Configuring SailPoint IdentityNow for ZIA 54
   Creating the Zscaler Source 54
   Additional Resources 57
      Working with Connectors and Sources 57
      Provisioning 57

Configuring SailPoint IdentityNow for ZPA 58
   Creating the Zscaler Source 58
   Additional Resources 61
      Working with Connectors and Sources 61
      Provisioning 61

Appendix A: Requesting Zscaler Support 62
   Gather Support Information 62
      Save Company ID 63
      Enter Support Section 64
## Terms and Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DPD</td>
<td>Dead Peer Detection (RFC 3706)</td>
</tr>
<tr>
<td>GRE</td>
<td>Generic Routing Encapsulation (RFC2890)</td>
</tr>
<tr>
<td>IKE</td>
<td>Internet Key Exchange (RFC2409)</td>
</tr>
<tr>
<td>IPSec</td>
<td>Internet Protocol Security (RFC2411)</td>
</tr>
<tr>
<td>OAM</td>
<td>Operation, Administration, and Management</td>
</tr>
<tr>
<td>PFS</td>
<td>Perfect Forward Secrecy</td>
</tr>
<tr>
<td>SD-WAN</td>
<td>Software Defined Wide Area Network</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Socket Layer (RFC6101)</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security (RFC5246)</td>
</tr>
<tr>
<td>XFF</td>
<td>X-Forwarded-For (RFC7239)</td>
</tr>
<tr>
<td>ZIA</td>
<td>Zscaler Internet Access (Zscaler)</td>
</tr>
<tr>
<td>ZPA</td>
<td>Zscaler Private Access (Zscaler)</td>
</tr>
<tr>
<td>DPD</td>
<td>Dead Peer Detection (RFC 3706)</td>
</tr>
</tbody>
</table>
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, go to Zscaler’s website or follow Zscaler on Twitter @zscaler.

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, please refer to:

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

Software Versions

This document was written using Zscaler Internet Access v6.0 and SailPoint IdentityIQ 8.0 and SailPoint IdentityNow.

Prerequisites

This guide provides 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 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 SailPoint IdentityIQ with administrator login credentials, or
  - A working instance of SailPoint IdentityNow with administrator login credentials
Request for Comments

- **For Prospects and Customers**: We value reader opinions and experiences. Please contact us at partner-doc-support@zscaler.com to offer feedback or corrections for this guide.

- **For Zcaler Employees**: Please 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 a specific use case between Zscaler and SailPoint. SailPoint uses the SCIM integration between Zscaler and SailPoint to import all users and groups from the Zscaler instance to the customer's SailPoint instance for the purpose of providing visibility of identity and entitlements in the organization. The more standard Zscaler IdP use case where SailPoint would provision users and groups dynamically based on identity store changes and user adds, moves, and changes is not covered in this deployment guide. Professional Services must implement this use case and it isn't supported by Zscaler as an integration.

Below are overviews of the Zscaler and SailPoint applications described in this section.

Zscaler Internet Access (ZIA) Overview

Zscaler Internet Access (ZIA) is a secure Internet and web gateway delivered as a service from the cloud. Think of it as a secure Internet onramp—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, CASB, and Browser Isolation, allowing you start with the services you need now and activate others as your needs grow.

Zscaler Private Access (ZPA) Overview

Zscaler Private Access (ZPA) is a cloud service that provides secure remote access to internal applications running on cloud or data center using a zero trust framework. With ZPA, applications are never exposed to the internet, making them completely invisible to unauthorized users. The service enables the applications to connect to users via inside-out connectivity rather than extending the network to them.

ZPA provides a simple, secure, and effective way to access internal applications. Access is based on policies created by the IT administrator within the ZPA Admin Portal and hosted within the Zscaler cloud. On each user device, a piece of software called Zscaler Client Connector is installed. Zscaler Client Connector ensures the user's device posture and extends a secure micro-tunnel 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.

<table>
<thead>
<tr>
<th>Name and Link</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZIA Help Portal</td>
<td>Help articles for ZIA</td>
</tr>
<tr>
<td>ZPA Help Portal</td>
<td>Help articles for ZPA</td>
</tr>
<tr>
<td>Zscaler Tools</td>
<td>Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.</td>
</tr>
<tr>
<td>Zscaler Training and Certification</td>
<td>Training designed to help you maximize Zscaler products.</td>
</tr>
<tr>
<td>Submit a Zscaler Support Ticket</td>
<td>Zscaler support portal for submitting requests and issues.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Name and Link</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SailPoint Getting Started Guide</td>
<td>Help articles for using SailPoint software.</td>
</tr>
<tr>
<td>SailPoint Customer Service</td>
<td>Site for getting SailPoint support.</td>
</tr>
<tr>
<td>SailPoint Community Site</td>
<td>Site for accessing the SailPoint online technical community.</td>
</tr>
<tr>
<td>SailPoint Developer Portal</td>
<td>Site for developer help and support.</td>
</tr>
</tbody>
</table>
Configuring SailPoint IdentityIQ for ZIA

The following describes how to configure SailPoint IdentityIQ for ZIA.

Create the Zscaler Application

1. Define a new application by clicking the Application > Application Definition navigation option.

   ![Create the Zscaler application definition](image1)

2. Add a new application by clicking the Add New Application button.

   ![Add new application](image2)
3. Select **SCIM 2.0** from the **Application Type** dropdown to configure the application type.

![Configure application type](image)

*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.

5. Test the connection by entering the connection parameters specific to your ZIA SCIM server:

   - The base URL to the SCIM server should be of 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.
6. Click the **Test Connection** button to ensure the parameters were entered correctly.

![Test connection](image-url)
7. Configure the schema by navigating to the Schema sub-tab under the Configuration tab. Click the Discover Schema Attribute button under the Object Type: account section.

*Figure 6. Schema Configuration*
8. The ZIA user attributes are populated into the object.

![ZIA user attributes](image)

*Figure 7. ZIA user attributes*
9. Next, click the **Discover Schema Attributes** under the **Object Type: group** section of the schema sub-tab.

![Figure 8. Discover schema attributes](image)

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

![Figure 9. Verify attributes](image)
11. Test the schema configuration by clicking the Preview button under each one (account, group).

![Preview button](image)

Figure 10. Test configuration

12. Preview the live data by clicking the Preview button. This displays live data from the ZIA SCIM server connection (account preview shown).

![Live data preview](image)

Figure 11. Preview Live Data

13. Next, configure provisioning plans. For this tutorial, a simple 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.

![Provisioning policies](image)

Figure 12. Configure provisioning plan
14. Then, click the **Create Policy Form**.

![Create Policy Form](image13.png)

**Figure 13. Create Policy Form**

15. Next, configure the policy form for ZIA. This step is a bit complex. Please refer to [SailPoint’s provisioning documentation](#) for more detail.

   - Enter a name of the create account policy.
   - Enter a description (not required).
   - Add a section to the policy form, in this case it was edited and named “Required Attributes”.
   - Click the + icon next to the section to add a new field.
   - For ZIA, new accounts require that a **userName** and **displayName** are populated. Create a field for each of these.

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

![Configure policy form for ZIA](image14.png)

**Figure 14. Configure policy form for ZIA**
16. Once completed, click the **Save** button.

17. Now, verify that the new provisioning policy appears next to the **Create** operation on the application definition.

![Verify configuration policy](image1.png)

**Figure 15. Verify configuration policy**

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

![Save Configuration Policy](image2.png)

**Figure 16. Save Configuration Policy**
19. Finally, the new application is now listed in the Application view of IdentityIQ.

Figure 17. Verify new application:

Configuring Aggregation Tasks

1. Click the Setup > Tasks link in the navigation bar.

Figure 18. Configuring aggregation tasks
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 19. Create new task*
3. Give the task a name, and make sure to select the previously defined ZIA application from the dropdown list for Applications to Scan.

![Configure task settings](image)

**Figure 20. Configure task settings**

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

![Save and Execute task](image)

**Figure 21. Save and Execute task**
5. Next, verify that the new task now shows up under the **Account Aggregation** section of the task list. Click the **Task Results** tab.

![Verify account aggregation task](image1)

**Figure 22. Verify account aggregation task**

6. Confirm that the account aggregation completed.

![Config account aggregation task completion](image2)

**Figure 23. Config account aggregation task completion**
7. You can view the task execution details by clicking the successful task.

Figure 24. View task execution details
8. Go back to the main tasks screen to create a group aggregation task. Click the New Task button in the top-right of the screen, and then select Account Group Aggregation.

![Create group aggregation task](image)

**Figure 25. Create group aggregation task**
9. Like the account aggregation, give the group aggregation a name and select the ZIA application for the **Applications to scan** list option.

![Figure 26. Link account aggregation](image)

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

![Figure 27. Save and Execute](image)
11. Confirm the group aggregation was successful by switching to the **Task Results** tab.

![Task Results](image)

*Figure 28. Confirm group aggregation*

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

![Task Detailed Summary](image)

*Figure 29. View task detailed summary*
Confirm Account Provisioning

In this next section confirms that the account provisioning was accurately set up.

1. Click the menu button in the top left of any screen in IdentityIQ. Select the Manage User Access > Manage Accounts link.

![Figure 30. Navigate to manage accounts](image-url)
2. Find the Identity for which you are creating a new ZIA account. Click the Manage button for that user's tile.

![Manage ZIA user](image)

Figure 31. Manage ZIA user

3. Next, request a ZIA user. This screen shows the identities currently provisioned application accounts. Click the Request Account button.

![Request ZIA user](image)

Figure 32. Request ZIA user
4. Select the ZIA application from the Application dropdown list.

![Request ZIA application](image1)

Figure 33. Request ZIA application

5. Confirm the ZIA application by clicking Confirm.

![Confirm ZIA application](image2)

Figure 34. Confirm ZIA application
6. Submit the user request by clicking the **Submit** button.

![Submit user request](image)

Figure 35. Submit user request

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

![Enter in user required fields](image)

Figure 36. Enter in user required fields
8. Fill in the **User Name** and **Display Name** fields. The username must be in the format of a valid email address. Click the **Ok** button to launch the request.

![Figure 37. Verify user email address](image)

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

![Figure 38. Confirm account provisioning](image)
Configuring SailPoint IdentityIQ for ZPA

This next section reviews how to configure SailPoint IdentityIQ for ZPA.

Creating the Zscaler Application

1. Define a new application by clicking the Application > Application Definition navigation option.

   ![Create the Zscaler application definition](image1)

   Figure 39. Create the Zscaler application definition

2. To add a new application, click the Add New Application button.

   ![Add new application](image2)

   Figure 40. Add new application
3. To set the application type, select **SCIM 2.0** from the **Application Type** dropdown.

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.

5. Test the connection by entering the connection parameters specific to your ZPA SCIM server:
   - The base URL to the SCIM server should be of the format `https://scim.zscalerbeta.net/<your_tenant_id>/scim`.
   - Select API Token as the Authentication Type.
   - Enter the API token provided by your ZPA administrator.
6. Click the **Test Connection** button to ensure the parameters were entered correctly.

Figure 43. Test connection
7. Set the schema configuration by navigating to Configuration > Schema. Click the Discover Schema Attributes button under the Object Type: account section.

Figure 44. Schema configuration
8. Check the populated ZPA attributes for a user.

![ZPA user attributes](image)

*Figure 45. ZPA user attributes*
9. Next, click the **Discover Schema Attributes** under the **Object Type: group** section of the schema sub-tab.

![Figure 46. Discover schema attributes](image)

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

![Figure 47. Verify attributes](image)
11. Test the configuration. Click the **Preview** button under each one (account, group).

![Add New Schema Attribute | Discover Schema Attributes | Delete Schema Attribute](image)

*Figure 48. Test configuration*

12. Preview the live data. The **Preview** button displays live data from the ZPA SCIM server connection (account preview shown).

![Preview live data](image)

*Figure 49. Preview live data*

13. The next step in application configuration is to configure provisioning plans. This tutorial shows a simple account creation plan. First, click the **Configuration > Provisioning Policies** sub-tab in the application definition. Click **Add Policy** next to the **Create** type in the **Object Type: account** section.

![Edit Application Zscaler ZPA](image)

*Figure 50. Configure provisioning plan*
14. Click the **Create Policy Form**.

![Create Policy Form](image1)

**Figure 51. Create policy form**

15. Next, configure the policy form for ZPA. This step is a bit complex. Please refer to SailPoint’s provisioning documentation for more detail:

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

![Policy Form Configuration](image2)

**Figure 52. Configure policy form for ZPA**
16. Verify the configuration policy. The new provisioning policy should appear next to the Create operation on the application definition.

![Figure 53. Verify configuration policy](image)

17. Save the configuration policy. Click the Save button at the bottom of the main application definition screen.

![Figure 54. Save configuration policy](image)
18. The new application is now be listed in the **Application** view of IdentityIQ.

![Verify New Application](image)

**Figure 55. Verify New Application**

### Configuring Aggregation Tasks

In this section we look at configuration aggregation tasks for ZPA and SailPoint IdentityIQ.

1. Click the **Setup > Tasks** link under in the navigation bar.

![Configuring aggregation tasks](image)

**Figure 56. Configuring aggregation tasks**
2. Create a new task. To create an account aggregation task, click the **New Task** button in the top-right of the screen, and then select **Account Aggregation**.

![Create new task](image-url)
3. Configure the task settings. Give the task a name, and make sure to select the previously defined ZPA application from the dropdown list for applications to scan.

![Configure task settings](image)

**Figure 58. Configure task settings**

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

![Save and Execute](image)

**Figure 59. Save and Execute task**
5. Verify the account aggregation task. The new task should now show up under the Account Aggregation section of the task list. Click the Task Results tab.

![Verify account aggregation task](image1.png)

6. Confirm that the account aggregation completed.

![Config account aggregation task completion](image2.png)
7. View the task execution details. Clicking the successful task brings up task execution details.

![Figure 62. View task execution details](image)

8. Create a group aggregation task back on the main tasks screen. Click the **New Task** button in the top-right of the screen, and then select **Account Group Aggregation**.

![Figure 63. Create group aggregation task](image)
9. Link the account aggregation, give the group aggregation a name, and select the ZPA application for the Applications to scan list option.

![Figure 64. Link account aggregation](image)

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

![Figure 65. Save and execute](image)
11. Confirm the group aggregation. Switch again to the Task Results tab, confirm that the group aggregation was successful.

![Confirm group aggregation](image)

Figure 66. Confirm group aggregation

12. View the detailed task summary. Clicking the task brings up a more detailed summary of the result.

![View task detailed summary](image)

Figure 67. View task detailed summary
Confirm Account Provisioning

Now you need to confirm the account provisioning in SailPoint and ZPA.

1. Click the menu button in the top left of any screen in IdentityIQ. Select the Manage User Access > Manage Accounts link.

---

Figure 68. Navigate to Manage Accounts
2. Manage the ZPA user. Find an identity for which to create a new account in ZPA. Click the Manage button for that users tile.

![Manage ZPA user](image1)

Figure 69. Manage ZPA user

3. Request the ZPA user. This screen shows the Identities currently provisioned application accounts. Click the Request Account button.

![Request ZPA user](image2)

Figure 70. Request ZPA user
4. Request a ZPA application. Select the ZPA application from the **Application** dropdown list and select **Submit**.

![Request ZPA application](image1)

**Figure 71. Request ZPA application**

5. Click **Confirm**.

![Confirm ZPA application](image2)

**Figure 72. Confirm ZPA application**
6. Submit a user request. Click the **Submit** button for the request.

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

---

*Figure 73. Submit user request*

*Figure 74. Enter user required fields*
8. Verify the user email address. Fill in the **User Name** and **Display Name** fields. The user name must be in the format of a valid email address. Click the **Ok** button to launch the request.

![Verify user email address](image_url)

Figure 75. Verify user email address

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

![Confirm account provisioning](image_url)

Figure 76. Confirm account provisioning
Configuring SailPoint IdentityNow for ZIA

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

Creating the Zscaler Source

1. Log into IdentityNow as an administrator and navigate to the administrative dashboard. Define a new Source by clicking the Connectors > Sources navigation option.

2. Click the +New button.

3. Select SCIM 2.0 from the Source Type dropdown. Give the source a Source Name, a Description, and select Direct Connection from the radio buttons. Click the Continue button.

4. Enter the connection parameters specific to your ZIA SCIM server:
   - Select your virtual appliance from the from the dropdown list.
   - Provide any governance group selection (if applicable).
5. Click the **Save** button to ensure the parameters were entered correctly.

![](image)

**Figure 80. Virtual application selection**

6. Configure connection settings
   - The **Host URL** should be set 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 the **Save** button to ensure the parameters were entered correctly.

![](image)

**Figure 81. Host URL, Authentication Type, and API Token configuration**
8. Click the **Review and Test** link on the left of the screen. Then click the **Test Connection** button to verify connectivity to the Zscaler SCIM server.

![Test connection successful](image)

**Figure 82. Test connection successful**

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

![Return to source configuration page](image)

**Figure 83. Return to source configuration page**

10. Navigate to the **Import Data** and click the **Account Schema** option in the left-hand menu. Click the **Options > Discover Schema** button on the right-hand side of the page.

![Schema discovery](image)

**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. The `groups` attribute should be flagged as entitlement and multi-valued.

![Account Schema: ZIA](image)

Figure 85. Flagging account id, name, and entitlement attributes in schema

12. Next, set up account correlation. This is likely a mapping of the attribute that includes a username in Zscaler (email address) number and the `work email` attribute of the Identity. This might be different or require additional correlation depending on your organization.

![Correlation Configuration](image)

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) please visit the following SailPoint community articles.

**Working with Connectors and Sources**


**Provisioning**

- The provisioning of a new user account requires that the `username` and the `display name` be populated – these are required attributes. The username must be of a valid email format. Creation fails if these conditions are not met.
Configuring SailPoint IdentityNow for ZPA

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

Creating the Zscaler Source

1. Log into IdentityNow as an administrator and navigate to the administrative dashboard. Define a new Source by clicking the Connectors > Sources navigation option.

![Navigating to Sources page](image)

2. Click the +New button.

![Creating new source](image)

3. Select SCIM 2.0 from the Source Type dropdown. Give the source a Source Name, a Description, and select Direct Connection from the radio buttons. Click the Continue button.

![Source creation fields](image)
4. Enter the Virtual Appliance information for the connection to the ZPA SCIM server.
   - Select your virtual appliance from the dropdown list.
   - Provide any governance group selection (if applicable).
   - Click the **Save** button to ensure the parameters were entered correctly.

   ![Base Configuration](image)

   **Figure 90. Virtual application selection**

5. Configure connection settings:
   - The **Host URL** should be set 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 the **Save** button to ensure the parameters were entered correctly.

   ![Connection Settings](image)

   **Figure 91. Host URL, Authentication Type, and API Token configuration**
6. Click the **Review and Test** link on the left of the screen. Then click the **Test Connection** button to verify connectivity to the Zscaler SCIM server.

![Figure 92. Test connection successful](image)

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

![Figure 93. Return to source configuration page](image)

8. Navigate to the **Import Data** and click the **Account Schema** option in the left-hand menu. Click the **Options > Discover** button on the right-hand side of the page.

![Figure 94. Schema discovery](image)
9. The attributes for a user in ZPA are populated. Flag the `id` attribute as **Account ID**. Flag the `userName` attribute as **Account Name**. The `groups` attribute should be flagged as entitlement and multi-valued.

```plaintext
<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Description</th>
<th>Type</th>
<th>Entitlement</th>
<th>Multi-Valued</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Account ID</td>
<td>string</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>externalId</td>
<td>A String that is an identifier for the resource as defined...</td>
<td>string</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>userName</td>
<td>A service provider’s unique identifier for the user, t...</td>
<td>string</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>name.firstName</td>
<td>The first name of the user, or first name in most ...</td>
<td>string</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>displayName</td>
<td>The name of the User, suitable for display</td>
<td>string</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>active</td>
<td>A Boolean value indicating the User’s administrative...</td>
<td>boolean</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>groups</td>
<td>A list of groups to which the user belongs,</td>
<td>group</td>
<td>entitlemen</td>
<td>Multi-Valued</td>
<td></td>
</tr>
<tr>
<td>department</td>
<td>department</td>
<td>string</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

**Figure 95. Flagging account id, name, and entitlement attributes in schema**

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

```plaintext
<table>
<thead>
<tr>
<th>Identity Attribute</th>
<th>Operation</th>
<th>Account Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work Email</td>
<td>Equal</td>
<td>UserName</td>
</tr>
</tbody>
</table>
```

**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 please visit the following SailPoint community articles.

### Working with Connectors and Sources


### Provisioning

- The provisioning of a new user account requires that the username and the display name be populated – these are required attributes. The username must be of a valid email format. Creation fails if these conditions are not met.
Appendix A: Requesting Zscaler Support

Gather Support Information

You might sometimes need Zscaler support for provisioning certain services, or to help troubleshoot configuration and service issues. Zscaler support is available 24/7 hours a day, year-round.

To contact Zscaler support, select Administration > Settings and then click Company profile.

![Figure 97. Collecting details to open support case with Zscaler TAC](image)
Save Company ID

Copy the Company ID, as shown below.

Figure 98. Company ID
Enter Support Section

Now that you have our company ID, you can open a support ticket. Navigate to Dashboard > Support > Submit a Ticket.

Figure 99. Submit ticket