SailPoint IdentityIQ SCIM integration

This document outlines how to configure a SCIM connector application within a SailPoint IdentityIQ tenant, and our supported scenarios.

Supported SCIM Scenarios

- Users
  - Create (POST)
  - Read (GET)
  - Update (PUT or PATCH)
  - Delete (DELETE)
- Groups
  - Create (POST)
  - Read (GET)
  - Update (PUT or PATCH)
  - Delete (DELETE)

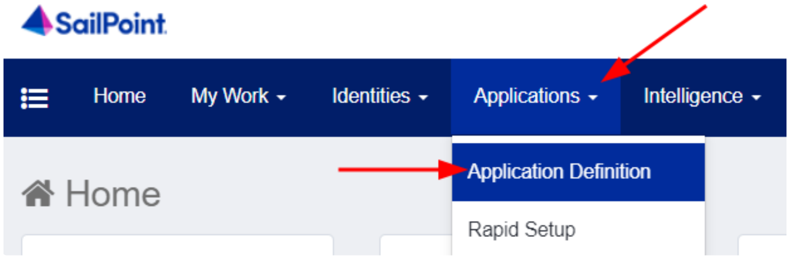
Before beginning

You will need a `Base URL` and an `API Token` from Axiad to configure a SCIM connector.

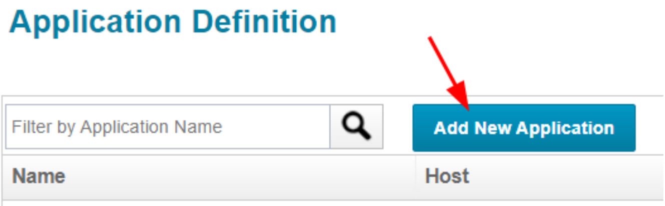
1. Please contact your customer success engineer directly to get this information shared securely.
   a. If you don’t have a direct contact, please email customer.success@axiad.com
2. Request your **SCIM URL** to be used to configure the `Base URL` in SailPoint
3. Request a **Bearer Token** to be used to configure the `API Token` in SailPoint

Configuration Instructions

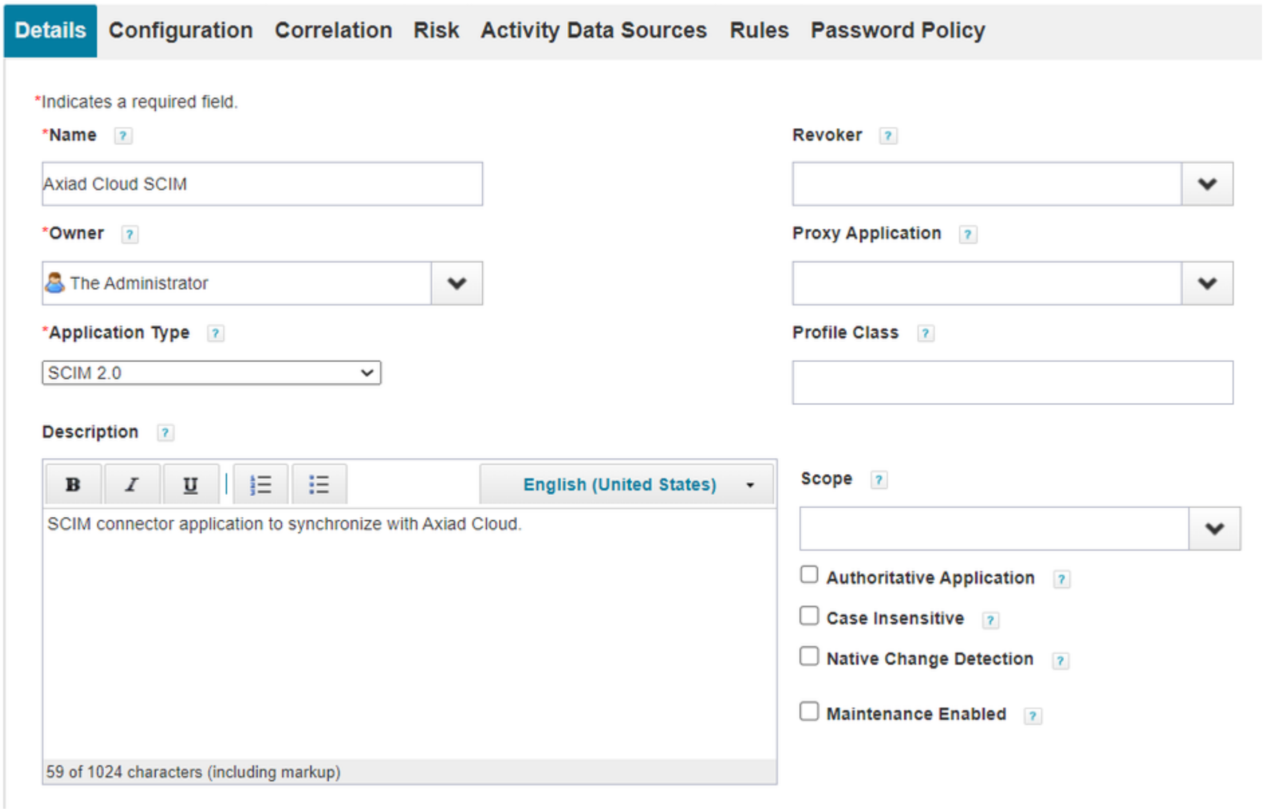
1. Sign in to your admin dashboard
2. Select `Applications` in the top ribbon, then select `Application Definition`



3. Select `Add New Application`



4. Set the `Name` as **Axiad Cloud SCIM** and set the `Application Type` as **SCIM 2.0**
   a. The rest of the details need to be filled out in accordance to your tenant requirements, below is how we configured for our demo environment.



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

*Indicates a required field.

*Name: Axiad Cloud SCIM

*Owner: The Administrator

*Application Type: SCIM 2.0

Description: SCIM connector application to synchronize with Axiad Cloud.

59 of 1024 characters (including markup)

Revoker:

Proxy Application:

Profile Class:

Scope:

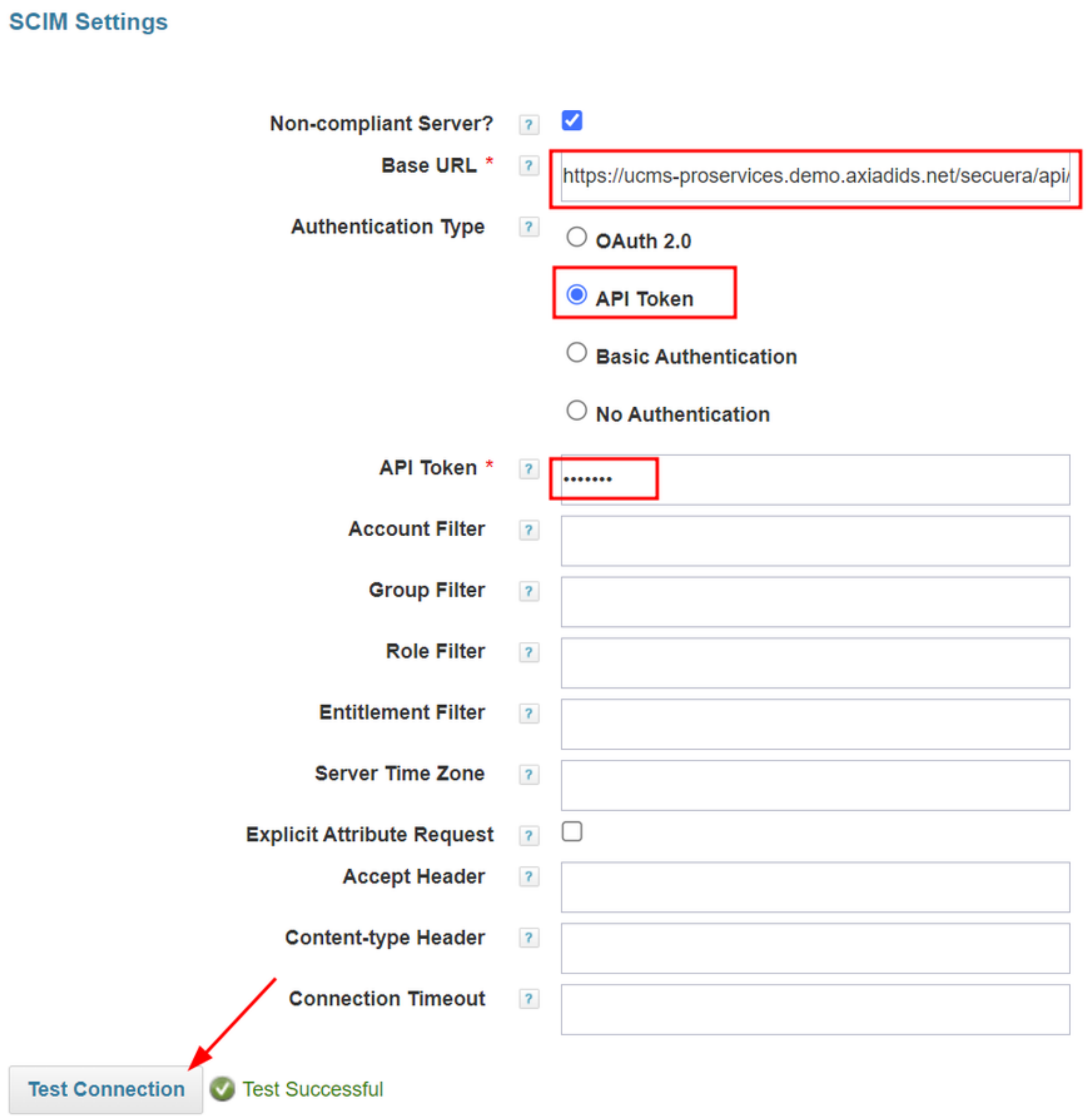
☐ Authoritative Application

☐ Case Insensitive

☐ Native Change Detection

☐ Maintenance Enabled

5. Select the `Configuration` tab
6. Configurations should be as follows:
    a. Check `Non-compliant Server`
    b. Fill in the `Base URL` with the SCIM URL provided by your Axiad customer success engineer
    c. Select `API Token`
    d. Enter the Bearer token provided by Axiad into the `API Token` section
    e. Then select `Test Connection` to verify the configuration



SCIM Settings

Non-compliant Server? ☑

Base URL * https://ucms-proservices.demo.axiadids.net/secuera/api/

Authentication Type
○ OAuth 2.0
● API Token
○ Basic Authentication
○ No Authentication

API Token * •••••••

Account Filter

Group Filter

Role Filter

Entitlement Filter

Server Time Zone

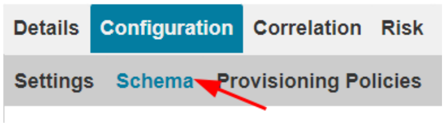
Explicit Attribute Request □

Accept Header

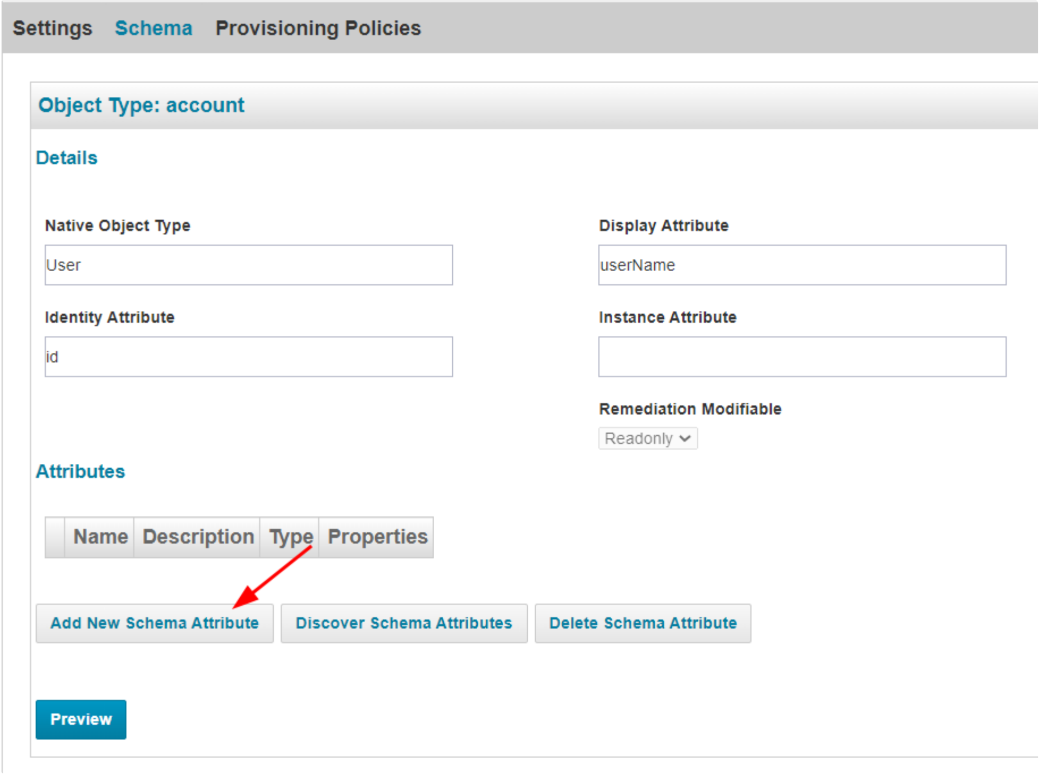
Content-type Header

Connection Timeout

7. Select `Schema` under the `Configuration` tab



8. In the section `Object Type: account` select `Add New Schema Attribute` to add the required schema attributes for Axiad Cloud



Object Type: account

Details

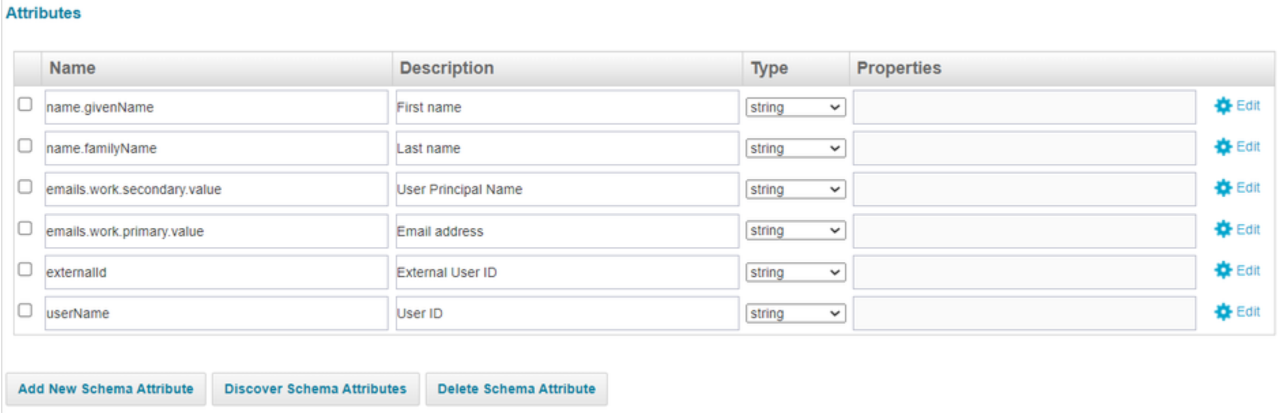
Native Object Type: User	Display Attribute: userName
Identity Attribute: id	Instance Attribute:
	Remediation Modifiable: Readonly

Attributes

	Name	Description	Type	Properties

9. Add the following attributes with description for ease of recognition

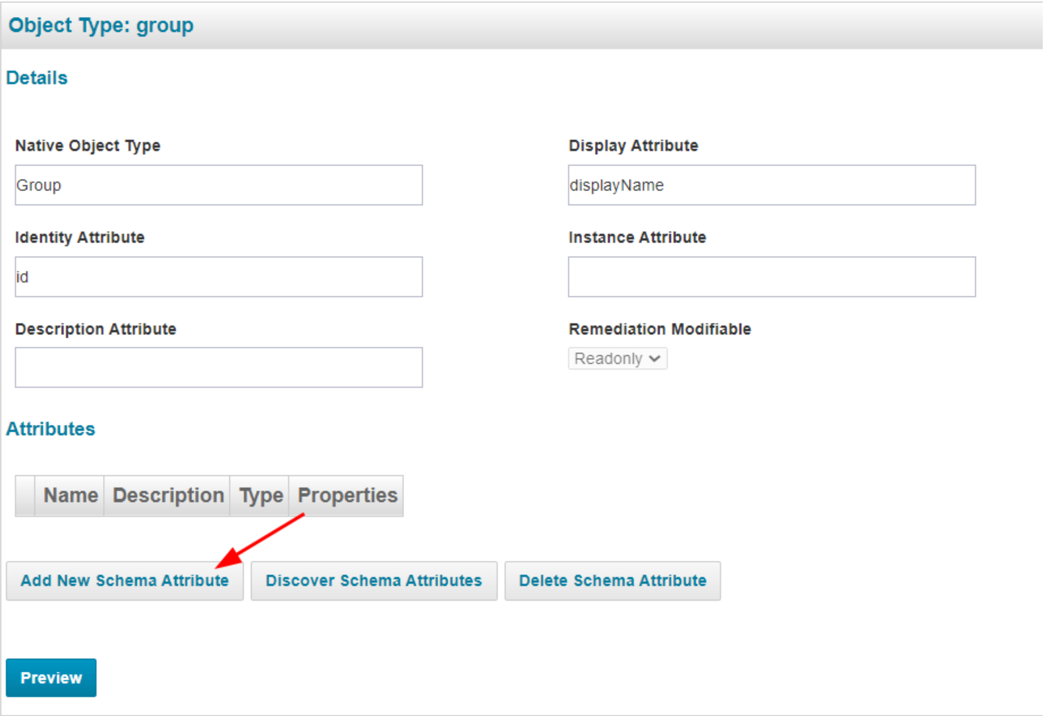
   INFORMATIONAL NOTE: `These are the minimum required attributes to work with Axiad Cloud. If you need additional functionality, such as MyCircle, please work with your Axiad customer success engineer to add any additional required attributes.`



Attributes

	Name	Description	Type	Properties	
□	name.givenName	First name	string		Edit
□	name.familyName	Last name	string		Edit
□	emails.work.secondary.value	User Principal Name	string		Edit
□	emails.work.primary.value	Email address	string		Edit
□	externalId	External User ID	string		Edit
□	userName	User ID	string		Edit

10. Leave the following sections **blank**, Axiad Cloud does not currently support `Entitlements` or `Roles`
    a. Scroll down to the section `Object Type: entitlements` and ensure there are no attributes listed
    b. Scroll down to the section `Object Type: roles` and ensure there are no attributes listed
11. Scroll down to the section `Object Type: group` and select `Add New Schema Attribute` to add the required attributes for Axiad Cloud



Object Type: group

Details

Native Object Type: Group

Display Attribute: displayName

Identity Attribute: id

Instance Attribute:

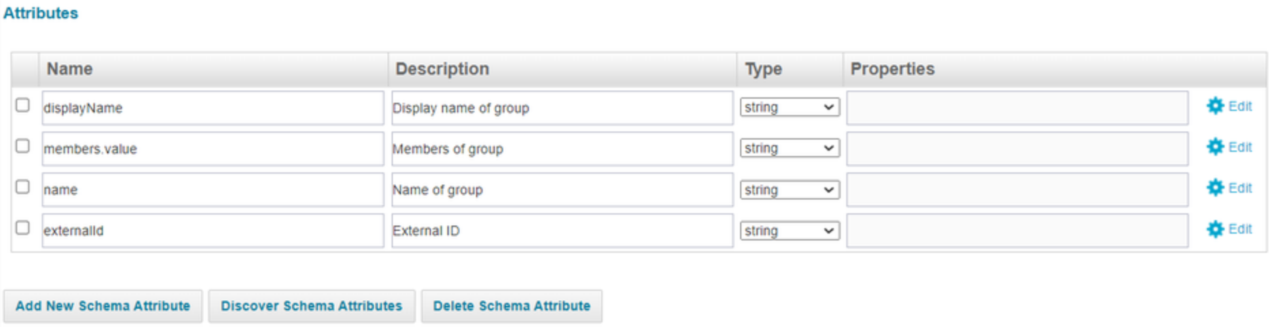
Description Attribute:

Remediation Modifiable: Readonly

Attributes

	Name	Description	Type	Properties

12. Add the following attributes with description for ease of recognition

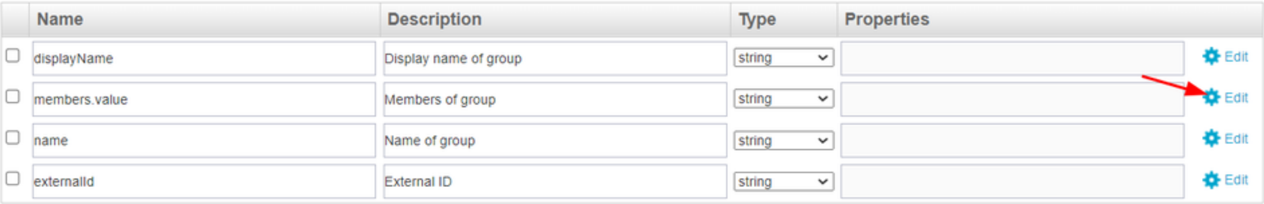


Attributes

	Name	Description	Type	Properties	
□	displayName	Display name of group	string		Edit
□	members.value	Members of group	string		Edit
□	name	Name of group	string		Edit
□	externalId	External ID	string		Edit

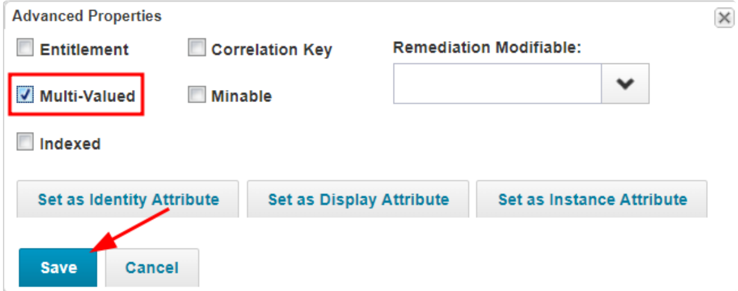
13. To properly get the `members` do the following:

    a. Select the `Edit` button on the right



	Name	Description	Type	Properties	
□	displayName	Display name of group	string		Edit
□	members.value	Members of group	string		Edit
□	name	Name of group	string		Edit
□	externalId	External ID	string		Edit

    b. In the pop-up window, check the box for `Multi-Valued` and select `Save`



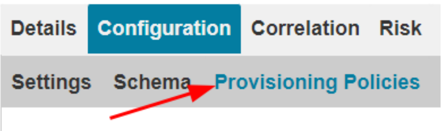
Advanced Properties

□ Entitlement □ Correlation Key Remediation Modifiable:

☑ Multi-Valued □ Minable

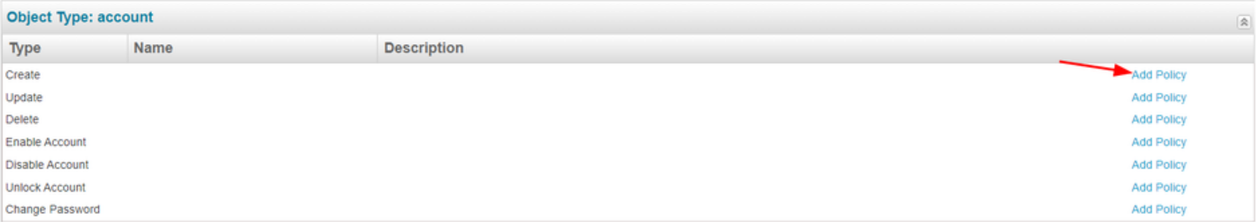
□ Indexed

14. Scroll back up to the top of the page and select `Provisioning Policies` under the `Configuration` tab



15. Create **Policy Forms** for `Create`, `Update`, and `Delete` sections

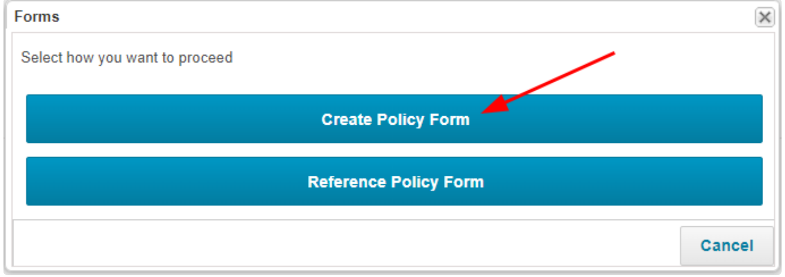
   a. Select `Add Policy` next to `Create`



Object Type: account

Type	Name	Description	
Create			Add Policy
Update			Add Policy
Delete			Add Policy
Enable Account			Add Policy
Disable Account			Add Policy
Unlock Account			Add Policy
Change Password			Add Policy

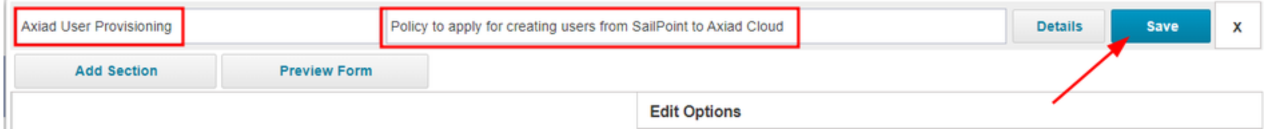
   b. There will be a pop-up window for `Forms` select `Create Policy Form`



Forms

Select how you want to proceed

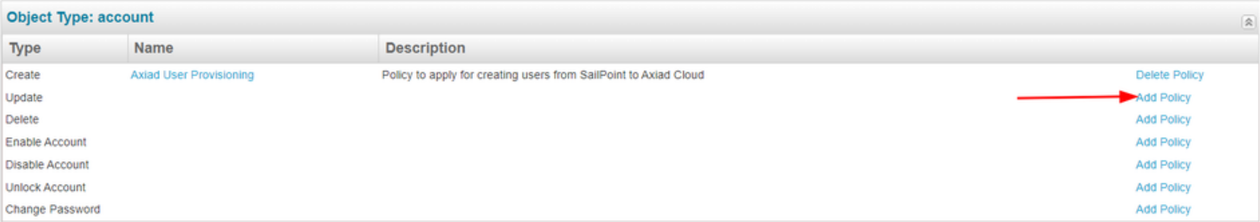
   c. Enter a `Form Name` and `Form Description` that are easily referenceable then select `Save`



Axiad User Provisioning

Policy to apply for creating users from SailPoint to Axiad Cloud

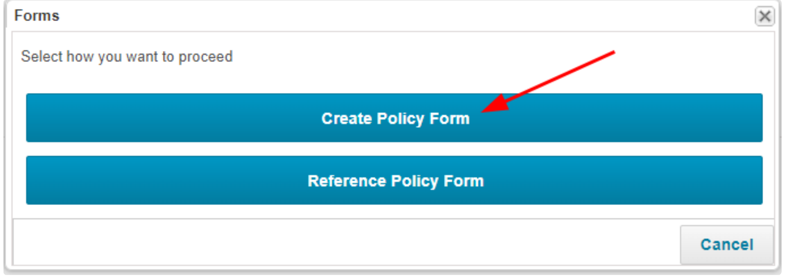
   d. Select `Add Policy` next to `Update`



Object Type: account

Type	Name	Description	
Create	Axiad User Provisioning	Policy to apply for creating users from SailPoint to Axiad Cloud	Delete Policy
Update			Add Policy
Delete			Add Policy
Enable Account			Add Policy
Disable Account			Add Policy
Unlock Account			Add Policy
Change Password			Add Policy

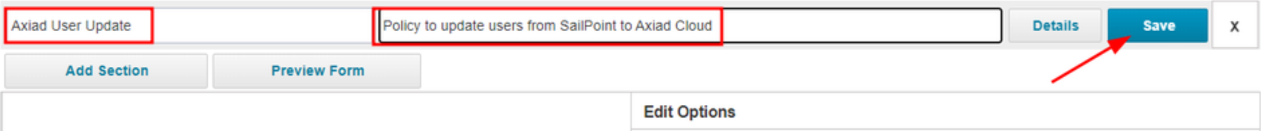
   e. There will be a pop-up window for `Forms` select `Create Policy Form`



Forms

Select how you want to proceed

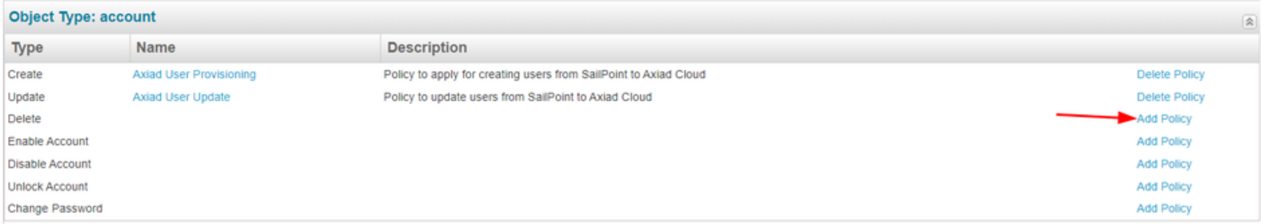
   f. Enter a `Form Name` and `Form Description` that are easily referenceable then select `Save`



Axiad User Update

Policy to update users from SailPoint to Axiad Cloud

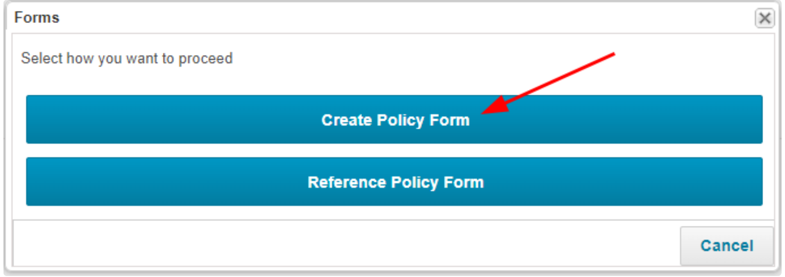
   g. Select `Add Policy` next to `Delete`



Object Type: account

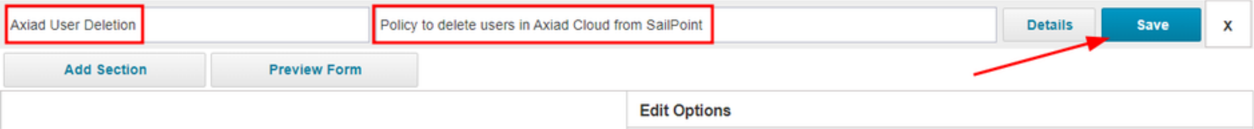
Type	Name	Description	
Create	Axiad User Provisioning	Policy to apply for creating users from SailPoint to Axiad Cloud	Delete Policy
Update	Axiad User Update	Policy to update users from SailPoint to Axiad Cloud	Delete Policy
Delete			Add Policy
Enable Account			Add Policy
Disable Account			Add Policy
Unlock Account			Add Policy
Change Password			Add Policy

   h. There will be a pop-up window for `Forms` select `Create Policy Form`



Select how you want to proceed

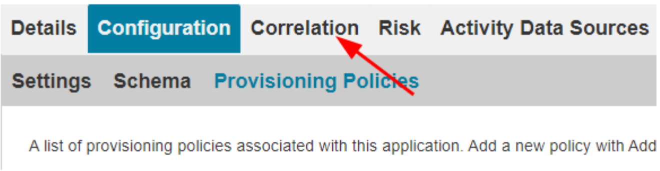
i. Enter a `Form Name` and `Form Description` that are easily referenceable then select `Save`



Axiad User Deletion

Policy to delete users in Axiad Cloud from SailPoint

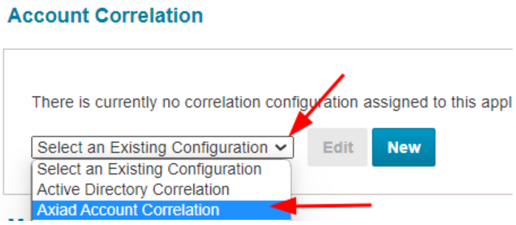
16. Select the `Correlation` tab



A list of provisioning policies associated with this application. Add a new policy with Add

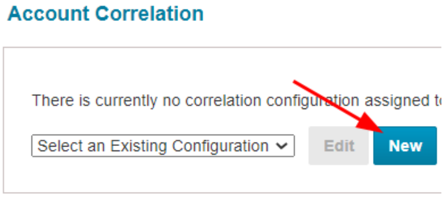
17. Correlation Configuration options:

a. If you have a correlation configuration created, select it from the drop down


Account Correlation
Select an Existing Configuration
Edit
New
Select an Existing Configuration
Active Directory Correlation
Axiad Account Correlation

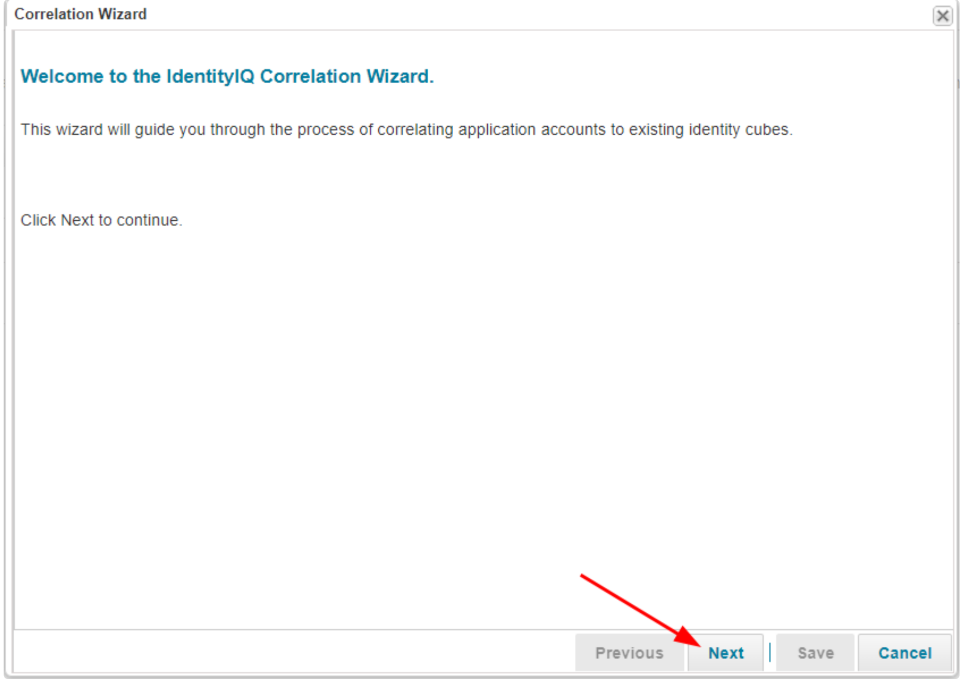
There is currently no correlation configuration assigned to this appl

b. If you don't have a configuration configured, select `New`



There is currently no correlation configuration assigned t

c. Select `Next` in the new pop-up window

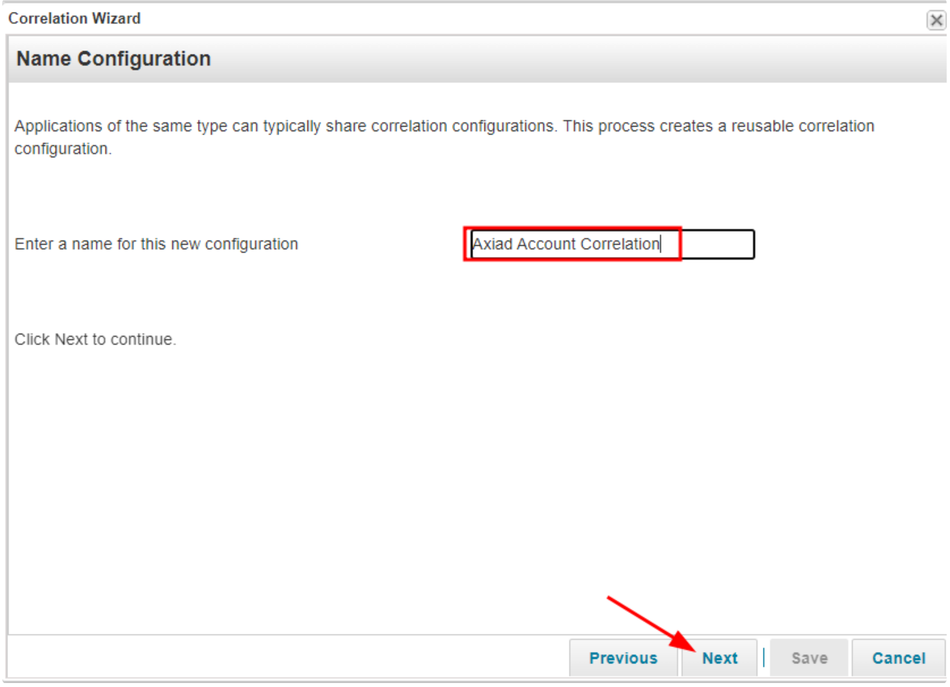

Correlation Wizard

Welcome to the IdentityIQ Correlation Wizard.

This wizard will guide you through the process of correlating application accounts to existing identity cubes.

Click Next to continue.

d. Enter a name for the configuration and select `Next`


Correlation Wizard

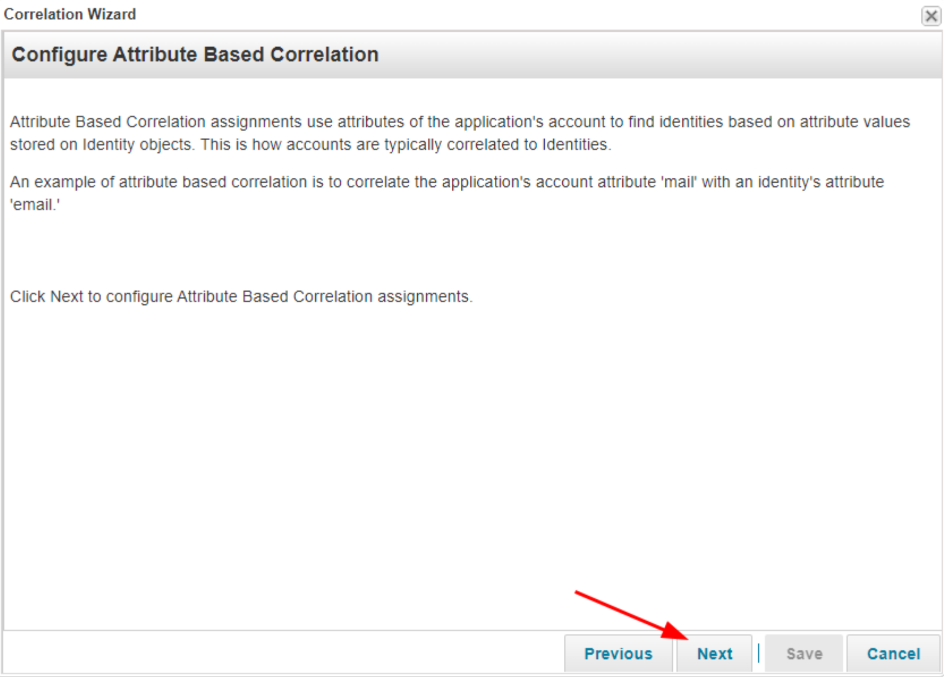
Name Configuration

Applications of the same type can typically share correlation configurations. This process creates a reusable correlation configuration.

Enter a name for this new configuration: Axiad Account Correlation

Click Next to continue.

e. Select `Next` again



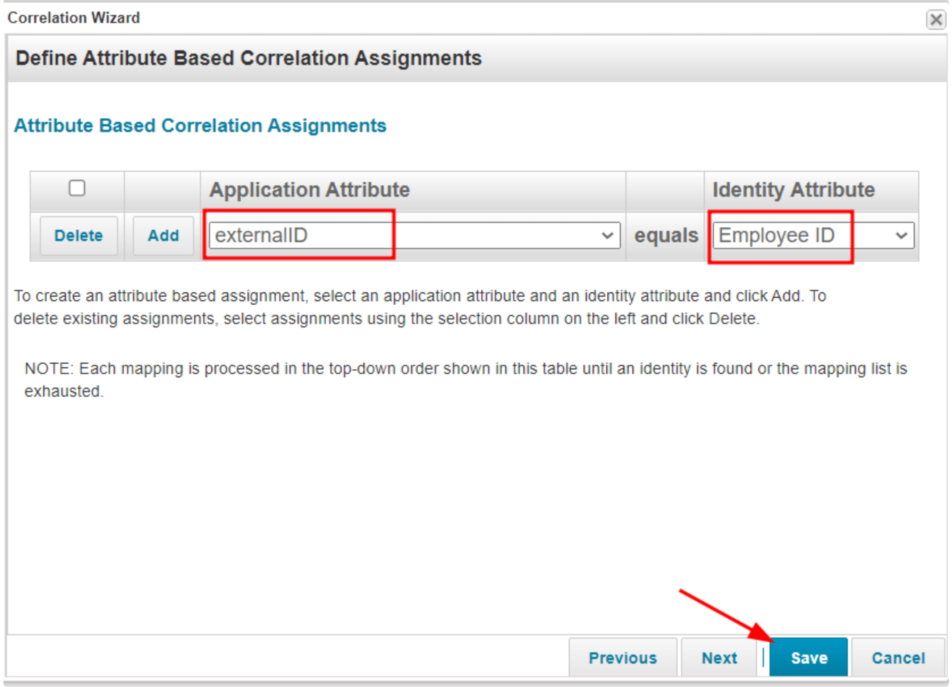
Configure Attribute Based Correlation

Attribute Based Correlation assignments use attributes of the application's account to find identities based on attribute values stored on Identity objects. This is how accounts are typically correlated to Identities.

An example of attribute based correlation is to correlate the application's account attribute 'mail' with an identity's attribute 'email.'

Click Next to configure Attribute Based Correlation assignments.

f. In the `Application Attribute` drop down select `externalID` and in the `Identity Attribute` drop down select `Employee ID` then select `Save`



Define Attribute Based Correlation Assignments

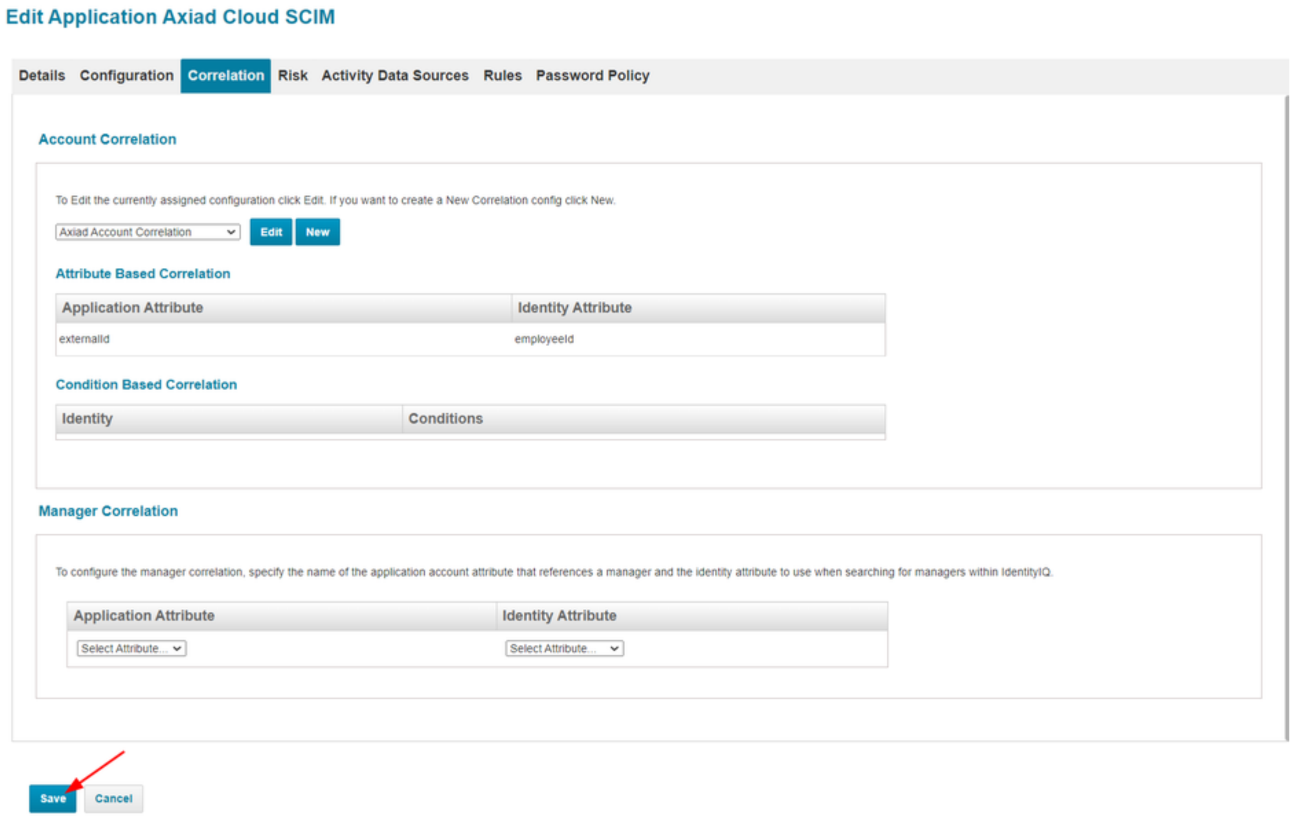
Attribute Based Correlation Assignments

□		Application Attribute		Identity Attribute
Delete	Add	externalID	equals	Employee ID

To create an attribute based assignment, select an application attribute and an identity attribute and click Add. To delete existing assignments, select assignments using the selection column on the left and click Delete.

NOTE: Each mapping is processed in the top-down order shown in this table until an identity is found or the mapping list is exhausted.

18. At the bottom of this page select `Save` to create the new application



Edit Application Axiad Cloud SCIM

Account Correlation

To Edit the currently assigned configuration click Edit. If you want to create a New Correlation config click New.

Axiad Account Correlation

Attribute Based Correlation

Application Attribute	Identity Attribute
externalId	employeeId

Condition Based Correlation

Identity	Conditions

Manager Correlation

To configure the manager correlation, specify the name of the application account attribute that references a manager and the identity attribute to use when searching for managers within IdentityIQ.

Application Attribute	Identity Attribute
Select Attribute...	Select Attribute...

Assigning the application

If you need to do a mass sync, or have a large number of users to assign, please work with your SailPoint customer success engineer to ensure this is done in accordance to specifications for your environment.

Best practice tips

It’s advised to configure your application to run events at certain times to prevent it from putting too much strain on your SailPoint environment. This can be done via LifeCycle events or Scheduled Tasks. Please work with your SailPoint customer success engineer to ensure this is done in accordance to specifications for your environment.

SCIM User Body definitions

Describes a user belonging to an organization

Name	Description	Schema
active *optional*	A Boolean value indicating the user’s administrative status. The definitive meaning of this attribute is determined by the service provider. As a typical example, a value of true implies that the user is able to log in, while a value of false implies that the user’s account has been suspended.	boolean
addresses *optional*	A physical mailing address for this user. Canonical type values of "work", "home", and "other".	< MultiValueAttribute > array
displayName *optional*	The name of the user, suitable for display to end-users. Each user returned MAY include a non-empty displayName value.	string
emails *optional*	Email addresses for the User.Service providers SHOULD canonicalize the value, e.g., "bjensen@example.com" instead of "bjensen@EXAMPLE.COM".	< MultiValueAttribute > array
entitlements *optional*	A list of entitlements for the user that represent a thing the user has. An entitlement may be an additional right to a thing, object, or service.	< MultiValueAttribute > array

externalId *optional*	Defined by the client, is required to be unique ONLY within the resources associated with the associated Tenant.	string
groups *optional*	A list of groups to which the user belongs, either through direct membership, through nested groups, or dynamically calculated.	< MultiValueAttribute > array
id *optional*	A unique identifier for a SCIM resource as defined by the service provider. Each representation of the resource MUST include a non-empty "id" value. This identifier MUST be unique across the SCIM service provider’s entire set of resources. The value of the "id" attribute is always issued by the service provider and MUST NOT be specified by the client.	string
ims *optional*	Instant messaging address for the user. No official canonicalization rules exist for all instant messaging addresses, but service providers SHOULD, when appropriate, remove allv whitespace and convert the address to lowercase.	< MultiValueAttribute > array
locale *optional*	Used to indicate the User’s default location for purposes of localizing such items as currency, date time format, or numerical representations.	string
meta *optional*	A complex attribute containing resource metadata. All "meta" sub-attributes are assigned by the service provider (have a "mutability" of "readOnly"), and all of these sub-attributes have a "returned" characteristic of "default". This attribute SHALL be ignored when provided by clients	UserMetadata
name *required*	The components of the user’s name. Service providers MAY return just the full name as a single string in the formatted sub-attribute, or they MAY return just the individual component attributes using the other sub-attributes, or they MAY return both. If both variants are returned, they SHOULD be describing the same name, with the formatted name indicating how the component attributes should be combined.	UserFullName
nickName *optional*	The casual way to address the user in real life. This attribute SHOULD NOT be used to represent a User’s username.	string
password *optional*	This attribute is intended to be used as a means to set, replace, or compare (i.e., filter for equality) a password. The cleartext value or the hashed value of a password SHALL NOT be returnable by a service provider. If a service provider holds the value locally, the value SHOULD be hashed.	string
phoneNumbers *optional*	Phone numbers for the user. The value SHOULD be specified according to the format 'tel:+1-201-555-0123'.	< MultiValueAttribute > array
photos *optional*	A URI that is a uniform resource locator that points to a resource location representing the user’s image. The resource MUST be a file (e.g., a GIF, JPEG, or PNG image file) rather than a web page containing an image.	< MultiValueAttribute > array
preferredLanguage *optional*	Indicates the user’s preferred written or spoken languages and is generally used for selecting a localized user interface	string
profileUrl *optional*	A URI that is a uniform resource locator. and that points to a location representing the user’s online profile.	string
roles *optional*	A list of roles for the user that collectively represent who the user is, e.g., "Student", "Faculty".	< MultiValueAttribute > array
timezone *optional*	The User’s time zone, in IANA Time Zone database format, also known as the "Olson" time zone database format (e.g., "America/Los_Angeles").	string
title *optional*	The user’s title.	string
urn:ietf:params:scim:schemas:extension:CustomExtensionName:2.0:User *optional*	Custom attributes of an user which is in key-value pair.	< string, object > map
urn:ietf:params:scim:schemas:extension:enterprise:2.0:User *optional*	Enterprise user schema extension.	EnterpriseUserExtension
userName *required*	A service provider’s unique identifier for the user. This identifier MUST be unique across the service provider’s entire set of Users. This attribute is REQUIRED and is case insensitive.	string
userType *optional*	Used to identify the relationship between the organization and the user.	string
x509Certificates *optional*	A list of certificates associated with the resource (e.g., a User). Each value contains exactly one DER-encoded X.509 certificate, which	< MultiValueAttribute > array

	MUST be base64 encoded.	

SCIM User Body Example

Request Body

```
`{
    "schemas": [
        "urn:ietf:params:scim:schemas:core:2.0:User",
        "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User"
    ],
    "externalId": "<externalId>",
    "userName": "mtest@axiad.dev",
    "name": {
        "familyName": "Test",
        "givenName": "Mitchell"
    },
    "displayName": "Mitchell Test",
    "title": "Partner Integrations Manager",
    "active": true,
    "emails": [
        {
            "type": "work",
            "primary": true,
            "value": "mtest@axiad.dev"
        }
    ],
    "addresses": [
        {
            "type": "work",
            "primary": true,
            "streetAddress": "900 Lafayette St #600",
            "locality": "Santa Clara",
            "region": "California",
            "postalCode": "95050",
            "country": "US"
        }
    ],
    "groups": [],
    "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User": {
        "employeeNumber": "000123854",
        "costCenter": "Integrations",
        "organization": "IT",
        "division": "Integrations",
        "department": "IT",
        "manager": {
            "value": "axiadmanager"
        }
    }
}
```

Response Body

```
`{
    "schemas":    [
       "urn:ietf:params:scim:schemas:core:2.0:User",
       "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User"
    ],
    "id": "<id>",
    "externalId": "<externalID",
    "meta":    {
       "resourceType": "user",
       "created": "2023-06-12T08:14:35Z",
       "lastModified": "2023-06-12T08:14:35Z",
       "location": "https://ucms-<tenantName>.
<tenantPlatform>.axiadids.net/secuera/api/v3/scim/<tenantName>/Users/<id>"
    },
    "userName": "mtest@axiad.dev",
    "name":    {
       "familyName": "Test",
       "givenName": "Mitchell"
    },
    "displayName": "Mitchell Test",
    "title": "Partner Integrations Manager",
    "active": true,
    "emails": [   {
       "type": "work",
       "primary": false,
       "value": "mtest@axiad.dev"
    }],
    "addresses": [   {
       "type": "work",
       "primary": false,
       "streetAddress": "900 Lafayette St #600",
       "locality": "Santa Clara",
       "region": "California",
       "postalCode": "95050",
       "country": "US"
    }],
    "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User":    {
       "employeeNumber": "000123854",
       "costCenter": "Integrations",
       "organization": "IT",
       "division": "Integrations",
       "department": "IT",
       "manager": {"value": "axiadmanager"}
    }
 }
```

SCIM Group Body definitions

Describes a group belonging to an organization

Name	Description	Schema
displayName *required*	The group’s display name	string
externalId *optional*	Defined by the client, is required to be unique ONLY within the resources associated with the associated Tenant.	string
id *required*	A unique identifier for a SCIM resource as defined by the service provider. Each representation of the resource MUST include a non-empty "id" value. This identifier MUST be unique across the SCIM service provider’s entire set of resources. The value of the "id" attribute is always issued by the service provider and MUST NOT be specified by the client.	string
members *optional*	A list of members of the Group. While values MAY be added or removed, sub-attributes of members are "immutable".	< Member > array
meta *required*	A complex attribute containing resource metadata. All "meta" sub-attributes are assigned by the service provider (have a "mutability" of "readOnly"), and all of these sub-attributes have a "returned" characteristic of "default". This attribute SHALL be ignored when provided by clients	GroupMetadata

Related articles

- SailPoint IdentityIQ Application Configuration Guide