



Starling Connect for Active Roles

Administration Guide

Copyright 2021 One Identity LLC.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC .

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (<http://www.OneIdentity.com>) for regional and international office information.


Patents

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <http://www.OneIdentity.com/legal/patents.aspx>.

Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal. All other trademarks are the property of their respective owners.

Legend

-  **WARNING:** A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.
-  **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

Contents

About this Guide	10
Starling Connect for Active Roles Overview	11
Starling Connect SCIM Endpoints	12
One Identity Starling for Active Roles	13
Supported connectors	14
Supported Browsers	16
Additional hardware and software requirements	16
Creating a New Organization	17
Signing in to Starling	17
Supported Cloud Applications	19
Configuring Connectors in Starling	20
Configuring Starling in Active Roles	20
Configuring Active Roles to join One Identity Starling	21
SCIM attribute mapping with Active Directory for users and groups	22
Disconnecting One Identity Starling from Active Roles	24
Salesforce	25
Supervisor Configuration Parameters	25
Supported Objects and Operations in Active Roles	26
Mandatory Fields	26
User and Group Mapping	27
Connector Limitations	29
Facebook Workplace	30
Supervisor Configuration Parameters	30
Supported Objects and Operations	30
Mandatory Fields	31
User and Group Mapping	31
Connector Limitations	33
SuccessFactors	34
Supervisor Configuration Parameters	34
Supported Objects and Operations	34
Mandatory Fields	35
User and Group Mapping	35
Connector Limitations	37

Amazon (S3 and AWS)	38
Supervisor Configuration Parameters	38
Supported Objects and Operations	38
Mandatory Fields	39
User and Group Mapping	39
Connector Limitations	40
ServiceNow	41
Supervisor Configuration Parameters	41
Supported Objects and Operations	41
Mandatory Fields	42
Configuring custom attributes in ServiceNow	42
User and Group Mapping	43
Connector Limitations	45
Azure Active Directory	46
Supervisor Configuration Parameters	46
Supported Objects and Operations	46
Mandatory Fields	47
User and Group Mapping	47
Connector Limitations	49
Box	50
Supervisor Configuration Parameters	50
Supported Objects and Operations	51
Mandatory Fields	51
User and Group Mapping	52
Trello	53
Supervisor Configuration Parameters	53
Supported Objects and Operations	53
Mandatory Fields	54
User and Group Mapping	54
Connector Limitations	55
Statuspage	57
Supervisor Configuration Parameters	57
Supported Objects and Operations	57
Mandatory Fields	58
Connector Limitations	58
SAP Cloud Platform	59
Supervisor Configuration Parameters	59

Supported Objects and Operations	59
Mandatory Fields	60
Connector Limitations	60
JIRA Server	61
Supervisor Configuration Parameters	61
Supported Objects and Operations	61
Mandatory Fields	62
Connector Limitations	63
RSA Archer	64
Supervisor Configuration Parameters	64
Supported Objects and Operations	65
Mandatory Fields	65
Connector Limitations	66
Dropbox	67
Supervisor Configuration Parameters	67
Supported Objects and Operations	67
Mandatory Fields	68
Connector Limitations	68
Crowd	70
Supervisor Configuration Parameters	70
Supported Objects and Operations	70
Mandatory Fields	71
Connector Limitations	71
AtlassianJC	72
Supervisor Configuration Parameters	72
Supported Objects and Operations	72
Mandatory Fields	73
Connector Limitations	73
Pipedrive	74
Supervisor Configuration Parameters	74
Supported Objects and Operations	74
Mandatory Fields	75
Connector Limitations	75
SuccessFactorsHR	76
Supervisor Configuration Parameters	76
Supported Objects and Operations	77
Connector Limitations	78

Nutshell	79
Supervisor Configuration Parameters	79
Supported Objects and Operations	79
Mandatory Fields	80
Connector Limitations	80
Insightly	82
Supervisor Configuration Parameters	82
Supported Objects and Operations	82
Mandatory Fields	83
Connector Limitations	83
Egnyte	84
Supervisor Configuration Parameters	84
Supported Objects and Operations	84
Mandatory Fields	85
Connector Limitations	86
SugarCRM	87
Supervisor Configuration Parameters	87
Supported Objects and Operations	87
Mandatory Fields	88
Connector Limitations	88
Oracle IDCS	89
Supervisor Configuration Parameters	89
Supported Objects and Operations	89
Mandatory Fields	90
Connector Limitations	90
Zendesk Sell	91
Supervisor Configuration Parameters	91
Supported Objects and Operations	91
Mandatory Fields	91
Connector Limitations	92
Workbooks	93
Supervisor Configuration Parameters	93
Supported Objects and Operations	93
Mandatory Fields	93
Connector Limitations	94
DocuSign	95
Supervisor Configuration Parameters	95

Supported Objects and Operations	95
Mandatory Fields	96
Connector Limitations	96
ShareFile	97
Supervisor Configuration Parameters	97
Supported Objects and Operations	97
Mandatory Fields	98
Connector Limitations	98
Zendesk	100
Supervisor Configuration Parameters	100
Supported Objects and Operations	100
Mandatory Fields	101
Connector Limitations	101
G Suite	102
Supervisor Configuration Parameters	102
Supported Objects and Operations	102
Mandatory Fields	103
Connector Limitations	103
Concur	104
Supervisor Configuration Parameters	104
Supported Objects and Operations	104
Mandatory Fields	105
Connector Limitations	105
Tableau	107
Supervisor Configuration Parameters	107
Supported Objects and Operations	107
Mandatory Fields	108
Connector Limitations	108
GoToMeeting	109
Supervisor Configuration Parameters	109
Supported Objects and Operations	109
Mandatory Fields	110
Connector Limitations	110
Coupa	112
Supervisor Configuration Parameters	112
Supported Objects and Operations	112
Mandatory Fields	113

Connector Limitations	113
AWS Cognito	114
Supervisor Configuration Parameters	114
Supported Objects and Operations	114
Mandatory Fields	115
Connector Limitations	115
Okta	116
Supervisor configuration parameters	116
Supported objects and operations	116
Mandatory fields	117
User and Group mapping	117
Connector limitations	119
DataDog	120
Supervisor configuration parameters	120
Supported objects and operations	120
Mandatory field	121
User mapping	121
Connector limitations	121
Hideez	122
Supervisor configuration parameters	122
Supported objects and operations	122
Mandatory fields	124
Mappings	126
Connector limitations	132
One Identity Manager E2E integration needs	132
Opsgenie	133
Supervisor configuration parameters	133
Supported objects and operations	133
Roles	134
Mandatory fields	134
Mappings	135
Connector limitations	136
Informatica Cloud Services	137
Supervisor configuration parameters	137
Supported objects and operations	137
Roles	138
Mandatory fields	138

Mappings	139
Connector limitations	140
OneLogin	141
Supervisor configuration parameters	141
Supported objects and operations	141
Roles	142
Mandatory fields	142
Mappings	143
Connector limitations	144
Appendix: Creating a service account in G Suite	145
Appendix: Setting a trial account on Salesforce	147
Appendix: Working with Azure Active Directory	149
Appendix: Generating a private key for service account in GoToMeeting	151
About us	152
Contacting us	152
Technical support resources	152

About this Guide

This guide describes each of the supported target cloud applications and how it is on boarded with Active Roles. This guide provides an overview of each supported cloud application. Information about each of the supported cloud applications functionality and associated limitations can be gathered from the guide. This guide is intended for end users, system administrators, consultants, analysts, and other IT professionals using the product.

NOTE: This guide describes Starling Connect for Active Roles functionality available to the default user. It is possible that not all the functions described here are available to you. This depends on your system configuration and permissions.

Starling Connect for Active Roles Overview

Today, more than ever, organizations must address the proliferation of cloud-based applications. While these applications often provide convenient and flexible access for employees and customers, they also present a new set of management and security challenges for IT and line-of-business managers.

One Identity Active Roles is an administrative and security tool for Microsoft Active Directory (AD), Azure AD (AAD), and related systems, such as Exchange and Office 365. It enables organizations to create flexible administration workflows, including automation of user and group provisioning and DE provisioning. These workflows can be easily customized for your needs while ensuring secure delegation of tasks, reduced workloads, increased accuracy and lower costs. It also enables the integration of diverse corporate data sources and provisioning processes, which can expedite workflows and eliminate data inconsistencies across platforms and environments.

One Identity Starling Connect – a cloud-based service – extends the provisioning capabilities of Active Roles (version 7.4.0 or later) to a growing collection of SaaS applications, which enables organizations to streamline processes and secure hybrid environments. This means you can extend your Active Roles on-premise deployment to provision many more applications, regardless of where they are located (on-premise or cloud-based).

Starling Connect SCIM Endpoints

Starling Connect SCIM endpoints are SCIM version 2.0 endpoints, that simplifies user management in the target cloud application. The SCIM endpoints define a schema for representing users, groups and a REST API for the necessary CRUD operations. For more information on the attribute mapping table, see [SCIM attribute mapping with Active Directory for users and groups](#).

One Identity Starling for Active Roles

Starling helps in creating a secure and customizable cloud service. Administrators use the Starling site to create a new organization, register new accounts, add services to their organization, and gain secure access to those services. Although the main Starling portal can be used to create a free Starling account and provides access to the services currently available for subscriptions, some of the services must be purchased in order for them to be available for full-time use. For more information on adding a service, use the information associated with each service.

There is a service information site (<http://status.cloud.oneidentity.com/>) for viewing the current operational status of each service. This site is useful if you are having difficulties connecting to a service and want to check if there are any reported issues prior to contacting Support for additional assistance.

Supported connectors

The following table lists the connectors and their status with respect to validation in the current release. Connectors with the status **Validated**, implies that the connector has been tested. Connectors with the status **Not Compatible** implies that the connector is not compatible with ARS.

Table 1: Connector Status

Connector	Status
Salesforce	Validated
Facebook Workplace	Validated
SuccessFactors	Validated
Amazon (S3 and AWS)	Validated
ServiceNow	Validated
Azure Active Directory	Validated
Box	Validated
Trello	Validated
Statuspage	Validated
SuccessFactorsHR	Not Applicable
SAP Cloud Platform	Preview
JIRA Server	Preview
RSA Archer	Preview
Dropbox	Preview
Crowd	Preview
AtlassianJC	Preview
Pipedrive	Preview
Nutshell	Validated
Insightly	Preview
Egnyte	Preview
SugarCRM	Validated
Oracle IDCS	Preview
Zendesk Sell	Not Applicable

Connector	Status
Workbooks	Not Applicable
DocuSign	Validated
ShareFile	Validated
Zendesk	Validated
G Suite	Validated
Concur	Preview
Tableau	Validated
GoToMeeting	Validated
Coupa	Validated
AWS Cognito	Validated
Okta	Validated
DataDog	Preview
Hideez	Preview
Opsgenie	Preview
Informatica Cloud Services	Preview
OneLogin	Preview

Supported Browsers

The following browsers are supported when accessing the Starling service:

Table 2: Supported Browsers

Browser	Minimum OS/Platform	Version
Internet Explorer	Windows 7	11
Google Chrome	Windows 10, Android, Mac OS X Yosemite	Latest
Mozilla Firefox	Windows 8.1	Latest
Microsoft Edge	Windows 10	Latest
Safari	Mac OS X Yosemite, iOS 8	See OS/Platform
Opera	Windows 7, Mac OS X Yosemite	Latest

Additional hardware and software requirements

In addition to the browser compatibility requirements for Starling (see [Supported Browsers](#)), some additional requirements may need to be met. See the table below for information on those requirements.

The services available through Starling may also include additional hardware and software requirements. Any requirements that must be met by users of a particular service are available within the documentation specific to the service.

Table 3: Additional Starling requirements

Work accounts	<p>To authenticate using a work account, you need the following:</p> <ul style="list-style-type: none">Fully configured Azure AD tenant capable of authenticating usersIn cases where an organization has registered an Azure AD tenant but it is not fully synchronized or an account has not yet been added, the owner of that account will be unable to use Starling at that time unless they register independently from the organization.
Event forwarding	<p>To use the event forwarding feature, you need the following:</p> <ul style="list-style-type: none">A service that supports SYSLOG (for example, Loggly)

Creating a New Organization

To begin using Starling and its associated services, you must first create an organization.

To create an organization and account

1. From the Starling home page (<https://www.cloud.oneidentity.com/>), click **TRY STARLING**.
2. In the email address field, enter the email address which will be associated with the account. The email address must be less than 64 characters for the local-part and for each domain part (the full email must be less than 255 characters). You need access to the specified email account to complete your registration and any future communications regarding your organization and account will be sent to this email address.
3. Click **Next**.
4. In the **Organization Name** field, enter the name of your organization (up to 100 characters long).
5. In the **First Name** field, enter the first name of the account holder (up to 64 characters long).
6. In the **Last Name** field, enter the last name of the account holder (up to 64 characters long).
7. In the **Password** field, enter a password for your account. The password must consist of eight to sixteen characters and include three of the following items: uppercase letter, lowercase letter, number, or symbol.
8. Enter a phone number for the account after selecting the relevant country.
9. Read through the Terms of Use, Privacy Policy, Software Transaction Agreement, and SaaS Addendum. If you agree, select the following check box: **I have read, I understand and I accept the Terms of Use, Privacy Policy, Software Transaction Agreement, and SaaS Addendum**.
10. Click **START**.
11. To subscribe to the **Starling** services, click **signing up for a free trial**.

Signing in to Starling

The following procedure applies to users that are accessing a Starling account that is not associated with an existing work account.

To sign in to Starling

1. From the Starling home page (<https://www.cloud.oneidentity.com/>), click **Sign in to Starling**.
2. In the email address field, enter the email address associated with your account.

3. Click **Next**.
4. Once Starling has confirmed there is no work account associated with your email address, a password prompt will appear. Enter your password then click **SIGN IN**. You are now signed in to Starling.

IMPORTANT: You must ensure the following:

- The **Port 443** must be enabled.
- The following IP addresses must be whitelisted in the Firewall:
 - EastUS - 23.96.58.177
 - WestUS - Navigate to <https://www.microsoft.com/en-us/download/details.aspx?id=41653> and download the XML file, that contains the list of IP addresses (uswest).
 - North EU - Navigate to <https://www.microsoft.com/en-us/download/details.aspx?id=56519> and download the XML file, that contains the list of IP addresses (eunorth).
 - STS - 168.63.72.218

Supported Cloud Applications

Each Starling Connect supported cloud application is explained in this document with the following information:

- Application Name
- Brief Description
- Supported Objects and Operations
- Mandatory Fields
- Known issues or limitations

NOTE: Different cloud applications, that are supported by Starling Connect are represented in this document. The document will be updated to reflect newly added support for other cloud applications, as and when new target cloud application connectors gets developed. For connectivity to other cloud applications which are not listed in this documents, please contact Alex Binotto (alex.binotto@oneidentity.com).

Configuring Connectors in Starling

Before you configure Starling using the Active Roles Configuration Center, ensure the following:

- Users must have acquired valid Starling Credentials, such as a Starling Organization Admin account or a Collaborator account associated with the One Identity Hybrid subscription. For more information on Starling, see the *One Identity Starling User Guide*.
- The Active Roles Administration Service must be running on the computer where you want to configure Starling.
- The Active Roles Administration Service must have a managed domain.

Configuring Starling in Active Roles

Active Roles version 7.4 supports integration with One Identity Starling services. The Starling Join feature in Active Roles now enables you to connect to One Identity Starling, the Software as a Service (SaaS) solution of One Identity. The Starling Join feature enables access to the Starling services through Active Roles thus allowing to benefit from the Starling services such as Two-factor Authentication and Identity Analytics and Risk Intelligence.

You can use the Active Roles Configuration Center to join One Identity Starling to Active Roles on the Starling wizard.

To start the wizard, click **Configure** in the **Starling** area on the Active Roles Dashboard page in the **Configuration Center** main window. The Starling wizard enables you to perform the Starling join operation.

Configuring Active Roles to join One Identity Starling

To configure Active Roles to join Starling

1. On the Active Roles Configuration Center, under Starling, click **Configure**.
2. Click **Join One Identity Starling**. The Get Started page on the Starling product is displayed.
3. On the Starling Get Started page, enter your work email address enabled with Starling, and click **Next**.
4. Enter the Starling credentials provided to you at the time of subscribing to Starling and follow the instructions displayed on the wizard to continue.

NOTE:

- If you have a Starling account, when a subscription is created for you, you will receive a Starling invitation email. Click the link in the email and log in to the Starling account.
- If you do not have a Starling account, when a subscription is created for you, you will get a Starling Sign-up email to complete a registration process to create a Starling account. Complete the registration and log in using the credentials that you have provided during registration. For account creation details, see the *One Identity Starling User Guide*.

The One Identity Starling dialog box in Active Roles with a progress message indicating the progress of joining Starling is displayed. A join confirmation page is displayed with the name of the Active Roles instance that is going to be joined to Starling .

After the operation is completed successfully, the Starling tab is displayed with **Account Joined** success message.

To view the Starling 2FA settings

1. On the Active Roles Configuration Center, in the left pane, click **Starling**.
2. Click **Starling** tab.
The status of the Starling connection is displayed.
3. Click **Starling 2FA** tab.
The status Starling 2FA is displayed.
4. To disable the Starling 2FA feature click **Disable Starling 2FA**. To enable it again, click **Enable Starling 2FA**.

SCIM attribute mapping with Active Directory for users and groups

Active Roles provides support to connect to Starling Connect to manage the user provisioning and deprovisioning activities for the registered connectors. This is achieved through the internal attribute mapping mechanism. The AD attributes are mapped to SCIM attributes to perform each operation.

SCIM attribute mapping with Active Directory for Users

SCIM	Active Directory
displayName	displayName
givenName	givenName
familyName	sn
middleName	middleName
title	title
password	edsaPassword
streetAddress	streetAddress
locality	city
postalCode	postalCode
region	state
country	c
active	edsaAccountIsDisabled
userName	edsvauserName
honorificPrefix	initials
formattedName	cn
emails	proxyAddresses,mail
preferredLanguage	preferredLanguage
description	description
emailEncoding	edsvaemailEncoding
alias	edsvaalias
division	division
company	company

department	department
homePage	wWWHomePage
lastLogon	lastLogon
accountExpires	accountExpires
timezone	edsvatimezone
entitlements	edsvaentitlements
employeeNumber	employeeNumber
cn	cn
userPermissionsMarketingUser	edsvauserPermissionsMarketingUser
userPermissionsOfflineUser	edsvauserPermissionsOfflineUser
userPermissionsAvantgoUser	edsvauserPermissionsAvantgoUser
userPermissionsCallCenterAutoLogin	edsvauserPermissionsCallCenterAutoLogin
userPermissionsMobileUser	edsvauserPermissionsMobileUser
userPermissionsSFContentUser	edsvauserPermissionsSFContentUser
userPermissionsKnowledgeUser	edsvauserPermissionsKnowledgeUser
userPermissionsInteractionUser	edsvauserPermissionsInteractionUser
userPermissionsSupportUser	edsvauserPermissionsSupportUser
userPermissionsLiveAgentUser	edsvauserPermissionsLiveAgentUser
locale	localeID
phoneNumbers	telephoneNumber,mobile,homePhone
manager	manager
nickname	edsvanickname
desiredDeliveryMediums	edsvadesiredDeliveryMediums

SCIM attribute mapping with Active Directory for Groups

SCIM	Active Directory
displayName	cn
members	member
email	mail
manager	managedBy

Disconnecting One Identity Starling from Active Roles

After you configure Active Roles to join Starling, in case you want to disconnect from Starling, on Starling tab in Starling page, click **Unjoin One Identity Starling**. Unjoin Starling operation will disconnect Active Roles from your subscription. You are prompted to confirm if you want to continue. Click **Yes** to disconnect Active Roles from your subscription and complete the Unjoin One Identity Starling operation.

Salesforce

Salesforce offers a cloud-based customer relationship management (CRM) platform that lets users track sales, service, and marketing. It includes a social networking plug-in and analytical tools including email alerts, Google search functionality, and access to contracts.

To login to the Salesforce application, you must create a trail account. For more information, see [Setting a trial account on Salesforce](#)

Supervisor Configuration Parameters

To configure the connector, following parameters are required:

- Connector Name
- Client ID - Consumer key of the connected app under API. Enable OAuth Settings (Left Menu | Build | Create | Apps).
- Client Secret - Consumer Secret of the connected app under API. Enable OAuth Settings (Left Menu | Build | Create | Apps).
- Username
- Password
- Token URL - Salesforce's token URL (*https://<salesforce_instance_url>/services/oauth2/token*)
- Grant Type : password

Supported Objects and Operations in Active Roles

Users

Table 4: Supported operations for Users

Operation	VERB
Create	POST
Update (id)	PUT
Delete (id)	DELETE
Deprovision	PUT
Undo Deprovision	PUT

Groups

Table 5: Supported operations for Groups

Operation	VERB
Create	POST
Update (id)	PUT
Delete (id)	DELETE
Deprovision	PUT
Undo Deprovision	PUT
Group Membership	PUT

Mandatory Fields

Users

- Last Name
- Email
- Alias (Auto populated with the combination of First and/or Last name)
- Username (Auto populated from email)
- Nickname (Auto populated from email; takes the name before "@")
- Email Encoding

- Locale Settings (Time Zone, Locale & Language)
- Entitlements - ProfileId

Groups

- Group Name

User and Group Mapping

The user and group mapping is listed in the table below.

Table 6: User Mapping

SCIM Parameter	Salesforce Parameter
Id	id
UserName	Username
ExternalId	FederationIdentifier
Name.GivenName	FirstName
Name.FamilyName	LastName
Name.Formatted	Name
DisplayName	Name
NickName	CommunityNickname
Emails.Value	Email
Photos.Value	FullPhotoUrl
Addresses.StreetAddress	Street
Addresses.Locality	City
Addresses.Region	State
Addresses.PostalCode	PostalCode
Addresses.Country	Country
PhoneNumbers.Values	Phone
UserType	UserType
Title	Title
PreferredLanguage	LanguageLocaleKey

SCIM Parameter	Salesforce Parameter
Locale	LocaleSidKey
Timezone	TimeZoneSidKey
Active	IsActive
Groups.value	GroupId
Entitlements.Value	Profile.Id
Entitlements.Display	Profile.Name
Roles.Value	UserRole.Id
Roles.Display	UserRole.Name
Extension.PasswordLastSet	LastPasswordChangeDate
Extension.EmailEncoding	EmailEncodingKey
Extension.Organization	CompanyName
Extension.Division	Division
Extension.Department	Department
Extension.Description	AboutMe
Extension.Manager.Value	Manager.Id
Extension.Manager.DisplayName	Manager.Name
Extension.LastLogon	LastLoginDate
Extension.EmployeeNumber	EmployeeNumber
Extension.Alias	Alias
Extension.UserPermissionsMobileUser	UserPermissionsMobileUser
Extension.UserPermissionsSFContentUser	UserPermissionsSFContentUser
Extension.UserPermissionsKnowledgeUser	UserPermissionsKnowledgeUser
Extension.UserPermissionsOfflineUser	UserPermissionsOfflineUser
Extension.UserPermissionsMarketingUser	UserPermissionsMarketingUser
Extension.UserPermissionsCallCenterAutoLogin	UserPermissionsCallCenterAutoLogin
Extension.UserPermissionsInteractionUser	UserPermissionsInteractionUser
Extension.UserPermissionsSupportUser	UserPermissionsSupportUser
Extension.FullPhotoUrl	FullPhotoUrl
Meta.Created	CreatedDate
Meta.LastModified	LastModifiedDate

Table 7: Group Mapping

SCIM Parameter	Salesforce Parameter
Id	Id
DisplayName	Name
Members.value	UserOrGroupId
Meta.Created	CreatedDate
Meta.LastModified	LastModifiedDate

Connector Limitations

- Even if the Count value is less than 2000, the resources are returned as 2000.
- Currently, the connector supports only salesforce api version 41.0.

Facebook Workplace

Workplace is a collaborative business platform run by Facebook to help users communicate through groups, chat, and social networking in a corporate environment.

Supervisor Configuration Parameters

To configure the connector, following parameters are required:

- Connector Name
- API Key

Supported Objects and Operations

Users

Table 8: Supported operations and objects for Users

Operation	VERB
Create	POST
Update (Id)	PUT
Delete (Id)	DELETE
Deprovision	PUT
Undo Deprovision	PUT

Groups

Table 9: Supported operations and objects for Groups

Operation	VERB
Create	POST
Update (Id)	PUT
Delete (Id)	DELETE
Group Membership	PUT

Mandatory Fields

Users

- User Name
- Name (Formatted)
- Active

Groups

- Group Name

User and Group Mapping

The user and group mappings are listed in the tables below.

Table 10: User Mapping

SCIM Parameter	FBWorkplace Parameter
Id	Id
UserName	userName
Name.Formatted	name.formatted
Name.GivenName	name.givenName
Name.FamilyName	name.familyName
Name.MiddleName	name.middleName

SCIM Parameter	FBWorkplace Parameter
Name.HonorificPrefix	name.honorificPrefix
Name.HonorificSuffix	name.honorificSuffix
DisplayName	displayName
NickName	nickName
UserType	userType
Title	title
PreferredLanguage	preferredLanguage
Locale	locale
Timezone	timezone
Active	active
Emails	emails
Addresses	addresses
PhoneNumbers	phoneNumbers
Groups.value	Group.id
Groups.display	Group.name
Roles.Value	Role.Id
Extension.Organization	organization
Extension.Division	division
Extension.Department	department
Extension.Manager.Value	manager.managerId
Extension.EmployeeNumber	employeeNumber
Extension.CostCenter	costCenter

Table 11: Group Mapping

SCIM Parameter	FBWorkplace Parameter
Id	Id
DisplayName	Name
Members.value	UserOrGroupId
Meta.Created	CreatedDate
Meta.LastModified	LastModifiedDate

Connector Limitations

- Removal of the last member of a group deletes the group automatically.
- At least one user must be a member of a group to use it.

SuccessFactors

SuccessFactors is an integrated human-resources platform. It offers users tools for onboarding, social business, and collaboration along with tools for learning management, performance management, recruiting, applicant tracking, succession planning, talent management, and HR analytics. It is also cloud-based.

Supervisor Configuration Parameters

To configure the connector, following parameters are required:

- Connector Name
- Username
- Password
- SCIM URL
(<https://apps.support.sap.com/sap/support/knowledge/public/en/2215682>)

NOTE: SuccessFactors Web Services API are based on OData protocol which is intended to enable access to data in the SuccessFactors system for create, read, update, or delete (CRUD) operations. For more information on SuccessFactors API, see <https://apps.support.sap.com/sap/support/knowledge/public/en/2613670>. For more information on SuccessFactors URLs and Data Centers, see <https://apps.support.sap.com/sap/support/knowledge/public/en/2089448>.

Supported Objects and Operations

Users

Table 12: Supported operations for Users

Operation	VERB
Create User	POST

Operation	VERB
Update User	PUT
Delete	PUT
Deprovision	PUT
Undo Deprovision	PUT

Mandatory Fields

Users

- User Name
- Employee Number
- Status

Groups

- Group Name
- Group Type
- Group Members

User and Group Mapping

The user and group mappings are listed in the tables below.

Table 13: User Mapping

SCIM Parameter	SuccessFactors Parameter
Id	userId
UserName	username
Name.GivenName	firstName
Name.FamilyName	lastName
Name.MiddleName	mi
Name.HonorificSuffix	suffix
Name.Formatted	defaultFullName

SCIM Parameter	SuccessFactors Parameter
DisplayName	defaultFullName
Emails.Value	email
Addresses.StreetAddress	addressLine1
Addresses.Locality	state
Addresses.Region	city
Addresses.PostalCode	zipCode
Addresses.Country	country
PhoneNumbers.Value	businessPhone
Groups.value	groupId
Groups.display	groupName
Roles.value	user.role.id
Roles.display	user.role.name
UserType	jobTitle
Title	title
Active	status
Locale	location
Timezone	timeZone
userExtension.EmployeeNumber	empId
userExtension.Division	division
userExtension.Department	department
userExtension.Gender	gender
userExtension.HireDate	hireDate
userExtension.DateOfBirth	dateOfBirth
Meta.Created	hireDate
Meta.LastModified	lastModified

Table 14: Group Mapping

SCIM Parameter	SuccessFactors Parameter
Id	groupID
displayName	groupName
groupType	groupType
groupExtension.value	userId
groupExtension.display	userName
Meta.LastModified	lastModifiedDate

Connector Limitations

- **Create** and **Delete** group operations are not supported due to cloud application limitations.
- When the active status is updated to false while performing the PUT operation for a user, the following error appears: *user not found*. This error occurs because a user is considered as a deleted user when the active status is false.
- User update does not support addition and removal of **Groups** or **Roles** for a particular user. We need to get it done via group update. This is not applicable for role update.
- User employee number cannot be updated because the cloud application considers employee number as a user Id.

Amazon (S3 and AWS)

Amazon (S3 and AWS) offers a suite of cloud-computing services that make up an on-demand computing platform. The most central and best-known of these are Amazon Elastic Compute Cloud (EC2) and Amazon Simple Storage Service (S3). AWS offers more than 70 services, including computing, storage, networking, database, analytics, application services, deployment, management, mobile, developer tools, and tools for the Internet of Things.

Supervisor Configuration Parameters

To configure the connector, following parameters are required:

- Connector Name
- Client Id of the cloud account
- Client Secret of the cloud account
- Region of the cloud account
- SCIM URL (Cloud application's REST API's base URL)

Supported Objects and Operations

Users

Table 15: Supported operations and objects for Users

Operation	VERB
Create	POST
Update	PUT
Delete	DELETE
Deprovision	PUT
Undo Deprovision	PUT

Groups

Table 16: Supported operations and objects for Groups

Operation	VERB
Create	POST
Update	PUT
Delete	DELETE
Deprovision	PUT
Undo Deprovision	PUT
Group Membership	PUT

Mandatory Fields

Users

- User Name
- Password - This is applicable only for the **Create** operation.

Groups

- Group Name

User and Group Mapping

The user and group mappings are listed in the tables below.

Table 17: User Mapping

SCIM Parameter	Amazon Web Services (AWS) Parameter
Id	UserName
UserName	UserName
Password	password
DisplayName	Arn
Active	(true)

SCIM Parameter	Amazon Web Services (AWS) Parameter
Groups	(ListGroupForUserResult)Group
Entitlements	(ListAttachedUserPoliciesResult)AttachedPolicies
Created	CreateDate
LastModified	PasswordLastUsed

Table 18: Group Mapping

SCIM Parameter	Amazon Web Services (AWS) Parameter
Id	GroupName
displayName	UserName
Entitlements	(ListAttachedGroupPoliciesResult)AttachedPolicies
Members	(GetGroupResult)Users
Created	CreateDate
LastModified	PasswordLastUsed

Connector Limitations

- Signature generation is embedded within a data process. Hence, the application performance is affected.
- The Last Modified date is not available. Hence, the field contains the value of recently used Password.
- While performing **Delete User** or **Delete Group** operation, users or groups that are part of the deleted users or groups get detached from the below mentioned services. However, some services must be detached manually.
 - AccessKey
 - Roles
 - Groups
- The task of assigning entitlements to groups is available with the connector. For successful working, certain changes must be made in Active Roles.

ServiceNow

ServiceNow is a service management platform that can be used for many different business units, including IT, human resources, facilities, and field services.

Supervisor Configuration Parameters

To configure the connector, following parameters are required:

- Connector Name
- Username
- Password
- SCIM URL (cloud application's REST API's base URL)

Supported Objects and Operations

Users

Table 19: Supported operations for Users

Operation	VERB
Create	POST
Update	PUT
Delete	DELETE
Deprovision	PUT
Undo Deprovision	PUT

Groups

Table 20: Supported operations for Groups

Operation	VERB
Create	POST
Update	PUT
Delete	DELETE
Deprovision	PUT
Undo Deprovision	PUT
Group Membership	PUT

Mandatory Fields

Users

- Username

Groups

- Group Name

Configuring custom attributes in ServiceNow

This feature allows you to configure custom attributes in Starling Connector during connector subscription. You can provide the list of custom attributes in a defined format with the name, type and allowed values of the attributes. The custom mappings in Active Roles provides the values for these custom attributes.

To configure custom attributes in ServiceNow:

1. Create a Custom Attribute in ServiceNow.
NOTE: The Starling Platform currently supports only the string types **dateTime**, **True/False** and **Choice**.
2. To configure the custom attributes in Starling UI, enter the **Custom Properties** in the specified format in the Starling Platform.
3. Map the created custom attributes that were specified in the Starling Platform.
4. Perform a synchronization and verify if the custom attributes are available.

NOTE:

- The Starling UI for registering a ServiceNow connector has an input field to provide the custom attributes to be mapped in the connector's **User resource** type apart from the default mapped attributes.

- The custom attributes in the **User resource** type must be in the following format:

```
{field_name}|{data_type}|{choice_value1,choice_value2,etc};{field_name}|{data_type}|{choice_value1,choice_value2,etc};etc.
```

Example:

```
u_employee_status|string;u_date_of_termination_of_employments|DateTime;u_test_field_with_canonical_values|string|Choice 1,Choice 2,Choice 3
```

- All custom attributes are mapped in the enterprise user extensions.
- The supported data types are **string**, **boolean** and **dateTime**.
Choice type in the ServiceNow will become **string** type in OneIM with Canonical Values.
- Only simple attributes are supported.
- All custom user attributes have '**mutability**': '**readWrite**', '**returned**': '**default**', '**caseExact**': '**false**', '**required**': '**false**', '**multiValued**': '**false**', '**uniqueness**': '**none**'.
- The Starling Platform currently supports only the string types **dateTime**, **True/False** and **Choice**.

User and Group Mapping

The user and group mapping is listed in the table below.

Table 21: User Mapping

SCIM Parameter	ServiceNow Parameter
userName	user_name
name.familyName	last_name
name.givenName	first_name
name.middleName	middle_name
displayName	name
emails[0].value	email
addresses[0].streetAddress	street
addresses[0].locality	city

SCIM Parameter	ServiceNow Parameter
addresses[0].region	state
addresses[0].postalCode	zip
addresses[0].country	country
phoneNumbers[0].value	phone
title	title
preferredLanguage	preferred_language
timeZone	time_zone
active	active
password	user_password
roles.value	{resource}.role.value
extension.organization	company
extension.department	department
extension.manager.value	manager.value
extension.employeeNumber	employee_number
id	sys_id
groups.value	{resource}.group.value
extension.lastLogon	last_login_time

Table 22: Group Mapping

SCIM Parameter	ServiceNow Parameter
id	sys_id
displayName	name
members.value	{resource}.user.value
extension.description	description
extension.email	email
extension.groupType	type
extension.manager.value	manager.value

Connector Limitations

- *ServiceProviderAuthority* contains only the **Id** field with the value being same as the instance id of the ServiceNow instance, as there are no APIs to fetch the tenant details in ServiceNow.
- If the department name and organization name is provided during user **create** or **update** operations, the user gets assigned to the department and organization if the department and organization with the same name exists in ServiceNow cloud application.
- If the invalid manager id is used for user's manager fields while performing user **create** or **update** operations, ServiceNow does not display any error. Instead, it invalid id is returned as the manager id.
- In the request, if there are invalid values for timezone, language, and so on, ServiceNow does not display any error. Instead, the fields with invalid values would be blank.
- **GET** Roles operation might not fetch all the roles. Some roles must be retrieved based on ServiceNow Access Control List (ACL).
- If an invalid role id is used for user **create** or **update** operation, no error is displayed. Instead, the same invalid id in the role list is returned.
- If an invalid member id is used for group **create** or **update**, no error is displayed. Instead, the same invalid id as the member id is returned.
- Create User operation with existing user details shows the status code as 403 instead 409. The status code and the status message cannot be interpreted.

Azure Active Directory

Azure Active Directory is a connector that gives users a cloud-based platform for their on-premises resources. Using single sign-on, companies have access to any number of network or web-based applications along with hosting access and identity management resources.

For more information on registering the application, providing permissions, retrieving client ID or client secret, see [Working with Azure Active Directory](#).

Supervisor Configuration Parameters

To configure the connector, following parameters are required:

- Connector name
- Client Id for the app
- Client Secret of the app
- Directory Id of the Active Directory
- Target URL (Cloud application's instance URL used as target URI in payload - For example, <https://graph.microsoft.com/v1.0>).

Supported Objects and Operations

Users

Table 23: Supported operations for Users

Operation	VERB
Create User	POST
Update User	PATCH
Deprovision	PUT
Undo Deprovision	PUT

Mandatory Fields

Users

- email.value
- nickName
- displayName
- password
- active

Groups

- displayName
- mailEnabled (value needs to be 'false')
- mailNickname
- securityEnabled (value needs to be 'true')

User and Group Mapping

The user and group mappings are listed in the tables below.

Table 24: User Mapping

SCIM Parameter	Azure AD Parameter
Id	id
userName	userPrincipalName
name.familyName	surname
name.givenName	givenName
displayName	displayName
nickName	mailNickname
emails[0].value	userPrincipalName
addresses[0].streetAddress	streetAddress
addresses[0].locality	city
addresses[0].region	state
addresses[0].postalCode	postalcode

SCIM Parameter	Azure AD Parameter
addresses[0].country	country
phoneNumbers[0].value	businessPhones[0]
title	jobTitle
active	accountEnabled
preferredLanguage	preferredLanguage
userType	userType
groups[].value	memberOf[].id
groups[].display	memberOf[].displayName
userExtension.organization	companyName
userExtension.department	department
userExtension.employeeNumber	employeeId
userExtension.manager.value	manager.id
userExtension.manager.displayName	manager.displayName
meta.created	createdDateTime

Groups

Table 25: User Mapping

SCIM Parameter	Azure AD Parameter
Id	id
displayName	displayName
members[].value	members[].id
members[].display	members[].displayName
enterpriseExtension.description	description
enterpriseExtension.mailNickname	mailNickname
meta.created	createdDateTime

Connector Limitations

- **lastModified** is not provided along with the **Users** and **Groups**.
- Groups are of two types: **Security groups** and **Office 365** groups. Azure AD supports users and groups as the members of groups. **Security groups** can have users and other Security groups as members. However, only users can be added as members for **Office 365** groups.
- With the trial Azure AD account, it is possible to create only **Security groups** through APIs. For information on mapping the appropriate properties, see **User and Group** section.
- Azure AD resource Id's follow GUID formats. When trying to edit, retrieve, or delete a group by Id with an invalid GUID format, the connector displays 400 as the response code. However with invalid id and a proper GUID format, connector displays 404 as the response code.
- Email value for the user should have only those domains which are verified in the selected Active Directory. To find out the verified domain, go to the Azure Active Directory in the Azure portal and in the **Overview** page above the directory name, the verified domain names are displayed.
- You can create multiple groups with the same name.
- For more information on password policy settings applied to user accounts that are created and managed in Azure AD, see, [Password policies that only apply to cloud user accounts](#).

Box

Box lets users securely store, access, share, and collaboratively work on files across devices. It is accessible through web and mobile applications and REST APIs. It features functions such as search, metadata, granular permission models, enterprise-grade security, retention policies, and preview capabilities.

Supervisor Configuration Parameters

To configure the connector, following parameters are required:

- Connector name
- Client Id
- Client Secret
- Public Key
- Private Key
- Pass Phrase
- Enterprise Id

To get the Box credentials

1. Create an account in Box.
2. Log in to the Box account . The URL will be similar to *https://{Business_Name}.app.box.com/folder/0*.
3. Navigate to the **Developer** console.
4. Create a new custom application.
5. Select **OAuth 2.0 with JWT** (server authentication) as the authentication method.
6. Enter a relevant name for the application that is to be created.
7. Click **View App** and navigate to the **Configuration** section.
8. Set the value of **Application Access** to *Enterprise*.
9. Enable the advanced features by selecting the following options:

- Perform action as Users
 - Generate User access token
10. In the **Add and manage public keys** section, click **generate Public/Private Key pair** button. A config JSON file gets downloaded and it includes the credentials, that are required to get the access token for authentication.

Supported Objects and Operations

Users

Table 26: Supported operations for Users

Operation	VERB
Create	POST
Update	PUT
Delete	DELETE
Deprovision	
Undo Deprovision	

Groups

Table 27: Supported operations for Groups

Operation	VERB
Create	POST

Mandatory Fields

Users

- DisplayName
- Email ID

Groups

- DisplayName

User and Group Mapping

The user and group mappings are listed in the tables below.

Table 28: User Mapping

SCIM Parameter	Box Parameter
id	id
email[0].value	login
userName	login
name.formatted	name
displayName	name
active	status
address[0].formatted	address
userType	type
PhoneNumbers[0].Value	phone
active	status
title	job_title
preferredLanguage	language
timezone	timezone
meta.created	created_at
meta.astModified	modified_at

Table 29: Group Mapping

SCIM Parameter	Box Parameter
id	id
name	displayName
created	created_at
lastModified	modified_at
members[].value	user[].id
members[].display	user[].name

Trello

Trello is a web-based project organizer with both free and paid services. Users can create projects, with room to add comments, additional information, and attachments.

Supervisor Configuration Parameters

To configure the connector, following parameters are required:

- Connector Name
- API Key for the cloud account
- Access token for the cloud account

Supported Objects and Operations

Groups

Table 30: Supported operations and objects for Groups

Operation	VERB
Create	POST
Update	PUT
Delete	DELETE
Deprovision	PUT
Undo Deprovision	PUT

Mandatory Fields

Groups

- displayName

User and Group Mapping

The user and group mappings are listed in the tables below.

Table 31: User Mapping

SCIM Parameter	Trello Parameter
id	id
userName	username
name.formatted	fullName
displayName	fullName
emails[0].value	email
active	confirmed
groups[].value	organizations[].id boards[].id
groups[].display	organizations[].displayName boards[].name

Table 32: Group Mapping

SCIM Parameter	Trello Parameter
id	id
displayName	organization.displayName board.name
extension.description	organization.desc board.desc
extension.name	organization.name
extension.organizationId	board.idOrganization
members[].value	members[].id
members[].display	members[].fullName

Connector Limitations

- The **Created** and **LastModified** dates are not supported for Users and Groups.
- Pagination is not supported for getting Users and Groups.
- Invalid Target URL throws the following status code and message:
 - Code: 500
 - Message: *There was an issue processing this request error*
- Create, Update and Delete operations are not supported for Users.
- When a group of the type board created without associating any organization or team, users can not be added to this board (group). Only the user whose credentials are used to create the board can be added.
- As there is no concept of users under an account under Trello, the *get users* operation is achieved by retrieving members of the groups (organizations and boards) to which the user (whose credentials are used for authorizing the API requests) has access.
- As there are no APIs to retrieve all users or groups, it is required to use /search API by setting the query with characters from [a-z] and [0-9]. This introduces a performance hit.
- Both organizations and boards of Trello are considered as groups in the connector. Boards can be associated with organizations but organizations cannot be associated with boards.
- A board cannot be added under organization via group membership operations. Instead, board can be associated with the organization by providing the organization id while performing create or update operation.
- While performing the group membership operation, removal of membership of a user, whose credentials are used for the authorization of the connector, from the group (organization or board) , will not be executed because after removing membership, any operation on that particular group cannot be performed with these credentials, as the user is unauthorized.
- While performing group membership operation, removal of the membership of a user who is the only admin of the group (organization or board), is not possible as the group requires at least one admin.
- Group update or deletion of a group (organization or board) is not possible if the user whose credentials are used to authorize the connector is not the admin of the particular group.
- All users would be added as *normal* users for group membership management operations.
- While performing the update of an organization (group) with the short name and invalid id, Trello initially checks for the uniqueness of the short name and then checks for the existence of the id.
- All group memberships are of the users type.

- A board can only be associated with a single organization. Disassociation of a board from organization is not possible. Hence, the group membership does not support addition or removal of boards as a member of the organization.

IMPORTANT: Please note the important points below:

- If the Organization short name is available, it has to be unique.
- While creating a group (of type either organization or board), the user will be a member of the group by default, whose credentials are used for the connector authorization.
- The *type* property will not be returned as a group response. To differentiate the group type, the *id* of the group will be appended with *@o* or *@b* for organization type or board type respectively.
- While creating a group, it is necessary to provide a property *type* in group extension to differentiate the type of the group (organization or board) that is created. The *type* property takes values *o* or *b* for organization and board respectively. If the *type* is not provided, it will be assumed as *o*.

Statuspage

Statuspage is a status and incident communication tool that helps service providers keep customers and employees informed during downtime. It lets users add separate components for each part of the infrastructure or functional part of service.

Supervisor Configuration Parameters

To configure the connector, following parameters are required:

- Connector name
- API key (user API key under **Manage Account** → **API** tab) for the cloud account
- Organization Id (Organization Id under **Manage Account** → **API** tab) for the cloud account
- Target URL of the cloud account

Supported Objects and Operations

Users

Table 33: Supported operations for Users

Operation	VERB
Create User	POST
Delete User	DELETE

Groups

Not Applicable

Mandatory Fields

Users

- emails.value
- password

Groups

Not Applicable

Connector Limitations

- Update operation for **Users**, resource type **Groups** and **Pagination** are not supported.
- Retrieving a specific user would be relatively slow due to API limitations.

SAP Cloud Platform

SAP Cloud Platform is an open Platform as a Service (PaaS) that offers users in-memory capabilities, core platform services, and business services for cloud applications.

IMPORTANT: This connector is provided as a preview to the customers. The connector is not completely tested and may not function as expected with Active Roles.

Supervisor Configuration Parameters

To configure the connector, following parameters are required:

- Connector name
- Username
- Password
- SCIM URL

Supported Objects and Operations

Users

Table 34: Supported operations for Users

Operation	VERB
Create	POST
Update (Id)	PUT
Delete (Id)	DELETE
Get (Id)	GET
Get	GET
Pagination	GET

Groups

Table 35: Supported operations for Groups

Operation	VERB
Create	POST
Update (Id)	PUT
Delete (Id)	DELETE
Get (Id)	GET
Get	GET

Mandatory Fields

Users

- Email
- Username

Groups

- Group Name
- Display Name

Connector Limitations

- A performance impact is expected, with a list response of Groups because each record is retrieved and counted, since SCP Groups APIs do not provide *totalResults*.
- *ServiceProviderAuthority* contains only **Id** field with the same value as the tenant id of the SCP instance, as there are no APIs that can fetch the tenant details in SCP.
- *Get All Groups* and *Get particular group with ID* operations do not retrieve **Created** and **Last Modified** fields for Groups object types.

JIRA Server

JIRA Server is an issue-tracking product used for project management, generating project reports, and bug tracking.

Supervisor Configuration Parameters

To configure the connector, following parameters are required:

- Connector name
- Username
- Password
- SCIM URL

Supported Objects and Operations

Users

Table 36: Supported operations for Users

Operation	VERB
Remove/Provision	POST
Update (Id)	PUT
Delete (Id)	DELETE
Get (Id)	GET
Get All Users	GET
Pagination	GET

Groups

Table 37: Supported operations for Groups

Operation	VERB
Create	POST
Update (Id)	PUT
Delete (Id)	DELETE
Get (Id)	GET
Get All Groups	GET
Get Groups (Id)	GET

Roles

Table 38: Supported operations for Roles

Operation	VERB
Get All Roles	GET
Get Role (Id)	GET

Mandatory Fields

Users

- User name
- Display name
- Email ID

Groups

- Group Name

Connector Limitations

- The following dates are not available in User and Group resources.
 - **created**
 - **lastModified**
- Pagination is not supported for Groups.
- Update Group can only be used for membership management.
- Since the application does not support **id**, the URL encoded user name or group name is assigned as **id** for the resource.
- Leading slash (/) in **clientRequest**, in the **RequestWrapper** is restricted in REST Client (Eg: Postman) testing.
- Invalid host name in target URL returns error 500.

RSA Archer

RSA Archer GRC Platform supports business-level management of governance, risk management, and compliance (GRC). It lets users adapt solutions to their own requirements, build new applications, and integrate with external systems without interacting with code.

Supervisor Configuration Parameters

To configure the connector, following parameters are required:

- Connector Name - <RSA Archer>
- Username
- Password
- Instance Name - <Tenant ID ex: 324022>
- Profile Module ID - <Internal ID of an application as specified in the Application Builder Application Detail Report ex: 486>
- Profile ID - <User Profile ID ex: 239109>
- Environment(ISMS) - <Cloud application's environment ex: Test, Prod>
- Field ID - <Filed Id to get specific attribute ex: 18746>
- SCIM URL - <Cloud application's instance URL used as targetURI in payload>

Supported Objects and Operations

Users

Table 39: Supported operations for Users

Operation	VERB
Create	POST
Update	PUT
Delete (Id)	DELETE
Get (Id)	GET
Get	GET
Pagination	GET

Groups

Table 40: Supported operations for Groups

Operation	VERB
Create	POST
Update (Id)	PUT
Delete (Id)	DELETE
Get (Id)	GET
Get	GET

Mandatory Fields

Users

- First Name
- Last Name

Groups

- Group Name

Connector Limitations

- The **Created date** and **last modified date** is not retrieved for users / groups.
- Cursor based pagination for Users is supported but pagination is not supported for groups.
- User's contact information cannot be created or updated.
- The following fields are read-only:
 - Phone number
 - Email
- Except the 401 error for Unauthorized and 400 error for Bad Requests, the application returns HTTP status code 500 for all other errors.
- If members are provided in group **create/update** request, the member type is mandatory to differentiate between a user or a group member.
- RSA Archer ISMS Groups that are retrieved in the Standard GROUPS object type are read-only.

NOTE: Test Connection validates the target system credentials and endpoints but not the configuration parameters.

Dropbox

Dropbox offers secure file sharing and storage. It helps users manage sharing capabilities with groups and external collaborators through central folders with granular permissions.

Supervisor Configuration Parameters

To configure the connector, following parameters are required:

- Connector name
- API key (access token) for the cloud account

Supported Objects and Operations

Users

Table 41: Supported operations for Users

Operation	VERB
Create	POST
Update	PUT
Delete	DELETE
Get all users	GET
Get user by Id	GET
Get users with pagination	GET

Groups

Table 42: Supported operations for Groups

Operation	VERB
Create	POST
Update	PUT
Delete	DELETE
Get all groups	GET
Get group by Id	GET
Get groups with pagination	GET

Roles

Table 43: Supported operations for Roles

Operation	VERB
Get all roles	GET
Get role by Id	GET

Mandatory Fields

Users

- emails.value

Groups

- displayName

Connector Limitations

- The **LastModified** date is not applicable for Groups.
- Both **created** and **lastModified** dates are not applicable for Users.
- Invalid Target URL returns the below mentioned status code and error message.

- Status code: 500
- Error message: *There was an issue processing this request error.*
- User's role cannot be updated.
- The user cannot be set as active while performing **create** or **update**.
- The information about groups will not be present in the Create user response.
- The Dropbox user statuses *active* and *invited* are considered as active in the connector.
- APIs are not available to retrieve roles from Dropbox. Hence, the endpoints of the connector's roles provide predefined set of roles.
- Deleted members cannot be added to a group. In a request to add multiple members to a group, if any user is deleted (*members_not_in_team*), then the entire request is not executed.
- The *userName* property for user is read-only. However, this can be updated by updating the *emails → value*. The *emails → value* has been mapped against *userName*.
- Dropbox returns error 500 without any message being shown, on cursor pagination with cursor length equal to 1. The same is observed when trying to update a deleted group. In this case, the connector returns the following error code and message:
 - Error Code: 400
 - Error message: *Error occurred.*

Crowd

Crowd is a single sign-on software that lets your system administrator connect multiple applications to one user login and password. Users only need one user ID and password to access any connected platform.

Supervisor Configuration Parameters

To configure the connector, following parameters are required:

- Connector Name
- Username
- Password
- SCIM URL

Supported Objects and Operations

Users

Table 44: Supported operations for Users

Operation	VERB
Create	POST
Update	PUT
Delete	DELETE
Get All Users	GET
Get User by Id	GET
Get All Users with pagination	GET

Groups

Table 45: Supported operations for Groups

Operation	VERB
Create	POST
Update	PUT
Delete	DELETE
Get All Groups	GET
Get Group by Id	GET
Get All Groups with pagination	GET

Mandatory Fields

Users

- Username
- Password

Groups

- DisplayName

Connector Limitations

- Crowd application does not have the ID field for Users and Groups. User name is considered as the **userId**, and the group name is considered as **groupId**.
- Crowd cloud application does not have a created date and modified date for Groups.
- **UserName** and **GroupName** must be used as a single term as the usage is same for **userId** and **groupId**.
- **UserName** cannot be updated because it is used as an Id in cloud application.
- **DisplayName** of Groups cannot be updated as required by the cloud application.

AtlassianJC

AtlassianJC is a connector that links Atlassian software with Jira software. It gives teams the ability to manage projects and track development efforts in the cloud.

| **NOTE:** AtlassianJC supports the Jira software and Confluence.

Supervisor Configuration Parameters

To configure the connector, following parameters are required:

- Connector Name
- Username
- API Key
- SCIM URL (Cloud application's instance URL used as targetURI in payload)

Supported Objects and Operations

Users

Table 46: Supported operations for Users

Operation	VERB
Create	POST
Delete	DELETE
Get All Users	GET
Get (Id)	GET
Get All Users with pagination	GET

Groups

Table 47: Supported operations for Groups

Operation	VERB
Create	POST
Update	PUT
Delete	DELETE
Get All Groups	GET
Get (Id)	GET

Mandatory Fields

Users

- DisplayName
- Email Id

Groups

- DisplayName

Connector Limitations

- Cloud application does not support the **Created date** and **Modified date**.
- **Timezone**, **Active**, and **Locale** are readonly fields.
- Cloud application does not support the PUT operation for User objects.
- While trying to create a duplicate user, the cloud application returns an error with the status code 201. But the existing user is retrieved as the result.
- The Stride application is no longer part of Atlassian.
- Cloud application does not supports the *Get All groups with pagination* operation.
- The cloud application attributes for the cloud API URL is case-sensitive.

Pipedrive

Pipedrive is a cloud-based sales management tool offered on a web platform and as a mobile app.

Supervisor Configuration Parameters

To configure the connector, following parameters are required:

- Connector name
- API key
- SCIM URL (Cloud application's instance URL used as targetURL in payload)

Supported Objects and Operations

Users

Table 48: Supported operations for Users

Operation	VERB
Create	POST
Update	PUT
Delete	DELETE
Get user by Id	GET
Get all users	GET

Mandatory Fields

Users

- Emails.value
- DisplayName

Connector Limitations

- The **Groups** object type is not supported.
- Pagination is not supported.
- Deleted user object can be retrieved using *Get user by ID*.
- Creation of a duplicate user does not return an error. Instead, the existing object is returned.
- Deactivated or Deleted users can be deactivated or deleted multiple number of times.
- Deactivated or Deleted users can be activated again.
- The *Update* operation supports only the change of active flag field.

SuccessFactorsHR

SuccessFactorsHR is an integrated human-resources platform. It offers users tools for onboarding, social business, and collaboration along with tools for learning management, performance management, recruiting, applicant tracking, succession planning, talent management, and HR analytics. It is also cloud-based.

Supervisor Configuration Parameters

To configure the connector, following parameters are required:

- Connector Name
- Username
- Password
- SuccessFactorsHR instance URL
(<https://apps.support.sap.com/sap/support/knowledge/public/en/2215682>)
- Minimal Attributes

NOTE: The default value is **false**. When the value is set to **true**, only the minimal set of attributes for all the objects including Employee, Department, Location, CostCenter will be queried from the SuccessFactorsHR system.

Table 49: Minimal set of attributes for the objects

SuccessFactorsHR	Attributes
Location	externalCode, name, description, timezone, geozoneFlx, status
Employee	EmpJob attributes: userId, department, costCenter, businessUnit, location, division, startDate, endDate, managerId, jobTitle, contractType, company User attributes: userId, username,

SuccessFactorsHR	Attributes
	defaultFullName, hireDate, lastModified, status, department, location, firstName, lastName, mi, suffix, email, addressLine1, state, city, zipCode, country, businessPhone, cellPhone
Department	name, description, externalCode, status, parent
CostCenter	name, description, externalCode, status

Supported Objects and Operations

Users

Not Applicable

Groups

Not Applicable

Table 50: Department Mapping

SCIM Parameter	SuccessFactorsHR Parameter
DepartmentName	id
Description	description
ImportSource	sourceSystem
Remarks	status
ShortName	name
vrtCostCentersMapping	costCenter
vrtDepartmentHead	headOfUnit
vrtLocationsMapping	location

Table 51: Location Mapping

SCIM Parameter	SuccessFactorsHR Parameter
Building	externalCode
Description	description
Ident_locality	id
ImportSource	sourceSystem
LongName	name
Room	status
RoomRemarks	locationGroup

Connector Limitations

- **Create** and **Delete** operations are not supported for any object.
- Currently, the **Update** functionality is functional only for the following attributes of the Employee object:
 - cellPhone
 - businessPhone
 - email

Nutshell

Nutshell is a customer relationship management (CRM) service. It can be integrated with other SaaS services for small businesses, including Google Apps.

Supervisor Configuration Parameters

To configure the connector, following parameters are required:

- Connector name
- Username for the cloud account
- Password - API Key
- Target URL of the cloud account

Supported Objects and Operations

Users

Table 52: Supported operations for Users

Operation	VERB
Create	POST
Update	PUT
Delete	DELETE
Deprovision	PUT
Undo Deprovision	PUT

Groups

Table 53: Supported operations for Groups

Operation	VERB
Create	POST
Update	PUT
Delete	DELETE

Mandatory Fields

Users

- emails.value

Groups

- displayName

Connector Limitations

- Error messages and status codes are not customized. The following status codes are returned:
 - 200
 - 201
 - 204
 - 400
 - 401
 - 404
- Members cannot be added or retrieved from teams (groups) via the team endpoints. This can be achieved using the user endpoints and, updating the individual users. However, considering the large number of users in live production environments, membership management is not supported by the connector, as performance issues may arise.
- The delete operation is soft delete. Hence, it is possible to delete, or retrieve the deleted user or group multiple number of times. However, a deleted group will not be retrieved as part of the list groups response.

- Multiple email addresses can be associated to a user. Hence, the first email Id from the Nutshell user response is considered as the email id for the SCIM user.
- The NutShell API does not provide information on retrieval of all resources through paginated requests. Hence, the connector provides a *nextCursor* value, when the total resource count is divisible by requested count.

Insightly

Insightly provides customer relationship management software for small and midsize businesses. It can be integrated with other applications such as Box, Dropbox, Gmail, Outlook, and QuickBooks. Its dashboard lets users create custom reports and track projects.

Supervisor Configuration Parameters

To configure the connector, following parameters are required:

- Connector name
- API Key
- SCIM URL (Cloud application's instance URL, used as the target URL in payload)

Supported Objects and Operations

Users

Table 54: Supported operations for Users

Operation	VERB
Get user by Id	GET
Get all users	GET

Groups

Table 55: Supported operations for Groups

Operation	VERB
Create	POST
Update	PUT
Delete	DELETE
Get group by Id	GET
Get all groups	GET

Mandatory Fields

Users

- Creation of users is not supported.

Groups

- DisplayName

Connector Limitations

- Create, Update, and Delete operation (for Users) are not supported.
- During the process of creating or updating a group, if the member data is incorrect, the operation fails with *Bad request* status code.
- It is possible to create multiple groups with the same name in Insightly cloud application.

Egnyte

Egnyte lets users store files on either a company's existing data center infrastructure or in the cloud. It can be integrated with the cloud, storage, devices, and business applications to let you control data with your current hardware.

Supervisor Configuration Parameters

To configure the connector, following parameters are required:

- Connector name
- Client_Id (API Key provided for the application)
- Username
- Password
- Target URL (cloud application's instance URL used as target URL in payload)

To get the Client_id

1. Login to the Egnyte cloud application.
2. Register an application under **My API Keys** menu. Registered Application will have an API key that can be used as Client_Id.

Supported Objects and Operations

Users

Table 56: Supported operations for Users

Operation	VERB
Create	POST
Update	PUT

Operation	VERB
Delete	DELETE
Get user by Id	GET
Get all users	GET
Get all users with pagination	GET

Groups

Table 57: Supported operations for Groups

Operation	VERB
Create	POST
Update	PUT
Delete	DELETE
Get all groups	GET
Get all groups with pagination	GET

Mandatory Fields

Users

- userName
- emails.value
- name.givenName
- name.familyName
- EnterpriseExtension.authType
- userType
- active

Groups

- displayName

Connector Limitations

- The Role object type is not supported by cloud application for trial account. Hence, the connector does not support the role endpoint.

SugarCRM

SugarCRM is a customer relationship management (CRM) system. It allows users to manage sales-force automation, marketing campaigns, customer support, collaboration, mobile CRM, social CRM, and reporting.

Supervisor Configuration Parameters

To configure the connector, following parameters are required:

- Connector name
- Client Id
- Client Secret
- Username
- Password
- Platform
- Target URL (cloud application's instance URL used as target URL in payload)

Supported Objects and Operations

Users

Table 58: Supported operations for Users

Operation	VERB
Create	POST
Update	PUT
Delete	DELETE
Deprovision	PUT
Undo Deprovision	PUT

Groups

Table 59: Supported operations for Groups

Operation	VERB
Create	POST
Update	PUT
Delete	DELETE

Mandatory Fields

Users

- UserName

Groups

- Not Applicable

Connector Limitations

- Creation of a duplicate user returns the following status code:
 - 403:Forbidden
- A CRUD operation on Users and Groups can be performed only by users with Admin credentials.
- Multiple groups can be created with same name.
- Group memberships cannot be added, retrieved, or modified using API calls.
- Cloud application allows creation of a group without the *Name* being specified.

Oracle IDCS

Oracle IDCS is a cloud-based identity management service that integrates with existing systems and directories. Users can develop, access and deploy their applications from one platform. It works with both cloud and on-premises applications.

Supervisor Configuration Parameters

To configure the connector, following parameters are required:

- Connector name
- Client Id for the trusted app
- Client Secret of the trusted app (see https://docs.oracle.com/en/cloud/paas/identity-cloud/rest-api/OATOAuthClientWebApp.html#GUID-51E5C29A-6B7E-487A-8832-5D709410C16A__RegisterAnOAuthClientWebApplication-29DDFF36 for more details).
- Target URL (Cloud application's instance URL used as target URI in payload - Example: `https://{tenant-base-url}/admin/v1`)

Supported Objects and Operations

Users

Table 60: Supported operations for Users

Operation	VERB
Create	POST
Update	PUT
Delete	DELETE

Operation	VERB
Get all users	GET
Get user by id	GET
Get users with Pagination	GET

Groups

Table 61: Supported operations for Groups

Operation	VERB
Create	POST
Update	PUT
Delete	DELETE
Get	GET
Get	GET

Mandatory Fields

Users

- userName
- emails.value
- name.familyName

Groups

- displayName

Connector Limitations

- Oracle IDCS does not validate the values provided for the **roles** in the user request and the same is getting assigned to the user. No validation is performed for the **type**, **value** properties for the **roles**. Same is the case with **entitlements**.
- Groups will not be returned with the create user response.
- Sub-Groups cannot be added in Group Memberships.

Zendesk Sell

Zendesk Sell provides a web-based sales platform with tools for emailing, phone dialing, pipeline management, forecasting, and reporting.

Supervisor Configuration Parameters

To configure the connector, following parameters are required:

- Connector name
- API Key
- Target URL (Cloud application's instance URL used as targetURI in payload)

Supported Objects and Operations

Users

Not Applicable

Groups

Not Applicable

Mandatory Fields

Users

Not Applicable

Groups

Not Applicable

Connector Limitations

- **Create**, **Update**, and **Delete** users are not supported by Zendesk Sell connector.
- The resultant (User) objects count of pagination is always in the multiples of 100, unless cloud has less than 100 records in a page.

Workbooks

Workbooks is a cloud-based CRM and business application for users in sales, marketing, and customer support. It also offers services for order management and fulfillment, invoicing, and supplier management.

Supervisor Configuration Parameters

To configure the connector, following parameters are required:

- Connector name
- API key for the cloud account (obtained from Start > Configuration > Email & Integration > API Keys in Workbooks Desktop instance)
- Target URL of the cloud account

Supported Objects and Operations

Users

Not Applicable

Groups

Not Applicable

Mandatory Fields

Users

Not Applicable

Groups

Not Applicable

Connector Limitations

- **Create, Update, and Delete** users are not supported.
- Groups and group memberships are not supported through APIs.
- Username is available only for the activated users.
- **Get All Users** retrieves automation users that are not listed in the users list in Workbooks user interface. The automation users are created while generating the first API key of type **automation** in Workbooks Desktop instance.
- The application returns the user details instead of 404 error though the user id is appended with alphabetic characters.

DocuSign

DocuSign allows users to manage digital transactions for electronic documents including contracts and signatures. Its features include authentication services, user identity management, and workflow automation.

Supervisor Configuration Parameters

To configure the connector, following parameters are required:

- Connector name
- Client Id
- User Name
- Password
- Account ID
- Target URL (Cloud application's instance URL used as targetURI in payload)

Supported Objects and Operations

Users

Table 62: Supported operations for Users

Operation	VERB
Create User	POST
Update User	PUT
Delete User	DELETE

Groups

Table 63: Supported operations for Groups

Operation	VERB
Create Group	POST
Update Group	PUT
Delete Group	DELETE
Deprovision	PUT
Undo Deprovision	PUT
Update Membership	PUT

Mandatory Fields

Users

- UserName
- Email

Groups

- DisplayName

Connector Limitations

- Username update is accepted only when no first and last name provided.
- Add and update of Users address not supported.
- Intermittently, you cannot update the users when the activation is in pending status.
- Active user cannot be created. After the created user activates the account through the email link, the user is considered to be an Active user.
- Combination of user name and email duplication will result in conflict error response.

ShareFile

ShareFile offers users a platform for secure content collaboration, file sharing, and synchronization for documents and workflows. It offers cloud-based and on-premises storage, virtual data rooms, and client portals.

Supervisor Configuration Parameters

To configure the connector, following parameters are required:

- Connector name
- UserName
- Password
- Client_Id
- Client_Secret
- Target URL (Cloud application's instance URL used as targetURI in payload)

Supported Objects and Operations

Users

Table 64: Supported operations for Users

Operation	VERB
Create User	POST
Update User	PATCH
Delete User	DELETE
Get User	GET
Get All Users	GET

Groups

Table 65: Supported operations for Groups

Operation	VERB
Create Group	POST
Update Group	PATCH
Delete Group	DELETE
Add Group Members	POST
Remove Group Members	DELETE
Deprovision	PUT
Undo Deprovision	PUT

Mandatory Fields

Users

- emails.value
- name.familyName
- name.givenName

Groups

Not Applicable

Connector Limitations

- Pagination is not supported by cloud application for both **Users** and **Groups** object
- Group Information such as, the groups to which the user is associated is not displayed when we retrieve **Users** object.
- Only 5 users can be created for trial instance on the Cloud Application.
- Email id is considered as your user name. To update the username, you should update the email id.
- **Last modified date** is not supported by the Cloud application for **User** object.
- **Last Modified** and **Created** date is not supported by the Cloud application for **Group** object.

- Deleted users can be retrieved as the Cloud application supports soft delete of users.
- Deleted user can be updated though the **User Id**.
- Group membership operation can be ignored when you have an invalid **User Id** in the members list.

Zendesk

Zendesk is a unified customer service platform. It features a common user interface, single login, and a platform for sharing customer data.

Supervisor Configuration Parameters

To configure the connector, following parameters are required:

- Connector name
- User Name
- Password
- Target URL (Cloud application's instance URL used as targetURI in payload)

Supported Objects and Operations

Users

Table 66: Supported operations for Users

Operation	VERB
Create User	POST
Update User	PUT
Delete User	DELETE
Deprovision	PUT
Undo Deprovision	PUT

Groups

Table 67: Supported operations for Users

Operation	VERB
Create Group	POST
Update Group	PUT
Delete Group	DELETE
Deprovision	PUT
Undo Deprovision	PUT
Update Membership	PUT

Mandatory Fields

Users

- DisplayName
- Email

Groups

DisplayName

Connector Limitations

- A user with **Agent** role only can be added to group membership.
- Get resource by pagination will always return the resources in multiples of hundred. For example, if the count is specified as 126, 200 records are returned.
- If any value for **startIndex** is passed when using get resources by pagination parameter, the result from the connector is always the nearest 100 records from the requested number.
- Users can be deleted multiple times as the cloud application supports soft delete.

G Suite

G Suite is a cloud computing, productivity, and collaboration tool. It includes the Google web applications Gmail, Drive, Hangouts, Calendar, and Docs. It also includes an interactive whiteboard. The enterprise version offers custom-domain email addresses, additional storage, and 24/7 phone and email support.

You must create a service account to access the G Suite services. For information on creating a service account, see [Creating a service account in G Suite](#).

Supervisor Configuration Parameters

To configure the connector, following parameters are required:

- Connector name
- UserName
- Private_Key (Whole JSON content of private key file created for service account)
- Target URL (Cloud application's instance URL used as targetURI in payload)

Supported Objects and Operations

Users

Table 68: Supported operations for Users

Operation	VERB
Create User	POST
Update User	PUT
Delete User	DELETE
Deprovision	PUT
Undo Deprovision	PUT

Groups

Table 69: Supported operations for Groups

Operation	VERB
Create Group	POST
Update Group	PUT
Delete Group	DELETE
Deprovision	PUT
Undo Deprovision	PUT
Update Membership	PUT

Mandatory Fields

Users

- FirstName
- LastName
- Password

Groups

Email

Connector Limitations

- Connector supports cursor based pagination even with any change at count in subsequent requests.
- **Created date** is displayed for **Users**. **Created date** and **Modified date** are not displayed for **Groups**.
- Group information of user is not displayed in user details.
- The **Email ID** of **Users** and **Groups** to be created should be provided along with the domain name of target instance.

Concur

Concur offers two on-demand Software as a Service (SaaS) products to help manage travel. Concur Travel & Expense gives you web and mobile solutions for travel and expense management, and TripIt is a mobile travel organizer for individuals.

Supervisor Configuration Parameters

To configure the connector, following parameters are required:

- Connector name
- Client Id
- Client Secret
- Username
- Password
- Geolocation
- Target URL (Cloud application's instance URL used as targetURI in payload)

Supported Objects and Operations

Users

Table 70: Supported operations for Users

Operation	VERB
Create User	POST
Update User	POST
Delete User	DELETE
Get User	GET

Operation	VERB
Get All Users	GET
Get All Users with Pagination	GET

Groups

NA

Mandatory Fields

Users

- userName
- name.givenName
- name.familyName
- enterpriseUserExtension.empId
- emails.value
- password
- scimUser.locale
- enterpriseUserExtension.ctrCode
- enterpriseUserExtension.crnKey
- enterpriseUserExtension.ledgerKey
- enterpriseUserExtension.custom21

Groups

NA

Connector Limitations

- Only user end-points are supported in Concur connector.
- Inactive user's information is not displayed when **Get All Users** operation is performed.
- The search result status for inactive user is **NotFound**.

- While **Get Users by Pagination** with **StartIndex** and **count** specified, next nearest multiple of 100 records to the **count** value are fetched.
- Invalid **Geolocation** url returns **BadRequest** status.
- **Created** and **LastModified** dates are not supported.
- API does not return the details of groups to which a user is associated.
- **POST** user with the details similar to that of existing user's id, email and EmpId will update existing user's information. In such case, status code 201 is returned.
- Inactive user cannot be created or edited.
- **GivenName** and **FamilyName** are not updated in **PUT** user operation.
- Custom21 value accepts only the Expense list code. For example, a valid Custom21 value are IN - 890, IN - 562, AU - 510, NL - 842, NO - 432, and so on.
- Currently, an authentication related issue is observed while **Get User** by Id for a user "cteadmin@quest.com". This issue causes integration failure. To fix this, two keys are introduced in **AppSettings** of function host named **ShouldExcludeUsers** and **ExcludeUserIds**.
- **ShouldExcludeUsers** key accepts either true or false as value, and **ExcludeUserIds** takes comma separated user's ids.
- If value for **ShouldExcludeUsers** is true, the user ids mentioned in **ExcludeUserIds** will not appear in GetAll Users response.

Tableau

Tableau offers data visualization software to let users upload files to a server or the cloud. You can create custom dashboards to analyze business intelligence and data.

Supervisor Configuration Parameters

To configure the connector, following parameters are required:

- Connector name
- Username
- Password
- Site name (Example: <https://online.tableau.com/#/site/MarketingTeam/users>)
- Target URL (Cloud application's instance URL used as target URI in payload - Example: <https://{instance-name}.online.tableau.com/api/{api-version}>)

Supported Objects and Operations

Users

Table 71: Supported operations for Users

Operation	VERB
Create User	POST
Update User	PUT
Delete User	DELETE
Deprovision	PUT
Undo Deprovision	PUT

Groups

Table 72: Supported operations for Groups

Operation	VERB
Create Group	POST
Update Group	PUT
Deprovision	PUT
Undo Deprovision	PUT
Update Membership	PUT

Mandatory Fields

Users

Email

Groups

displayName

Connector Limitations

- User update is supported for **User** role only.
- **Created** and **last modified** dates are not available.
- Group deletion is not supported.
- Adding or removing a member from a renamed group is possible only after a full synchronization .

GoToMeeting

GoToMeeting is an online tool for meeting planning. The connector integrates with multiple other products and plug-ins, allowing users to easily connect to create, organize, and host meetings across a common platform.

For more information on generating a private key for a service account, see [Generating a private key in GoToMeeting](#).

Supervisor Configuration Parameters

To configure the connector, following parameters are required:

- Connector name
- Username
- Password
- Client Id
- Client Secret
- Account key
- Target URL (Cloud application's instance URL used as target URI in payload - Example: <https://api.getgo.com/admin/rest/v1/>)

Supported Objects and Operations

Users

Table 73: Supported operations for Users

Operation	VERB
Create User	POST

Operation	VERB
Update User	PUT
Delete User	DELETE
Deprovision	PUT
Undo Deprovision	PUT

Groups

Table 74: Supported operations for Groups

Operation	VERB
Create Group	POST
Update Group	PUT
Delete Group	DELETE

Mandatory Fields

Users

- Email
- givenName
- familyName

Groups

displayName

Connector Limitations

- For **Users** and **Groups** objects, the **Created** and **Last Modified** date are not displayed.
- When trying to create a duplicate entry of the user who already exists, the connector returns status code 201.
- Group membership operation is not supported.
- When trying to retrieve a user by their ID using invalid alphanumeric IDs, the connector returns status code 502 instead of 404.

- When trying to create a new user with the same email ID of a deleted user, the connector activates the deleted user instead of creating a new user.

Coupa

A **Coupa** connector allows users to move data in and out of Coupa. It lets you manage spend more efficiently by being able to integrate and access spend management and data for expenses, and integrate with other cloud applications.

Supervisor Configuration Parameters

To configure the connector, the following parameters are required:

- Connector name
- API key
- Target URL (Cloud application's instance URL used as target URI in payload)

Supported Objects and Operations

Users

Table 75: Supported operations for Users

Operation	VERB
Create User	POST
Update User	PUT
Deprovision	PUT
Undo Deprovision	PUT

Mandatory Fields

Users

- Username
- Email
- FirstName
- LastName

Groups

NA

Connector Limitations

- Total results are not supported due to cloud application limitations.
- The target application supports soft delete of users. The deleted users are returned in **GET** and **GET All**. The users can also be deleted repeatedly.
- **Account-Groups** will not work as of now. It will work when the Coupa team shares the source of information.
- **Approval-Groups** will not work as of now. It will work when the new endpoint is implemented.
- **User-Groups** will not work as of now. It will work when the new endpoint is implemented.

AWS Cognito

AWS Cognito is a connector from Amazon Web Services that helps developers build web and mobile apps that are more secure. It helps to better authenticate users. It also handles user data, including passwords, token-based authentication, scalability, permissions, and so on.

Supervisor Configuration Parameters

To configure the connector, following parameters are required:

- Connector name
- AccessKey Id
- Access Secret
- Region
- User Pool Id
- Target URL (Cloud application's instance URL used as target URI in payload)

Supported Objects and Operations

Users

Table 76: Supported operations for Users

Operation	VERB
Create User	POST
Update User	PUT
Delete User	DELETE

Groups

Table 77: Supported operations for Groups

Operation	VERB
Create Group	POST
Update Group	PUT
Delete Group	DELETE
Deprovision	PUT
Undo Deprovision	PUT
Update Membership	PUT

Mandatory Fields

Users

- Username
- Email

Groups

DisplayName

Connector Limitations

- Creating or updating the User or a Group executes in multiple steps. Failure in any step is reported as a complete failure of operation. However, the record is persisted until succeeded steps.
- Noncompliance to password policy returns an error. However, an User is created.
- **DesiredDeliveredMedium** is write only property. By default, SMS is the default option and it is not returned in **Get specific user** response.
- A User can be a member of a maximum of 25 groups.

Okta

Okta provides cloud software that helps companies manage and secure user authentication into modern applications, and for developers to build identity controls into applications, website web services and into devices.

Supervisor configuration parameters

To configure the connector, following parameters are required:

- Connector name
- Token
- Target URL (Cloud application's instance URL used as targetURI in payload)

Supported objects and operations

Users

Table 78: Supported operations for Users

Operation	VERB
Create User	POST
Update User	PUT
Delete User	DELETE

Groups

Table 79: Supported operations for Groups

Operation	VERB
Create Group	POST
Update Group	PUT
Delete Group	DELETE
Create Membership	POST
Add Membership	POST
Delete Membership	DELETE

Mandatory fields

Users

- GivenName
- FamilyName
- Username
- Email
- Password

Groups

- DisplayName

User and Group mapping

The user and group mappings are listed in the tables below.

Table 80: User mapping

SCIM parameter	Okta parameter
Id	id
UserName	login
DisplayName	displayName

SCIM parameter	Okta parameter
NickName	nickName
Name.GivenName	firstName
Name.FamilyName	lastName
Name.MiddleName	middleName
Name.HonorificPrefix	honorificPrefix
Name.HonorificSuffix	honorificSuffix
Addresses.StreetAddress	streetAddress
Addresses.Locality	city
Addresses.Region	state
Addresses.PostalCode	zipCode
Addresses.Country	countryCode
Emails.value	email
PhoneNumbers.value	primaryPhone
UserType	userType
Title	title
PreferredLanguage	preferredLanguage
Locale	locale
Timezone	timezone
Groups[].value (On Demand)	Id (groupsForUserResponse)
Groups[].display (On Demand)	Profile.name (groupsForUserResponse)
Active	status == "ACTIVE"
Extension.EmployeeNumber	employeeNumber
Extension.Division	division
Extension.Department	department
Extension.CostCenter	costCenter
Extension.Organization	organization
Extension.Manager.value	managerId
Extension.Manager.DisplayName	manager
Meta.Created	created
Meta.LastModified	lastUpdated

Groups

Table 81: Group mapping

SCIM parameter	Okta parameter
Id	id
displayName	profile.name
Extension.Description	profile.description
Members[].value	id (GetGroupMembersResponse[])
Members[].display	profile.displayName (GetGroupMembersResponse[])
Meta.Created	created
Meta.LastModified	lastUpdated

Connector limitations

- **Get Users** and **Groups** by pagination will return resources in multiples of 100. The **resource count** will be same as the next nearest multiple of 100. For example, if the count is specified as 325, the resource count will be 400.
- **Disabled User** can be still be fetched.
- Password update is not possible through the connector since it expects old and new passwords as parameter. Old password can never be fetched for any user.
- Username should be in the format of **email id**.
- When you delete a user for the first time, the user will be deactivated. When you delete the user for the second time, the user will be deleted permanently from target system.
- When you modify the email value, both the **username** and **email** values get updated. But when you modify the username alone, only the username gets updated with the username value.

DataDog

DataDog is a monitoring service for cloud-scale applications. It provides monitoring services for monitoring servers, databases, tools, and services, using a SaaS-based data analytics platform.

Supervisor configuration parameters

To configure the connector, following parameters are required:

- Connector name
- API Key
- Application Key
- SCIM URL (Cloud application's REST API's base URL)

Supported objects and operations

Users

Table 82: Supported operations for Users

Operation	VERB
Create User	POST
Update User	PUT
Delete User	DELETE
Get User by id	GET
Get All Users	GET

Mandatory field

Users

- email (email_Id)

User mapping

The user mappings are listed in the tables below.

Table 83: User mapping

SCIM parameter	DataDog parameter
Id	handle
UserName	email
Name.Formatted	name
DisplayName	name
Emails[].Value	email
Roles[].Value	access_role
Roles[].Display	roles[].name
Active	disabled

Connector limitations

- The email ID of users cannot be updated.
- You cannot create duplicate users. When you try to create a duplicate user, you do not get any warning message.
- The list of roles for the connector require timely update according to the changes at the target system.
- The creation of an user with administration access role requires administrators application key.
- Users are created with DataDog Standard role by default if it is not specified in the request.
- Test Connectivity may display 502 Bad Gateway error inconsistently, due to cloud application behavior.

Hideez

Hideez Group is a US based office development company that manufactures wireless multifunctional security key class electronic devices.

Supervisor configuration parameters

To configure the connector, following parameters are required:

- Connector name
- Username
- Password
- Target URL

Supported objects and operations

AccessProfile

Table 84: Supported operations for AccessProfile

Operation	VERB
Create AccessProfile	POST
Update AccessProfile	PUT
Delete AccessProfile	DELETE
Get AccessProfile	GET
Get All AccessProfiles	GET

Companies

Table 85: Supported operations for Companies

Operation	VERB
Create Company	POST
Update Company	PUT
Delete Company	DELETE
Get Company	GET
Get All Companies	GET

Departments

Table 86: Supported operations for Departments

Operation	VERB
Create Department	POST
Update Department	PUT
Delete Department	DELETE
Get Department	GET
Get All Departments	GET

Devices

Table 87: Supported operations for Devices

Operation	VERB
Update Devices	PUT
Get Devices	GET
Get All Devices	GET

Positions

Table 88: Supported operations for Positions

Operation	VERB
Create Positions	POST
Update Positions	PUT
Delete Positions	DELETE
Get Positions	GET
Get All Positions	GET

Workstations

Table 89: Supported operations for Workstations

Operation	VERB
Update Workstation	PUT
Get Workstation	GET
Get All Workstations	GET

Employees

Table 90: Supported operations for Employees

Operation	VERB
Create Employee	POST
Update Employee	PUT
Delete Employee	DELETE
Get Employee	GET
Get All Employees	GET

Mandatory fields

This section lists the mandatory fields required to create a resource type.

AccessProfiles

Table 91: Mandatory feilds for AccessProfiles

Attribute name	Mandatory	Can be updated
Name	Yes	Yes
PinLength	Yes	Yes
PinTryCount	Yes	Yes
PinExpiration	Yes	Yes
buttonBonding	No	Yes
buttonConnection	No	Yes
buttonNewChannel	No	Yes
pinNewChannel	No	Yes
masterKeyConnection	No	Yes
masterKeyNewChannel	No	Yes

Companies

- Name

Departments

- Name
- CompanyId

Devices (Update)

- RFIId

Positions

- Name

Workstations (Update)

- DepartmentId
- RFIId

Employees

- FirstName
- LastName
- Email
- DepartmentId
- PositionId

Mappings

The mappings are listed in the tables below.

Table 92: Employee mapping

SCIM parameter	Hideez parameter
Id	id
UserName	UserName
firstName	firstName
lastName	lastName
email	email
phoneNumber	phoneNumber
departmentId	departmentId
positionId	positionId
device.id	device.id
device.mac	device.mac
device.model	device.model
device.rfid	device.rfid
device.mac	device.mac
device.model	device.model
device.rfid	device.rfid
device.batterydevice.battery	device.batterydevice.battery
device.firmware	deviceirmware
device.state	device.state

SCIM parameter	Hideez parameter
device.lastSynced	device.lastSynced
device.employeeId	device.employeeId
device.primaryAccountId	device.primaryAccountId
device.acceessProfileId	device.acceessProfileId
device.masterPassword	device.masterPassword
device.importedAt	device.importedAt
device.isOnline	device.isOnline
device.deviceAccessProfile.Id	device.deviceAccessProfile.Id
device.deviceAccessProfile. name	device.deviceAccessProfile. name
device.deviceAccessProfile.createdAt	device.deviceAccessProfile. createdAt
device.deviceAccessProfile. updatedAt	device.deviceAccessProfile. updatedAt
device.deviceAccessProfile. buttonBonding	device.deviceAccessProfile. buttonBonding
device.deviceAccessProfile. buttonCon- nection	device.deviceAccessProfile. buttonCon- nection
device.deviceAccessProfile. buttonNewChannel	device.deviceAccessProfile. buttonNewChannel
device.deviceAccessProfile. pinBonding	device.deviceAccessProfile. pinBonding
device.deviceAccessProfile.pinConnection	device.deviceAccessProfile.buttonConnecti on
device.deviceAccessProfile.pinNewChannel	device.deviceAccessProfile.buttonNewChan nel
device.deviceAccessProfile.masterKeyBond ing	device.deviceAccessProfile.pinBonding
device.deviceAccessProfile.masterKeyConn ection	device.deviceAccessProfile.pinConnection
device.deviceAccessProfile.masterKeyNew Channel	device.deviceAccessProfile.pinNewChannel
device.deviceAccessProfile.pinExpiration	device.deviceAccessProfile.pinExpiration
device.deviceAccessProfile.pinLength	device.deviceAccessProfile.pinLength
device.deviceAccessProfile.pinTryCount	device.deviceAccessProfile.pinTryCount
device.deviceAccessProfile.pinExpirationCo nverted	device.deviceAccessProfile.pinExpirationCo nverted

SCIM parameter	Hideez parameter
device.deviceAccessProfile.pinExpirationString	device.deviceAccessProfile.pinExpirationString
department.Id	department.Id
department.companyId	department.companyId
department.name	department.name
department.company.id	department.company.id
department.company.name	department.company.name
position.id	position.id
position.name	position.name
fullName	fullName
empCompany	empCompany
empDepartment	empDepartment
currentDevice	currentDevice

Table 93: AccessProfile mapping

SCIM parameter	Hideez parameter
Id	Id
name	name
createdAt	createdAt
updatedAt	updatedAt
buttonBonding	buttonBonding
buttonConnection	buttonConnection
buttonNewChannel	buttonNewChannel
pinBonding	pinBonding
pinConnection	pinConnection
pinNewChannel	pinNewChannel
masterKeyBonding	masterKeyBonding
masterKeyConnection	masterKeyConnection
masterKeyNewChannel	masterKeyNewChannel

SCIM parameter	Hideez parameter
pinExpiration	pinExpiration
pinLength	pinLength
pinTryCount	pinTryCount
pinExpirationConverted	pinExpirationConverted
pinExpirationString	pinExpirationString
device.id	device.id
device.mac	device.mac
device.model	device.model
device.rfid	device.rfid
device.battery	device.battery
device.firmware	device.firmware
device.battery	device.battery
device.state	device.state
device.lastSynced	device.lastSynced
device.employeeId	device.employeeId
device.primaryAccountId	device.primaryAccountId
device.acceessProfileId	device.acceessProfileId
device.masterPassword	device.masterPassword
device.importedAt	device.importedAt
device.isOnline	device.isOnline

Table 94: Company mapping

SCIM parameter	Hideez parameter
id	id
name	name

Table 95: Department mapping

SCIM parameter	Hideez parameter
Id	Id
companyId	companyId
name	name
company.id	company.id
company.name	company.name

Table 96: Device mapping

SCIM parameter	Hideez parameter
Id	Id
mac	mac
model	model
rfid	rfid
battery	battery
firmware	firmware
state	state
lastSynced	lastSynced
employeeId	employeeId
primaryAccountId	primaryAccountId
acceessProfileId	acceessProfileId
masterPassword	masterPassword
importedAt	importedAt
isOnline	isOnline
deviceAccessProfile.Id	deviceAccessProfile.Id
deviceAccessProfile.name	deviceAccessProfile.name
deviceAccessProfile.createdAt	deviceAccessProfile.createdAt
deviceAccessProfile.updatedAt	deviceAccessProfile.updatedAt
deviceAccessProfile.buttonBonding	deviceAccessProfile.buttonBonding
deviceAccessProfile.buttonConnection	deviceAccessProfile.buttonConnection

SCIM parameter	Hideez parameter
deviceAccessProfile.buttonNewChannel	deviceAccessProfile.buttonNewChannel
deviceAccessProfile.pinBonding	deviceAccessProfile.pinBonding
deviceAccessProfile.pinConnection	deviceAccessProfile.pinConnection
deviceAccessProfile.pinNewChannel	deviceAccessProfile.pinNewChannel
deviceAccessProfile.masterKeyBonding	deviceAccessProfile.masterKeyBonding
deviceAccessProfile.masterKeyConnection	deviceAccessProfile.masterKeyConnection
deviceAccessProfile.masterKeyNewChannel	deviceAccessProfile.masterKeyNewChannel
deviceAccessProfile.pinExpiration	deviceAccessProfile.pinExpiration
deviceAccessProfile.pinLength	deviceAccessProfile.pinLength
deviceAccessProfile.pinTryCount	deviceAccessProfile.pinTryCount
deviceAccessProfile.pinExpirationConverted	deviceAccessProfile.pinExpirationConverted
deviceAccessProfile.pinExpirationString	deviceAccessProfile.pinExpirationString

Table 97: Position mapping

SCIM parameter	Hideez parameter
id	id
name	name

Table 98: Workstation mapping

SCIM parameter	Hideez parameter
Id	Id
name	name
domain	domain
clientVersion	clientVersion
departmentId	departmentId
departmentName	departmentName
os	os
ip	ip
lastSeen	lastSeen

SCIM parameter	Hideez parameter
approved	approved
rfid	rfid
companyId	companyId
companyName	department.company.name
proximityDevices[].Id	proximityDevices[].Id
proximityDevices[].deviceId	proximityDevices[].deviceId
proximityDevices[].workstationId	proximityDevices[].workstationId
proximityDevices[].lockProximity	proximityDevices[].lockProximity
proximityDevices[].unlockProximity	proximityDevices[].unlockProximity
proximityDevices[].lockTimeout	proximityDevices[].lockTimeout

Connector limitations

You cannot edit an unapproved workstation. You can only edit approved workstations.

One Identity Manager E2E integration needs

For more information, see [One Identity Manager E2E integration needs for Hideez connector](#).

Opsgenie

Opsgenie is a modern incident management platform for operating always-on services, empowering Dev & Ops teams to plan for service disruptions and stay in control during incidents. With over 200 deep integrations and a highly flexible rules engine, Opsgenie centralizes alerts, notifies the right people reliably, and enables them to collaborate and take rapid action. Throughout the entire incident lifecycle, Opsgenie tracks all activity and provides actionable insights to improve productivity and drive continuous operational efficiencies.

Supervisor configuration parameters

To configure the connector, following parameters are required:

- Connector name
- API
- Target URL (Cloud application's instance URL used as target URI in payload - Example: <https://api.opsgenie.com/v2> and for EU region it will be <https://api.eu.opsgenie.com/v2>)

Supported objects and operations

Users

Table 99: Supported operations for Users

Operation	VERB
Create User	POST
Get User	GET
Get Users	GET

Operation	VERB
Update User	PUT
Delete User	DELETE

Groups

Table 100: Supported operations for Groups

Operation	VERB
Create Group	POST
Get Group	GET
Get Groups	GET
Update Group	PUT
Delete Group	DELETE

Roles

Table 101: Supported operations for Roles

Operation	VERB
Get custom user role	GET
Get custom user roles	GET

Mandatory fields

This section lists the mandatory fields required to create a **User** or **Group**.

Users

- emails[].value
- displayName

Groups

- displayName

Mappings

The mappings are listed in the tables below.

Users

Table 102: User mapping

SCIM parameter	Opsgenie parameter
id	id
username	userName
fullName	name.formatted
fullName	displayName
username	emails[0].value
userAddress.line	addresses[].streetAddress
userAddress.city	addresses[].locality
userAddress.state	addresses[].region
userAddress.zipCode	addresses[].postalCode
userAddress.country	addresses[].country
blocked	active
locale	locale
timeZone	timezone
role.id	roles[].value
user teams[].id	groups[].value
skypeUsername	userExtension.skypeUsername
createdAt	meta.created

Groups

Table 103: Group mapping

SCIM parameter	Opsgenie parameter
id	id
name	displayName

SCIM parameter	Opsgenie parameter
members[]user.id	members[].value
description	extension.description
createdAt	meta.created

Connector limitations

- When you update an user, the updated emailID will not be retrieved until it is verified by the user.
- When you create or update a Group, you can use only dots, dashes and underscores for Group names.

Informatica Cloud Services

Informatica Cloud Services deliver purpose-built data integration cloud applications that allow business users to integrate data across cloud-based applications and on-premise systems and databases. **Informatica Cloud Services** address specific business processes and point-to-point data integration.

Supervisor configuration parameters

To configure the connector, following parameters are required:

- Connector name
- Username
- Password
- Target URL (The URL of the login page of the **Informatica Cloud Service** account. For example: <https://dm-ap.informaticacloud.com/ma/home>)

Supported objects and operations

Users

Table 104: Supported operations for Users

Operation	VERB
Create User	POST
Get User	GET
Get all Users	GET
Delete User	DELETE

Groups

Table 105: Supported operations for Groups

Operation	VERB
Create Group	POST
Get Group	GET
Get all Groups	GET
Delete Group	DELETE

Roles

Table 106: Supported operations for Roles

Operation	VERB
Get all roles	GET
Get role	GET

Mandatory fields

This section lists the mandatory fields required to create a User or Group:

Users

- userName
- name.givenName
- name.familyName
- emails[].value
- entitlements[].value

NOTE: The first available entitlement from the target system would be assigned to **entitlements[].value** if the property is not provided in the SCIM request. The entitlement property is **Roles** from the target system.

Groups

- displayName
- entitlements[].value

NOTE: The first available entitlement from the target system would be assigned to **entitlements[].value** if the property is not provided in the SCIM request. The entitlement property is **Roles** from the target system.

Mappings

The user and group mappings are listed in the tables below.

Table 107: User mapping

SCIM Parameter	Informatica parameter
id	id
userName	userName
lastName	name.familyName
firstName lastName	name.formatted
firstName lastName	displayName
email	emails[0].value
title	title
state	active
locale	locale
timeZoneId	timezone
roles[].id	roles[].value
roles[].roleName	roles[].display
groups[].id	groups[].value
groups[].userGroupName	groups[].display
orgId	userExtension.orgId
description	userExtension.description
authentication	userExtension.authentication
forcePasswordChange	userExtension.forcePasswordChange
maxLoginAttempts	userExtension.maxLoginAttempts
createTime	meta.created
updateTime	meta.lastModified

Groups

Table 108: Group mapping

SCIM parameter	Informatica parameter
id	id
userGroupName	displayName
users[].id	members[].value
users[].userName	members[].display
roles[].id	roles[].value
roles[].roleName	roles[].display
orgId	userExtension.orgId
description	extension.description
createTime	meta.created
updateTime	meta.lastModified

Roles

Table 109: Roles mapping

SCIM parameter	Informatica parameter
id	id
name	roleName

Connector limitations

- The connector does not support update operation for users and groups as the target cloud system does not support update operation for users and groups.
- Target system roles are mapped against the entitlements in SCIM connector.
- While creating a user or a group, role ids (entitlements) are required. It is not possible to assign entitlements from One Identity Manager client during the creation of users or groups. Hence, a logic has been added in the **Starling Connect** to retrieve all the roles from the target system and assign the first role (except for those which contain **admin** in role name) to the create resource request.

OneLogin

OneLogin Inc. is a cloud-based identity and access management (IAM) provider that designs, develops, and sells a unified access management system (UAM) platform to enterprise-level businesses and organizations. Founded in 2009, by brothers Thomas Pedersen and Christian Pedersen, OneLogin is a late stage venture, privately held company. The OneLogin UAM platform is an access management system that uses single sign-on (SSO) and a cloud directory to enable organizations to manage user access to on-premises and cloud applications. The platform also includes user provisioning, lifecycle management, and multi-factor authentication (MFA).

Supervisor configuration parameters

To configure the connector, following parameters are required:

- Connector name
- Client Id
- Client secret
- SCIM URL (The base URL of the REST API of the Cloud application.)

Supported objects and operations

Users

Table 110: Supported operations for Users

Operation	VERB
Create User	POST
Update User	PUT
Delete User	DELETE

Operation	VERB
Get User by id	GET
Get All Users	GET
Get All Users with pagination	GET

Groups

Table 111: Supported operations for Groups

Operation	VERB
Get Group by id	GET
Get All Groups	GET
Get All Groups with pagination	GET

Roles

Table 112: Supported operations for Roles

Operation	VERB
Get Role by id	GET
Get All Roles	GET
Get All Roles with pagination	GET

Mandatory fields

This section lists the mandatory fields required to create a User or a Group:

Users - Create

- userName
- name.givenName
- name.familyName
- emails.value

Users - Update

userName or emails.value

Groups

Not Applicable

Mappings

The user and group mappings are listed in the tables below.

Table 113: User mapping

SCIM Parameter	OneLogin parameter
Id	Id
UserName	username
ExternalId	external_id
Name.GivenName	firstname
Name.FamilyName	lastname
Name.Formatted	firstname + " " + lastname
DisplayName	firstname + " " + lastname
Emails[0].Value	email
PhoneNumbers[0].Value	phone
Title	title
Roles[.].Value	role_id[]
Groups[0].value	group_id
Active	status
Locale	locale_code
Extension.Manager.Value	manager_user_id
Extension.Organization	company
Extension.Department	department
Extension.OpenIdName	openid_name
Extension.DistinguishedName	distinguished_name
Extension.SamAccountName	samaccountname
Extension.UserPrincipalName	userprincipalname
Extension.MemberOf	member_of

SCIM Parameter	OneLogin parameter
Extension.DirectoryId	directory_id
Meta.Created	created_at
Meta.LastModified	updated_at

Groups

Table 114: Group mapping

SCIM parameter	OneLogin parameter
Id	id
DisplayName	name

Roles

Table 115: Role mapping

SCIM parameter	OneLogin parameter
Id	id
Name	name

Connector limitations

- The target cloud application supports the below given integer values for **Status** field:
 - Unactivated: 0
 - Active: 1
 - Suspended: 2
 - Locked: 3
 - Password expired : 4
 - Awaiting password reset: 5
 - Pending password: 7
 - Security questions required: 8
 - | **NOTE:** All these status cannot be considered in the connector.
- Add Group** and **Remove Group** can be achieved through the **User update** operation. Only one group can be assigned to a user.

Creating a service account in G Suite

You must obtain a JSON file with Private Key to authorize the APIs to access data on G Suite domain. Create and enable the service account to obtain the private key (JSON file).

To create a project and enable the API

1. Login to **Google Cloud Platform**.
2. Click on the drop-down list next to the **Google Cloud Platform** label and select an organization.
The **Select a Project** window is displayed.
3. Click **New Project**.
The **New Project** page is displayed.
4. Enter the specific details in the relevant text field.
5. Click **Create**.
6. Click on the drop-down list next to the **Google Cloud Platform** label and select the project you created.
7. Click **APIs & Services** tab.
8. Click **Library** tab.
9. Search for the phrase **Admin SDK** in the search bar and select **Admin SDK** from the results.

The **API Library** page is displayed.

10. Click **Enable** to enable the API.

To create a service account

1. Click **APIs & Services** tab.
2. Click **Credentials**.

3. On the **Credentials** tab, click **Manage Service Accounts** available at the bottom right corner.

The **Service Accounts** window is displayed.

4. Click **+ CREATE SERVICE ACCOUNT**.

Create service account window is displayed.

5. Enter the name of the service account in **Service account name** text field.
6. Select **Owner** as the **Role** from the drop-down menu.
7. Select the service **JSON** as an account **Key type**.

IMPORTANT: A JSON file is required to generate an access token and it is downloaded automatically after selecting the above option.

8. Click **Create**.

To select and authorize the API scopes

1. Login to the G Suite admin console with your domain.
2. On the Admin console home page, click **Security**.
3. Click **Advanced settings**.
4. Click **Managed API client access**.
5. Enter the client name and the description in the **Name** and **Description** text field respectively.
6. Enter the email in the **Email** text field.
7. Add the preferred API scopes that you want to use.

For example, API scopes can be

<https://www.googleapis.com/auth/admin.directory.user>,
<https://www.googleapis.com/auth/admin.directory.group>, or
<https://www.googleapis.com/auth/admin.directory.group.member>.

For more information on API scopes, see

<https://developers.google.com/identity/protocols/googlescopes>

8. After adding the API scopes, click **Authorize**.

The unique Id and the scopes added is displayed.

Setting a trial account on Salesforce

To login to the Salesforce application, you must create a trail account. The sections below briefs about the process to create a trial account .

To setup a trial account

1. Login to the Salesforce developer edition link:
<https://developer.salesforce.com/signup?d=70130000000td6N>.
2. Provide the relevant details and click **Sign me up**.
A trail account is created and an instance is assigned.
3. Switch the view to Salesforce classic view by clicking **Switch to Salesforce Classic**.
4. Click the **Setup** tab.
5. Click **Build | Create | Apps**.
6. In the **Connected Apps** section, click **New**.
7. In the **Basic Information** section, enter the relevant details.
8. In the **API (Enable OAuth Settings)** section, select **Enable OAuth Settings** checkbox.
9. Provide the <https://app.getpostman.com/oauth2/callback> URL in the **Callback URL** text field.
10. From the **Selected OAuth Scopes** drop-down menu, select **Full Access (full)**.
11. Click **Save**.
12. From the **API (Enabel OAuth Settings)** section, retrieve the **Consumer Key** and **Consumer Secret**.

To generate a security token

A security token is sent to the registered email address. If not received, follow the below steps to generate a token.

1. On the home page, click **My Settings**.
2. Click **Personal | Reset My Security Token**.
3. Review the information displayed on the screen and click **Reset Security Token**.

4. Provide the relevant information such as:

- Client Id: Consumer key
- Client Secret: Consumer secret
- Username
- Password and security token
- Token URL (<https://login.salesforce.com/services/oauth2/token>)

IMPORTANT: Replace this text with a notation that requires the reader's attention.

- To enable API in Salesforce, see <https://ebstalimited.zendesk.com/hc/en-us/articles/229295368-How-do-I-enable-API-access-in-Salesforce> and <https://developer.salesforce.com/forums/?id=906F0000000BaW7IAK>.
- By default, REST API permission is enable in **Developer Edition, Enterprise Edition, Unlimited Edition, Performance Edition**.
- The API package is not available for purchase on the **Contact Edition** and **Group Edition**.
- The API feature can be requested for **Professional Edition** through purchase. To enable the REST API, contact the Salesforce support team.

Working with Azure Active Directory

The following procedure briefs about the steps to register application, provide appropriate permissions, retrieve client ID, and client secret.

Working with Azure AD

1. Login to the Microsoft Azure portal and select **Azure Active Directory** from **FAVORITES**.
2. From Manage section, select **App Registrations (Preview)**.
NOTE: For Safeguard for Privileged Passwords, the Azure AD application registration must be public.
3. Click **New registration** and provide the necessary details.
Provide the following details:
 - Application name[X.X]
 - Redirect URL: <https://connect-supervisor.cloud.oneidentity.com/v1/consent>.
4. Select the created application and click **View API Permissions**.
5. Add the required permissions for Microsoft Graph API (delegated and application permissions).
The registered application must have **User.ReadBasic.All**, **User.Read**, **User.ReadWrite**, **User.ReadWrite.All**, **Directory.Read.All**, **Directory.ReadWrite.All**, **Directory.AccessAsUser.All**, **Group.Read.All**, and **Group.ReadWrite.All** permissions.
6. Click **Grant admin consent for Default Directory** checkbox to grant necessary permissions.
7. From the created application, click App Registrations (Preview) and note the **Application (client) ID** and **Directory (tenant) ID**.
8. Select **Certificates & secrets** and click **New client secret** to generate the secret.
9. Paste the following URL in the browser,
https://login.microsoftonline.com/common/adminconsent?client_id={Client

ID}&state=12345&redirect_uri=http://localhost/myapp/permissions.

10. Click **Accept**.

Providing permission to update or delete users password

1. Install the Azure AD PowerShell v1 module (MSOnline).
2. Connect to your Azure AD B2C tenant.
3. Use the Application(client) ID in the PowerShell script to assign the application the user account administrator role.

For more details on Azure AD, refer the following links:

- To register an application: <https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app>.
- To configure an application to access web APIs: <https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-configure-app-access-web-apis>.
- To Configure an application to expose web APIs: <https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-configure-app-expose-web-apis>.
- To modify the accounts supported by an application: <https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-modify-supported-accounts>
- To configure permissions to update or delete permission for the application: <https://docs.microsoft.com/en-us/azure/active-directory-b2c/active-directory-b2c-devquickstarts-graph-dotnet#configure-delete-or-update-password-permissions-for-your-application>.

Generating a private key for service account in GoToMeeting

A private key has to be generated to access the GoToMeeting service account.

Generating a private key

1. Create an account in **GoToMeeting**.
2. Login to the **GoTo Developer Center**. For more information use the link here: <https://goto-developer.logmeininc.com/>.
3. Click **MyApp** and create an application. Note the **Consumer key** and **Consumer secret**.
4. Login to the GoToMeeting administrator portal to find the admin key in the URL.

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales and other inquiries, such as licensing, support, and renewals, visit <https://www.oneidentity.com/company/contact-us.aspx>.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at <https://support.oneidentity.com/>.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product