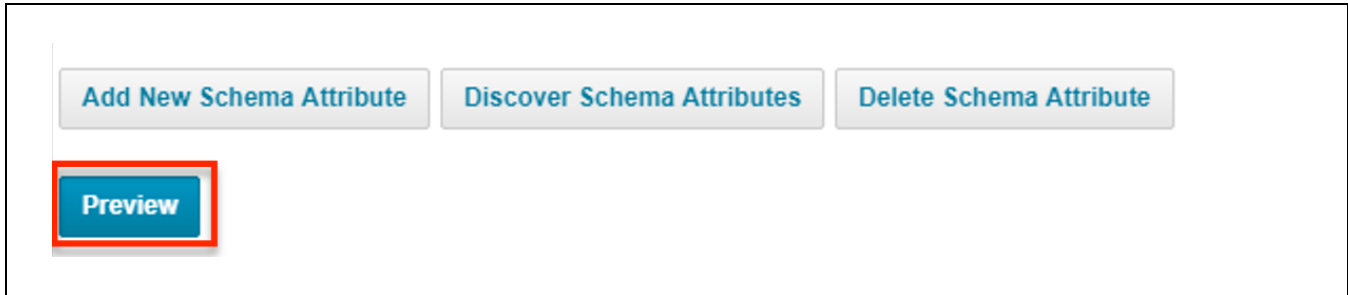


Figure 10: Test Configuration

2.1.10 Preview Live Data

Step 11: Clicking the 'Preview' button will display live data from the ZIA SCIM server connection (account preview shown)

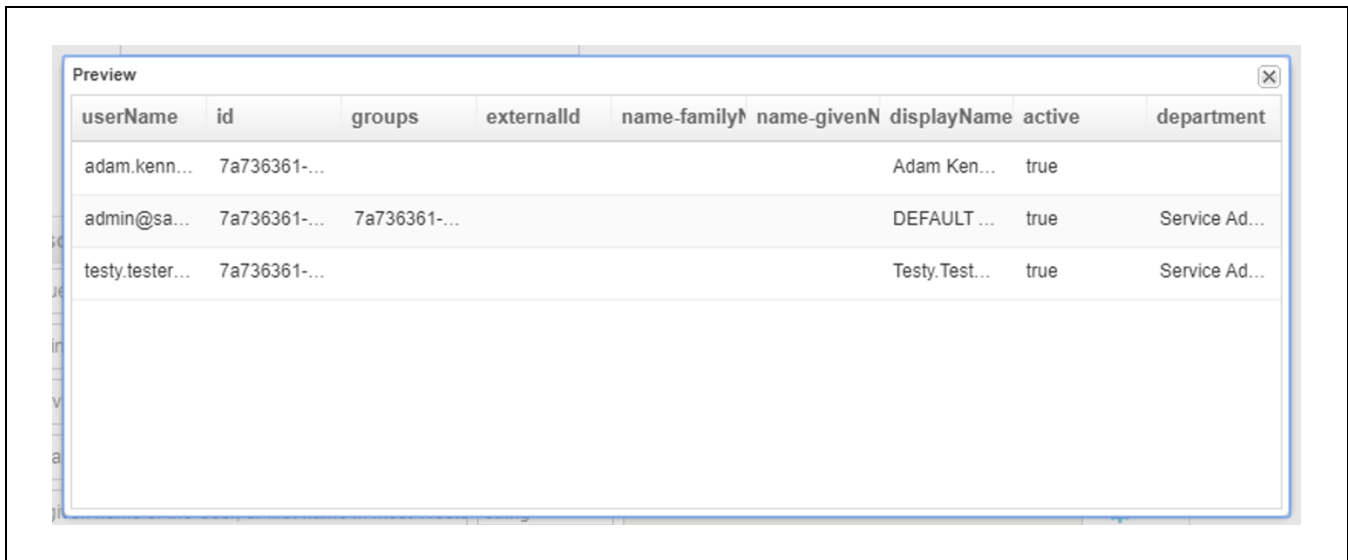


Figure 11: Preview Live Data



2.1.11 Configure Provisioning Plan

Step 12: The next step in application configuration is to configure provisioning plans. For this tutorial, a simple 'account creation' plan will be shown. First, click the 'Provisioning Policies' sub-tab under the 'Configuration' tab in the application definition. Click 'Add Policy' next to the 'Create' type in the 'Object Type: account' section.

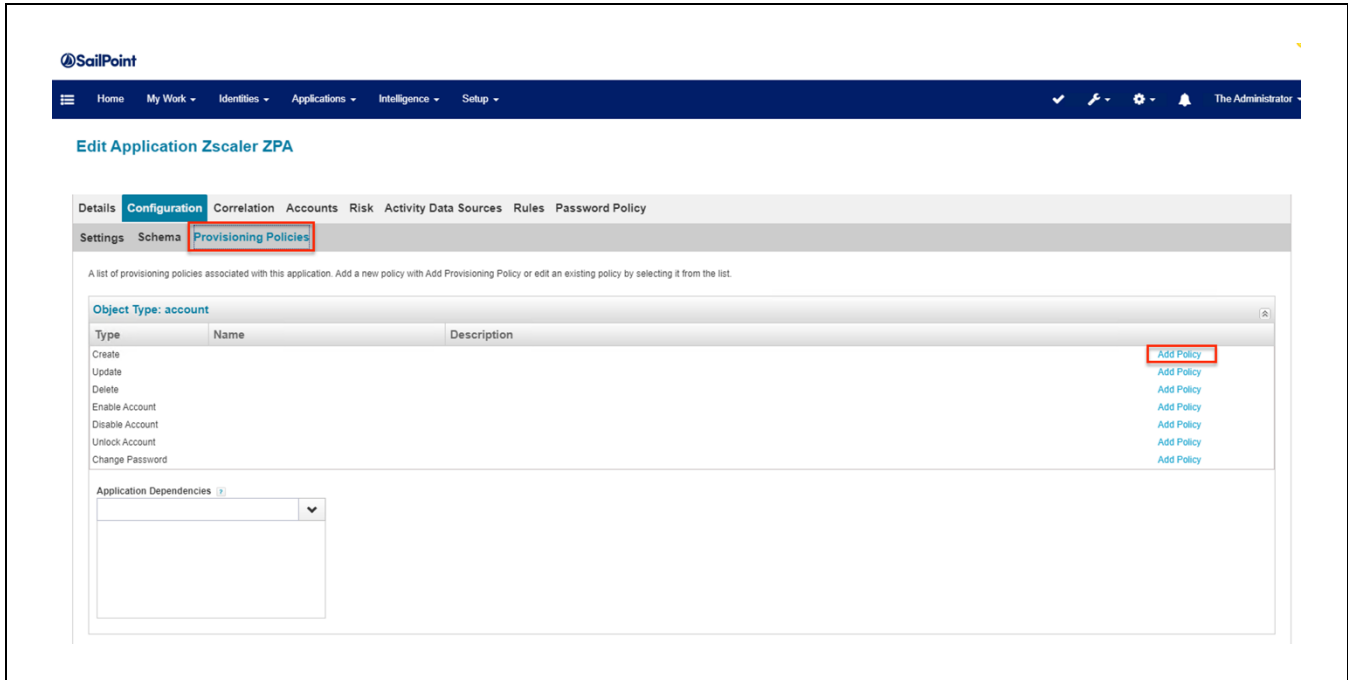


Figure 12: Configure Provisioning Plan



2.1.12 Create Policy Form

Step 13: Click the 'Create Policy Form'

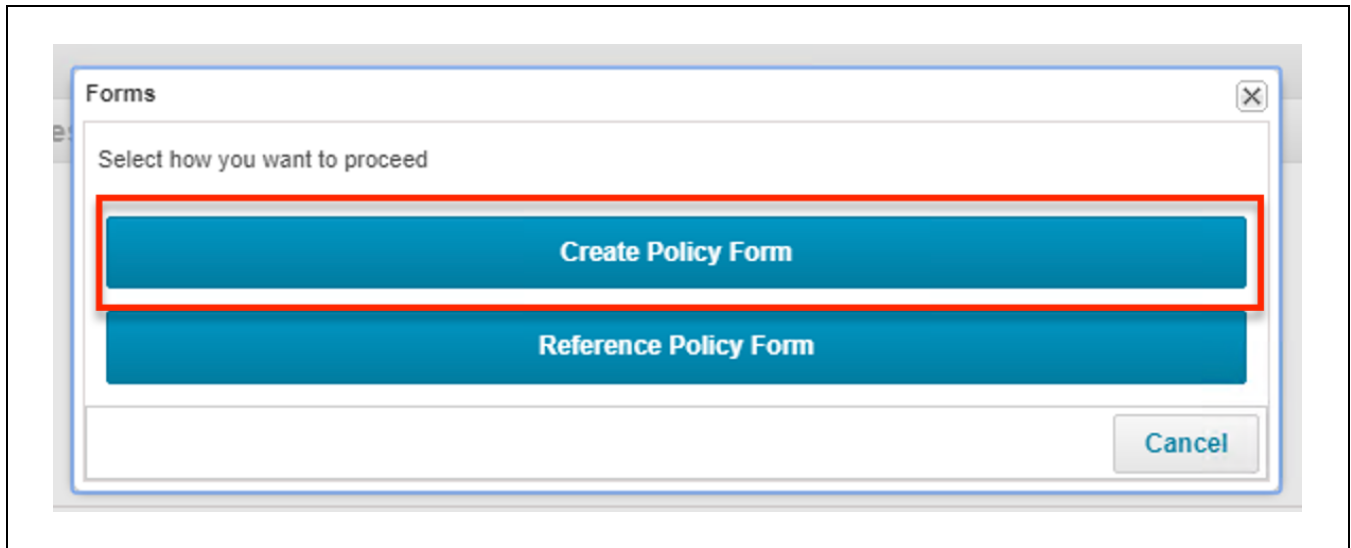


Figure 13: Create Policy Form



2.1.13 Configure Policy Form for ZIA

Step 14: This step is a bit complex. Please refer to SailPoint's provisioning documentation for more detail. Steps below Figure 14.

Figure 14: Configure Policy Form for ZIA

1. Enter a name of the create account policy
 2. Enter a description (not required)
 3. Add a section to the policy form, in this case it was edited and named 'Required Attributes'
 4. Click the '+' icon next to the section to add a new 'field'
 5. For ZIA, new accounts require that a 'userName' and 'displayName' are populated. Create a 'field' for each of these
 6. For each 'field' make sure to check the 'required' checkbox under Type Settings
- Once completed, click the 'Save' button



2.1.14 Verify Configuration Policy

Step 15: The new provisioning policy should appear next to the 'Create' operation on the application definition

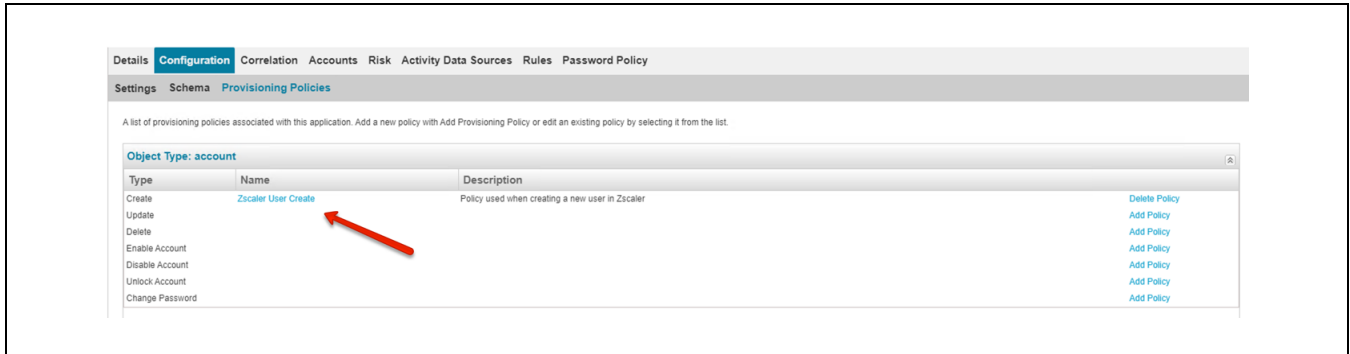


Figure 15: Verify Configuration Policy

2.1.15 Save Configuration Policy

Step 16: Click the 'Save' button at the bottom of the main application definition screen.



Figure 16: Save Configuration Policy

2.1.16 Verify New Application

Step 17: The new application will now be listed in the Application view of IdentityIQ



Figure 17: Verify New Application



2.2 Configuring Aggregation Tasks

Step 1: Click the 'Tasks' link under the 'Setup' option in the navigation bar

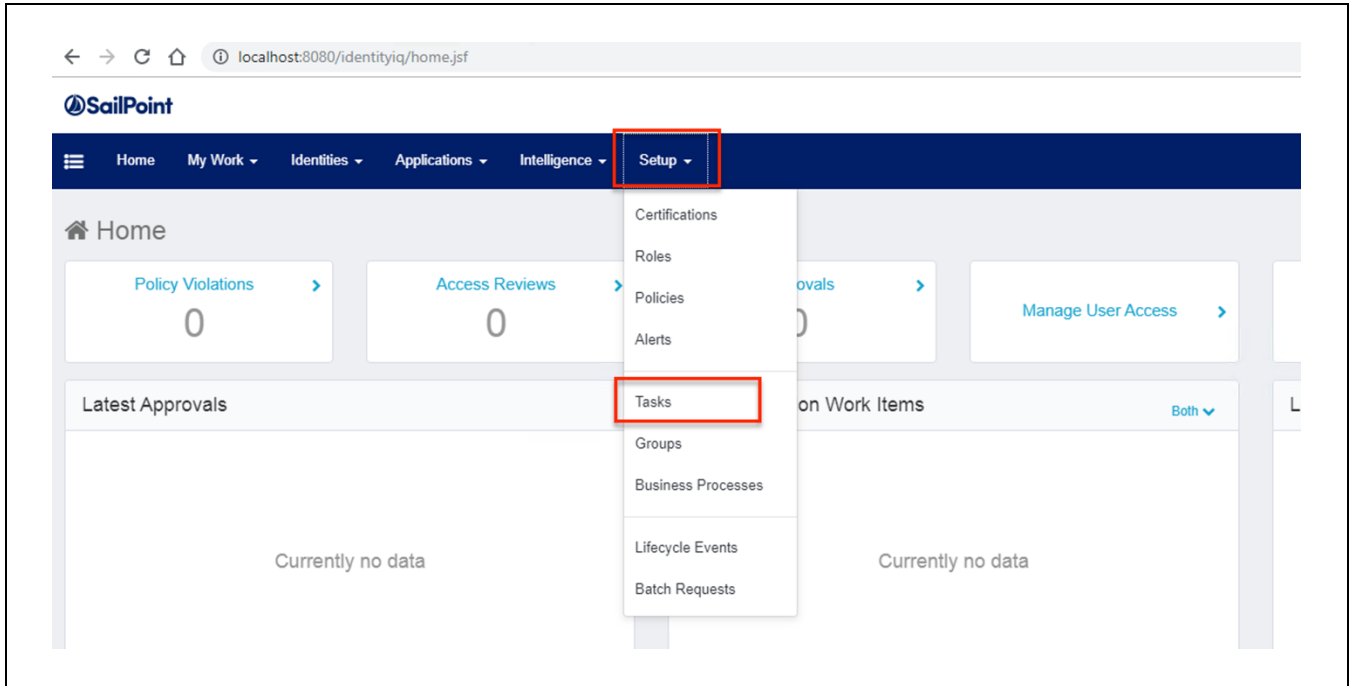


Figure 20: Configuring Aggregation Tasks



2.2.1 Create New Task

Step 2: To create an account aggregation task, click the 'New Task' button in the top-right of the screen, and then select 'Account Aggregation'

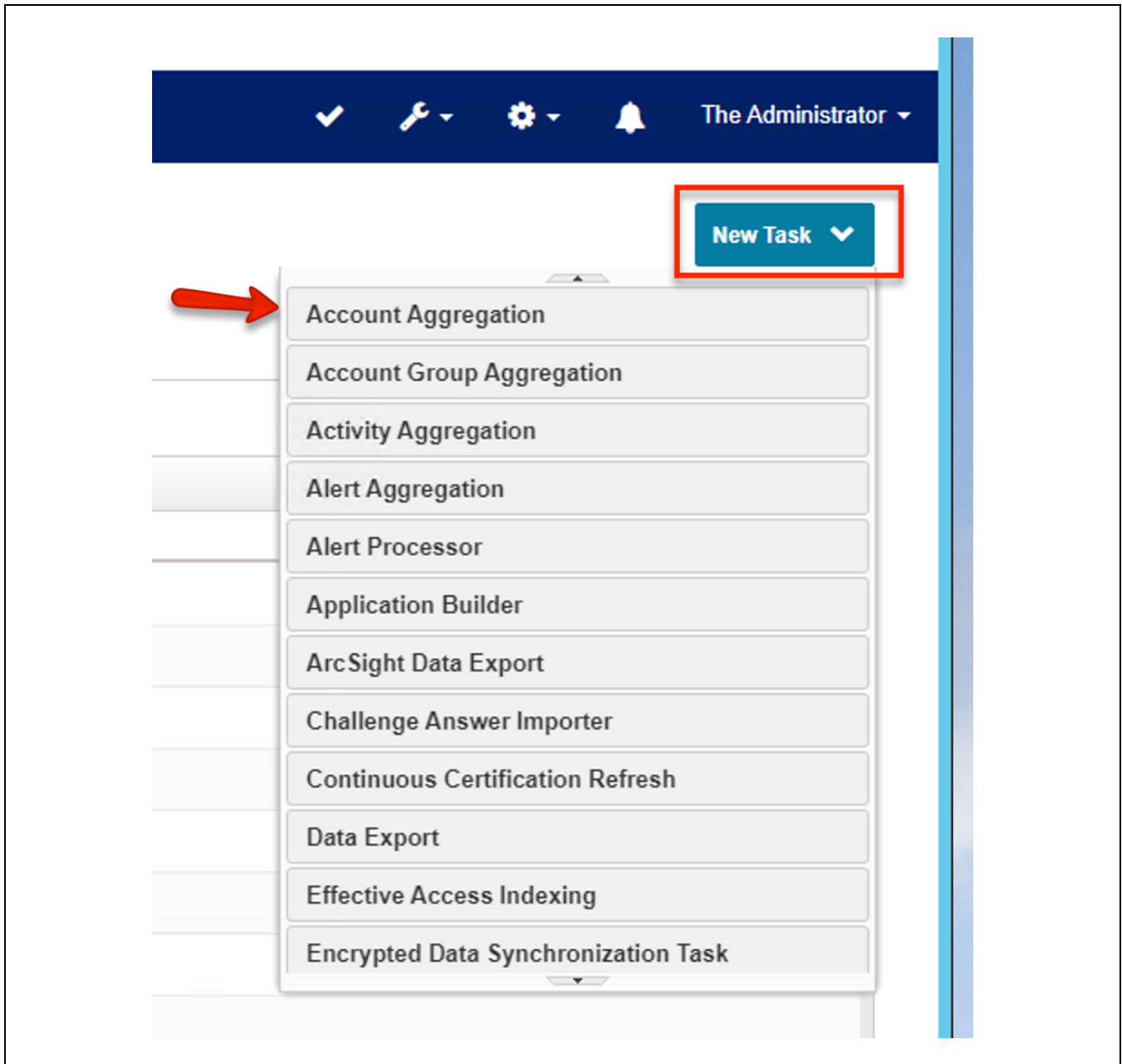


Figure 21: Create New Task



2.2.2 Configure Task Settings

Step 3: Give the task a name, and make sure to select the previously defined ZIA application from the dropdown list for 'Applications to Scan'

The screenshot shows the 'New Task' configuration interface. At the top, there is a navigation bar with 'Home', 'My Work', 'Identities', 'Applications', 'Intelligence', and 'Setup'. Below this, the 'New Task' section is titled. Under 'Standard Properties', the 'Name' field is highlighted with a red box and contains the text 'Zscaler Account Aggregation'. To the right of the 'Name' field, there is a 'Previous Result Action' dropdown set to 'Delete'. Below the 'Name' field is a 'Description' text area containing 'Task template for application account scanning.' Other fields include 'Allow Concurrency' (checkbox), 'Require Signoff' (checkbox), 'Host' (text input), 'Number of Runs' (0), and 'Average Run Time' (0:00:00). A 'Reset Run Statistics' button is located below these fields. Under 'Email Task Alerts', 'Email Notification' is set to 'Disabled' and 'Scope' is a dropdown menu. The 'Account Aggregation Options' section has a 'Select applications to scan*' dropdown menu with 'Zscaler' selected, indicated by a red arrow. Below this is an 'Optionally select a rule to assign capabilities or perform other processing on new identities' dropdown menu set to '-- Select Rule --'.

Figure 22: Configure Task Settings



2.2.3 Save and Execute Task

Step 4: Click 'Save and Execute' at the bottom of the task configuration page

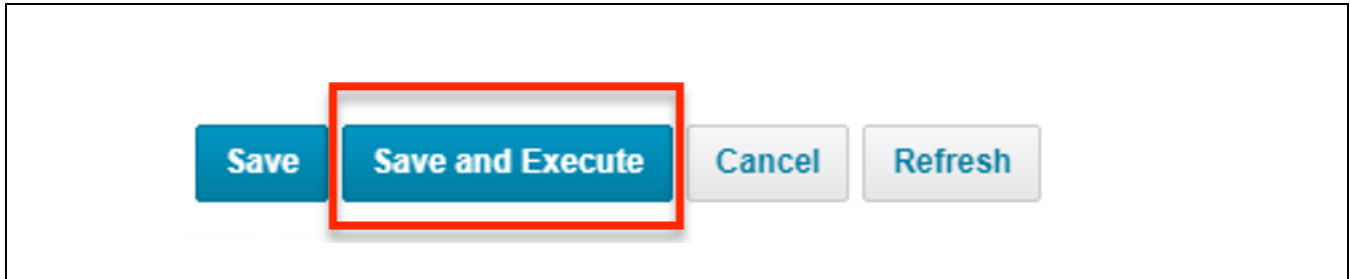


Figure 23: Save and Execute Task

2.2.4 Verify Account Aggregation Task

Step 5: The new task should now show up under the 'Account Aggregation' section of the task list. Click the 'Task Results' tab

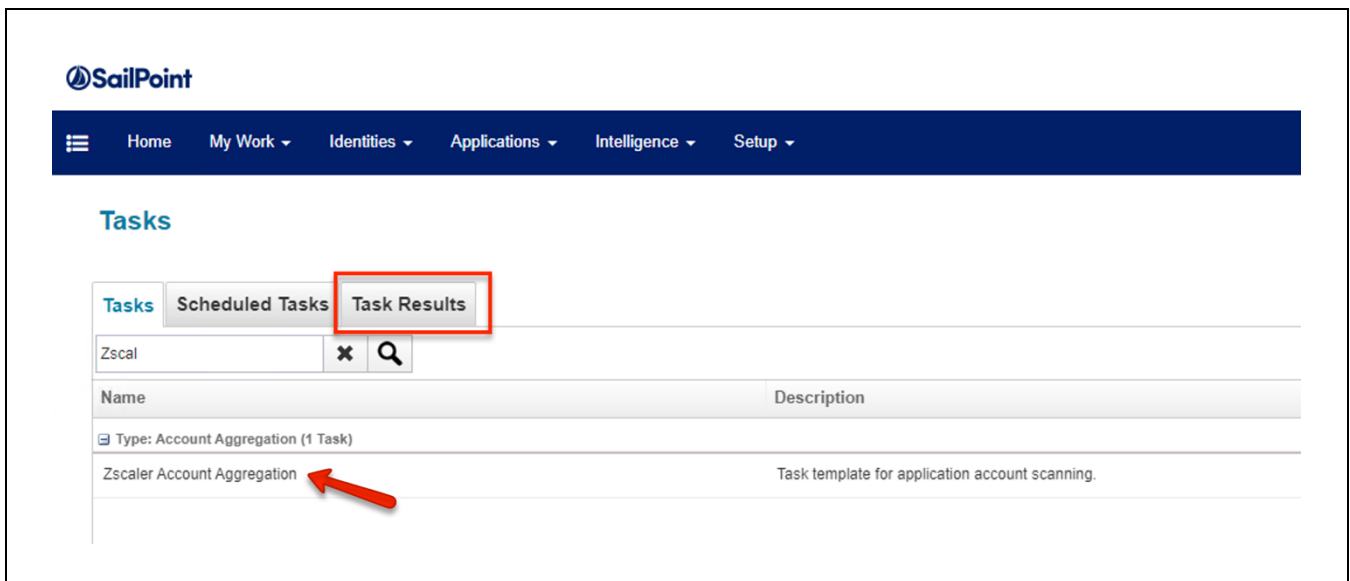


Figure 24: Verify Account Aggregation Task



2.2.5 Confirm Account Aggregation Task Completion

Step 6: Confirm that the account aggregation completed

The screenshot shows the SailPoint interface. At the top is the SailPoint logo and a navigation bar with links: Home, My Work, Identities, Applications, Intelligence, and Setup. Below this is the 'Tasks' section with three tabs: 'Tasks', 'Scheduled Tasks', and 'Task Results'. The 'Task Results' tab is active. A search bar contains the text 'Zscal'. Below the search bar is a table with columns: 'Name', 'Date Complete', and 'Result'. A single row is highlighted with a red border, showing the task 'Zscaler Account Aggregation' completed on '12/10/19 12:03 PM' with a 'Success' result.

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

Figure 25: Config Account Aggregation Task Completion



2.2.6 View Task Execution Details

Step 7: Clicking the successful task will bring up task execution details

The screenshot shows the 'Task Result' page in the SailPoint interface. The task is titled 'Zscaler Account Aggregation' and has a status of 'Success'. Below the task details is a table titled 'Zscaler Account Aggregation Attributes' with the following data:

Attribute	Value
Applications scanned	Zscaler
Accounts scanned	3
Accounts optimized	3

Figure 26: View Task Execution Details



2.2.7 Create Group Aggregation Task

Step 8: Back on the main tasks screen - create a group aggregation task. Click the 'New Task' button in the top-right of the screen, and then select 'Account Group Aggregation'

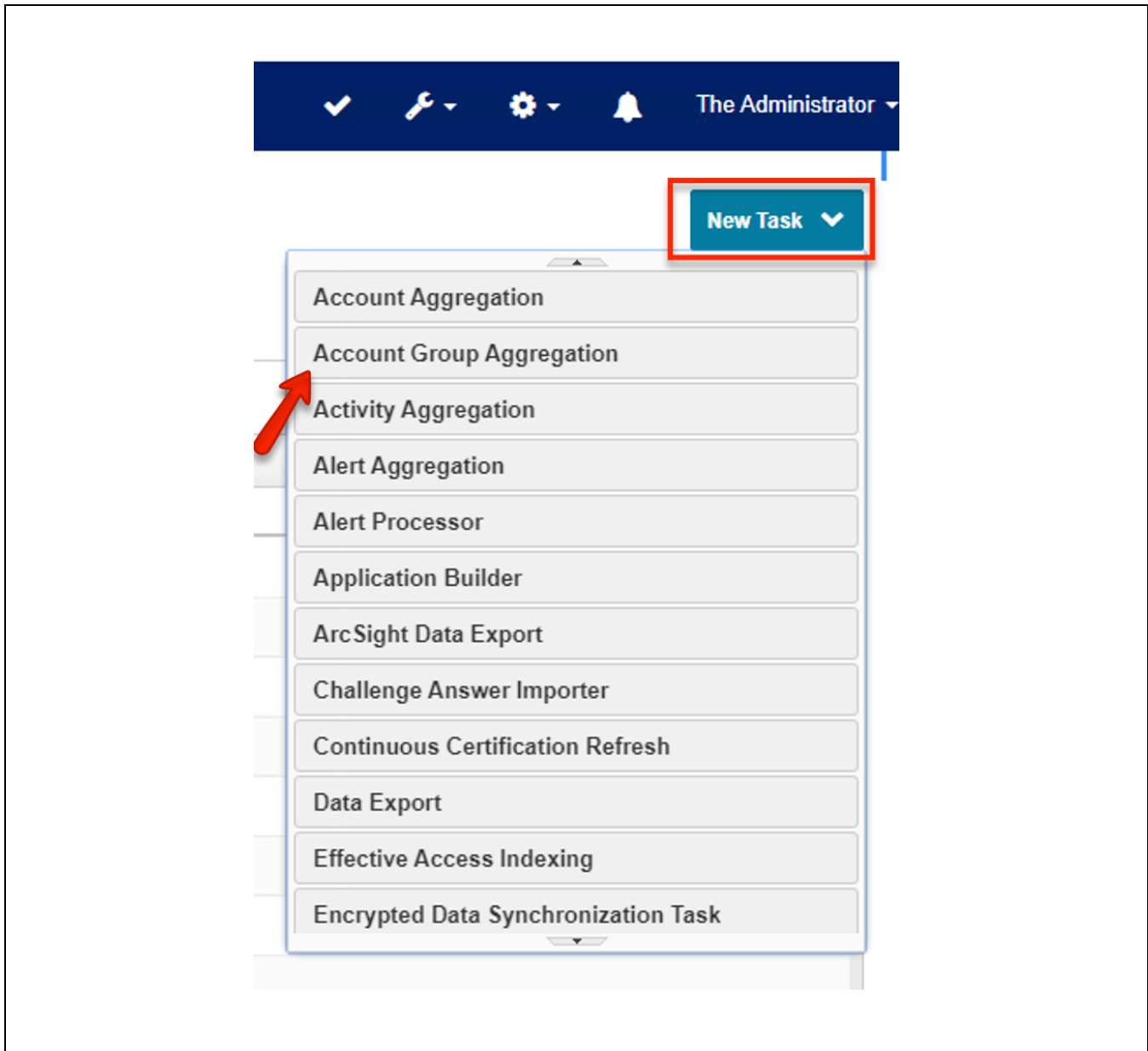


Figure 27: Create Group Aggregation Task



2.2.8 Link Account Aggregation

Step 9: Like the account aggregation, give the group aggregation a name, and select the ZIA application for the 'Applications to scan' list option

The screenshot shows the 'New Task' configuration page in the SailPoint interface. The page title is 'New Task' and the sub-section is 'Standard Properties'. The 'Name*' field is highlighted with a red box and contains the text 'Zscaler Group Aggregation'. Below this, there are fields for 'Description' (containing 'Task template for application group scanning.'), 'Allow Concurrency' (checkbox), 'Require Signoff' (checkbox), 'Host' (text field), 'Number of Runs' (0), and 'Average Run Time' (0:00:00). There is a 'Reset Run Statistics' button. Under 'Email Task Alerts', 'Email Notification' is set to 'Disabled' and 'Scope' is a dropdown menu. The 'Account Group Aggregation Options' section has a 'Select applications to scan*' label and a dropdown menu with 'Zscaler' selected. A red arrow points to the 'Zscaler' option in the dropdown. The 'Previous Result Action' field is empty.

Figure 28: Link Account Aggregation



2.2.9 Save and Execute

Step 10: Click the 'Save and Execute' button at the bottom of the task configuration page

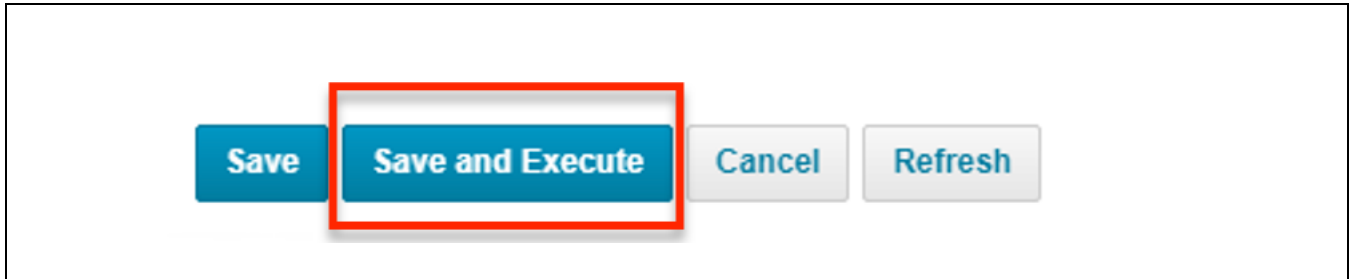


Figure 29: Save and Execute

2.2.10 Confirm Group Aggregation

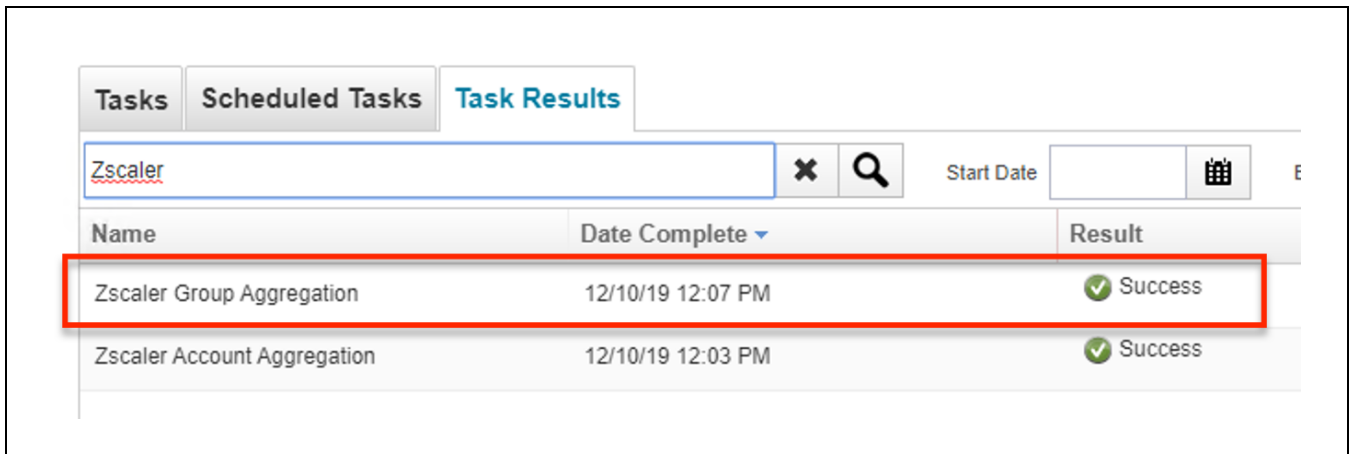


Figure 30: Confirm Group Aggregation

Step 10: Switching once again to the 'Task Results' tab, confirm that the group aggregation was successful



2.2.11 View Task Detailed Summary

Step 11: Clicking the task will bring up a more detailed summary of the result

The screenshot shows a 'Task Result' window with the following details:

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

Below the details is a 'Return to Tasks' button. Two tables are highlighted with a red border:

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 31: View Task Detailed Summary



2.3 Confirm Account Provisioning

2.3.1 Navigate to Manage Accounts

Step 1: Click the 'menu' button in the top left of any screen in IdentityIQ. Under 'Manage User Access' click the 'Manage Accounts' link.

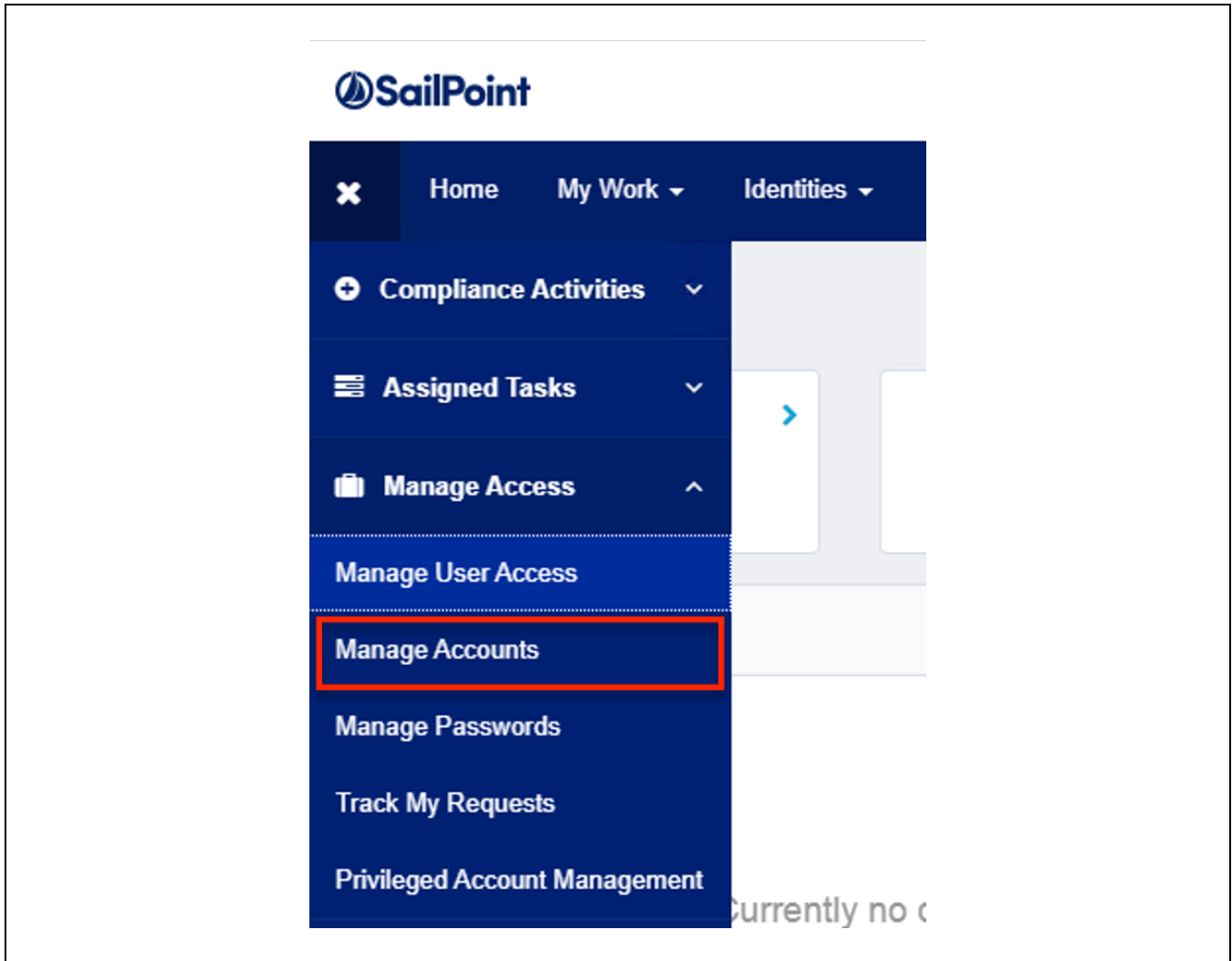


Figure 40: Navigate to Manage Accounts



2.3.2 Manage ZIA User

Step 2: Find an Identity for which a new account should be created in ZIA. Click the 'Manage' button for that users tile

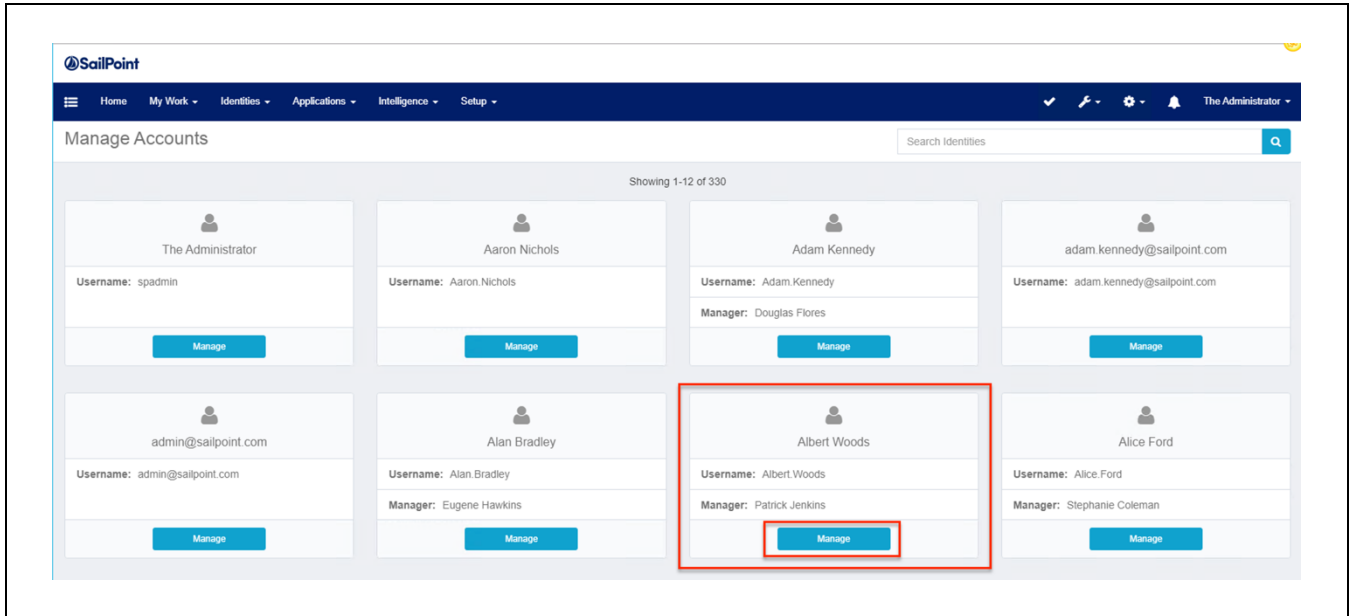


Figure 41: Manage ZIA User



2.3.3 Request ZIA User

Step 3: This screen shows the Identities currently provisioned application accounts. Click the 'Request Account' button

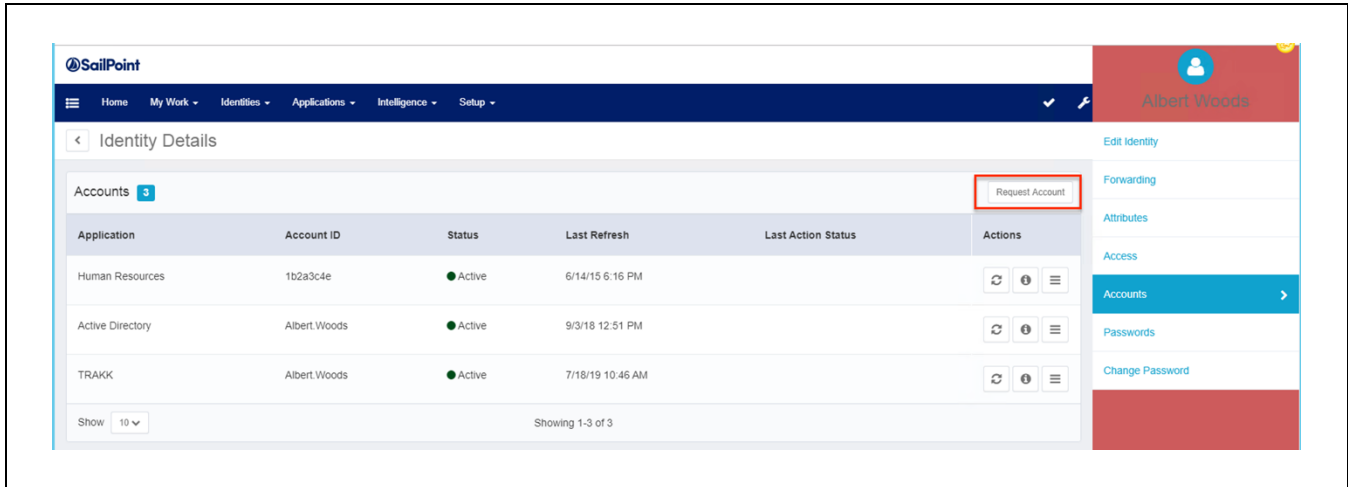


Figure 42: Request ZIA User



2.3.4 Request ZIA Application

Step 4: Select the ZIA application from the 'Application' dropdown list

The screenshot shows a web form titled "Request Account" with a close button in the top right corner. Below the title is a section titled "Summary of Request for Albert Woods" with the instruction "Verify the changes you have requested below." The form contains a required field labeled "Application *" which is a dropdown menu. The dropdown menu is open, showing "Zscaler" as the selected option. Below the dropdown is a text area with the placeholder "Type your comment here". At the bottom right of the form are two buttons: "Submit" and "Cancel". A red rectangular box highlights the dropdown menu.

Figure 43: Request ZIA Application



2.3.5 Confirm ZIA Application

Step 5: Click 'Confirm'

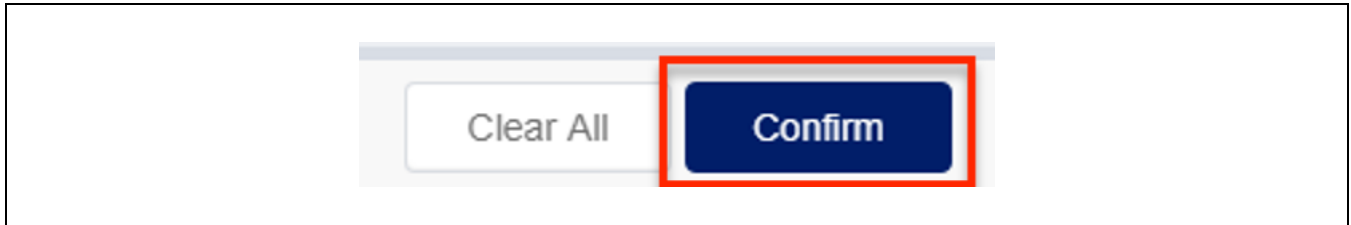


Figure 44: Confirm ZIA Application



2.3.6 Submit User Request

Step 6: Click the 'Submit' button for the request

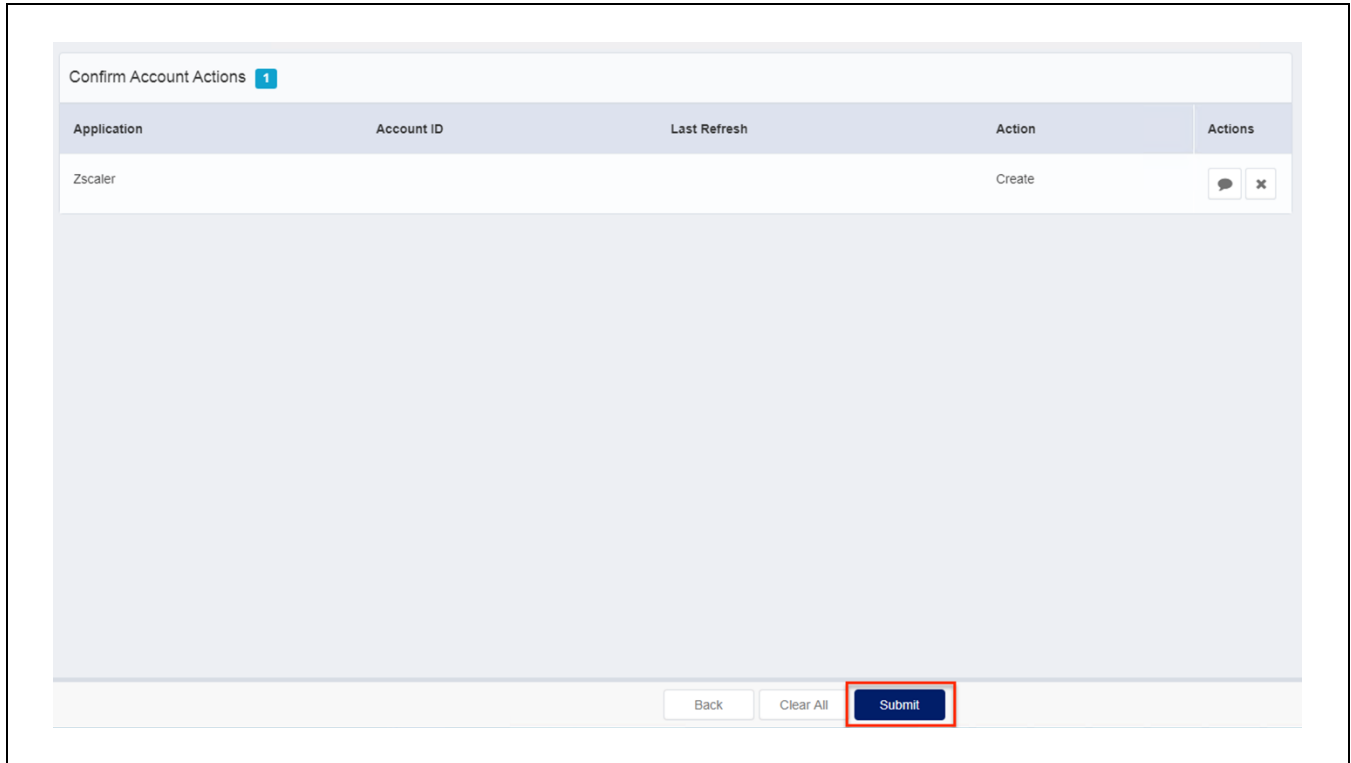


Figure 45: Submit User Request



2.3.7 Enter in User Required Fields

Step 7: Because our 'create' provisioning policy had a number of required fields (username, displayName) the IdentityIQ interface will prompt the requestor with a form to provide those values. Click 'Complete Form'.

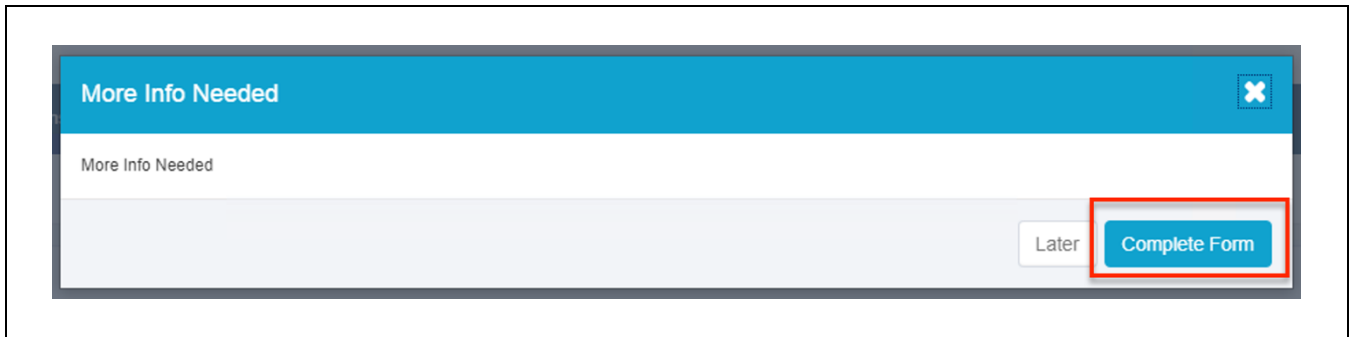


Figure 46: Enter In User Required Fields



2.3.8 Verify User Email Address

Step 8: Fill in the UserName and Display Name fields. The username must be in the format of a valid email address. Click the 'Ok' button 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 47: Verify User Email Address



2.3.9 Confirm Account Provisioning

Step 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	7a736361-6c65-7200-7363-896d0060484f	CorrelateManual	Albert.Woods	undetermined

Figure 48: Confirm Account Provisioning



3 Configuring SailPoint for ZPA

3.1 Creating the Zscaler Application

Step 1: Define a new application by clicking the 'Application' -> 'Application Definition' navigation option

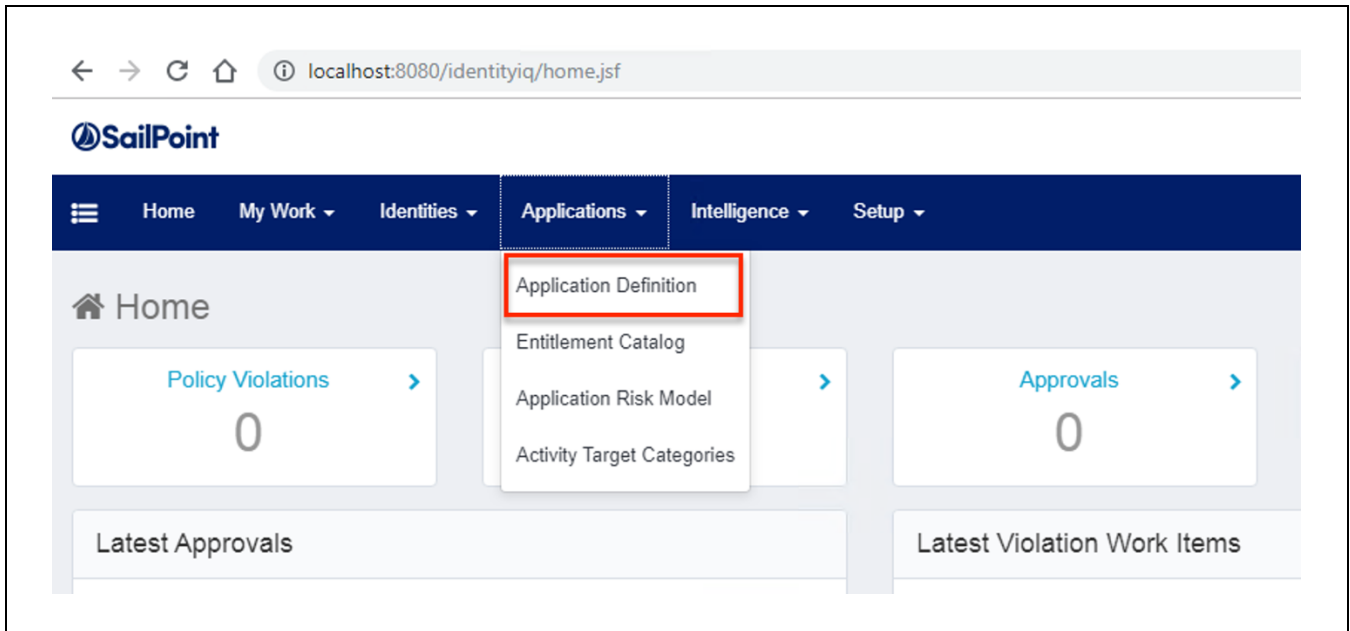


Figure 50: Create the Zscaler Application Definition



3.1.1 Add New Application

Step 2: Click the 'Add New Application' button

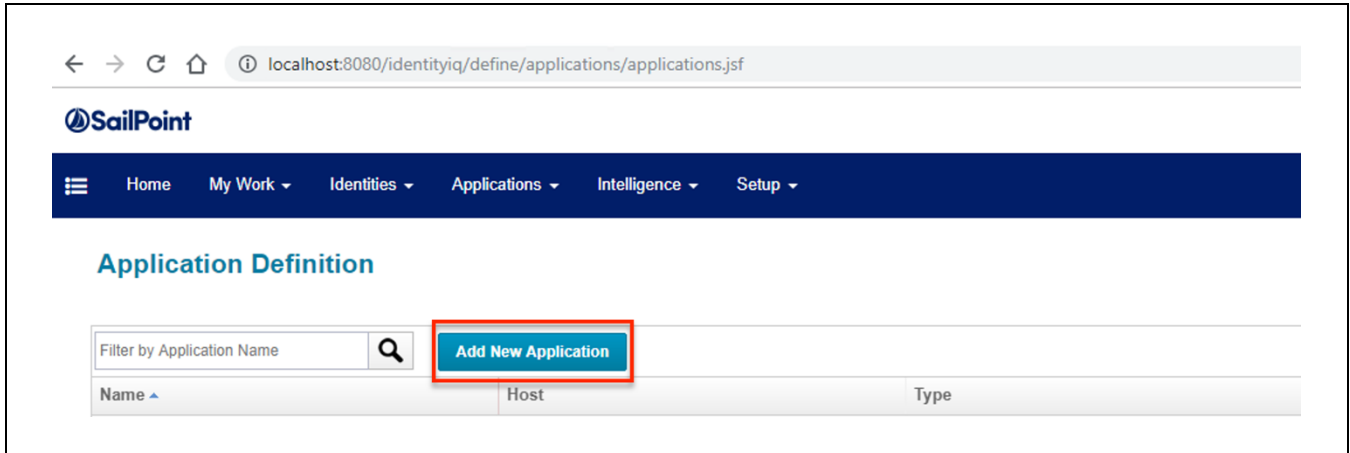


Figure 51: Add New Application



3.1.2 Configure Application Type

Step 3: Select 'SCIM 2.0' from the Application Type dropdown

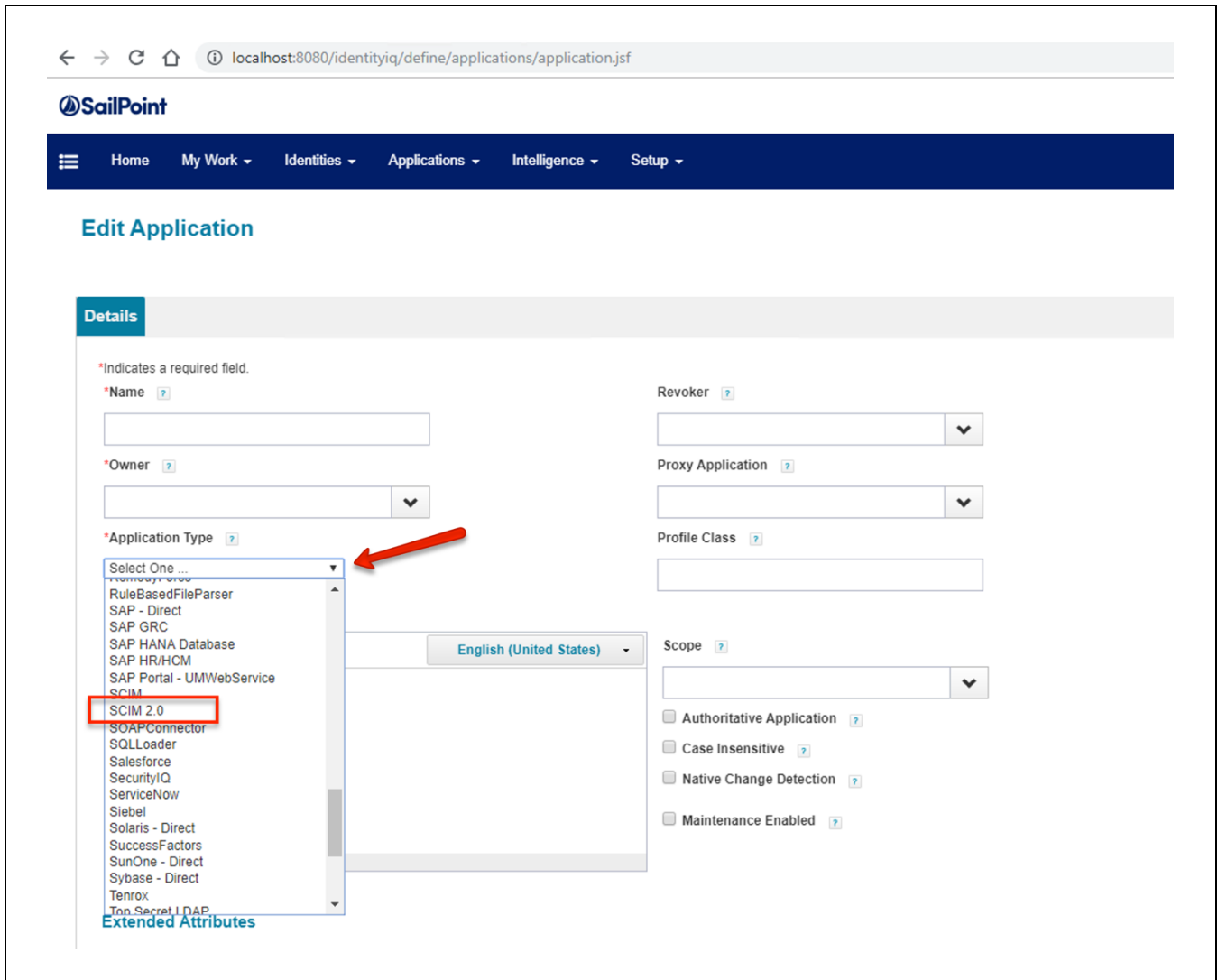


Figure 52: Configure Application Type



3.1.3 Creating the Zscaler Application

Step 4: Enter an application name, and an application owner for the Zscaler Private Access application. For more information on how IdentityIQ uses these fields, refer to the SailPoint product documentation

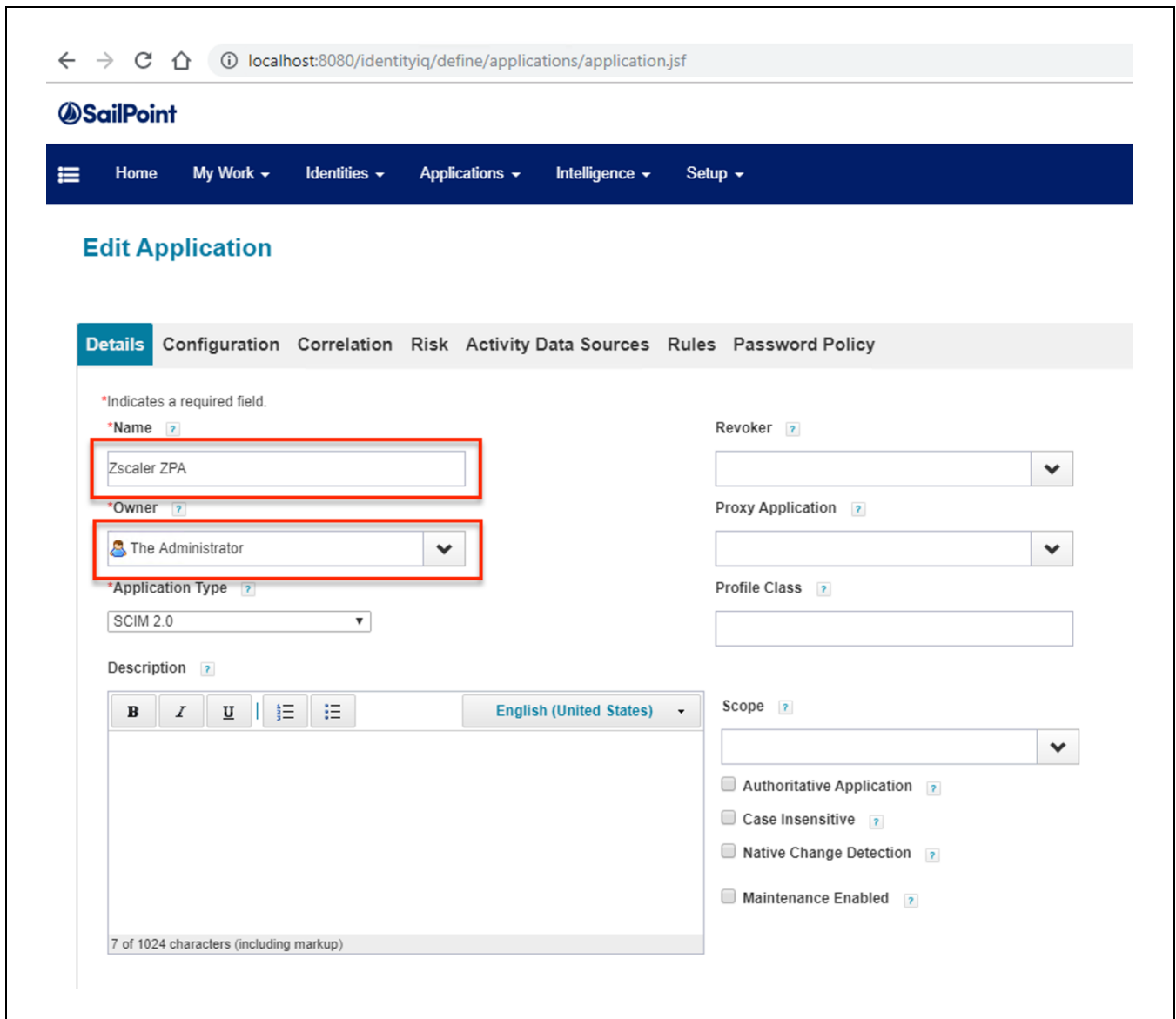


Figure 53: Log Into Zscaler



3.1.4 Test Connection

Step 5: Enter the connection parameters specific to your ZPA SCIM server.

1. The base url to the SCIM server should be of the format 'https://scim.zscalerbeta.net/<your_tenant_id>/scim
2. Select 'API Token' as the authentication type
3. Enter the API token provided by your ZPA administrator

Click the 'Test Connection' button to ensure the parameters were entered correctly

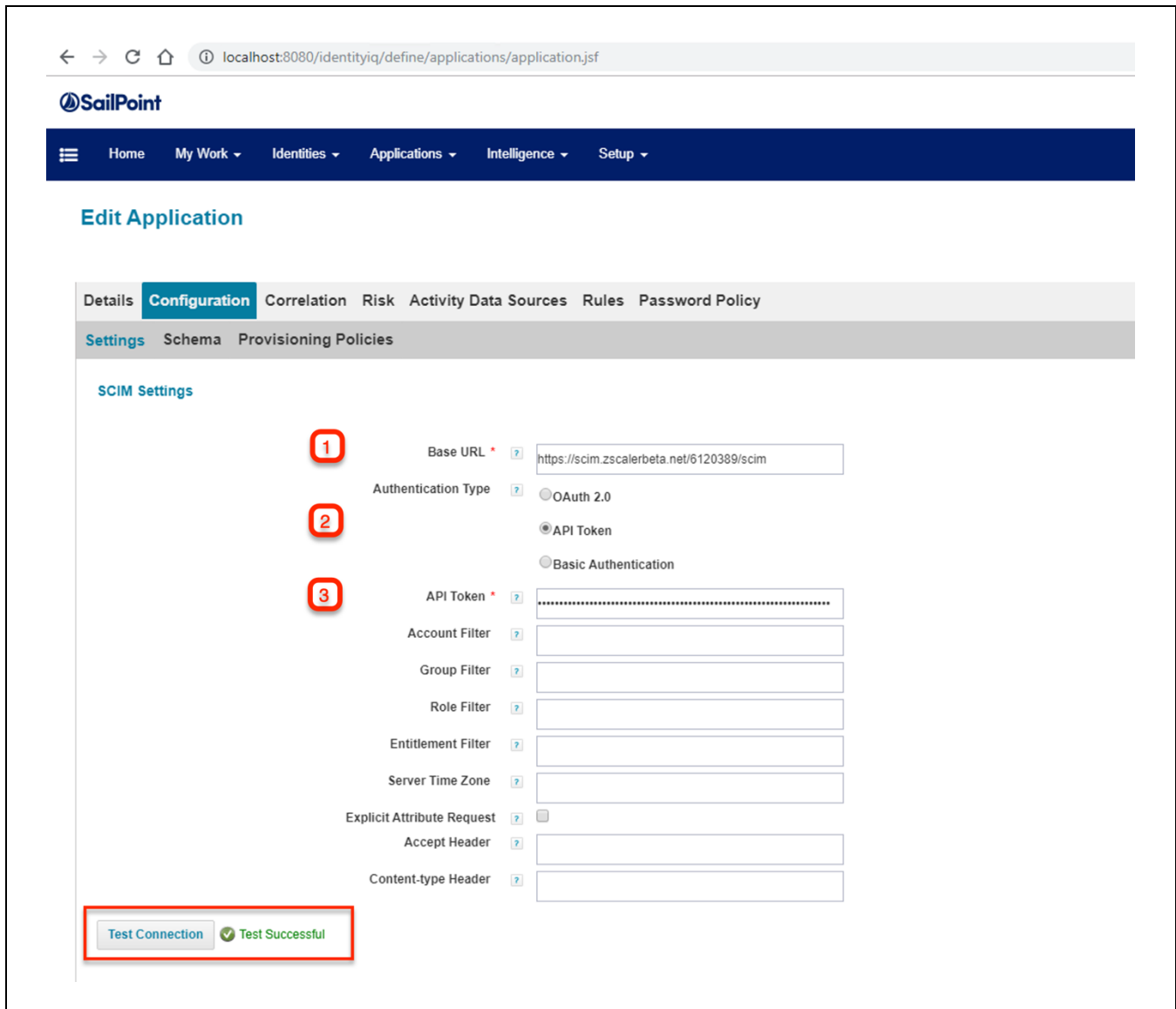


Figure 54: Test Connection



3.1.5 Schema Configuration

Step 6: Navigate to the 'Schema' sub-tab under the 'Configuration' tab. Click the 'Discover Schema Attributes' button under the 'Object Type: account' section.

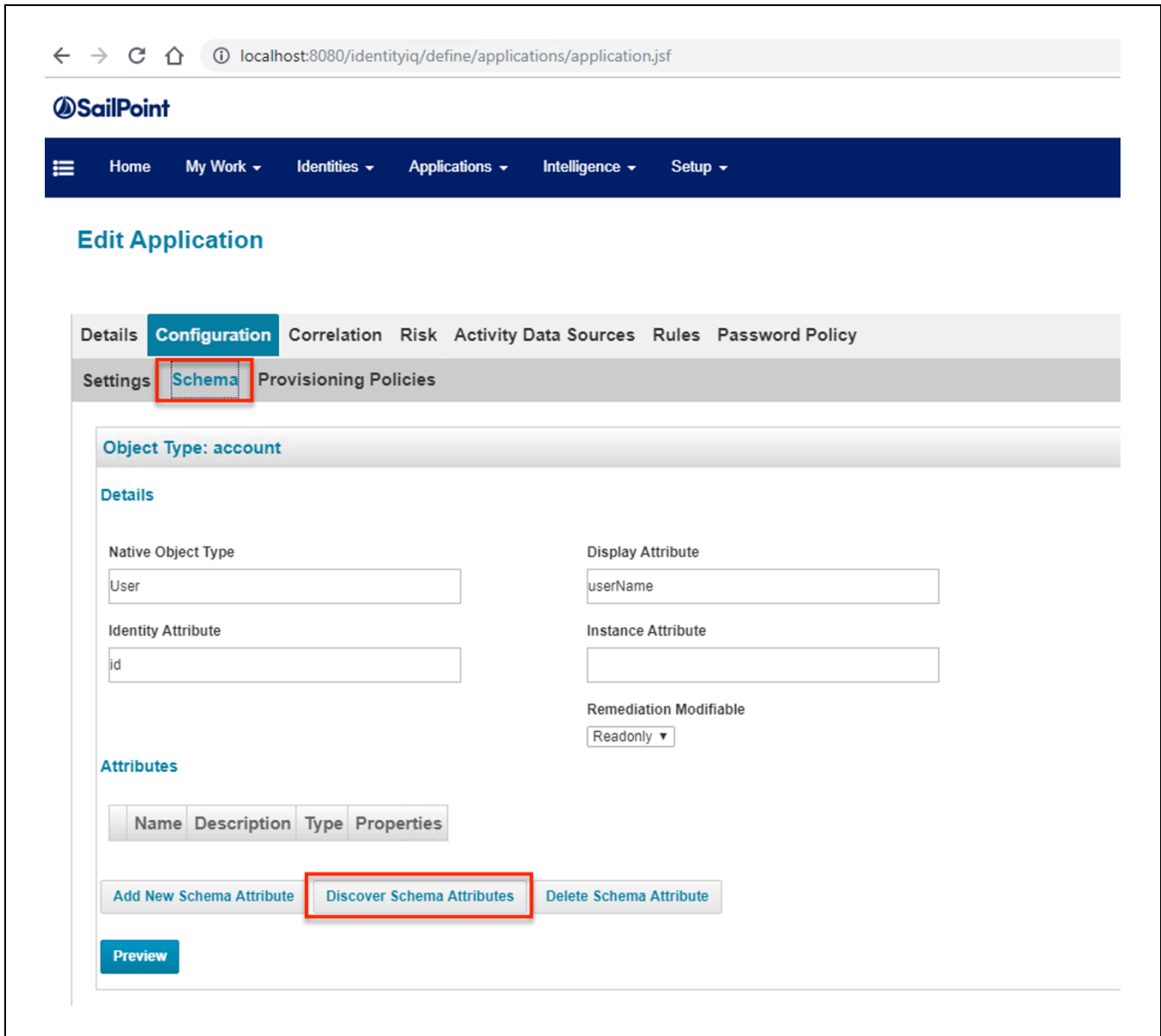


Figure 55: Schema Configuration



3.1.6 ZIA User Attributes

Step 7: The attributes for a user in ZPA will be populated

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 Weste	string		Edit
<input type="checkbox"/> name.givenName	The given name of the User, or first name in most Weste	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 56: ZPA User Attributes



3.1.7 Discover Schema Attributes

Step 8: Next, click the '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

Attributes

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

Figure 57: Discover Schema Attributes



3.1.8 Verify Attributes

Step 9: The attributes for a group in ZPA will be populated

Object Type: group

Details

<p>Native Object Type <input type="text" value="Group"/></p> <p>Identity Attribute <input type="text" value="id"/></p> <p>Description Attribute <input type="text"/></p>	<p>Display Attribute <input type="text"/></p> <p>Instance Attribute <input type="text"/></p> <p>Remediation Modifiable Readonly ▾</p>
--	---

Attributes

Name	Description	Type	Properties	
<input type="checkbox"/> id	Unique identifier for the SCIM Resource as defined by th	string ▾	<input type="text"/>	Edit
<input type="checkbox"/> externalId	A String that is an identifier for the resource as defined t	string ▾	<input type="text"/>	Edit
<input type="checkbox"/> displayName	A human-readable name for the Group. REQUIRED.	string ▾	<input type="text"/>	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 58: Verify Attributes



3.1.9 Test Configuration

Step 10: To test the configuration of the schemas, click the 'Preview' button under each one (account, group)

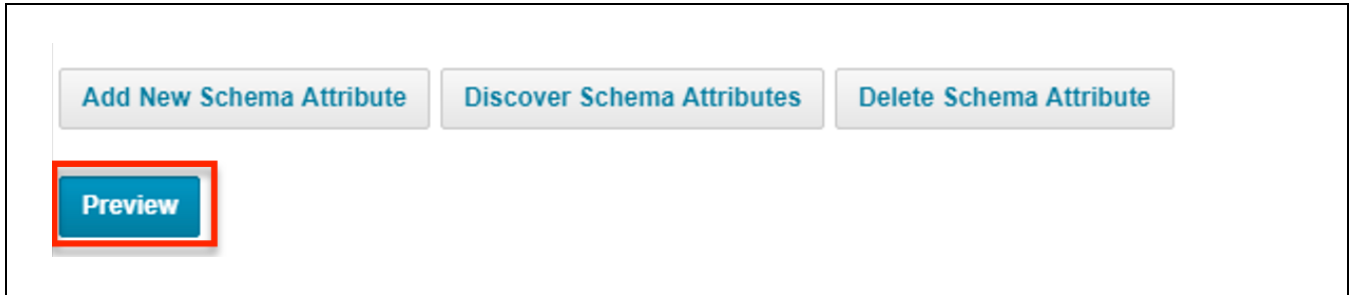


Figure 59: Test Configuration

3.1.10 Preview Live Data

Step 11: Clicking the 'Preview' button will display live data from the ZPA SCIM server connection (account preview shown)

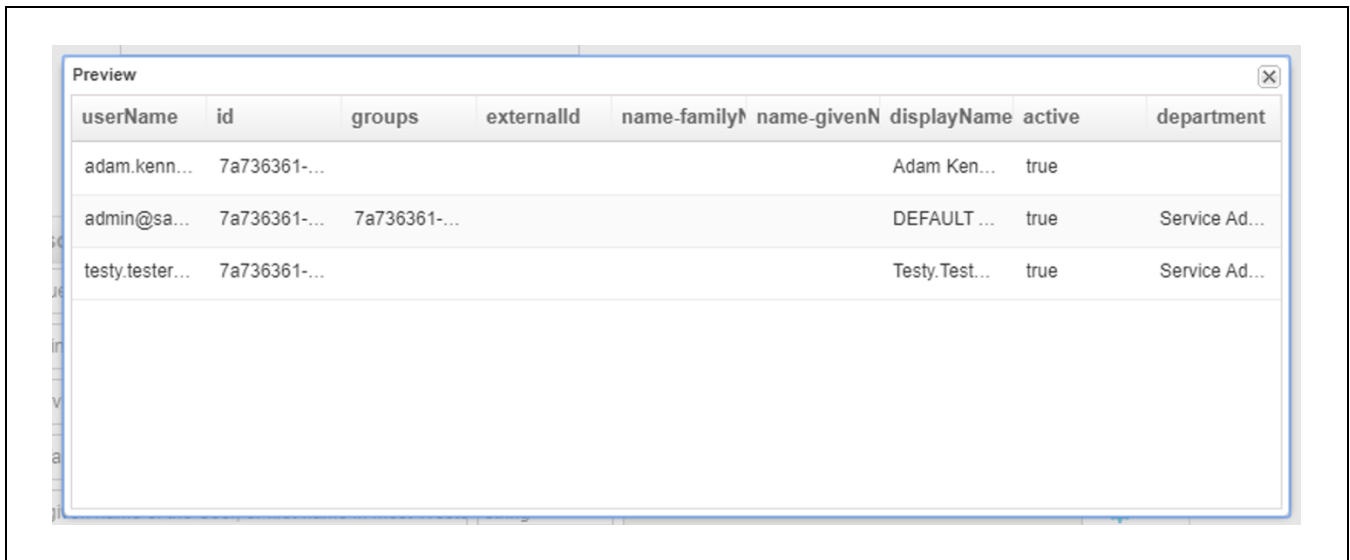


Figure 60: Preview Live Data



3.1.11 Configure Provisioning Plan

Step 12: The next step in application configuration is to configure provisioning plans. For this tutorial, a simple 'account creation' plan will be shown. First, click the 'Provisioning Policies' sub-tab under the 'Configuration' tab in the application definition. Click 'Add Policy' next to the 'Create' type in the 'Object Type: account' section.

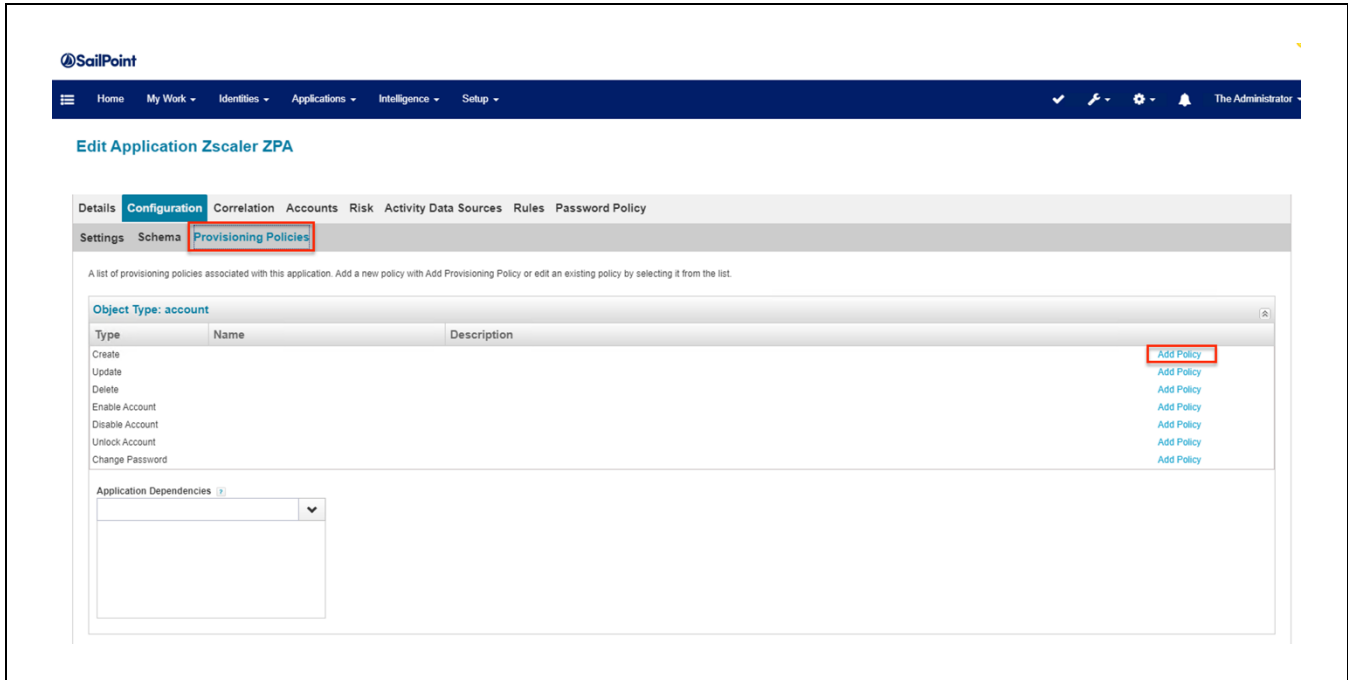


Figure 61: Configure Provisioning Plan



3.1.12 Create Policy Form

Step 13: Click the 'Create Policy Form'

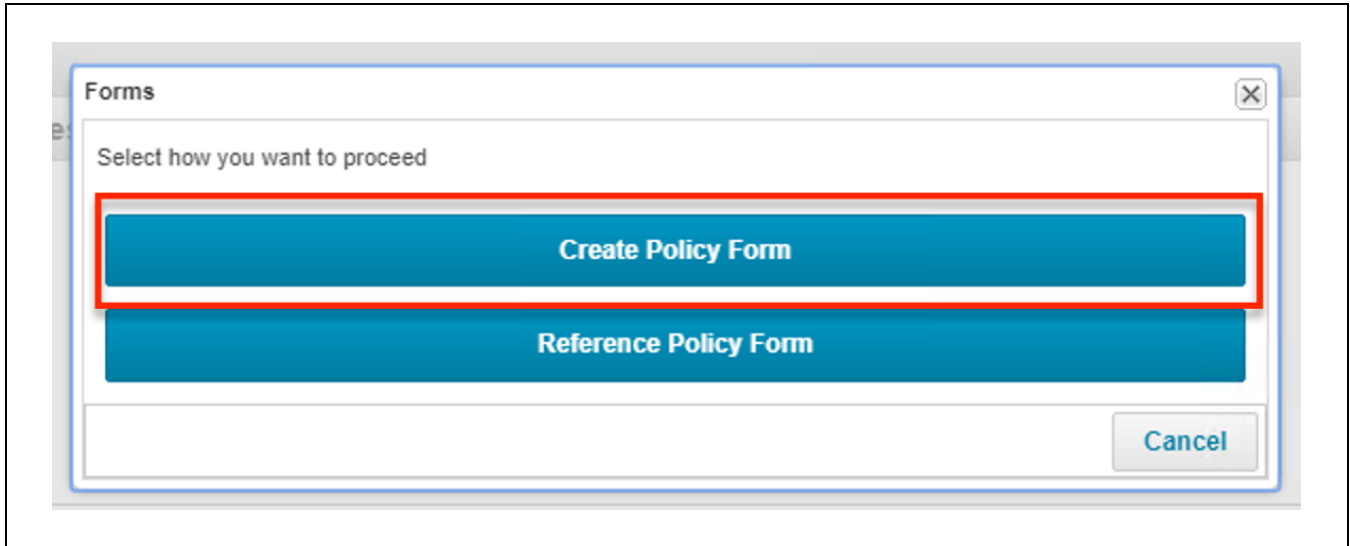


Figure 62: Create Policy Form



3.1.13 Configure Policy Form for ZPA

Step 14: This step is a bit complex. Please refer to SailPoint's provisioning documentation for more detail. Steps below Figure 63.

Figure 63: Configure Policy Form for ZPA

7. Enter a name of the create account policy
 8. Enter a description (not required)
 9. Add a section to the policy form, in this case it was edited and named 'Required Attributes'
 10. Click the '+' icon next to the section to add a new 'field'
 11. For ZPA, new accounts require that a 'userName' and 'displayName' are populated. Create a 'field' for each of these
 12. For each 'field' make sure to check the 'required' checkbox under Type Settings
- Once completed, click the 'Save' button



3.1.14 Verify Configuration Policy

Step 15: The new provisioning policy should appear next to the 'Create' operation on the application definition

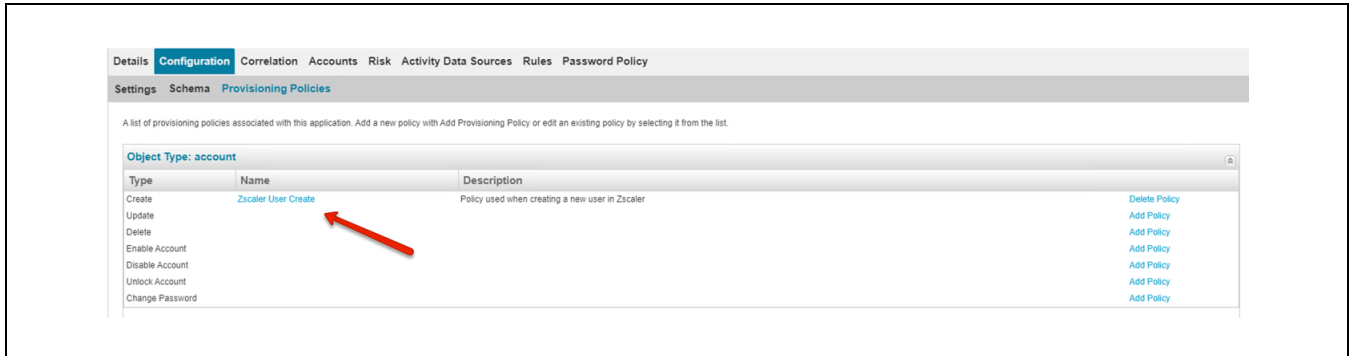


Figure 64: Verify Configuration Policy

3.1.15 Save Configuration Policy

Step 16: Click the 'Save' button at the bottom of the main application definition screen.



Figure 65: Save Configuration Policy

3.1.16 Verify New Application

Step 17: The new application will now be listed in the Application view of IdentityIQ



Figure 66: Verify New Application



3.2 Configuring Aggregation Tasks

Step 1: Click the 'Tasks' link under the 'Setup' option in the navigation bar

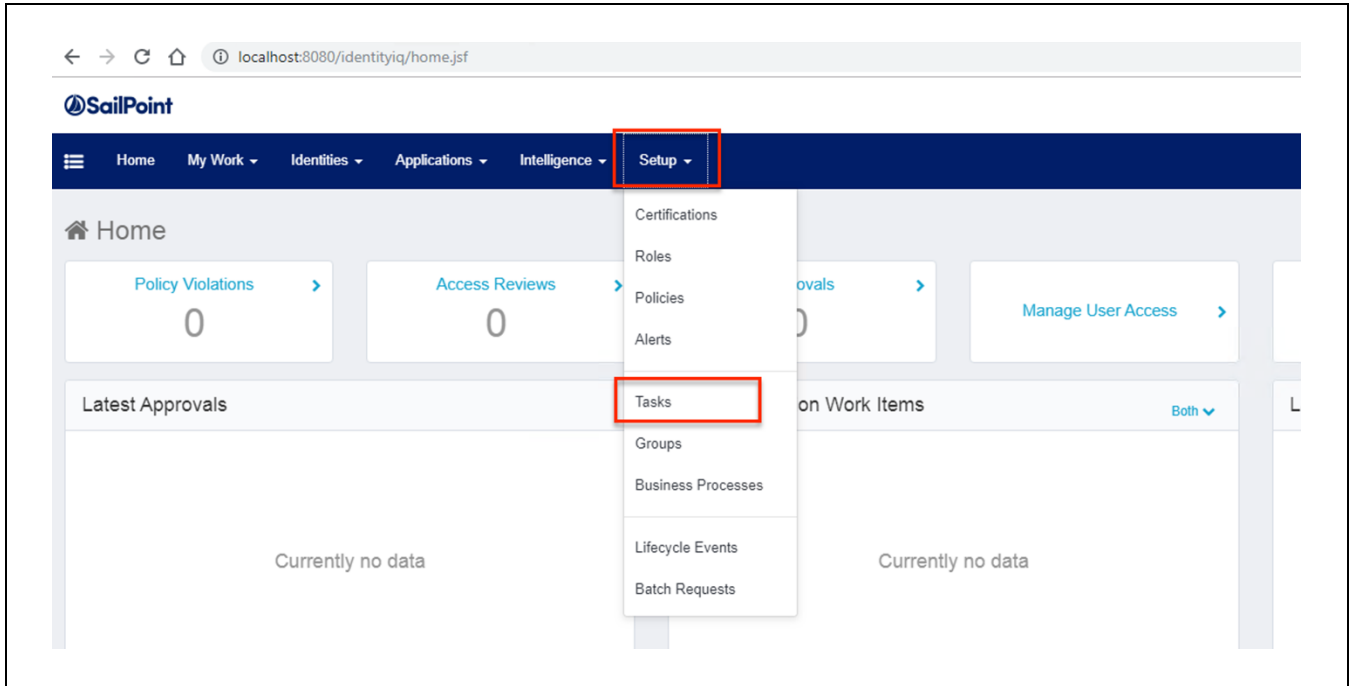


Figure 70: Configuring Aggregation Tasks



3.2.1 Create New Task

Step 2: To create an account aggregation task, click the 'New Task' button in the top-right of the screen, and then select 'Account Aggregation'

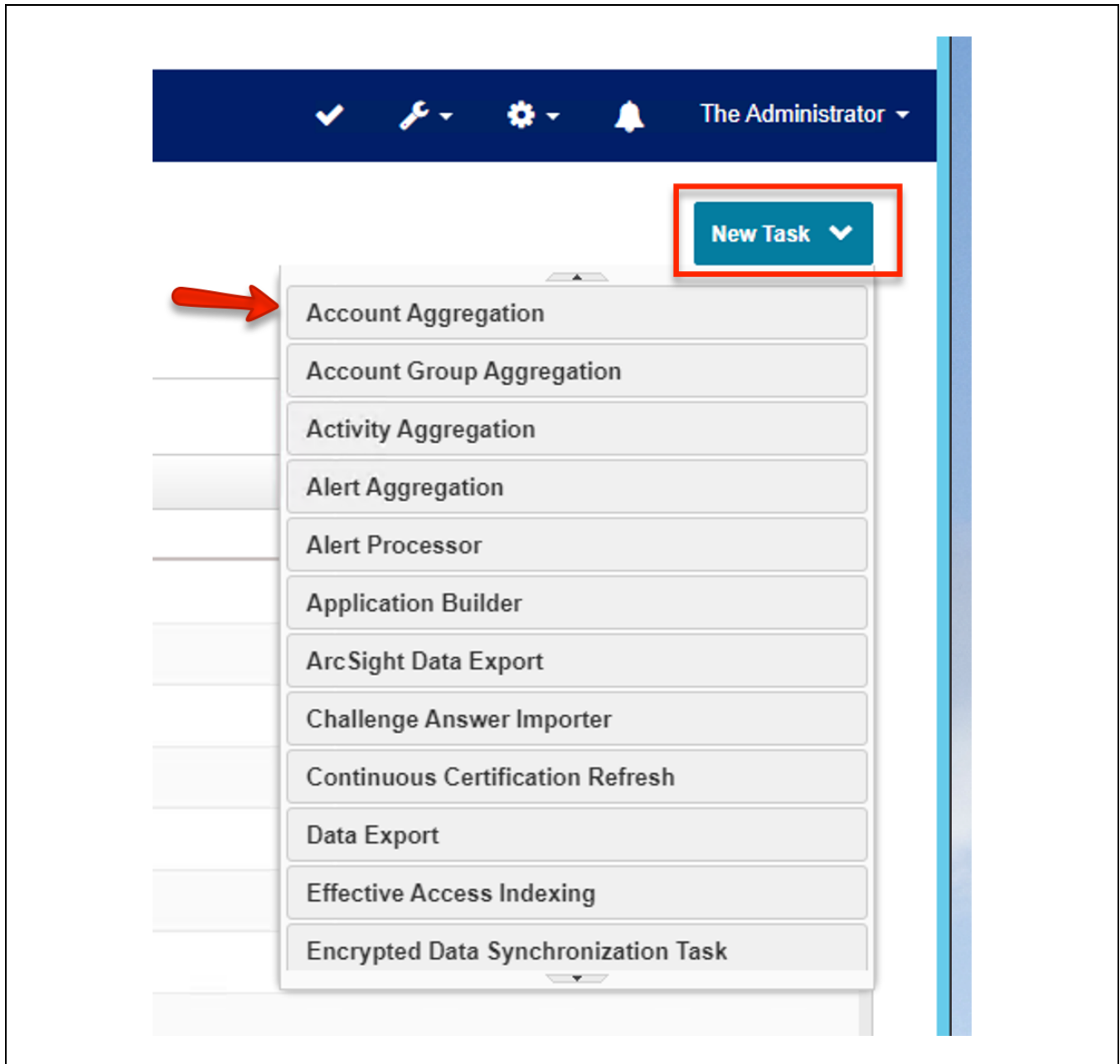


Figure 71: Create New Task



3.2.2 Configure Task Settings

Step 3: Give the task a name, and make sure to select the previously defined ZPA application from the dropdown list for 'Applications to Scan'

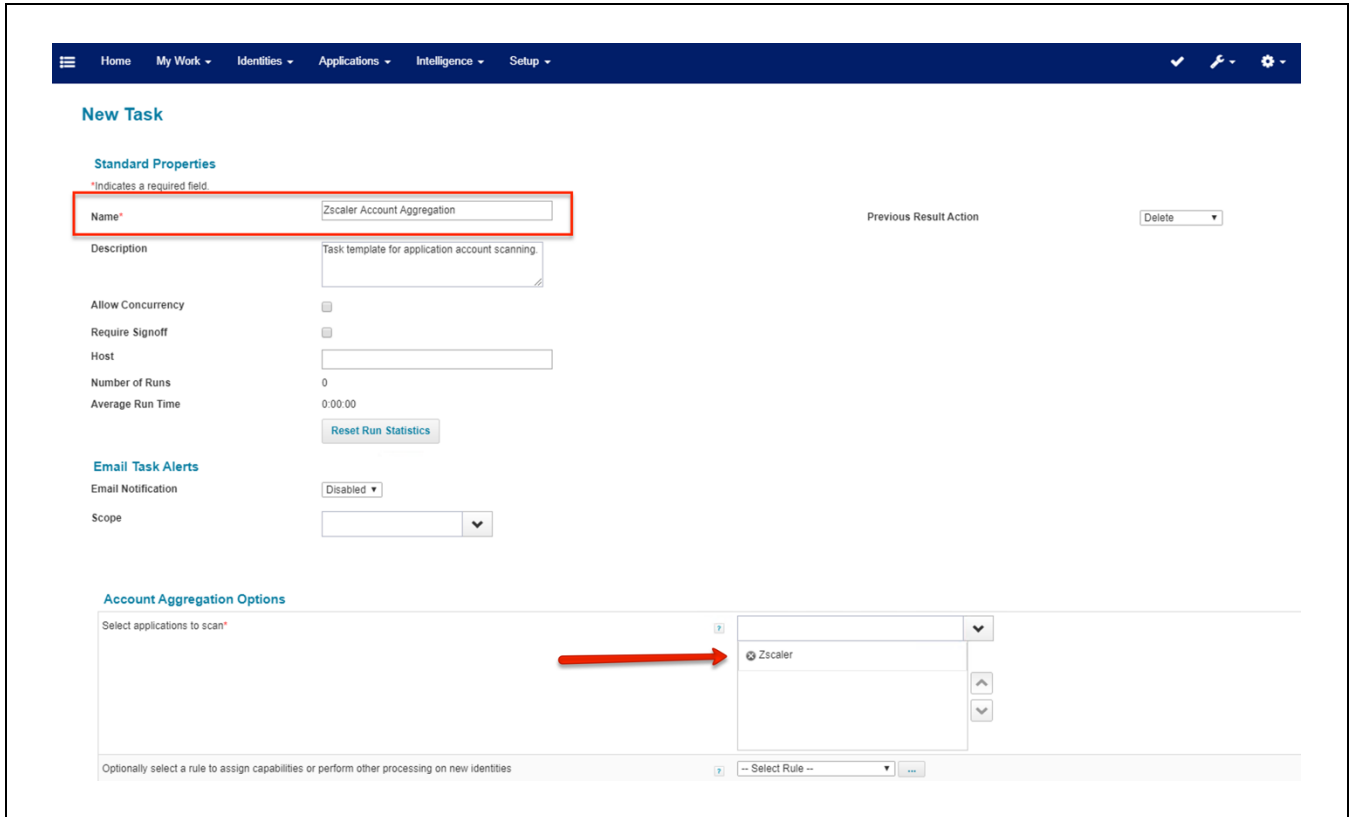


Figure 72: Configure Task Settings



3.2.3 Save and Execute Task

Step 4: Click 'Save and Execute' at the bottom of the task configuration page

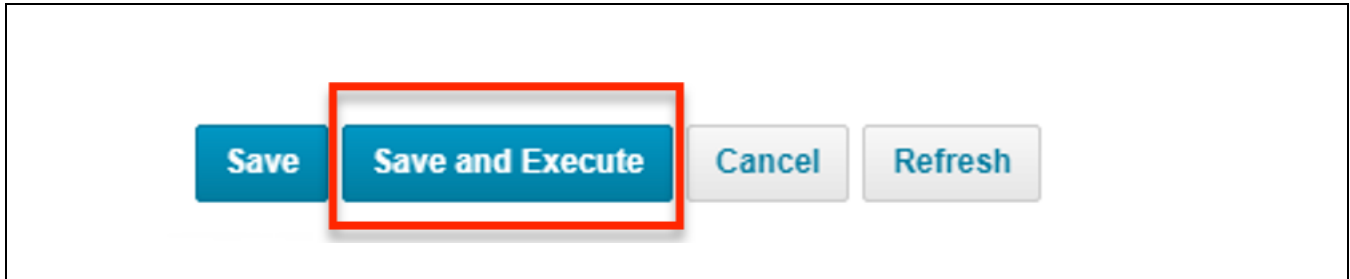


Figure 73: Save and Execute Task

3.2.4 Verify Account Aggregation Task

Step 5: The new task should now show up under the 'Account Aggregation' section of the task list. Click the 'Task Results' tab

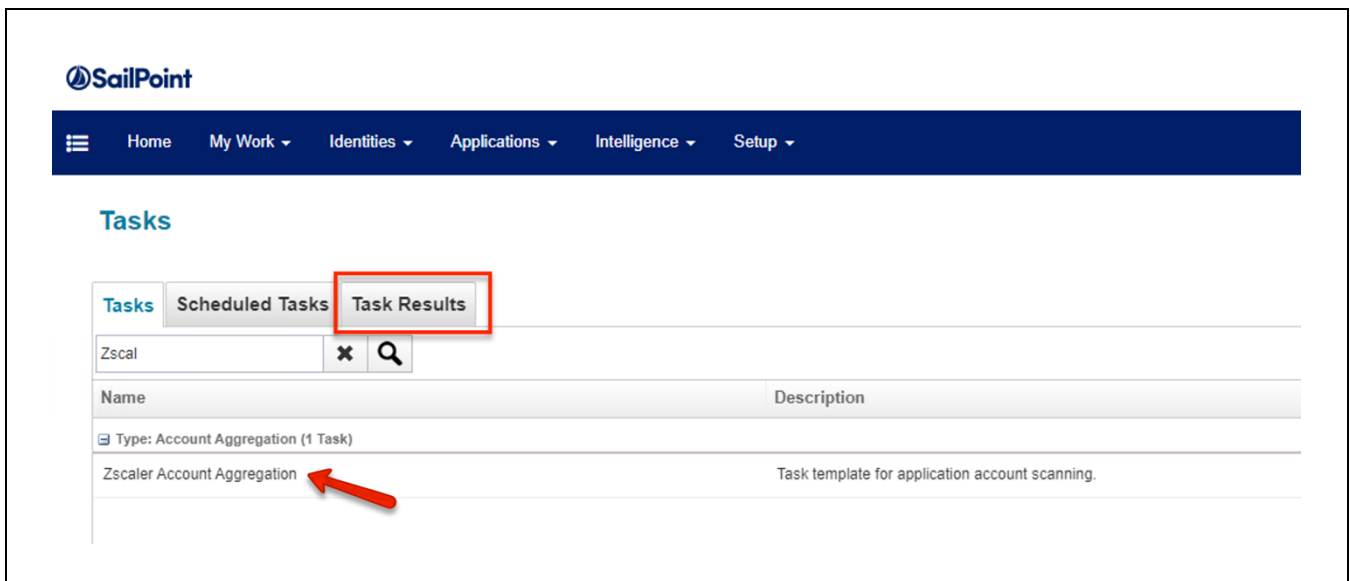


Figure 74: Verify Account Aggregation Task



3.2.5 Confirm Account Aggregation Task Completion

Step 6: Confirm that the account aggregation completed

The screenshot shows the SailPoint interface. At the top is the SailPoint logo and a navigation bar with links: Home, My Work, Identities, Applications, Intelligence, and Setup. Below this is the 'Tasks' section with three tabs: 'Tasks', 'Scheduled Tasks', and 'Task Results'. The 'Task Results' tab is active. A search bar contains 'Zscal' and a 'Start Date' field is empty. Below the search bar is a table with columns: Name, Date Complete, and Result. A red box highlights the first row of the table, which contains the text 'Zscaler Account Aggregation', '12/10/19 12:03 PM', and 'Success' with a green checkmark icon.

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

Figure 75: Config Account Aggregation Task Completion



3.2.6 View Task Execution Details

Step 7: Clicking the successful task will bring up task execution details

Task Result

Details

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

[Return to Tasks](#)

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

Figure 76: View Task Execution Details



3.2.7 Create Group Aggregation Task

Step 8: Back on the main tasks screen - create a group aggregation task. Click the 'New Task' button in the top-right of the screen, and then select 'Account Group Aggregation'

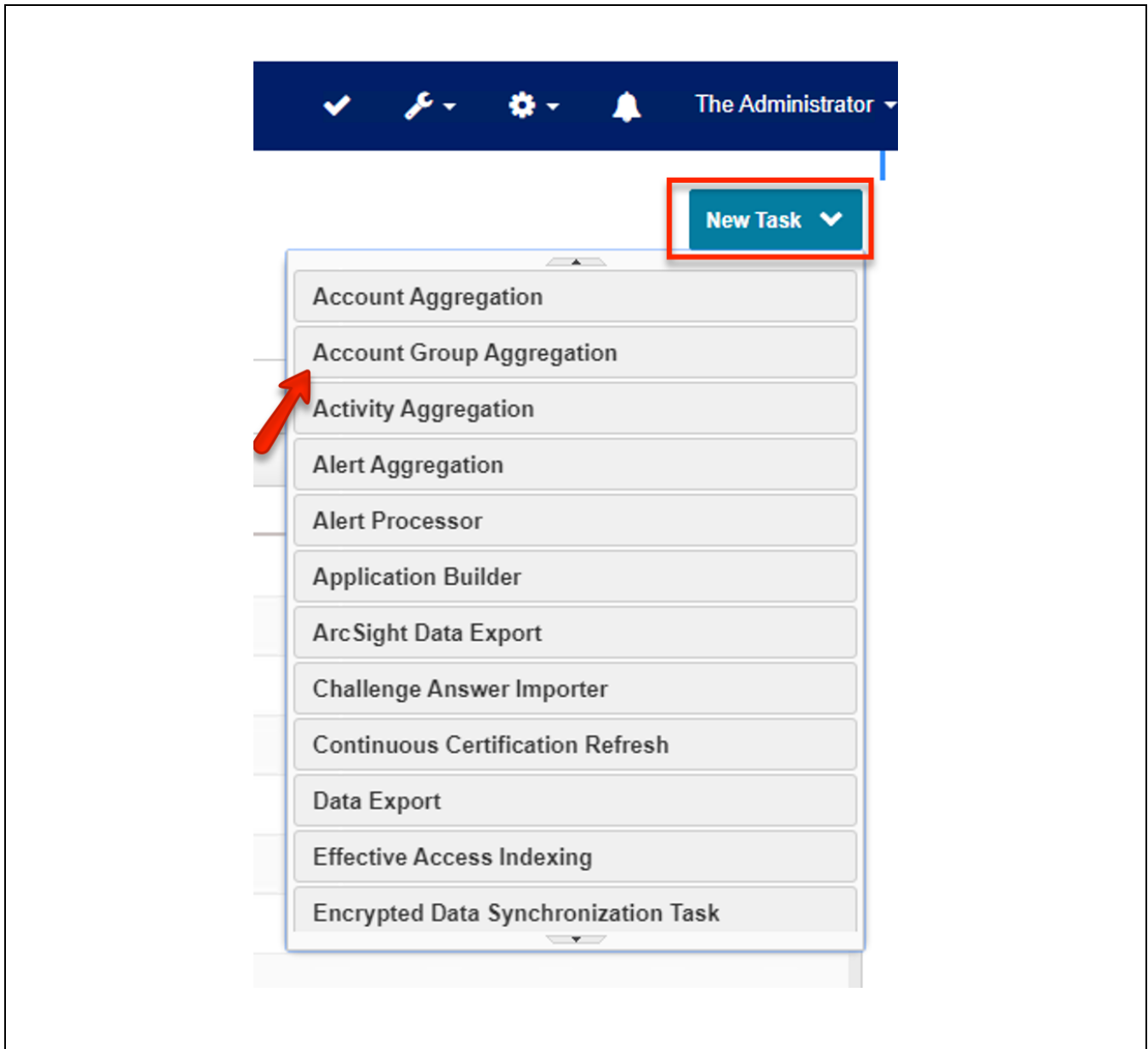


Figure 77: Create Group Aggregation Task



3.2.8 Link Account Aggregation

Step 9: Like the account aggregation, give the group aggregation a name, and select the ZPA application for the 'Applications to scan' list option

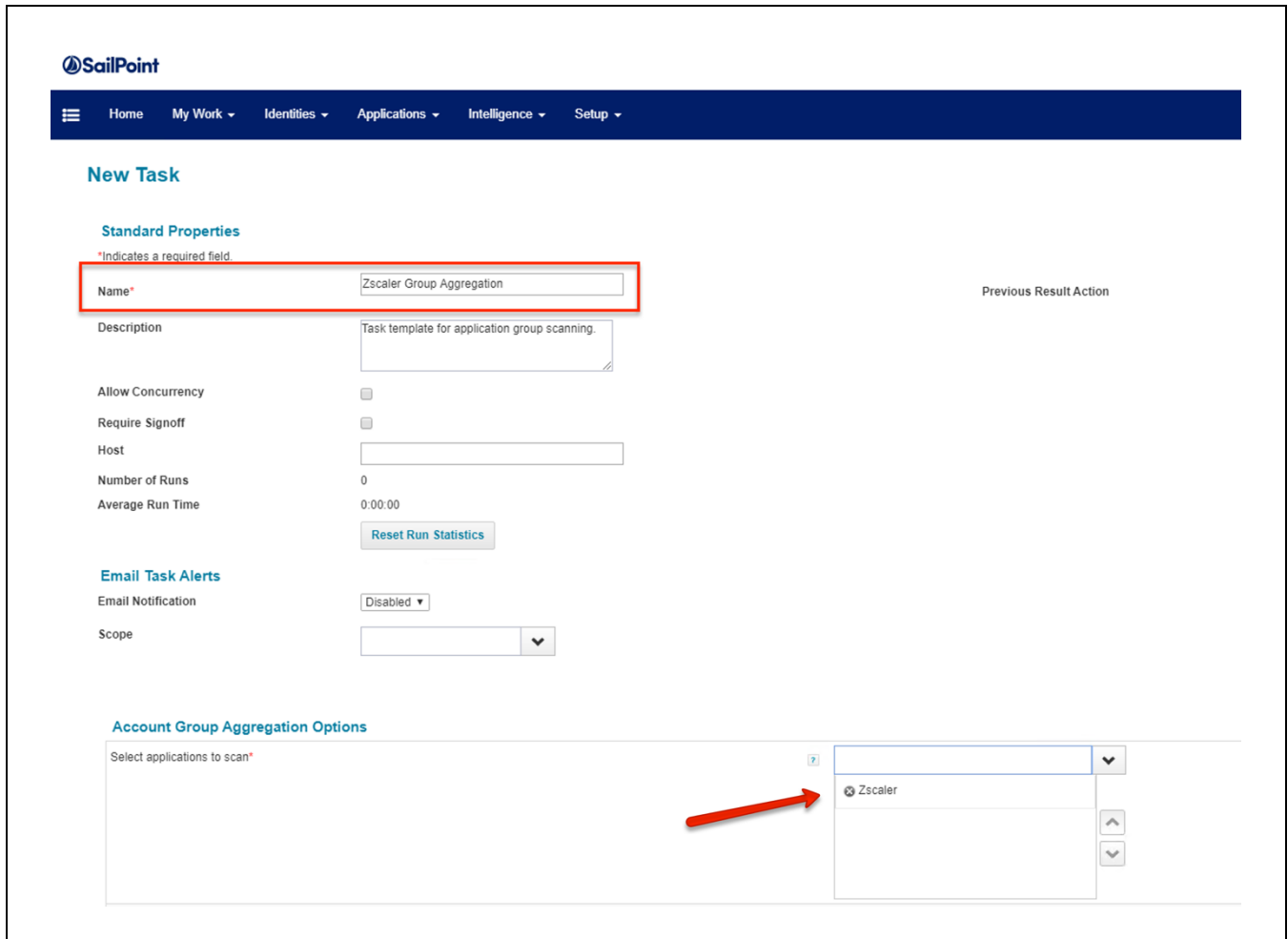


Figure 78: Link Account Aggregation



3.2.9 Save and Execute

Step 10: Click the 'Save and Execute' button at the bottom of the task configuration page

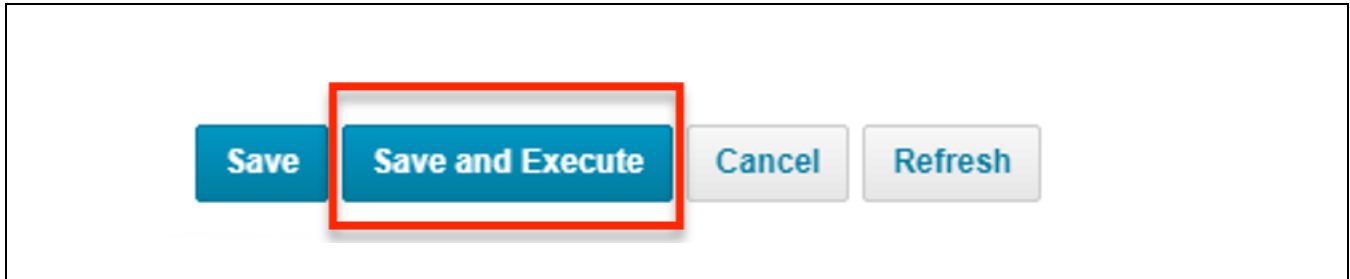


Figure 79: Save and Execute

3.2.10 Confirm Group Aggregation

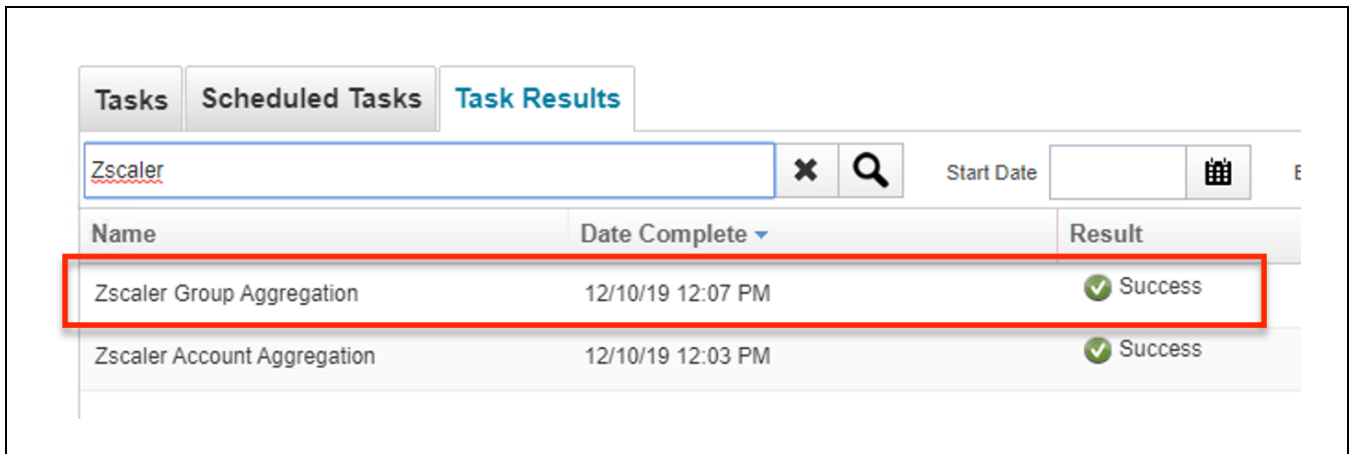


Figure 80: Confirm Group Aggregation

Step 10: Switching once again to the 'Task Results' tab, confirm that the group aggregation was successful



3.2.11 View Task Detailed Summary

Step 11: Clicking the task will bring up a more detailed summary of the result

The screenshot shows a 'Task Result' window with the following details:

Zscaler Group Aggregation		The Administrator	
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

Below the details are two summary tables:

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 81: View Task Detailed Summary



3.3 Confirm Account Provisioning

3.3.1 Navigate to Manage Accounts

Step 1: Click the 'menu' button in the top left of any screen in IdentityIQ. Under 'Manage User Access' click the 'Manage Accounts' link.

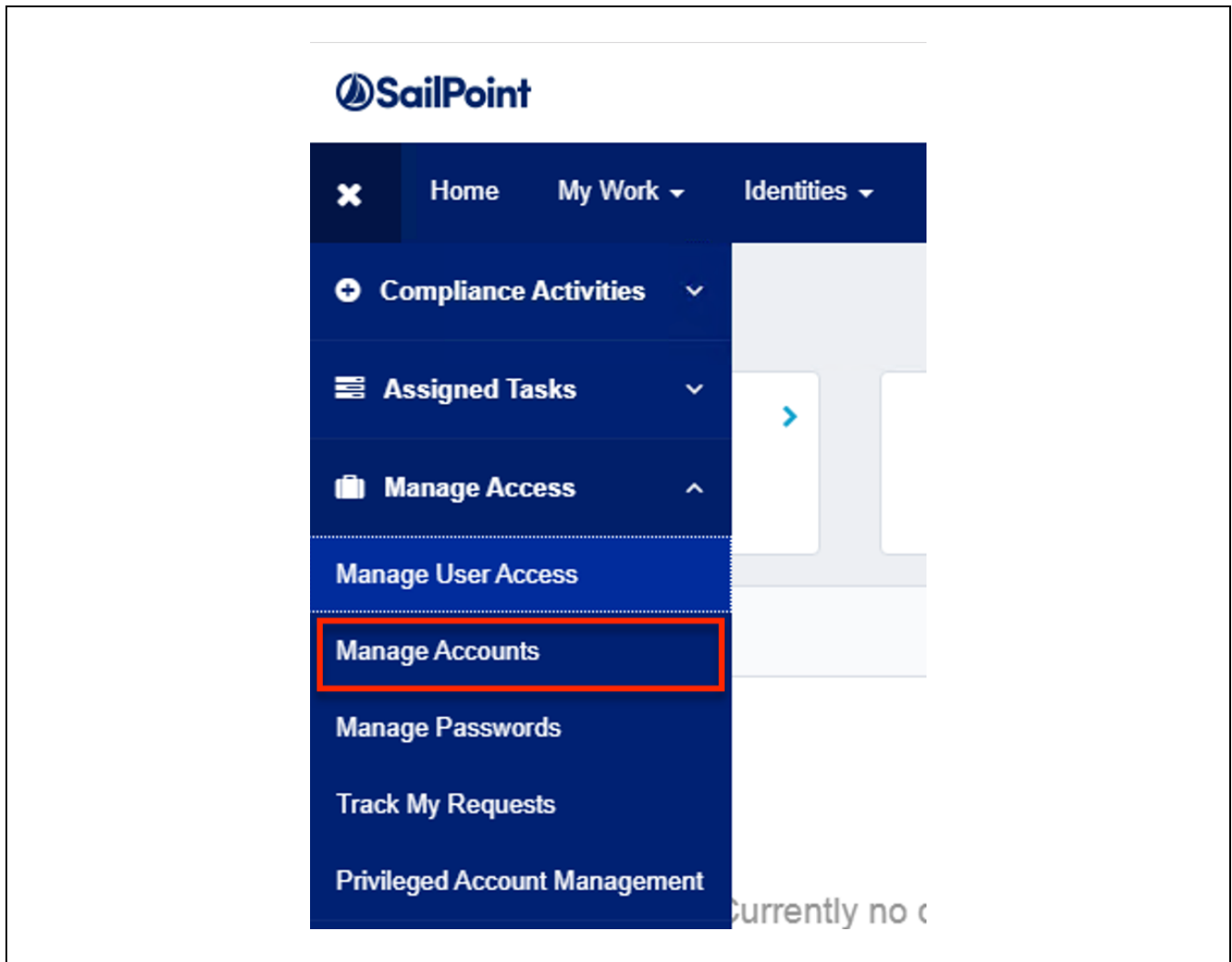


Figure 90: Navigate to Manage Accounts



3.3.2 Manage ZPA User

Step 2: Find an Identity for which a new account should be created in ZPA. Click the 'Manage' button for that users tile

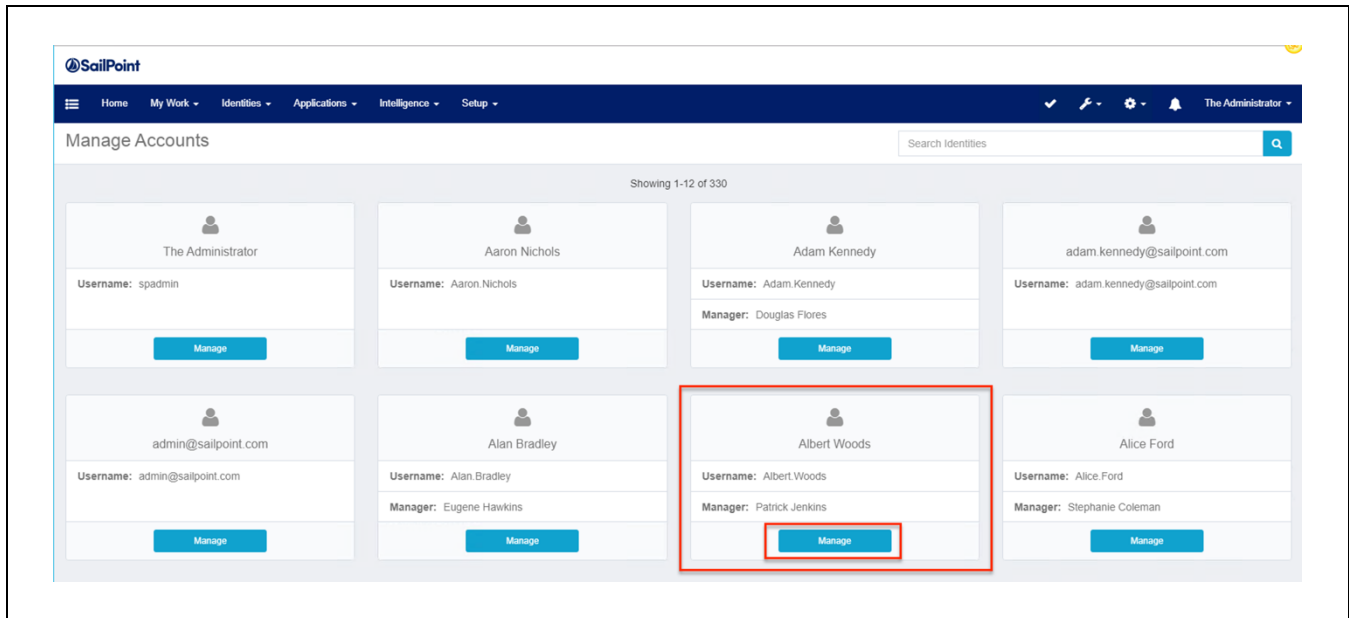


Figure 91: Manage ZPA User



3.3.3 Request ZPA User

Step 3: This screen shows the Identities currently provisioned application accounts. Click the 'Request Account' button

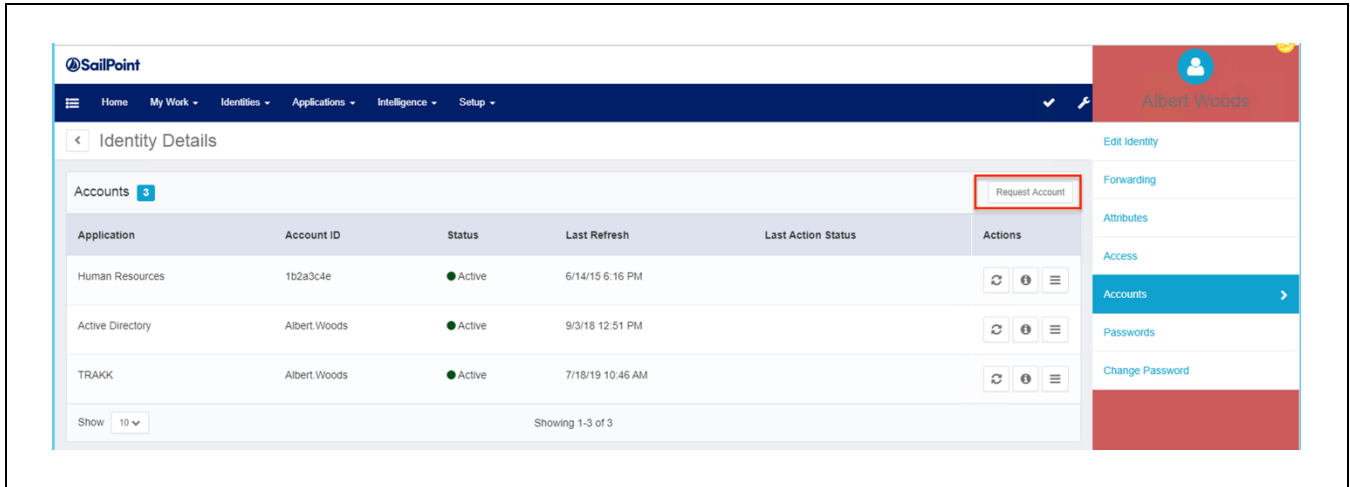


Figure 92: Request ZPA User



3.3.4 Request ZPA Application

Step 4: Select the ZPA application from the 'Application' dropdown list

The screenshot shows a web form titled "Request Account" with a close button in the top right corner. Below the title is a section titled "Summary of Request for Albert Woods" with the instruction "Verify the changes you have requested below." The form contains a required field labeled "Application *" which is a dropdown menu. The dropdown menu is open, showing "Zscaler" as the selected option. Below the dropdown is a text area with the placeholder "Type your comment here". At the bottom right of the form are two buttons: "Submit" and "Cancel". A red rectangular box highlights the dropdown menu.

Figure 93: Request ZPA Application



3.3.5 Confirm ZPA Application

Step 5: Click 'Confirm'

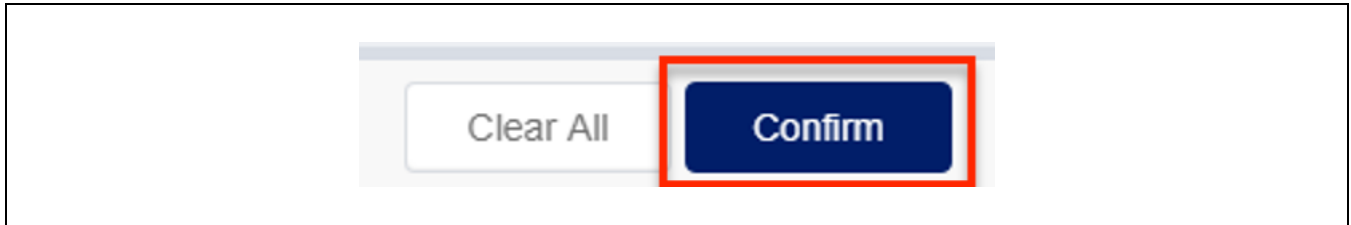


Figure 94: Confirm ZPA Application

3.3.6 Submit User Request

Step 6: Click the 'Submit' button for the request

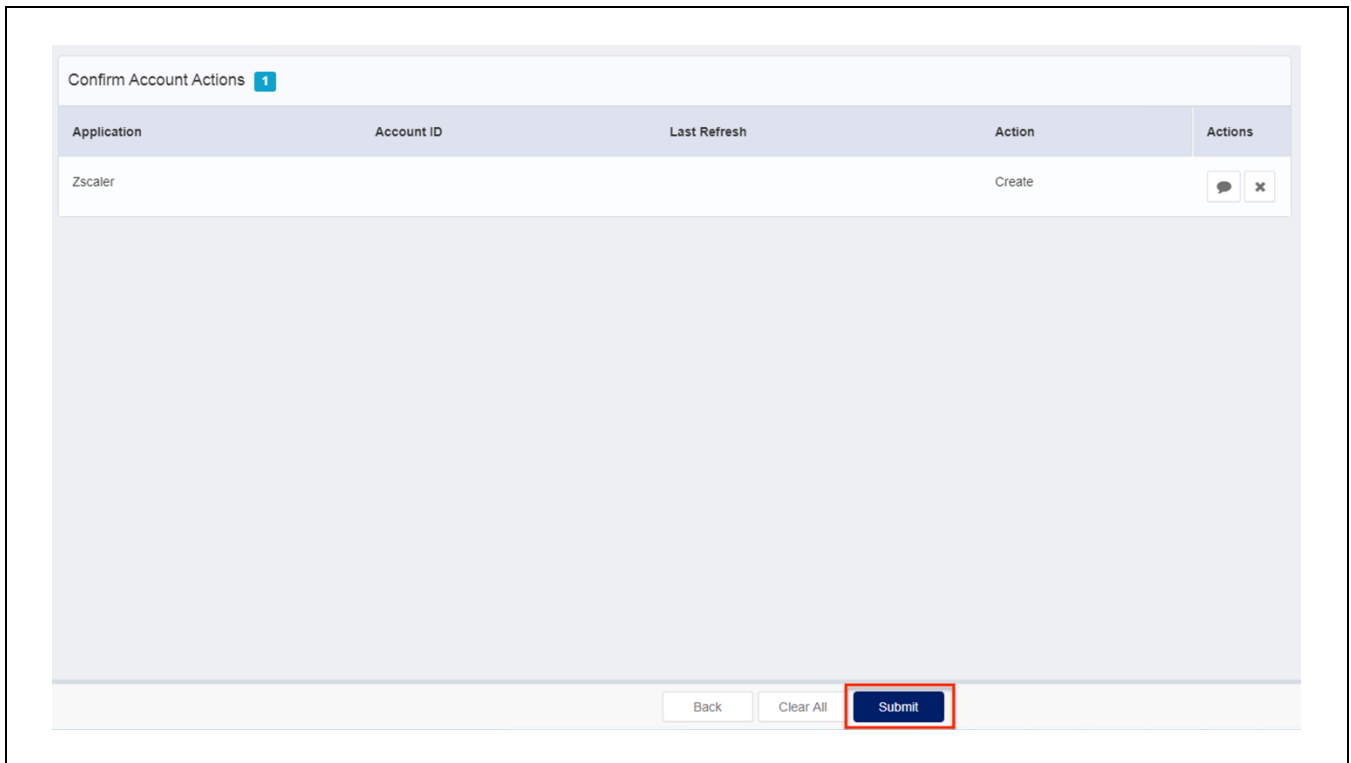


Figure 95: Submit User Request



3.3.7 Enter in User Required Fields

Step 7: Because our 'create' provisioning policy had a number of required fields (username, displayName) the IdentityIQ interface will prompt the requestor with a form to provide those values. Click 'Complete Form'.

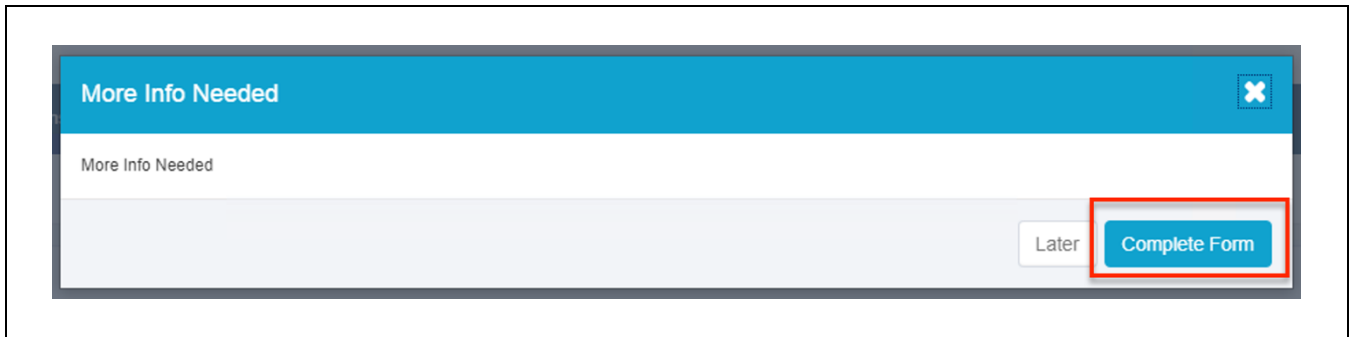


Figure 96: Enter In User Required Fields



3.3.8 Verify User Email Address

Step 8: Fill in the UserName and Display Name fields. The username must be in the format of a valid email address. Click the 'Ok' button 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 97: Verify User Email Address



3.3.9 Confirm Account Provisioning

Step 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	7a736361-6c65-7200-7363-896d0060484f	CorrelateManual	Albert.Woods	undetermined

Figure 98: Confirm Account Provisioning



4 Appendix A: Zscaler Resources

Zscaler Knowledge Base:

<https://support.zscaler.com/hc/en-us/?filter=documentation>

Zscaler Tools:

<https://www.zscaler.com/tools>

Zscaler Training and Certification:

<https://www.zscaler.com/resources/training-certification-overview>

Zscaler Submit a Ticket:

<https://help.zscaler.com/submit-ticket>

ZIA Test Page

<http://ip.zscaler.com/>

4.1 Zscaler IP Pages

<https://ips.zscaler.net/cenr/>

<https://ips.zscalerbeta.net/cenr/>

<https://ips.zscalerone.net/cenr/>

<https://ips.zscalertwo.net/cenr/>

<https://ips.zscalerthree.net/cenr/>



5 Appendix B: SailPoint Resources

SailPoint Getting Started Guide:

<https://www.sailpoint.com/identity-journey/>

SailPoint Customer Service:

<https://community.sailpoint.com/t5/Contact-Support/ct-p/Contact-Support>