Starling Connect for Identity Manager

Administration Guide

Copyright 2024 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.

Starling Connect Administration Guide
Updated - March 2024

Contents

About this guide **36**

One Identity Starling Connect overview **37**

One Identity Starling Connect architecture 38

One Identity Manager Synchronization Editor 38

Starling Connect SCIM endpoints 39

Connectors available for use with One Identity Safeguard for Privileged Passwords 39

One Identity Starling **40**

Supported browsers 41

System requirements 42

One Identity Manager limitations 42

Supported cloud applications **43**

Working with connectors **44**

Configuring a connector 44

Editing a connector 46

Deleting a connector 47

Connector versions **48**

Salesforce **49**

Supervisor configuration parameters 49

Supported objects and operations in Salesforce version 1.0 50

- Users 50
- Groups 50
- Roles 51
- Profiles 51
- PermissionSets 51

Mandatory fields 52

- Users 52
- Groups 52
- Permissions Sets 52

Mappings for Salesforce version 1.0 52

Connector limitations 56
Salesforce connector for Safeguard for Privileged Passwords 56
Connector versions and features 57
Features available exclusively in Salesforce version 2.0 57
Mappings for Salesforce version 2.0 57
Features available exclusively in Salesforce v.3.0 57
Features available exclusively in Salesforce v.4.0 58
Support for filter condition 58
Synchronization and integration of PermssionSets object type with One Identity Manager 60

Facebook Workplace 61
Supervisor configuration parameters 61
Supported objects and operations 61
Users 61
Groups 62
Mandatory fields 62
Users 62
Groups 62
User and Group mapping 62
Connector limitations 64

SAP Cloud Platform 65
Supervisor configuration parameters 65
Supported objects and operations 65
Users 65
Groups 66
Mandatory fields 66
Users 66
Groups 66
User and Group mapping 66
Connector limitations 68

JIRA Server 69
Supervisor configuration parameters 69
Supported objects and operations 69
Users 69

Groups ... 70
Roles ... 70
Mandatory fields ... 70
Users ... 70
Groups ... 70
User and Group mapping ... 71
Connector limitations ... 71

RSA Archer ... 73
Supervisor configuration parameters ... 73
Supported objects and operations ... 74
Users ... 74
Groups ... 74
Roles ... 75
Profiles ... 75
Mandatory fields ... 75
Users ... 75
Groups ... 75
Mappings for RSA Archer versions ... 75
Connector limitations ... 77
Connector versions and features ... 78
Features available exclusively in RSA Archer v.2.0 ... 78
Features available exclusively in RSA Archer v.3.0 ... 78

SuccessFactors ... 79
Supervisor configuration parameters ... 79
Supported objects and operations ... 80
Users ... 80
Groups ... 80
Mandatory fields ... 81
Users (v1.0-v3.0) ... 81
Users v4.0 ... 81
User and Group mapping ... 81
Connector limitations ... 84
Disable attributes ... 84
Connector versions and features ... 84

Features available exclusively in SuccessFactors v.1.0 85
Features available exclusively in SuccessFactors v.2.0 85
Features available exclusively in SuccessFactors v.3.0 85
Features available exclusively in SuccessFactors v.4.0 86
Features available exclusively in SuccessFactors v.5.0 86
Support for filter condition 86
Supported attributes for filter 87

AWS IAM S3 89
Supervisor configuration parameters 89
Supported objects and operations 90
Users 90
Groups 90
Profiles 90
Roles 91
Mandatory fields 91
Users 91
Groups 91
Mappings 91
Connector limitations 93
Connector versions and features 93
Features available exclusively in AWS IAM S3 v.2.0 93
Amazon S3 AWS connector for Safeguard for Privileged Passwords 94

ServiceNow 95
Supervisor configuration parameters for ServiceNow v.1.0 95
Configuring custom attributes for ServiceNow v.1.0 95
Supervisor configuration parameters for ServiceNow v.2.0 96
Configuring custom attributes for ServiceNow v.2.0 96
Supported objects and operations 97
Mandatory fields 98
Users 98
Groups 98
User and Group mapping 98
Connector versions and features 99
Supported Versions 99

Connector limitations 100

Dropbox **101**

Supervisor configuration parameters 101

Supported objects and operations 101

Users 101

Groups 102

Roles 102

Mandatory fields 102

Users 102

Groups 102

User and Group mapping 102

Connector limitations 103

Crowd **105**

Supervisor configuration parameters 105

Supported objects and operations 105

Users 105

Groups 106

Mandatory fields 106

Users 106

Groups 106

User and Group mapping 106

Connector limitations 107

Atlassian JIRA Confluence **108**

Supervisor configuration parameters 108

Supported objects and operations 108

Users 108

Groups 109

Mandatory fields 109

Users 109

Groups 109

User and Group mapping 109

Connector limitations 110

Trello **111**

Supervisor configuration parameters 111

Supported objects and operations 111
Users 111
Groups 112
Mandatory fields 112
Groups 112
User and Group mapping 112
Connector limitations 113

Box 115
Supervisor configuration parameters 115
Supported objects and operations 116
Users 116
Groups 116
Mandatory fields 117
Users 117
Groups 117
User and Group mapping 117
Connector limitations 118

Pipedrive 119
Supervisor configuration parameters 119
Supported objects and operations 119
Users 119
Mandatory fields 120
Users 120
User mapping 120
Connector limitations 120

SuccessFactors HR 122
Supervisor configuration parameters 122
Supported objects and operations 124
Employees 124
Companies 125
BusinessUnits 125
Departments 125
Locations 125
Divisions 126

CostCenters 126
JobCodes 126
Positions 126
EmpEmployments 127
PerPersonals 127
PerPhones 127
EventReasons 127
PicklistLabels 128
PerEmails 128
PerEmails 128
FutureDatedEmployees (in v5.0 and above) 129
EmpJobRelationship (in v10.0 and above) 129
Mandatory Fields 129
Employee 129
PerEmail 129
PerPhone 130
FutureDatedEmployees 130
Mappings 130
Endpoints mapping 130
Attributes mapping 131
Connector limitations 147
Connector versions and features 147
Features available exclusively in SuccessFactors HR v.2.0 147
Features available exclusively in SuccessFactors HR v.3.0 148
Features available exclusively in SuccessFactors HR v4.0 148
Features available exclusively in SuccessFactors HR v5.0 148
Features available exclusively in SuccessFactors HR v6.0 149
Features available exclusively in SuccessFactors HR v7.0 149
Features available exclusively in SuccessFactors HR v8.0 149
Features available exclusively in SuccessFactors HR v9.0 149
Features available exclusively in SuccessFactors HR v10.0 150
Features available exclusively in SuccessFactors HR v10.1 150
Features available exclusively in SuccessFactors HR v10.2 150
Support for Filter Condition 151
List of Attributes for Filter Condition 152

Configuring changes in One Identity Manager to support filter conditions 157
Conditions on "Fetch Effective Dated Records Only" & "Separate Effective And Future Dated Employees Endpoints" flags based on different use cases (for version v.5.0 and above) 157

NutShell **159**
Supervisor configuration parameters 159
Supported objects and operations 159
Users 159
Groups 160
Mandatory fields 160
Users 160
Groups 160
User and Group mapping 160
Connector limitations 161

Insightly **163**
Supervisor configuration parameters 163
Supported objects and operations 163
Users 163
Groups 164
Mandatory fields 164
Users 164
Groups 164
User and Group mapping 164
Connector limitations 165

Egnyte **166**
Supervisor configuration parameters 166
Supported objects and operations 167
Users 167
Groups 167
Mandatory fields 167
Users 167
Groups 168
User and Group mapping 168
Connector limitations 169

SugarCRM **170**
Supervisor configuration parameters 170
Supported objects and operations 171
Users 171
Groups 171
Mandatory fields 171
Users 171
Groups 172
User and Group mapping 172
Connector limitations 173

Oracle IDCS **174**
Supervisor configuration parameters 174
Supported objects and operations 175
Users 175
Groups 175
Mandatory fields 175
Users 175
Groups 176
User and Group mapping 176
Connector limitations 178

Statuspage **179**
Supervisor configuration parameters 179
Supported objects and operations 179
Users 179
Groups 180
Mandatory fields 180
Users 180
Groups 180
User and Group mapping 180
Groups 181
Connector limitations 181

Zendesk Sell **182**
Supervisor configuration parameters 182
Supported objects and operations 182

Users 182
Groups 183
Mandatory fields 183
Users 183
Groups 183
User and Group mapping 183
Groups 184
Connector limitations 184

Workbooks 185
Supervisor configuration parameters 185
Supported objects and operations 185
Users 185
Groups 186
Mandatory fields 186
Users 186
Groups 186
User and Group mapping 186
Groups 187
Connector limitations 187

DocuSign 188
Supervisor configuration parameters 188
Supported objects and operations 189
Users 189
Groups 189
Mandatory fields 190
Users 190
Groups 190
User and Group mapping 190
Connector limitations 191

Citrix ShareFile 192
Supervisor configuration parameters 192
Supported objects and operations 192
Users 192
Groups 193

Mandatory fields ... 193
Users ... 193
Groups ... 193
User and Group mapping ... 194
Groups ... 194
Connector limitations ... 195

Zendesk ... 196
Supervisor configuration parameters ... 196
Supported objects and operations ... 196
Users ... 196
Groups ... 197
Mandatory fields ... 197
Users ... 197
Groups ... 197
User and Group mapping ... 198
Groups ... 198
Connector limitations ... 198

Azure AD ... 200
Connector Configuration ... 200
Supervisor configuration parameters for single tenant connector ... 200
Supervisor configuration parameters for multi tenant connector ... 201
Supported objects and operations ... 201
Users ... 201
Groups ... 202
Application ... 202
Mandatory fields ... 202
Create/Update User ... 202
Groups ... 203
Invite User ... 203
User Group and Application mapping ... 203
Groups ... 204
Application ... 205
Connector limitations ... 205
Azure AD connector for Safeguard for Privileged Passwords ... 206

Google Workspace **207**
Supervisor configuration parameters 207
Supported objects and operations 208
Users 208
Groups 208
Mandatory fields 208
Users 208
Groups 209
User and Group mapping 209
Groups 210
Connector limitations 210
Google Workspace connector for Safeguard for Privileged Passwords 210

Concur **211**
Supervisor configuration parameters 211
Supported objects and operations 212
Users 212
Groups 212
Mandatory fields 213
Users (v1.0) 213
Users (v2.0) 213
Groups 213
User and Group mapping 214
Groups 217
Connector limitations 217
Connector versions and features 217
Features available exclusively in Concur v.2.0 218
Connector SCIM configuration 218
Support for filter condition 218

Tableau **219**
Supervisor configuration parameters 219
Supported objects and operations 219
Users 219
Groups 220
Mandatory fields 220

Users 220
Groups 220
User and Group mapping 220
Groups 221
Connector limitations 221

GoToMeeting 222
Supervisor configuration parameters 222
Supported objects and operations 223
Users 223
Groups 223
Mandatory fields 223
Users 223
Groups 224
User and Group mapping 224
Groups 224
Connector limitations 225

Coupa 226
Supervisor configuration parameters for Coupa v.1.0 226
Configuring custom attributes for Coupa v.1.0 226
Supervisor configuration parameters for Coupa v.1.1 227
Supervisor configuration parameters for Coupa v.2.0 227
Configuring custom attributes for Coupa v.2.0 227
Supported objects and operations 228
Users 228
Groups 228
Roles 229
UserGroups 229
AccountGroups 229
Mandatory fields 229
Users 229
Groups 230
User and Group mapping 230
Groups 232
Roles 232

UserGroups 233
AccountGroups 233
Connector versions and features 233
Supported Versions 233
Features available exclusively in Coupa v.1.1 234
Features available exclusively in Coupa v.2.0 234
Connector limitations 234
Synchronization and integration of Roles object type with One Identity Manager 235
User centric membership configuration for Coupa 235

AWS Cognito 236
Supervisor configuration parameters 236
Supported objects and operations 237
Users 237
Groups 237
Mandatory fields 238
Users 238
Groups 238
User and Group mapping 238
Groups 239
Connector limitations 239

Okta 240
Supervisor configuration parameters 240
Configuring custom attributes for Okta 240
Support for MultiValued Custom attributes 241
Supported objects and operations 241
Users 241
Groups 241
Mandatory fields 242
Users 242
Groups 242
User and Group mapping 242
Groups 244
Connector limitations 244

DataDog 246

Supervisor configuration parameters 246
Supported objects and operations 246
Users 246
Mandatory field 247
Users 247
User mapping 247
Connector limitations 247
Synchronization and integration of Roles object type with One Identity Manager 248

Hideez 249
Supervisor configuration parameters 249
Supported objects and operations 249
AccessProfile 249
Companies 250
Departments 250
Devices 250
Positions 251
Workstations 251
Employees 251
Mandatory fields 252
AccessProfiles 252
Companies 252
Departments 252
Devices (Update) 252
Positions 253
Workstations (Update) 253
Employees 253
Mappings 253
Connector limitations 259
One Identity Manager E2E integration needs 260

Opsgenie 261
Supervisor configuration parameters 261
Supported objects and operations 261
Users 261
Groups 262

Roles 262
Mandatory fields 262
Users 263
Groups 263
Mappings 263
Users 263
Groups 264
Connector limitations 264
Synchronization and integration of Roles object type with One Identity Manager 264

Informatica Cloud Services 265
Supervisor configuration parameters 265
Supported objects and operations 266
Users 266
Groups 266
Roles 266
Mandatory fields 266
Users 267
Groups 267
Mappings 267
Groups 268
Roles 269
Connector limitations 269

AppDynamics 270
Supervisor configuration parameters 270
Supported objects and operations 270
Users 270
Groups 271
Roles 271
Mandatory fields 271
Users 271
Groups 272
Mappings 272
Groups 272
Roles 273

Connector limitations 273
Synchronization and integration of Roles object type with One Identity Manager 274
User centric membership configuration for AppDynamics 274

Marketo 275
Supervisor configuration parameters 275
Supported objects and operations 275
Users 275
Roles 276
Workspaces 276
Mandatory fields 276
Users 276
Mappings 277
Roles 277
Workspaces 278
Connector limitations 278
Synchronization and integration of Roles object type with One Identity Manager 279
Synchronization and integration of Workspaces object type with One Identity Manager 279
Add Roles ID and Workspaces ID to create and update users for Marketo connector 279

Workday HR 280
Supervisor configuration parameters 280
Supported objects and operations 282
Employees 282
Locations 283
CustomOrgs 283
JobClassifications 283
JobProfiles 284
FutureDatedEmployees 284
DeltaSyncEmployees 284
Positions 285
Mappings 285
Endpoint Mapping 285
Attributes Mapping 285
Filter Resource 323

Supported attributes for Filtering Employee Resource 324
More information about Filtering Resource 324
One IM Configuration for Delta Synchronization 325
Modifying the FullProjection process 325
Modifying the synchronization project 328
Connector limitations 329
Connector versions and features 330
Features available exclusively in Workday HR v.2.0 330
Features available exclusively in Workday HR v.3.0 331
Features available exclusively in Workday HR v.3.1 331
Features available exclusively in Workday HR v.3.2 331

OneLogin 333
Supervisor configuration parameters 333
Supported objects and operations 334
Users 334
Groups 334
Roles 334
Application 335
Mandatory fields 335
Users - Create (in v.1.0) 335
Users - Create (in v.2.0) 335
Users - Update 335
Roles - Update 335
Set Role Apps - update 336
Mappings 336
Groups 337
Roles 337
Application 338
Connector SCIM configuration 338
Connector limitations 338
Connector versions and features 339
Features available exclusively in OneLogin v.2.0 339
OneLogin connector for Safeguard for Privileged Passwords 340
User centric membership configuration for OneLogin 340

PingOne **342**
Supervisor configuration parameters 342
Supported objects and operations 342
Mandatory fields 343
User and Group mapping 343
Connector limitations 345

Aha! **346**
Supervisor configuration parameters 346
Supported objects and operations 346
Users 346
Roles 347
Products 347
Mandatory fields 347
Users 347
Groups 348
Mappings 348
Roles 348
Products 349
Connector limitations 349
Synchronization and integration of Roles object type with One Identity Manager 350
Synchronization and integration of Products object type with One Identity Manager 350
Add Roles ID and Product ID to create and update users for Aha connector 350

SAP Litmos **352**
Supervisor configuration parameters 352
Supported objects and operations 352
Users 352
Groups 353
Mandatory fields 353
Users 353
Groups 353
User and Group mapping 353
Groups 355
Connector limitations 355

HackerRank **357**

Supervisor configuration parameters 357
Supported objects and operations 357
Users 357
Groups 358
Roles 358
Mandatory fields 358
Users 358
Groups 359
User and Group mapping 359
Users 359
Groups 360
Connector limitations 361

Slack 362
Connector Configuration 362
Supervisor configuration parameters 362
Supported objects and operations 363
Users 363
Groups 363
Mandatory fields 363
User 364
Group 364
User and Group mapping 364
Groups 365
Connector limitations 366

ActiveCampaign 367
Supervisor configuration parameters 367
Supported objects and operations 367
Users 367
Groups 368
Mandatory fields 368
Users 368
Groups 368
User and Group mapping 369
Users 369

369
Connector limitations 370

Webex **371**
Connector configuration 371
Supervisor configuration parameters 371
Supported objects and operations 372
Users 372
Groups 372
Roles 372
Profiles 373
Mandatory fields 373
Users 373
Groups 373
User and Group mapping 373
Groups 374
Connector limitations 374

Apigee **376**
Supervisor configuration parameters 376
Supported objects and operations 376
Users 376
Roles 377
Mandatory fields 377
Users 377
User and Group mapping 377
Role 378
Connector limitations 378
Synchronization and integration of Roles object type with One Identity Manager 379

Databricks **380**
Supervisor configuration parameters 380
Supported objects and operations 380
Users 380
Groups 381
Mandatory fields 381
Users 381

Groups ... 381
User and Group mapping ... 381
Group ... 382
Connector limitations ... 382

Hive ... 384
Supervisor configuration parameters ... 384
Supported objects and operations ... 384
Users ... 384
Groups ... 385
Mandatory fields ... 385
Users ... 385
Groups ... 385
User and Group mapping ... 385
Groups ... 386
Connector limitations ... 386

PagerDuty ... 387
Supervisor configuration parameters ... 387
Supported objects and operations ... 387
Users ... 387
Groups ... 388
Mandatory fields ... 388
Users ... 388
Groups ... 388
User and Group mapping ... 388
Groups ... 389
Connector limitations ... 389

Dayforce ... 390
Supervisor configuration parameters ... 390
Supported objects and operations ... 391
Employees ... 391
Departments ... 391
Locations ... 391
Organizations ... 391
Mappings ... 392

Filter Resource 400
Supported attributes for Dayforce 400
More information about Filtering Resource 401
Connector SCIM Configuration 402
One IM Configuration for Delta Synchronization 404
Modifying the synchronization project 407
Connector limitations 407

Smartsheet 409
Supervisor Configuration Parameters 409
Supported objects and operations 409
Users 409
Groups 410
Mandatory Fields 410
Users 410
Groups 410
Mappings 410
Connector limitations 412

Pingboard 413
Supervisor configuration parameters 413
Supported objects and operations 413
Users 413
Groups 414
Mandatory fields 414
Users 414
Groups 414
User and Group mapping 415
Connector limitations 416

SAP Cloud for Customer 417
Supervisor configuration parameters 417
Supported objects and operations 417
Users 417
Roles 418
Mandatory fields 418
Users 418

Mappings 418
Connector limitations 420

Azure Infrastructure 421
Supervisor configuration parameters 421
Supported objects and operations 422
ManagementGroups 422
Subscriptions 422
ResourceGroups 422
AzResource 423
AzResourceTypes 423
Locations 423
Roles 423
RoleAssignments 424
Mandatory fields 424
RoleAssignments 424
Attributes Mappings 424
Connector limitations 428

Oracle Fusion Cloud 429
Supervisor configuration parameters 429
Supported objects and operations 429
Users 429
Roles 430
Employees 430
Data Securitiees 430
Mandatory Fields 431
Users 431
Employees 431
Data Securities 431
Mappings 432
Attributes mapping 432
Steps to sync the roles in OracleFusionCloud 439
OneIM E2E Integration Needs 440
Connector Limitations 440

Majesco 441

Supervisor configuration parameters 441
Supported objects and operations 441
Users 441
Roles 442
Mandatory fields 442
Users 442
Roles 442
User and Role mapping 442
Connector limitations 444

LuccaHR 445
Supervisor configuration parameters 445
Supported objects and operations 445
Users 445
Departments 446
Mandatory fields 446
Users 446
Departments 446
User and Department mapping 446
Connector limitations 448

OpenText 449
Supervisor configuration parameters 449
Supported objects and operations 449
Users 449
Group 450
Mandatory fields 450
Users 450
Groups 450
User and Groups mapping 450
Connector limitations 452

JFrog Artifactory 453
Supervisor Configuration Parameters 453
Supported objects and operations 453
Users 453
Groups 454

Mandatory Fields 454
Users 454
Groups 454
Mappings 454
Connector limitations 455

xMatters 456
Supervisor Configuration Parameters 456
Supported objects and operations 456
Users 456
Groups 457
Roles 457
Mandatory Fields 457
Users 457
Groups 458
Mappings 458
Connector limitations 459

Discourse 460
Supervisor Configuration Parameters 460
Supported objects and operations 460
Users 460
Groups 461
Mandatory Fields 461
Users 461
Groups 461
Mappings 462
Connector limitations 462

Testrail 464
Supervisor Configuration Parameters 464
Supported objects and operations 464
Users 464
Groups 465
Mandatory Fields 465
Users 465
Groups 465

Mappings 465
Connector limitations 466

ChipSoft 467
Supervisor Configuration Parameters 467
Supported objects and operations 467
Users 467
Login Groups 468
User Groups 468
Mandatory Fields 468
Users 468
Mappings 468
Connector limitations 470

PingOne Platform 471
Supervisor configuration parameters 471
Supported objects and operations 471
Users 471
Groups 472
Populations 472
Mandatory fields 472
Users 472
Groups 472
User mapping 473
Groups 474
Population mapping 475
Connector SCIM configuration 475
Connector limitations 476

Azure DevOps 477
Supervisor configuration parameters 477
Supported objects and operations 477
Users 477
Groups 478
Projects 478
Mandatory fields 478
Users (for v1.0 & v2.0) 479

Groups (for v1.0 & v2.0) ... 479
Projects (for v1.0 & v2.0) ... 479
Attributes Mappings ... 479
Connector limitations ... 485

UKG PRO ... 487
Supervisor configuration parameters ... 487
Supported objects and operations ... 488
Employees ... 488
EmpJobs ... 488
EmpEmployments ... 488
Attributes Mappings ... 488
Connector SCIM configurations ... 492
Connector limitations ... 492

Atlassian Cloud ... 493
Supervisor configuration parameters ... 493
Supported objects and operations ... 494
Users ... 494
Groups ... 494
Mandatory fields ... 494
Users ... 494
Groups ... 495
User mapping ... 495
Groups ... 496
Connector limitations ... 496

Appendix: Creating a service account in Google Workspace ... 497

Appendix: Setting a trial account on Salesforce ... 499

Registering the application, providing necessary permissions, retrieving Client Id and Client Secret from the Azure AD tenant ... 501
More details on Azure AD ... 502

Appendix: Generating a private key for service account in GoToMeeting ... 504

Appendix: Configuring Amazon S3 AWS connector to support entitlements for User and Group ... 505
Configuring Amazon S3 AWS connector to support entitlements for User ... 505

Viewing the default custom process for User ... 506
Configuring Amazon S3 AWS connector to support entitlements for User using the Synchronization Editor ... 506
Configuring Amazon S3 AWS connector to support entitlements for Group ... 507
Creating a custom process for Amazon S3 AWS connector to support entitlements for Group using the Designer tool ... 507
Configuring Amazon S3 AWS connector to support entitlements for Group using the Synchronization Editor ... 509

Configuring Box connector to support additional email IDs for users ... 511
Adding new columns for Users using the Schema Extension Tool ... 511
Creating a custom property using Designer tool ... 512
Mapping custom properties using the Synchronization Editor ... 513

Appendix: One Identity Manager E2E integration needs for Hideez connector ... 515

Appendix: Configuring custom attributes for ServiceNow v.1.0 ... 516

Appendix: Configuring custom attributes for Coupa v.1.0 ... 518

Appendix: Configuring custom attributes in connectors ... 520

Appendix: Disabling attributes ... 522

Configuring a connector that uses the consent feature ... 524

Appendix: Synchronization and integration of Roles object type with One Identity Manager ... 525

Appendix: Synchronization and integration of Workspaces object type with One Identity Manager ... 527

Appendix: Synchronization and integration of Products object type with One Identity Manager ... 529

Appendix: User centric membership ... 531
Creating a new schema class using Synchronization Editor ... 531
Configuring User centric membership for Groups, UserGroups and AccountGroups using Synchronization Editor ... 532
Configuring User centric membership for Groups ... 532
Configuring User centric membership for UserGroups ... 535
Configuring User centric membership for AccountGroups ... 539
Creating a new column in UCIUser table and CSMUser table using Extension Tool ... 543
Creating a new column in UCIUser table ... 544

Creating a new column in CSMUser table 544
Creating custom process using Designer 545

Appendix: Creating multi-valued custom fields in One Identity Manager 548

Synchronization and assignment of PermissionSets to Users with One Identity Manager 550
Creating mapping for PermissionSets using Synchronization Editor 550
Creating a Process Chain using Designer 552

Appendix: Connectors that support password attribute in User object 555

Appendix: Connectors that do not support special characters in the object ID 556
Connectors that do not support special characters in the object ID 556

Appendix: Creating an app for using SCIM on Slack Enterprise Grid Organization 557

Appendix: Creating a Webex integration application, providing necessary scopes, retrieving Client Id and Client Secret 559

Retrieving the API key from Facebook Workplace 560

Appendix: Outbound IP addresses 561
Salesforce 563
Facebook Workplace 564
SAP Cloud Platform 565
JIRA Server 567
RSA Archer 568
Successfactors 569
Amazon S3 AWS 570
ServiceNow 572
Dropbox 573
Crowd 574
Atlassian JIRA Confluence 575
Trello 577
Box 578
Pipedrive 579
SuccessFactors HR 580
NutShell 582
Insightly 583

Egnyte 584
SugarCRM 585
Oracle IDCS 587
Statuspage 588
Zendesk Sell 589
Workbooks 590
DocuSign 592
Citrix ShareFile 593
Zendesk 594
Azure AD 595
Google Workspace 597
Concur 598
Tableau 599
GoToMeeting 600
Coupa 602
AWS Cognito 603
Okta 604
Apigee 605
DataDog 607
Hideez 608
OpsGenie 609
Informatica Cloud Services 610
AppDynamics 612
OneLogin 613
Marketo 614
Workday HR 615
PingOne 617
Aha! 618
Hacker Rank 619
SAP Litmos 620
Slack 622
ActiveCampaign 623
WebEx 624
Databricks 625
Hive 627

PagerDuty 628
Dayforce 629
Smartsheet 630
Pingboard 632

Appendix: Values for customer-specific configuration parameters in Workday HR connector 634
Additional configuration for update 648
Configuration changes required for update operation in Employees V3 650

Appendix: Initiate an OAuth connection to SuccessFactors 653

Appendix: Creating custom editable/upsertable attributes in Success-factors employee central 655
Making the custom attribute upsertable 655
Managing the custom attribute's visibility in the Employee Data 656

Appendix: Custom Foundation Objects in Successfactors HR connector 657
Example Custom FO Configuration 657
Implementation in the Starling Connect Connector 658
New version 658
Mapping 658
Limitations 658

Appendix: Configuring additional datetime offset in connectors 660

Appendix: How to Create custom attribute for Users in SuccessFactors portal 661

Appendix: SAP Cloud for Customer - Steps to add custom fields at One Identity Manager attributes 662
Steps to add custom fields at One Identity Manager for TimeZone attribute for Users 662
Steps to add custom fields at One Identity Manager for Role attribute for Users 663

Appendix: Creating a Service Principal for the Azure Infrastructure Connector 665

Appendix: Workday permissions needed to integrate via the Starling Connector 666
Creating an integration system user 666
Creating an integration security group 666
Configuring domain security policy permissions 667
Edit business process security policies 668

Activating security policy changes 669

Appendix: Configuring integration application in DocuSign 670

Appendix: Creating integration Connect Client in Coupa 672

Appendix: Retrieving Azure DevOps Personal Access Token (PAT) 673

Appendix: Setup integration system and field override service in Workday 674

Configuration 674

Retrieving Atlassian Cloud API Key and Directory ID 676

About us 677

Contacting us 677

Technical support resources 677

1

About this guide

This guide describes each of the supported target cloud applications and how it is on boarded with One Identity Manager. 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.

It also covers configuration information for connectors that will be registered in Safeguard for Privileged Passwords.

NOTE: This guide describes One Identity Starling Connect 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.

2

One Identity Starling Connect 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.

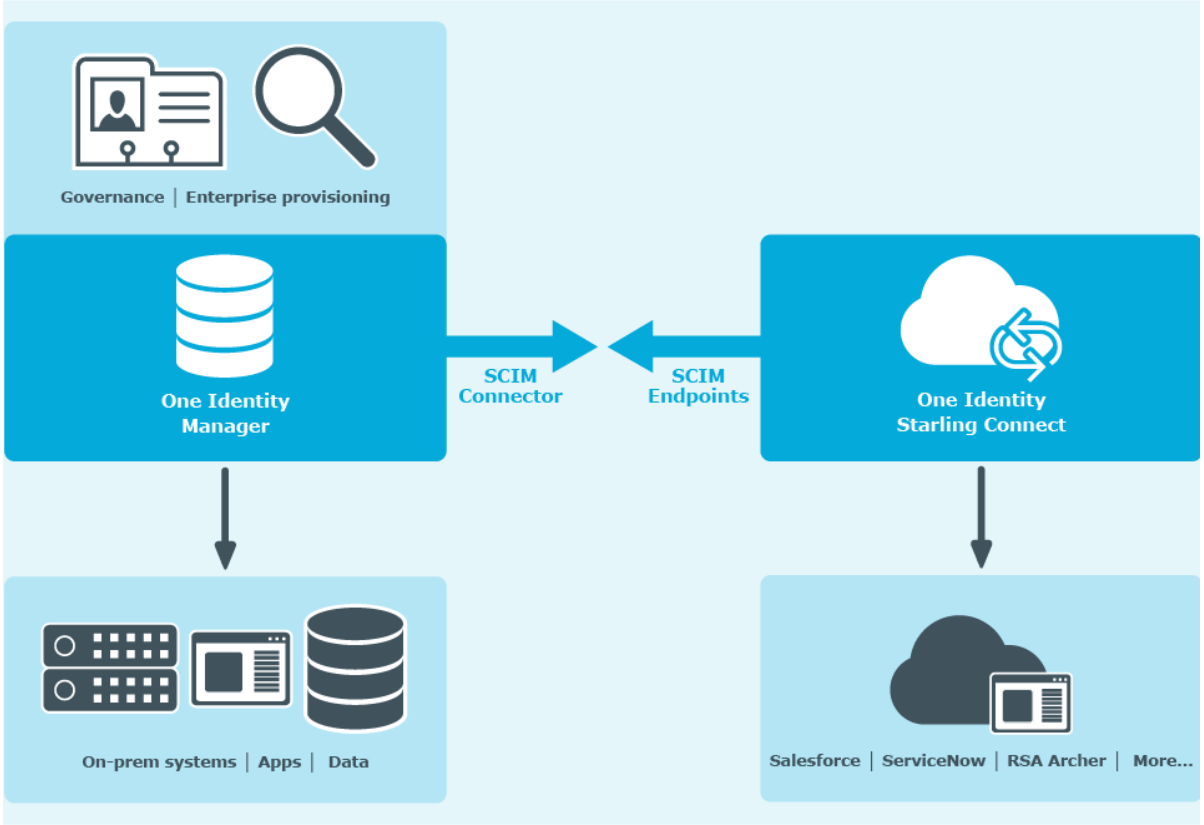
For efficiency and simplicity, an organization's Identity and Access Management (IAM) solution needs to provide an aggregated view of identities across all systems. Additionally, an IAM solution should enable managers to easily define and enforce the policies of their governance initiatives, including those that are on-premises, hybrid and cloud. The above mentioned activities can be performed by One Identity Starling Connect.

A cloud based, managed-service offering, Starling Connect extends the governance capabilities of One Identity Manager (version 7.1.3 or later) to enable organizations to enjoy the benefits of secure hybrid environments. Now, you can extend your One Identity Manager on-premise deployment, to control all your applications, regardless of their installation (on-premise or cloud based).

With Starling Connect, you can extend your investment in identity governance beyond on-premises apps to cloud applications used by your partners. Starling Connect builds on One Identity Manager to unify governance, extend access controls, ensure compliance and to reduce the time taken to provision / de-provision users and groups.

One Identity Starling Connect architecture

Figure 1: Overview of Starling Connect and One Identity Manager integration



One Identity Manager Synchronization Editor

Synchronization Editor enables you to connect different target systems using the One Identity Manager SCIM Connector. This tool helps you to configure data synchronization for the supported cloud target system, and to specify which cloud target system data is mapped to the One Identity Manager database.

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.

Connectors available for use with One Identity Safeguard for Privileged Passwords

The following connectors are available for use with One Identity Safeguard for Privileged Passwords.

- Azure AD
- Amazon S3 AWS
- Google Workspace
- Salesforce
- ServiceNow
- OneLogin

Configuration information that is specific to Safeguard for Privileged Sessions has been included for each connector.

One Identity Starling

Starling helps to combine products from the One Identity line to create 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.

IMPORTANT: One Identity Manager should be configured with merge mode for **Users** and **Groups** synchronization to prevent data loss.

NOTE: For more information about the following topics, see One Identity Starling Hosted User Guide on the One Identity Support site:

- One Identity Starling
- Introduction to One Identity Starling
- Signing in to Starling
- Creating an Organization
- Organization creation and management

Supported browsers

The following browsers are supported when accessing the Starling service:

Table 1: Supported desktop browsers

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

Table 2: Supported mobile browsers

Browser	Minimum OS/platform	Version
Google Chrome	Android	Latest
Safari	iOS	Latest

NOTE: Starling as well as some of the services to which you can subscribe are compatible with mobile devices. Also, be aware that due to space constraints some tables may be condensed when viewed in portrait mode to only display key columns. For more information about Supported browsers, see One Identity Starling Hosted User Guide on the One Identity Support site.

System requirements

This section describes the system requirements for Starling Connect.

System requirements

IMPORTANT: You must ensure the following:

- The **Port 443** must be enabled.

  NOTE: All the below endpoints are https.

DNS name	Purpose
• connect.cloud.oneidentity.com • connect.cloud.oneidentity.eu	Landing page for Connect UI
• connect-supervisor.cloud.oneidentity.com • connect-supervisor.cloud.oneidentity.eu	API endpoint for Connect functionality

- Alternatively for DNS configuration, the following IP addresses must be present in the Firewall allow list:
  - 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
    - starling-k8s-eastus-prod: 52.151.230.102
    - starling-k8s-westus-prod: 13.88.74.234
  - For information about Outbound IP Addresses, see Outbound IP addresses

One Identity Manager limitations

This section gives the list of limitations that are common for all Staring Connect connectors.

This limitation is common for all connectors:

- Group memberships should be handled either at group side as **members** or user side as **groups**. This should not be handled at both **Users** and **Groups Objects**.

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 Sebastian Kuebbeler (Sebastian.Kuebbeler@oneidentity.com).

Working with connectors

Starling subscribers must register a connector for the required target cloud application by providing the connection details. After successful registration, the connector can be used by One Identity Manager, a SCIM client.

Starling Connect allows you to configure, edit and delete a connector.

This section describes the procedures to:

- Configure a connector. For more information, see Configuring a connector.
- Edit a connector. For more information, see Editing a connector.
- Delete a connector. For more information, see Deleting a connector.

Configuring a connector

When you configure a connector in Starling Connect, you create a Starling Connect connector connection to your cloud application. Once you configure your connector, Starling Connect auto generates certain values. You can use these values to connect to One Identity Manager, hence allowing you to establish a connection between your cloud application and One Identity Manager.

This section describes the procedure to configure a connector in Starling Connect.

NOTE:

- To configure a connector, you must first sign into **Starling**, and then either subscribe to the **Connect** service or use a trial service.
  For more information, see **One Identity Starling Hosted User Guide** on the One Identity Support site.
- When you subscribe to the **Connect** service or use the trial service, you can select **United States** (for the United States data center) or **European Union** (for the European Union data center) based on your location.

To configure a connector in Starling Connect

1. Navigate to the **Connectors** tab in the **Connect** page.

   The **Connectors** tab displays the available connectors in the **Connector Catalog** section at the bottom of the page.

2. In the **Connector Catalog**, search for the connector that you want to configure and click the connector tile.

   NOTE: Click **LOAD MORE** to see more connectors.

3. Enter the configuration details in the **General Configuration** page.

   NOTE:

   - The connector displays the available versions. Select the version that you require. You can also change the connector version later by using the edit connector option.
     For more information, see Connector versions and Editing a connector
   - Every connector license that you have, allows you to configure two different connections, one in the **Production** environment and the other in the **Development** environment. Hence, you can configure the connector to create a Starling Connect connector connection in your **Development** environment for testing, and then, configure it in your **Production** environment.
   - Each connector requires a different set of configuration details. For more information about the configuration details for each connector, navigate to the section **Supervisor configuration parameters** for the connector that you want to configure, in this document.

4. Click **TEST CONNECTION**.

   If the configuration details that you entered are correct, the message **TEST CONNECTION SUCCESSFUL** is displayed.

5. Click **SAVE**.

   Starling Connect auto generates the following values:

   - SCIM URL
   - Legacy SCIM URL
   - SCIM Client Credentials
     - SCIM Client ID
     - SCIM Client secret
     - SCIM Token Endpoint URL

   NOTE: You must use the above values when you configure your connector in One Identity Manager, a SCIM client.

6. Click **CLOSE** in the dialog box that displays the **SCIM URL** and **Legacy SCIM URL**.

   The configured connector is displayed in the **Active Connectors** section. You have now established a connection between Starling Connect and your cloud application.

Editing a connector

You can use the edit connector option when you want to:

- Disable or enable attributes
- Configure custom attributes
- Change the version of the connector
- Change the instance of the configured connector

This section describes the procedure to edit a connector.

To edit a connector

1. Navigate to the configured connector in the **Active Connectors** section and click the configured connector tile.

   The **Configuration** page displays the configuration details of the connector.

2. Click **EDIT**.

   The **General Configuration** section displays new versions of the connector, if available.

   The **Schema Configuration** section:

   - displays the **Custom Attributes** section, if this feature is available in your connector.
   - highlights the attributes that can be disabled, if this feature is available in your connector.

3. Select the required version, select the required options and enter the values in the fields that you want to change.
4. Click **TEST CONNECTION**.

   If the details that you entered are correct, the message **TEST CONNECTION SUCCESSFUL** is displayed.

5. Click **SAVE**.

   The configured connector is displayed in the **Active Connectors** section as earlier.

   When you perform a synchronization, the values that you changed in the connector configuration are reflected in One Identity Manager.

   > NOTE: If there are any schema updates when you edit the connector, and you have an existing One Identity Manager Synchronization Project configured for the connector, you must perform a **Update Schema** on the One Identity side. Schema updates could be as a result of the changes related to:
   >
   > - Custom attributes
   > - Disable or enable attributes
   > - Connector version for some connectors

For more information, see Connector versions

Deleting a connector

You may want to delete a connector when you are no longer using the associated cloud application.

This section describes the procedure to delete a connector.

To delete a connector

1. Navigate to the configured connector in the **Active Connectors** section and click the configured connector tile.

   The **Configuration** page displays the configuration details of the connector.

2. Click **DELETE CONNECTOR** in the **Configuration** page.

3. Click **DELETE** in the confirmation pop up.

   The deleted connector is removed from the **Active Connectors** section.

   You will no longer be able to synchronize the data between your cloud application database and the One Identity Manager database if you are still using the associated cloud application.

   NOTE:

   - If you have deleted your connector by mistake and want to enable data synchronization again, you must reconfigure the connector in Starling Connect and re-establish the connection between your cloud application and One Identity Manager using the newly generated **SCIM URL**.
   - For more information, see Configuring a connector.

6

Connector versions

Starling Connect versioning enables administrators to choose the desired version that a customer wants to be on. This enables backward compatibility for the changes done incrementally on the connectors. For example, if the target system APIs are updated or any authentication method is revised.

All the available versions that are available for the connector are displayed. V1.0 is the lowest available version for all the connectors. Also, the latest version is selected by default. Availability of new versions are notified with pop-up messages before and after configuring the connector. You can also change the version later.

Major versions include new features, enhancements, and changes at the target system whereas minor versions consist of bug fixes on the connector.

When you migrate to another version of a connector, you must perform **Update Schema** on One Identity Manager for an already existing One Identity Manager Synchronization Project.

For more information, see Configuring connectors.

7

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 trial account. For more information, see Setting a trial account on Salesforce

Salesforce connectors are available for use with One Identity Safeguard for Privileged Passwords.

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 - <Login password><Security token received over email>
- Token URL - Salesforce's token URL (*https://<saleforce_instance_url>/services/oauth2/token*)
- Grant Type : password
- Instance: This field corresponds with the datacenter the connector should access.
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details).

Supported objects and operations in Salesforce version 1.0

Users

Table 3: Supported operations for Users

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

Groups

Table 4: Supported operations for Groups

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

Roles

Table 5: Supported operations for Roles

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

Profiles

Table 6: Supported operations for Profiles

Operation	VERB
Get All Profiles	GET
Get Profile (Id)	GET

PermissionSets

Table 7: Supported operations for PermissionSets

Operation	VERB
Create PermissionSets	POST
Update PermissionSets	PUT
Delete PermissionSets	DELETE
Add PermissionSet members	POST
Remove PermissionSet members	DELETE
Get All PermissionSets	GET
Get All PermissionSets by Id	GET

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

Permissions Sets

- Name
- Label

Mappings for Salesforce version 1.0

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

Table 8: User mapping for Salesforce version 1.0

SCIM parameter	Salesforce parameter
Id	id
UserName	Username
ExternalId	FederationIdentifier

SCIM parameter	Salesforce parameter
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
Locale	LocaleSidKey
Timezone	TimeZoneSidKey
Active	IsActive
password	[* another API Call]
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

SCIM parameter	Salesforce parameter
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 9: Group mapping for SalesForce version 1.0

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

Table 10: Role mapping for SalesForce version 1.0

SCIM parameter	Salesforce parameter
Id	Id

SCIM parameter	Salesforce parameter
Name	Name
Members[].value	RoleMembers[].Id
Members[].display	RoleMembers[].Name
Meta.Created	CreatedDate
Meta.LastModified	LastModifiedDate

Table 11: Profile mapping for SalesForce version 1.0

SCIM parameter	Salesforce parameter
Id	Id
Name	Name
Members[].value	ProfileMembers[].Id
Members[].display	ProfileMembers[].Name
Meta.Created	CreatedDate
Meta.LastModified	LastModifiedDate

Table 12: Permission Sets mapping for Salesforce version 1.0

SCIM parameter	Salesforce parameter
Id	ID
Name	Name
Label	Label
Members[].value	PermissionSetMembers[].Id
Members[].display	PermissionSetMembers[].Name
Meta.Created	CreatedDate
Meta.LastModified	LastModifiedDate
PermissionSetGroupId	PermissionSetGroupId
PermissionSetType	Type

NOTE: The "permissionSetType" is theoretically not updatable in the Salesforce. This is designed to be 'immutable' in the connector schemas simply for handling the update

scenario from SCIM client appropriately.

Connector limitations

- Even if the Count value is less than 2000, the resources are returned as 2000.

  NOTE: Salesforce connector currently supports Salesforce api version 53.0.
- Salesforce does not display an error when you create Duplicate Groups. It returns the existing group information. A duplicate group will not be created.
- Connector updates the count value of pagination property to 500 when it is more than 500. This is done to solve common validation error.
- Due to target API behaviour, only membership management is supported in Permission set groups in the connector.
- If you disable a parent attribute in the target system, for example **manager**, but do not disable it in the Starling Connect UI under **EnterpriseUser**; instead you disable only the child attribute **manager.value** in the Starling Connect UI, then the connector cannot determine whether the other child attributes **manager.displayName** and **manager.$ref** under the parent attribute **manager** are enabled or not in the target system. Hence, in this case, the request query will contain the other the child attributes **manager.displayName** and **manager.$ref** but not the **manager.value**. The solution is to disable the entire parent attribute **manager** in the Starling Connect UI.
- You cannot update the password of an inactive user due to target system limitations. When you try to create an inactive user, the error message **Password cannot be updated of an inactive user** is displayed. However, the user is created by the system. This is because the **User Create** operation for inactive user is internally carried out as **Create User** and **Set Password** operations, one after the another.
- The connector supports assignment of roles and profiles to account in accordance with the Salesforce data model.

Salesforce connector for Safeguard for Privileged Passwords

- The Instance parameter (which corresponds with the datacenter the connector should access) is required when configuring the supervisor.
- The user account used to register the connecter must have sufficient authorization to change another user's password.

Connector versions and features

The following subsections describe the different connector version(s) and features available with them.

Features available exclusively in Salesforce version 2.0

Following are the features that are available exclusively in **Salesforce v.2.0**:

- The below listed additional attributes are available for the **User** object:
  - Extension.UserPreferencesContentEmailAsAndWhen
  - Extension.UserPreferencesContentNoEmail
  - Extension.CallCenterId

  NOTE: The above three attributes are available in **Salesforce v.2.0** in addition to the attributes that are available in version 1.0.

Mappings for Salesforce version 2.0

Table 13: User mapping for Salesforce version 2.0

SCIM parameter	Salesforce parameter
Extension.UserPreferencesContentEmailAsAndWhen	UserPreferencesContentEmailAsAndWhen
Extension.UserPreferencesContentNoEmail	UserPreferencesContentNoEmail
Extension.CallCenterId	CallCenterId

NOTE: The above three attributes are available in **Salesforce v.2.0** in addition to the attributes that are available in version 1.0.

Features available exclusively in Salesforce v.3.0

Following are the features that are available exclusively in **Salesforce v.3.0**:

- You can configure custom attributes for the **Salesforce v.3.0** SCIM connector in Starling Connect for the **User** object.

  NOTE:

  - For more information about how to configure custom attributes, see Configuring custom attributes in connectors.
  - As the Salesforce target system does not support the disabling attributes feature, the **Salesforce** connector is enhanced only to support the configuration of custom attributes in the SCIM connector in version 3.0.

Features available exclusively in Salesforce v.4.0

Following are the features that are available exclusively in **Salesforce v.4.0**:

You can disable attributes in the **Salesforce v.4.0** SCIM connector in Starling Connect for the **User** object.

NOTE:

- For more information, see Disabling attributes.
- Although the **Salesforce** target system does not support disabling attributes, the **Salesforce** connector is enhanced to support the disable attributes feature to remove the attributes for all **USER** operations in v.4.0.

Support for filter condition

Salesforce connector supports filter condition for User objects. Filters can be applied and the Users filtered absed on the provided condition can be retrieved.

To configure changes to One Identity Manager to support filter conditions

1. Open the **Synchronization Editor** tool.
2. Select **SCIM connector**.
3. Select the **Target system** and navigate to **Schema Classes**.
4. Add a new schema class for the user.
5. Add the **System filter** and **Select Object** condition. Click **Commit to Database**.
6. In User mappings, edit the **Target system schema class** with the recently created schema and click **Commit to Database**.
7. Run the synchronization.

   Filter conditions are created.

IMPORTANT:

- The connector supports filter condition on all versions but only for User objects.
- Supports only AND and OR logical operators.
- Supports only parenthesis () for grouping the condition.
- Filter condition can be applied for any of the User attributes supported by Salesforce workbench.
- Complex attributes are not supported in filter condition. For example, name or email. Only sub-attributes are supported (email.value, name.familyName).
- Filter condition should follow the below syntax

  For example:

  Example 1.<attribute_name><space><operator><space>'<string_value or date_value>' Example 2.<attribute_name><space><operators><space><int_value or bool_value>
- The attribute name should not contain or be preceded with a Schema URN.
- Filter condition values should not have single quotes or percentage with the filter condition value. For example, (userName co 'O'Malley') or (userName co 'O%Malley%').
- Filter condition is not supported by connector for Custom attributes.
- The filter condition related to Id fields attribute VALUES are case sensitive in the target system. For example, manager.value, roles.value.
  - Target system has the Id of Manager as 'aB12eqQ'
    - manager.value ='aB12eqQ' - condition matches and returns the results.
    - manager.value ='ab12eqq' - condition does not match and doesn't return the results.
- Supports the following operators to filter the values with example should apply in OneIM.

Table 14: Supported operators to filter values

Operators	OneIM System filters	OneIM Select Objects
eq → equal to	userType eq 'Standard'	userType = 'Standard'
ne → not equal to	userType ne 'Standard'	userType <> 'Standard'
co → contains	userType co 'Standard'	userType like '%Standard%'
sw → starts with	userType sw 'Standard'	userType like 'Standard%'

Operators	OneIM System filters	OneIM Select Objects
ew → ends with	userType ew 'Standard'	userType like '%Standard'
gt → greater than	userType gt 100	userType > 100
lt → less than	userType lt 100	userType < 100
ge → greater than or equal to	userType ge 500	userType >= 500
le → less than or equal to	userType le 500	userType <= 500

Examples of filter conditions that must be applied at OneIM:

- userType co 'stand'
- userType eq 'standard'
- emails.value co 'baskar.may' or emails.value co 'test.user'
- userType co 'stand' and (emails.value co 'baskar.may' or emails.value co 'test.user')

Synchronization and integration of PermssionSets object type with One Identity Manager

For more information, see Synchronization and assignment of PermissionSets to Users with One Identity Manager.

8

Facebook Workplace

Facebook 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
- Target URL
- Graph API URL

NOTE: For more information, see Retrieving the API key from Facebook Workplace.

- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details)

Supported objects and operations

Users

Table 15: Supported operations and objects for Users

Operation	VERB
Create	POST
Update (Id)	PUT

Operation	VERB
Delete (Id)	DELETE
Get (Id)	GET
Get	GET
Pagination	GET

Groups

Table 16: Supported operations and objects for Groups

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

Mandatory fields

Users

- User Name

Groups

- Group Name

User and Group mapping

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

Table 17: User mapping

SCIM parameter	Facebook Workplace parameter
Id	Id
UserName	userName
Name.Formatted	name.formatted
Name.GivenName	name.givenName
Name.FamilyName	name.familyName
Name.MiddleName	name.middleName
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
Extension.Organization	organization
Extension.Division	division
Extension.Department	department
Extension.Manager.Value	manager.managerId
Extension.EmployeeNumber	employeeNumber
Extension.CostCenter	costCenter
Meta.Created	Meta.created

Table 18: Group mapping

SCIM Parameter	Facebook Workplace parameter
Id	Id
DisplayName	Name
Members.value	UserOrGroupId
Meta.Created	CreatedDate
Meta.LastModified	LastModifiedDate
Extension.description	description
Extension.email	email
Extension.manager.value	owner.id
Extension.privacy	privacy

Connector limitations

- Only the trial subscriptions created using a business email ID with valid domain account will have the access to API integration. The subsequent subscriptions will not have the access.
- **Create Groups**, **Update Groups** and **Delete Groups** are not supported at the free subscription provided by target system.
- You can use a **Group** object only if at least one member associated with it.
- The **Group** will get deleted automatically when the last member is removed from the membership association.
- Connector supports **Add Group Manager** and **Modify Group Manager**, however the group details returned by connector will not have **Group Manager** information unless the group is created using the user interface of **Facebook Workplace**. This is due to the limitations of API provided by the target system.

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.

Supervisor configuration parameters

To configure the connector, following parameters are required:

- Connector name
- Username
- Password
- SCIM URL
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details)

Supported objects and operations

Users

Table 19: Supported operations for Users

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

Operation	VERB
Get (Id)	GET
Get	GET
Pagination	GET

Groups

Table 20: 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

User and Group mapping

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

Table 21: User mapping

SCIM parameter	SAP Cloud Platform parameter
Id	id
UserName	userName
Name.GivenName	givenName
Name.FamilyName	familyName
Name.HonorificPrefix	name.honorificPrefix
DisplayName	displayName
Emails.Value	email.value
Addresses.StreetAddress	addresses.streetAddress
Addresses.Locality	addresses.locality
Addresses.Region	addresses.region
Addresses.PostalCode	addresses.postalCode
Addresses.Country	addresses.country
Addresses.Type	addresses.type
PhoneNumbers.value	phoneNumbers.value
UserType	userType
Locale	locale
Timezone	timeZone
Active	active
Groups.value	group.$ref
Groups.display	group.display
Extension.Organization	extension.organization
Extension.Division	extension.division
Extension.Department	extension.department
Extension.Manager.Value	extension.manager.value
Extension.Manager.DisplayName	extension.manager.displayName
Extension.ContactPreferenceTelephone	contactPreferenceTelephone
Extension.IndustryCrm	industryCrm
Extension.PasswordStatus	passwordStatus

SCIM parameter	SAP Cloud Platform parameter
Extension.MailVerified	mailVerified
Extension.CompanyRelationship	companyRelationship
Extension.ContactPreferenceEmail	contactPreferenceEmail
Extension.SourceSystem	sourceSystem
Extension.CostCenter	extension.costCenter
Extension.EmployeeNumber	extension.employeeNumber
Extension.CorporateGroups	corporateGroups.value
Extension.customAttributes.name	attributes.name
Extension.customAttributes.value	attributes.value
Meta.Created	meta.created
Meta.LastModified	meta.lastModified

Table 22: Group mapping

SCIM parameter	SAP Cloud Platform parameter
id	name
DisplayName	displayName
Members.value	members.value
Members.display	members.display
Extension.GroupName	extension.name
Extension.Description	extension.description

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.

10

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 23: 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 24: 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 25: 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

User and Group mapping

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

Table 26: User mapping

SCIM parameter	JIRA Server parameter
Id	name
UserName	name
password	password
Name.Formatted	displayName
DisplayName	displayName
Emails.Value	emailAddress
Locale	locale
Timezone	timeZone
Active	active
Groups.value	group.name
Groups.display	group.name

Table 27: Group mapping

SCIM parameter	JIRA Server parameter
Id	name
DisplayName	name
Members.value	user.name
Members.display	user.displayName

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.
- The connector does not support special characters in the object ID. For more information, see Connectors that do not support special characters in the object ID

11

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>
- User Record Creation - <Is record creation needed> [only in v3.0]
- 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> [only in v1.0 and v2.0]
- Field ID - <Filed Id to get specific attribute ex: 18746>
- Reporting Filter Field Id - <Reporting Filter Field Id> [only in v3.0]
- ISMS Group Functionality - <Is ISMS Group Functionality Required> [only in v3.0]
- ISMS Id - <ISMS Id> [only in v3.0]
- ISMS Module Id - <ISMS Module Id> [only in v3.0]
- ISMS Name - <ISMS Name> [only in v3.0]
- ISMS Coach - <ISMS Coach> [only in v3.0]
- ISMS Lead - <ISMS Lead> [only in v3.0]

- ISMS Lead Backup - <ISMS Lead Backup> [only in v3.0]
- Profiles Resource - <Is Profiles Resource Required> [only in v3.0]
- Delete User - <Is permanent User Delete Required> [only in v3.0]
- SCIM URL - <Cloud application's instance URL used as targetURI in payload>
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details).

Supported objects and operations

Users

Table 28: Supported operations for Users

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

NOTE: The **Delete User** operation is supported only in v3.0

Groups

Table 29: Supported operations for Groups

Operation	VERB
Update (Id)	PUT
Get (Id)	GET
Get	GET

NOTE: The Archer API supports the **CREATE** Group, **DELETE** Group and **DELETE** User operations, but they are currently unavailable in the connector. If you need the connector to support these operations, please contact support.

Roles

Table 30: Supported operations for Roles

Operation	VERB
Get (Id)	GET
Get	GET
Update	PUT

Profiles

Table 31: Supported operations for Profiles

Operation	VERB
Get (Id)	GET
Get	GET

Mandatory fields

Users

- userName
- name.givenName
- name.familyName
- active

Groups

- displayName

Mappings for RSA Archer versions

The user and group mappings for RSA Archer version are listed in the tables below.

Table 32: User mapping for RSA Archer version

SCIM parameter	RSA Archer parameter
Active	system.status
Address.country	--
Address.formatted	address
Address.locality	--
Address.postalCode	--
Address.region	--
Address.streetAddress	--
Emails	contactItems.value if <contactItems.type = Email>
Extension.Company (only in v3.0)	system.company
Extension.Notes (only in v3.0)	notes
Extension.SecurityParameter (only in v3.0)	system.securityParameter
Extension.UserDomain (only in v3.0)	system.userDomain
Groups.Id	groups.id
Groups.Name	groups.name
Id	system.userId
Locale	system.locale
Name.FamilyName	name.last
Name.GivenName	name.first
Name.MiddleName	name.middle
PhoneNumbers	contactItems.value if <contactItems.type = phone>
Roles.Id	roles.id
Roles.Name	roles.Name
Timezone	timeZone.id
Title	system.title
UserName	system.userName

Table 33: Roles mapping for RSA Archer version

SCIM parameter	RSA Archer parameter
id	id
Name	name
Members.value	RoleMemberships []RequestedObject.UserIds[]

Table 34: Profiles mapping for RSA Archer version

SCIM parameter	RSA Archer parameter
id	Profile Id from the Starling UI Config

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
- 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.
- For the feature **Update User's default Email**, RSA Archer provides an option to update contact information. However, the API document does not have any information about how to pass **ContactRecordId** into update contact info. The operation fails with a **BadRequest** error. As a workaround, the existing default email ID is deleted and the required email ID is created.
- While doing role memberships update, it is not possible to remove those users that only have this role assigned to it (no other role assigned).

Connector versions and features

The following subsections describe the different connector version(s) and features available with them.

Features available exclusively in RSA Archer v.2.0

Following are the features that are available exclusively in **RSA Archer v.2.0**:

In version 2.0 of the connector, the following fields have been removed from User Mapping and schema:

- StreetAddress
- Locality
- Country
- PostalCode

> NOTE: To avoid any breakage in the existing system, these changes have been implemented only in the version 2.0 of the connector.

Features available exclusively in RSA Archer v.3.0

- v3.0 of the Archer connector, supports generic User, Groups, Roles and Profiles endpoints.
- The ids for each resource is modified as id@ResourceName - > where ResourceName can be User, Group, Role & Profile.
- Supports update role to manage the role memberships.

12

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 (Format: <userId (not the value for username) of the SuccessFactors service account>@<company_id>)
- Password (needed till v.4.0)
- OData URL (Refer the note below)
- Private Key (v.5.0)
- Client Id (v.5.0
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details).

  > 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 and https://apps.support.sap.com/sap/support/knowledge/public/en/2215682

- Retry Server Call

  > IMPORTANT:
  >
  > - Retry Server Call is used to make a retry request to the Successfactors system in-case of failures related with an unreachable instance at a given

point in time.

- By default the value is set to false. The customer can enable it in-case such failures are encountered.

Supported objects and operations

Users

Table 35: Supported operations for Users

Operation	VERB
Create User	POST
Update User	PUT
Delete (only till v3.0)	DELETE
Get User (Id)	GET
Get All Users	GET
Get All Users with pagination	GET

Groups

Table 36: Supported operations for Groups

Operation	VERB
Update Group	PUT
Get All Groups	GET
Get Groups (Id)	GET
Get All Groups with pagination	GET

Mandatory fields

Users (v1.0-v3.0)

- User Name
- Employee Number
- Status

Users v4.0

- UserName
- UserId
- Status

User and Group mapping

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

Table 37: 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
DisplayName	defaultFullName
Emails.Value	email
Addresses.StreetAddress	addressLine1
Addresses.Locality	city

SCIM parameter	SuccessFactors parameter
Addresses.Region	state
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	defaultLocale
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 38: Additional mapping from v4.0 onwards

SCIM parameter	SuccessFactors parameter
Location	location
UserExtension.UserId	userId
userExtension.JobCode	jobCode
userExtension.Custom01	custom01
userExtension.Custom02	custom02
userExtension.Custom03	custom03

SCIM parameter	SuccessFactors parameter
userExtension.Custom04	custom04
userExtension.Custom05	custom05
userExtension.Custom06	custom06
userExtension.Custom07	custom07
userExtension.Custom08	custom08
userExtension.Custom09	custom09
userExtension.Custom10	custom10
userExtension.Custom11	custom11
userExtension.Custom12	custom12
userExtension.Custom13	custom13
userExtension.Custom14	custom14
userExtension.Custom15	custom15
userExtension.Hr.UserId	hr.userId
userExtension.Hr.Email	hr.email
userExtension.Hr.Username	hr.username
userExtension.Hr.Active	hr.status
userExtension.Manager.UserId	manager.userId
userExtension.Manager.Email	manager.email
userExtension.Manager.Username	manager.username
userExtension.Manager.Active	manager.status

Table 39: Group mapping

SCIM parameter	SuccessFactors parameter
Id	groupID
displayName	groupName
members.value	userId
members.display	userName
groupExtension.groupType	groupType
groupExtension.staticGroup	staticGroup
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. (applicable for version V1 to V3)
- User update does not support addition and removal of **Groups** or **Roles** for a particular user. It is done using group update. This is not applicable for role update.
- Due to the API limitation of the target system, only the groups with type "permission" and "ectworkflow" are supported by version 3.0 of the connector.
- User employee number cannot be updated because the cloud application considers employee number as a user Id. (applicable from version V1 till V3)
- The UPDATE of Static Group supports the change of name and memberships. However, the UPDATE of Dynamic Group supports only the change of name but not the memberships. This is due to the target system behavior.
- The manager/hr attribute gets added under user only if manager/hr in the request has the status as active.
- Non-existing users should not be assigned as manager/hr while creating/updating user.

Disable attributes

The **Disable attribute** feature can be used when you want to skip an attribute that exists in the target system.

For the **SuccessFactors** connector, the attributes of the **User** object, including those of **Enterprise User**, can be disabled or enabled while configuring the connector based on your requirements.

NOTE:

- Mandatory attributes cannot be disabled.
- For more information about how to disable attributes in Starling Connect, see Disabling attributes in the Appendix section.

Connector versions and features

The following subsections describe the different connector version(s) and features available with them.

Features available exclusively in SuccessFactors v.1.0

Following are the features that are available exclusively in **SuccessFactorsv.1.0**:

- Update of basic attributes on Static and Dynamic Groups are supported.
- Update of Group membership on Static and Dynamic Groups are supported.
- Update of Dynamic Groups will remove the associated Dynamic Clauses.
- Supported insert / update / upsert on inactive users using extended permissions.

Features available exclusively in SuccessFactors v.2.0

Following are the features that are available exclusively in **SuccessFactors v.2.0**:

- Update of basic attributes on Dynamic Groups are supported.
- Update of Group membership on Static Groups are supported.
- Dynamic Group supports group basic attributes update, but not group memberships.
- Supported insert / update / upsert on inactive users using extended permissions.
- Static Group Update (supports only **Add** and **Remove** operations for Group Members)
- Dynamic Group Update (supports **Group Update** without removing the existing dynamic clauses)

  NOTE:

  - These features are available from version 2.0 onwards.
  - In version 1.0, only **Dynamic Group Update** is supported. **Static Group Update** is not supported in version 1.0.
  - Version 2.0 is enhanced to allow you to use the **Dynamic Group Update** operation to update the attributes of a **Dynamic Group** without removing the dynamic clause that you have added for that **Dynamic Group**.

    This feature is available from version 2.0 onwards. In version 1.0 of the connector, the **Dynamic Group Update** function removes the existing dynamic clause that was added for the **Dynamic Group**.

Features available exclusively in SuccessFactors v.3.0

Following are the features that are available exclusively in **SuccessFactorsv.3.0**:

- Supports all the features from v2.0.
- Filtering of resources by selected attributes are supported.
- Synchronization has been improved by limiting the groups type to 'Permission' and 'ectworkflow'.
- Supports insert / update / upsert on inactive users using extended permissions.

Features available exclusively in SuccessFactors v.4.0

Following are the features that are available exclusively in **SuccessFactorsv.4.0**:

- Supported insert / update / upsert on inactive users using extended permissions.
- Additional attributes (userId, jobCode, location, All available "CustomXX", hr (complex), manager(complex)) supported under users.
- Setting up a custom unique UserID on CREATE is supported.
- DELETE operation not supported in Users endpoint.
- Supported Custom Attributes for Users. Refer How to create custom attributes for users in Successfactors portal

Features available exclusively in SuccessFactors v.5.0

Following are the features that are available exclusively in **SuccessFactorsv.5.0**:

- v.5.0 has no feature change only addition is that it supports OAuth Authentication.
- For detailed explanation on setting up OAuth Authentication, refer SetUp OAuth.

Support for filter condition

SuccessFactors connector supports filter condition for User objects. Filter condition can be applied, and the Users can be retrieved selectively. Based on the supported operators and values provided at the filter the User objects are returned in the response from the connector.

To configure changes to One Identity Manager to support filter conditions

1. Open the **Synchronization Editor** tool.
2. Select **SCIM connector**.

3. Select the **Target system** and navigate to **Schema Classes**.

   For example - id ne '10056' AND (locale eq 'Cleveland (1000-2011)')
4. Add a new schema class for the user.
5. Add the **System filter** and **Select Object** condition.

   Click **Commit to Database**.
6. In User mappings, create or edit the **Target system schema class** with the recently created schema and click **Commit to Database**.
7. Run the synchronization.
8. Filter conditions are created.

Supported attributes for filter

- Id
- lastModified
- givenName
- familyName
- locale
- division
- urn:ietf:params:scim:schemas:extension:enterprise:2.0:User.division
- department
- urn:ietf:params:scim:schemas:extension:enterprise:2.0:User.department

NOTE:

- The connector supports filter condition on version 3.0 but only for User objects.
- Supports only AND and OR logical operators.
- Supports only parenthesis () for grouping the condition.
- Only the sub-attributes of a complex attribute are supported in filter condition. For example, givenName or familyName

Table 40: Supported operators to filter values

S. No	Operators	OneIM System Filters	OneIM Select Objects
1	eq → equal to	lastModified eq 2020-08-27T15:22:52	lastModified = 2020-08-27T15:22:52
2	ne → not equal to	lastModified ne 2020-08-27T15:22:52	lastModified <> 2020-08-27T15:22:52
3	gt → greater than	lastModified gt 2020-08-	lastModified > 2020-08-

S. No	Operators	OneIM System Filters	OneIM Select Objects
		27T15:22:52	27T15:22:52
4	lt → less than	lastModified lt 2020-08-27T15:22:52	lastModified < 2020-08-27T15:22:52
5	ge → greater than or equal to	lastModified ge 2020-08-27T15:22:52	lastModified >= 2020-08-27T15:22:52
6	le → less than or equal to	lastModified le 2020-08-27T15:22:52	lastModified <= 2020-08-27T15:22:52

13

AWS IAM S3

AWS IAM S3 (formerly Amazon S3 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.

Amazon S3 AWS connectors are available for use with One Identity Safeguard for Privileged Passwords.

For more information about configuring Amazon S3 AWS connector with One Identity Manager, see Configuring Amazon S3 AWS connector to support entitlements for User and Group.

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)
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details).

Supported objects and operations

Users

Table 41: Supported operations and objects for Users

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

Groups

Table 42: Supported operations and objects for Groups

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

NOTE: Currently, addition or removal of entitlements for Groups is not supported by One Identity Manager.

Profiles

Table 43: Supported operations for Profiles

Operation	VERB
Get All Profiles	GET
Get Profile	GET

Roles

Table 44: Supported operations for Roles

Operation	VERB
Get Role	GET
Get All Roles	GET

Mandatory fields

Users

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

Groups

- Group Name

Mappings

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

Table 45: User mapping

SCIM parameter	Amazon S3 AWS parameter
Id	UserName
UserName	UserName
Password	password
DisplayName	Arn
Active	(true)
Groups	(ListGroupsForUserResult)Group

SCIM parameter	Amazon S3 AWS parameter
Entitlements	(ListAttachedUserPoliciesResult)AttachedPolicies
Created	CreateDate
LastModified	PasswordLastUsed

Table 46: Group mapping

SCIM parameter	Amazon S3 AWS parameter
Id	GroupName
displayName	UserName
Entitlements	(ListAttachedGroupPoliciesResult)AttachedPolicies
Members	(GetGroupResult)Users
Created	CreateDate
LastModified	PasswordLastUsed

Table 47: Profile mapping

SCIM parameter	Amazon S3 AWS parameter
Id	Arn
displayName	PolicyName
Created	CreateDate
LastModified	UpdateDate

Table 48: Roles mapping

SCIM parameter	Amazon S3 AWS parameter
Id	RoleName
Name	RoleName
Entitlements	(ListAttachedGroupPoliciesResult)AttachedPolicies
description	Description
Created	CreateDate

Table 49: Mappings for v2.0

SCIM parameter	Amazon S3 AWS parameter
Id	Base64encoded(id)
targetId	id

NOTE: Applicable for all object types except Profiles.

Connector limitations

- Signature generation is embedded within a data process. Hence, the performance of the application is affected.
- The Last Modified date is not available. Hence, the field contains the value of the 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 One Identity Manager.
- **Roles** has no assignment relations with **Users** and **Groups** object types. **Entitlements** is the only object type associated with **Roles**.
- The connector does not support special characters in the object ID. For more information, see Connectors that do not support special characters in the object ID

Connector versions and features

The following subsections describe the different connector version(s) and features available with them.

Features available exclusively in AWS IAM S3 v.2.0

Following are the features that are available exclusively in AWS IAM S3 v.2.0:

- All the endpoints except Profiles return one new attribute “targetId”.
- The "id" in the SCIM response will be base64 encoded in all the endpoint except Profiles.

Amazon S3 AWS connector for Safeguard for Privileged Passwords

- The service account must have the following minimum IAM permissions:
  - GetUser
  - GetGroup
  - ListAttachedUserPolicies
  - ListEntitiesForPolicy
  - ListGroups
  - ListGroupsForUser
  - ListUsers
  - ListUserPolicies
  - SimulatePrincipalPolicy
  - UpdateLoginProfile
- If manually adding an account to an AWS asset, the username to enter is the simple account username (not the ARN).
- Only AWS passwords are managed (not User Api keys).
- Users must have a manually set password in AWS prior to management by Safeguard for Privileged Passwords. You cannot call "ChangePassword" on an account that has never had a password set.
- Safeguard for Privileged Password "Roles" are used for account discovery map to AWS Policies (not AWS "Roles").
- When a "Roles" filter is used in account discovery it only captures accounts for which a matching policy is directly assigned to the user (not policies it inherits through a group).

14

ServiceNow

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

ServiceNow connectors are available for use with One Identity Safeguard for Privileged Passwords.

Supervisor configuration parameters for ServiceNow v.1.0

To configure the connector, following parameters are required:

- Connector name
- Username for the cloud account
- Password for the cloud account
- Custom Properties (List of custom properties, if any, to be mapped)
  For more information, see Configuring custom attributes for ServiceNow v.1.0.
- SCIM URL (Cloud application's REST API's base URL)

Configuring custom attributes for ServiceNow v.1.0

You can configure custom attributes for the **ServiceNow v.1.0** connector when you configure the connector in Starling Connect by adding the custom attributes in the **Custom Properties** field in the defined format.

NOTE: For more information about how to configure custom attributes in **ServiceNow v.1.0** , see Configuring custom attributes for ServiceNow v.1.0.

Supervisor configuration parameters for ServiceNow v.2.0

To configure the connector, following parameters are required:

- Connector name
- Username for the cloud account
- Password for the cloud account
- SCIM URL (Cloud application's REST API's base URL)

Configuring custom attributes for ServiceNow v.2.0

You can configure custom attributes for the **ServiceNow v.2.0** SCIM connector in Starling Connect for **Users**, **Groups** and **Roles** in the **Custom Attributes** section in **Schema Configuration**.

NOTE:

- For more information about how to configure custom attributes in **ServiceNowv.2.0**, see Configuring custom attributes in connectors.
- As the ServiceNow target system does not support disabling of attributes, the **ServiceNow** connector is enhanced only to support the configuration of custom attributes in the SCIM connector.
- If a custom attribute is a complex attribute, then you must enter it in the following format in Starling Connect:

  `<custom_attribute>$$<nested_attribute>.`

  For example,

  ```
  "parent": {
  "link": "https://dev60043.service-now.com/api/now/table/sys_user_group/b85d44954a3623120004689b2d5dd60a",
  "value": "b85d44954a3623120004689b2d5dd60a"
  }
  ```

  you must enter as `parent$$value` in Starling Connect.
- The connector supports single level of navigation only.

Supported objects and operations

Users

Table 50: Supported operations for Users

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

Groups

Table 51: Supported operations for Groups

Operation	VERB
Create	POST
Update	PUT
Delete	DELETE
Get all groups	GET
Get (id)	GET
Get	GET
Pagination	GET

Roles

Table 52: Supported operations for Roles

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

Mandatory fields

Users

- Username

Groups

- Group Name

User and Group mapping

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

Table 53: 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
addresses[0].region	state
addresses[0].postalCode	zip
addresses[0].country	country
phoneNumbers[0].value	phone
title	title
preferredLanguage	preferred_language
timeZone	time_zone

SCIM parameter	ServiceNow parameter
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 54: 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 versions and features

The following subsections describe the different connector version(s) and features available with them.

Supported Versions

The supported versions of **ServiceNow** connector are:

- v.1.0
- v.2.0

NOTE: For more information, see Connector versions.

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.

15

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
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details).

Supported objects and operations

Users

Table 55: 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 56: 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 57: Supported operations for Roles

Operation	VERB
Get all roles	GET
Get role by Id	GET

Mandatory fields

Users

- emails.value

Groups

- displayName

User and Group mapping

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

Table 58: User mapping

SCIM parameter	Dropbox parameter
id	profile.team_member_id
externalId	profile.external_id
userName	profile.email
name.familyName	profile.name.surname
name.givenName	profile.name.given_name
name.formatted	profile.name.display_name
displayName	profile.name.display_name
emails[0].value	profile.email
active	profile.status[".tag"]
groups	profile.groups
roles	role[".tag"]
meta.created	profile.joined_on

Table 59: Group mapping

SCIM parameter	Dropbox parameter
id	group_id
displayName	group_name
members[].value	members[].profile.team_member_id
members[].display	members[].profile.name.display_name
enterpriseExtension.externalId	group_external_id
meta.created	created

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 carried out.
- 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*.

16

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
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details)

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 All Users with pagination	GET

Groups

Table 61: 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

User and Group mapping

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

Table 62: User mapping

SCIM parameter	Crowd parameter
Id	name
userName	name
password	password
active	active
givenName	first-name
familyName	last-name
displayName	display-name
Formatted	display-name
email.value	email
Created	createdDate
LastModified	lastModified

Table 63: Group mapping

SCIM parameter	Crowd parameter
Id	name
GroupName	name
Active	active
Description	description
members.value	members.name

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.
- The connector does not support special characters in the object ID. For more information, see Connectors that do not support special characters in the object ID

Atlassian JIRA Confluence

Atlassian JIRA Confluence 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 64: 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 65: 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

User and Group mapping

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

Table 66: User mapping

SCIM parameter	Atlassian JIRA Confluence parameter
Id	accountId
userName	emailAddress
password	password

SCIM parameter	Atlassian JIRA Confluence parameter
Name.Formatted	displayName
DisplayName	displayName
email.value	emailAddress
Active	active
Timezone	timeZone
Locale	locale
Groups.Value	name

Table 67: Group mapping

SCIM parameter	Atlassian JIRA Confluence parameter
Id	name
DisplayName	name
members.value	accountId
members.display	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.

18

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

Users

Table 68: Supported operations and objects for Users

Operation	VERB
Get (Id)	GET
Get all users	GET

Groups

Table 69: Supported operations and objects for Groups

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

Mandatory fields

Groups

- displayName

User and Group mapping

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

Table 70: 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 71: 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 drop in performance.
- 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 carried out 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*.

19

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
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details)

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 72: Supported operations for Users

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

Groups

Table 73: Supported operations for Groups

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

Mandatory fields

Users

- DisplayName
- Email ID

Groups

- DisplayName

User and Group mapping

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

Table 74: User mapping

SCIM parameter	Box parameter
id	id
login	email[0].value
login	userName
name	name.formatted
name	displayName
status	active
address	address[0].formatted
type	userType
phone	PhoneNumbers[0].Value
status	active
job_title	title
language	preferredLanguage
timezone	timezone

SCIM parameter	Box parameter
created_at	meta.created
modified_at	meta.lastModified
emailAliases.entries[].id	userExtension.additionalEmails[].id
emailAliases.entries[].email	userExtension.additionalEmails[].value
emailAliases.entries[].is_confirmed	userExtension.additionalEmails[].is_confirmed

Table 75: Group mapping

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

Connector limitations

There might be a performance impact when you add or remove multiple email aliases since the cloud application processes them one by one.

NOTE: For more information, see Configuring Box connector to support additional email IDs for users

20

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)
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details)

Supported objects and operations

Users

Table 76: 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

NOTE: Additional features supported: Pipedrive connector supports attribute selection for the response based on the attributes mentioned in the query parameters ?attributes=.

User mapping

The user mappings are listed in the tables below.

Table 77: User mapping

SCIM parameter	Pipedrive parameter
Id	id
userName	email
displayName	name
Name.Formatted	name
email.value	email
Active	active_flag
Timezone	timezone_name
Locale	locale
Created	created
LastModified	modified

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.

21

SuccessFactors HR

SuccessFactors HR 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 (Format: <userId (not the value for username) of the SuccessFactors service account>@<company_id>)
- Password (needed till v.5.0)
- SuccessFactors HR instance URL (https://apps.support.sap.com/sap/support/knowledge/public/en/2215682).
- Private key (v.6.0 onwards)
- Client Id (v.6.0 onwards)
- Custom Object Types (v9.0 onwards)
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details)
- Minimal Attributes (in v1.0 and v2.0)

  NOTE: The default value is **false**. When the value is set to **true**, only the minimal set of attributes for all the objects will be queried from the **SuccessFactors HR** system.
- Fetch Effective Dated Records Only (v3.0 onwards)

  NOTE: The default value is **false**. When the value is set to **true**, only the effective dated employees will be queried from the **SuccessFactorsHR** system.
- Activate Custom Attributes With Full Name (v5.0 onwards)

NOTE: The default value is **false**. When the value is set to **true**, then custom attributes would be prefixed with the full name of the navigational attributes.

- Separate Effective And FutureDated Employees Endpoints (v5.0 onwards)

  NOTE: The default value is **false**. When the value is set to **true**, the employees would be separated into two endpoints - the effective dated and future dated.

- Retry Server Call

  IMPORTANT:

  - Retry Server Call is used to make a retry request to the SuccessFactorsHR system in-case of failures related with an unreachable instance at a given point in time.
  - By default the value is set to false. The customer can enable it in-case such failures are encountered.

- loginMethod (v9.0 onwards)

  NOTE: The default value is **false**. When the value is set to **true**, the employees would have loginMethod attribute in the response.

- Use base 64 encoded id in synchronization (on v10.1)

  NOTE: The default value is **false**. Set this to **true** if the id contains special characters and needs the base 64 encoding to support the synchronization.

Table 78: Minimal set of attributes for the objects

SuccessFactors HR	Attributes
BusinessUnit	externalCode, name, description, status, startDate, createdOn, lastModifiedOn
Company	externalCode, name, description, status, createdOn, lastModifiedOn
CostCenter	name, description, externalCode, status, startDate, createdOn, lastModifiedOn
Division	externalCode, name, description, status, startDate, createdOn, lastModifiedOn
Department	name, description, externalCode, status, startDate, createdOn, lastModifiedOn
EmpEmployment	userID, startDate, createdOn, lastModifiedOn
Employee	EmpJob attributes: userId, businessUnit, company, costCenter, createdOn, division, event, eventReason, jobTitle, location, managerId, emplStatus, startDate, jobCode, position User attributes: dateOfBirth, userId, username, defaultFullName, hireDate, lastModified, status, department, location, firstName, lastName, mi, suffix, email, addressLine1, state, city, zipCode,

SuccessFactors HR	Attributes
	country, businessPhone, cellPhone
EventReason	externalCode, name, status, event, createdOn, lastModifiedOn
JobCode	externalCode, name, description, status, createdOn, lastModifiedOn
Location	externalCode, name, description, status, geozoneFlx, createdOn, lastModifiedOn
PerPersonal	personIdExternal, firstName, lastName, preferredName, createdOn, lastModifiedOn
PerPhone	personIdExternal, phoneNumber, phoneType, createdOn, lastModifiedOn
PicklistLabel	id,externalCode, status
PicklistOption	id,externalCode, status
Position	code, description, jobTitle, effectiveStatus, jobCode, businessUnit, company, department, externalName_defaultValue, createdDate, lastModifiedDate

NOTE: For consuming Starling Connect HR connectors (for example, SuccessFactors HR) into the One Identity Manager Synchronization Client, the One Identity Manager CHS module has to be installed and configured. You can download the appropriate CHS module from the One Identity Manager Support site.

Supported objects and operations

Employees

Table 79: Supported operations for Employees

Operation	VERB
Get Employee	GET
Get All Employees with Pagination	GET
Update Employees	PUT

Companies

Table 80: Supported operations for Companies

Operation	VERB
Get Company	GET
Get All Company With Pagination	GET

BusinessUnits

Table 81: Supported operations for BusinessUnits

Operation	VERB
Get BusinessUnit	GET
Get All Business Units with Pagination	GET

Departments

Table 82: Supported operations for Departments

Operation	VERB
Get Department	GET
Get All Departments with Pagination	GET

Locations

Table 83: Supported operations for Locations

Operation	VERB
Get Location	GET
Get All Locations with Pagination	GET

Divisions

Table 84: Supported operations for Divisions

Operation	VERB
Get Division	GET
Get All Division With Pagination	GET

CostCenters

Table 85: Supported operations for CostCenters

Operation	VERB
Get CostCenter	GET
Get All CostCenter with Pagination	GET

JobCodes

Table 86: Supported operations for JobCodes

Operation	VERB
Get JobCode	GET
Get All JobCodeWith Pagination	GET

Positions

Table 87: Supported operations for Positions

Operation	VERB
Get Position	GET
Get All Position With Pagination	GET

EmpEmployments

Table 88: Supported operations for EmpEmployments

Operation	VERB
Get EmpEmployment	GET
Get All EmpEmployment With Pagination	GET

PerPersonals

Table 89: Supported operations for PerPersonals

Operation	VERB
Get PerPersonal	GET
Get All PerPersonal With Pagination	GET

PerPhones

Table 90: Supported operations for PerPhones

Operation	VERB
Get PerPhone	GET
Get All PerPhone With Pagination	GET
Create PerPhone	POST
Update PerPhone	PUT

EventReasons

Table 91: Supported operations for EventReasons

Operation	VERB
Get EventReason	GET
Get All EventReason With Pagination	GET

PicklistLabels

Table 92: Supported operations for PicklistLabels

Operation	VERB
Get PicklistLabel	GET
Get All PicklistLabel With Pagination	GET

PerEmails

Table 93: Supported operations for PerEmails

Operation	VERB
Get PerEmail	GET
Get All PerEmails With Pagination	GET
Update PerEmail	PUT
Create PerEmail	POST
Delete PerEmail	DELETE

PerEmails

Table 94: Supported operations for PerEmails

Operation	VERB
Get PerEmail	GET
Get All PerEmails With Pagination	GET
Update PerEmail	PUT
Create PerEmail	POST
Delete PerEmail	DELETE

FutureDatedEmployees (in v5.0 and above)

Table 95: Supported operations for FutureDatedEmployees

Operation	VERB
Get Employees	GET
Get All Employees with Pagination	GET
Update Employees	PUT

EmpJobRelationship (in v10.0 and above)

Table 96: Supported operations for EmpJobRelationship

Operation	VERB
Get EmpJobRelationship	GET
Get EmpJobRelationship With Pagination	GET

Mandatory Fields

This section lists the mandatory fields required to **CREATE/UPDATE**, **Employees**, **PerEmails**, **PerPhones**, and **FutureDatedEmployees**:

Employee

- userId
- username

PerEmail

- personIdExternal
- emailType

PerPhone

- personIdExternal
- phoneType
- phoneNumber

FutureDatedEmployees

- userId
- username

NOTE: Employees and FutureDatedEmployees endpoints support UPDATE operation only.

Mappings

Endpoints mapping

Table 97: Target system objects mapping

SCIM endpoints	Target system objects
Employees	EmpJob
BusinessUnits	FOBusinessUnit
Departments	FODepartment
CostCenters	FOCostCenter
Locations	FOLocation
Divisions	Divisions
Companies	FOCompany
JobCodes	FOJobCode
Positions	Position
EmpEmployments	EmpEmployment
PerPersonals	PerPersonal
PerPhones	PerPhone

SCIM endpoints	Target system objects
PicklistLabels	PicklistLabel
PicklistOptions	PicklistOption
PerEmails	PerEmail
EventReasons	EventReason

Attributes mapping

Different mappings associated with this connector are listed in the tables below.

Table 98: Employee mapping

SCIM parameter	SuccessFactors HR parameter
Addresses.Country	userNav/country
Addresses.Locality	userNav/state
Addresses.PostalCode	userNav/zipCode
Addresses.Region	userNav/city
Addresses.StreetAddress	userNav/addressLine1
businessUnit	businessUnit
company	company
contractType	contractType
costCenter	costCenter
countryOfCompany	countryOfCompany
createdBy	createdBy
dateOfBirth	userNav/dateOfBirth
department	department
DisplayName	userNav/defaultFullName
division	division
Emails[0].Value	userNav/email
employeeClass	employeeClass
employmentType	employmentType
emplStatus	emplStatus

SCIM parameter	SuccessFactors HR parameter
empRelationship	empRelationship
endDate	endDate
event_	event_
eventReason	eventReason
familyRelationshipWithEmployer	familyRelationshipWithEmployer
FutureDatedEmployees	EmpJob
hazard	hazard
holidayCalendarCode	holidayCalendarCode
Id	id
isCompetitionClauseActive	isCompetitionClauseActive
isFulltimeEmployee	isFulltimeEmployee
isSideLineJobAllowed	isSideLineJobAllowed
jobCode	jobCode
jobTitle	jobTitle
laborProtection	laborProtection
location	location
managerId	managerId
matrixManagers[].displayName	userNav/matrixManager[].defaultFullName
matrixManagers[].value	userNav/matrixManager[].userId
Meta.Created	createdOn
Meta.LastModified	userNav/lastModified
Name.Familyname	userNav/lastName
Name.Formatted	userNav/defaultFullName
Name.GivenName	userNav/firstName
Name.HonorificSuffix	userNav/suffix
Name.MiddleName	userNav/mi
payGrade	payGrade
payScaleArea	payScaleArea
payScaleGroup	payScaleGroup

SCIM parameter	SuccessFactors HR parameter
payScaleLevel	payScaleLevel
payScaleType	payScaleType
PersonIdExternal	employmentNav/personIdExternal
PhoneNumbers.businessPhone	userNav/businessPhone
PhoneNumbers.cellPhone	userNav/cellPhone
position	position
probationPeriodEndDate	probationPeriodEndDate
regularTemp	regularTemp
retired	retired
seqNumber	seqNumber
standardHours	standardHours
startDate	startDate
status	status
timeRecordingVariant	timeRecordingVariant
timeTypeProfileCode	timeTypeProfileCode
timezone	timezone
travelDistance	travelDistance
userId	userId
UserName	userNav /username
workerCategory	workerCategory
workingDaysPerWeek	workingDaysPerWeek
workingTimeDirective	workingTimeDirective
workLocation	workLocation
workscheduleCode	workscheduleCode
Additional mapping of Employees in version 9	
loginMethod	userNav/loginMethod
Additional mapping of Employees in version 10.3	
isContingentWorker	employmentNav/isContingentWorker

Table 99: FutureDatedEmployees mapping

SCIM parameter	SuccessFactors HR parameter
Addresses.Country	userNav/country
Addresses.Locality	userNav/state
Addresses.PostalCode	userNav/zipCode
Addresses.Region	userNav/city
Addresses.StreetAddress	userNav/addressLine1
businessUnit	businessUnit
company	company
contractType	contractType
costCenter	costCenter
countryOfCompany	countryOfCompany
createdBy	createdBy
dateOfBirth	userNav/dateOfBirth
department	department
DisplayName	userNav/defaultFullName
division	division
Emails[0].Value	userNav/email
employeeClass	employeeClass
employmentType	employmentType
emplStatus	emplStatus
empRelationship	empRelationship
endDate	endDate
event_	event_
eventReason	eventReason
familyRelationshipWithEmployer	familyRelationshipWithEmployer
hazard	hazard
holidayCalendarCode	holidayCalendarCode
Id	id
isCompetitionClauseActive	isCompetitionClauseActive

SCIM parameter	SuccessFactors HR parameter
isFulltimeEmployee	isFulltimeEmployee
isSideLineJobAllowed	isSideLineJobAllowed
jobCode	jobCode
jobTitle	jobTitle
laborProtection	laborProtection
location	location
managerId	managerId
matrixManagers[].displayName	userNav/matrixManager[].defaultFullName
matrixManagers[].value	userNav/matrixManager[].userId
Meta.Created	createdOn
Meta.LastModified	userNav/lastModified
Name.Familyname	userNav/lastName
Name.Formatted	userNav/defaultFullName
Name.GivenName	userNav/firstName
Name.HonorificSuffix	userNav/suffix
Name.MiddleName	userNav/mi
payGrade	payGrade
payScaleArea	payScaleArea
payScaleGroup	payScaleGroup
payScaleLevel	payScaleLevel
payScaleType	payScaleType
PersonIdExternal	employmentNav/personIdExternal
PhoneNumbers.businessPhone	userNav/businessPhone
PhoneNumbers.cellPhone	userNav/cellPhone
position	position
probationPeriodEndDate	probationPeriodEndDate
regularTemp	regularTemp
retired	retired
seqNumber	seqNumber

SCIM parameter	SuccessFactors HR parameter
standardHours	standardHours
startDate	startDate
status	status
timeRecordingVariant	timeRecordingVariant
timeTypeProfileCode	timeTypeProfileCode
timezone	timezone
travelDistance	travelDistance
userId	userId
UserName	userNav /username
workerCategory	workerCategory
workingDaysPerWeek	workingDaysPerWeek
workingTimeDirective	workingTimeDirective
workLocation	workLocation
workscheduleCode	workscheduleCode
Additional mapping of FutureDatedEmployee in version 10.3	
isContingentWorker	employmentNav/isContingentWorker

Table 100: Departments mapping

SCIM parameter	SuccessFactors HR parameter
costCenter	costCenter
createdBy	createdBy
createdOn	createdOn
description	description
endDate	endDate
externalCode	externalCode
headOfUnit	headOfUnit
Id	externalCode
lastModifiedBy	lastModifiedBy
lastModifiedDateTime	lastModifiedDateTime
lastModifiedOn	lastModifiedOn

SCIM parameter	SuccessFactors HR parameter
Meta.Created	createdOn
Meta.LastModified	lastModifiedOn
name	name
parent	parent
startDate	startDate
status	status

Table 101: Locations mapping

SCIM parameter	SuccessFactors HR parameter
createdBy	createdBy
createdDateTime	createdDateTime
description	description
endDate	endDate
externalCode	externalCode
geozoneFlx	geozoneFlx
Id	externalCode
lastModifiedBy	lastModifiedBy
lastModifiedDateTime	lastModifiedDateTime
lastModifiedOn	lastModifiedOn
locationGroup	locationGroup
locationGroupFlx	locationGroupFlx
Meta.Created	createdOn
Meta.LastModified	lastModifiedOn
name	name
standardHours	standardHours
startDate	startDate
status	status
timezone	timezone

Table 102: BusinessUnits mapping

SCIM parameter	SuccessFactors HR parameter
createdBy	createdBy
createdOn	createdOn
description	description
description_de_DE	description_de_DE
endDate	endDate
externalCode	externalCode
headOfUnit	headOfUnit
Id	externalCode
lastModifiedBy	lastModifiedBy
lastModifiedOn	lastModifiedOn
Meta.Created	createdOn
Meta.LastModified	lastModifiedOn
name	name
name_de_DE	name_de_DE
startDate	startDate
status	status

Table 103: Custom object type mapping

SCIM parameter	SuccessFactors HR parameter
Id	Base 64 encoded Composite Key or Simple Key of the object
Meta.Created	createdDateTime
meta.lastModified	lastModifiedDateTime
All other non-navigational attribute will have same names at both sides	

Table 104: Mapping for V10.1

SCIM parameter	SuccessFactors HR parameter
Id	Base64encoded(id)
targetId	id

NOTE: Applicable for all object types.

Table 105: Divisions mapping

SCIM parameter	SuccessFactors HR parameter
createdBy	createdBy
createdDateTime	createdDateTime
createdOn	createdOn
description	description
endDate	endDate
externalCode	externalCode
headOfUnit	headOfUnit
Id	externalCode
lastModifiedBy	lastModifiedBy
lastModifiedDateTime	lastModifiedDateTime
lastModifiedOn	lastModifiedOn
Meta.Created	createdOn
Meta.LastModified	lastModifiedOn
name	name
parent	parent
startDate	startDate
status	status

Table 106: CostCenters mapping

SCIM parameter	SuccessFactors HR parameter
Id	externalCode
name	name
description	description
createdBy	createdBy
externalCode	externalCode
costcenterManager	costcenterManager
status	status
startDate	startDate

SCIM parameter	SuccessFactors HR parameter
endDate	endDate
parent	parent
lastModifiedOn	lastModifiedOn
createdOn	createdOn
lastModifiedBy	lastModifiedBy
Meta.LastModified	lastModifiedOn
Meta.Created	createdOn

Table 107: Companies mapping

SCIM parameter	SuccessFactors HR parameter
Id	externalCode
name	name
description	description
externalCode	externalCode
status	status
startDate	startDate
endDate	endDate
defaultLocation	defaultLocation
country	country
standardHours	standardHours
defaultPayGroup	defaultPayGroup
Meta.LastModified	lastModifiedOn
Meta.Created	createdOn

Table 108: JobCodes mapping

SCIM parameter	SuccessFactors HR parameter
Id	externalCode

SCIM parameter	SuccessFactors HR parameter
name	name
description	description
externalCode	externalCode
status	status
startDate	startDate
endDate	endDate
lastModifiedOn	lastModifiedOn
lastModifiedBy	lastModifiedBy
createdBy	createdBy
createdOn	createdOn
parentJobCode	parentJobCode
supervisorLevel	supervisorLevel
defaultSupervisorLevel	defaultSupervisorLevel
standardHours	standardHours
workerCompCode	workerCompCode
grade	grade
isFulltimeEmployee	isFulltimeEmployee
jobFunction	jobFunction
regularTemporary	regularTemporary
employeeClass	employeeClass
defaultJobLevel	defaultJobLevel
isRegular	isRegular
jobLevel	jobLevel
defaultEmployeeClass	defaultEmployeeClass
Meta.LastModified	lastModifiedOn
Meta.Created	createdOn

Table 109: Positions mapping

SCIM parameter	SuccessFactors HR parameter
Id	code
code	code
description	description
effectiveStartDate	effectiveStartDate
effectiveEndDate	effectiveEndDate
effectiveStatus	effectiveStatus
standardHours	standardHours
department	department
businessUnit	businessUnit
division	division
location	location
costCenter	costCenter
createdBy	createdBy
jobTitle	jobTitle
employeeClass	employeeClass
jobCode	jobCode
company	company
payGrade	payGrade
comment	comment
createdDate	createdDate
jobLevel	jobLevel
lastModifiedBy	lastModifiedBy
lastModifiedDate	lastModifiedDate
positionTitle	positionTitle
vacant	vacant
regularTemporary	regularTemporary
payRange	payRange
Meta.LastModified	lastModifiedDate

SCIM parameter	SuccessFactors HR parameter
Meta.Created	createdDate
lastModifiedDateTime	lastModifiedDateTime

NOTE: Disable the **lastModifiedDate** or **lastModifiedDateTime** attribute based on the availability in the instance. Disabling both at the same time may introduce performance issues.

Table 110: EmpEmployments mapping

SCIM parameter	SuccessFactors HR parameter
Id	userId
userId	userId
personIdExternal	personIdExternal
startDate	startDate
createdBy	createdBy
createdOn	createdOn
firstDateWorked	firstDateWorked
lastDateWorked	lastDateWorked
lastModifiedBy	lastModifiedBy
Meta.LastModified	lastModifiedOn
Meta.Created	createdOn

Table 111: PerPersonals mapping

SCIM parameter	SuccessFactors HR parameter
createdBy	createdBy
createdOn	createdOn
emails[].displayName	personNav/emailNav/result[].emailAddress
emails[].emailType	personNav/emailNav/result[].emailType
emails[].primary	personNav/emailNav/result[].isPrimary
emails[].value	personNav/emailNav/result [].personIdExternal,personNav/emailNav/result [].emailType

SCIM parameter	SuccessFactors HR parameter
firstName	firstName
gender	gender
Id	personIdExternal
lastModifiedBy	lastModifiedBy
lastName	lastName
Meta.Created	createdOn
Meta.LastModified	lastModifiedOn
personIdExternal	personIdExternal
preferredName	preferredName
startDate	startDate

Table 112: PerPhones mapping

SCIM parameter	SuccessFactors HR parameter
areaCode	areaCode
countryCode	countryCode
createdBy	createdBy
createdOn	createdOn
Id	personIdExternal,phoneType
isPrimary	isPrimary
lastModifiedBy	lastModifiedBy
lastModifiedOn	lastModifiedOn
Meta.Created	createdOn
Meta.LastModified	lastModifiedOn
personIdExternal	personIdExternal
phoneNumber	phoneNumber
phoneType	phoneType

NOTE: The **PerPhones** table of SuccessFactors HR Instance supports composite key-based lookup. The composite key consists of **personIdExternal** and **phoneType**.

Table 113: EventReasons mapping

SCIM parameter	SuccessFactors HR parameter
Id	externalCode
externalCode	externalCode
name	name
status	status
event_	event_
emplStatus	emplStatus
description	description
startDate	startDate
createdOn	createdOn
createdBy	createdBy
lastModifiedOn	lastModifiedOn
lastModifiedBy	lastModifiedBy
Meta.LastModified	lastModifiedOn
Meta.Created	createdOn

Table 114: PicklistOptions mapping

SCIM parameter	SuccessFactors HR parameter
externalCode	externalCode
Id	id
status	status

Table 115: PicklistLabels mapping

SCIM parameter	SuccessFactors HR parameter
Id	optionId
id_	id
label	label
locale	locale
optionId	optionId

Table 116: PerEmails mapping

SCIM parameter	SuccessFactors HR parameter
createdBy	createdBy
createdDateTime	createdDateTime
createdOn	createdOn
emailAddress	emailAddress
emailType	emailType
Id	personIdExternal,emailType
isPrimary	isPrimary
lastModifiedBy	lastModifiedBy
lastModifiedDateTime	lastModifiedDateTime
lastModifiedOn	lastModifiedOn
Meta.LastModified	lastModifiedOn
personIdExternal	personIdExternal

NOTE: The **PerEmails** table of SuccessFactors HR Instance supports composite key-based lookup. The composite key consists of **personIdExternal** and **emailType**.

Table 117: EmpJobRelationship mapping

SCIM parameter	SuccessFactors HR parameter
Id	base 64 encoded (userId+startDate+relationshipType)
originalId	userId+startDate+relationshipType
relationshipType	relationshipType
userId	userId
relUserId	relUserId
startDate	startDate
endDate	endDate
createdBy	createdBy
lastModifiedBy	lastModifiedBy
meta.LastModified	lastModifiedOn
meta.CreatedOn	createdOn

Connector limitations

- **DELETE** operation is supported only by the **PerEmails** endpoint.
- Except for **PerEmails** and **PerPhones**, **CREATE** operation is also not supported by any other endpoints.
- **UPDATE** operation is supported by two endpoints on selected attributes as listed below:
  - Employees - username, cellPhone, businessPhone, and email
  - PerEmails - emailAddress, emailType.
  - PerPhones - phoneNumber, phoneType, areaCode, countryCode, and isPrimary.
- If there are multiple records with same 'startDate' coming in at a later point, then it would not be handled since 'startDate' doesn't have a time stamp.
- 'startDate' is in servertime. Hence, it can't be converted into UTC as the timezone information of the SAP server is unavailable.
- PerPhones and PerEmails endpoints do not support filters on "id" attribute of SCIM response.

Connector versions and features

The following subsections describe the different connector version(s) and features available with them.

Features available exclusively in SuccessFactors HR v.2.0

Following are the features that are available exclusively in **SuccessFactors HR v.2.0**:

- For the **Employees** object, the **Get Employee** operation has been modified to get both **active** and **inactive Employees**.

  NOTE: To insert only Active Members in One Identity Manager, the synchronization workflow configuration must be modified to have a filter based on status attribute in the insert step.
- **Employees** endpoint is enhanced to return the Future Hires of the HR system.

Features available exclusively in SuccessFactors HR v.3.0

Following are the features that are available exclusively in **SuccessFactors HR v.3.0**:

- The attributes of all object schemas can be disabled or enabled while configuring the connector based on your requirements.

  NOTE:

  - Mandatory attributes cannot be disabled.
  - For more information about how to disable attributes, see Disabling attributes

- You can configure custom attributes for the **SuccessFactors HR v.3.0** SCIM connector in Starling Connect for all objects.

  NOTE:

  - For more information about how to configure custom attributes, see Configuring custom attributes in connectors

- The connector supports new **PerEmails** endpoint that allows you to browse and synchronize the data. It also allows you to update and create email records in the **PerEmail** table.
- Fetching of future-dated employees/updates can be prevented by enabling the **Fetch effective dated records only** flag.

Features available exclusively in SuccessFactors HR v4.0

Following are the features that are available exclusively in SuccessFactors HR v.4.0:

- The naming convention for all the custom attributes has been enhanced that belongs to a navigational object class.
- Support for UTC date time.
- Support for multi-level navigational custom attributes.

Features available exclusively in SuccessFactors HR v5.0

- The Employees endpoint is enhanced to consider lastModified date of both EmpJob and User table.

- Added a flag 'Separate Effective And FutureDated Employees Endpoints' which when enabled, makes the **Employees** endpoint to return effective dated employees only and provides a new endpoint 'FutureDatedEmployees' to return future dated records only.
- Added a flag 'Activate Custom Attributes With Full Name' which when enabled, the naming convention for all the custom attributes will not be prefixed with the navigational attribute names.
- Support for multi-level navigational custom attributes with the flag "Activate Custom Attributes with full name" ON.

Features available exclusively in SuccessFactors HR v6.0

- All the features are available which is supported in v.5.0.
- v.6.0 has no feature change only addition is that it supports OAuth Authentication.
- For detailed explanation on setting up the OAuth authentication, refer SetUp OAuth.

Features available exclusively in SuccessFactors HR v7.0

- v.7.0 has consistent names for all resource types in ResourceTypes endpoint as well as in individual resource endpoints.

Features available exclusively in SuccessFactors HR v8.0

- The FutureDatedEmployees endpoint is modified to return the next effective record.

Features available exclusively in SuccessFactors HR v9.0

- READ operations on Custom Foundation Objects are supported. (Refer Custom Foundation Objects in Successfactors HR connector)

- Update operation on Custom attribute supported. (Refer Creating custom editable/upsertable attributes in Successfactors employee central)

  | NOTE: Supported under Employees, EmpEmployments and PerPersonals.

- PickListLables "id" attribute value changes to "optionId,locale".
- Support for loginMethod attributes with the flag "loginMethod" ON.

Features available exclusively in SuccessFactors HR v10.0

- Positions Endpoint return FutureDated positions using query parameter (?futureDated=true).
- PerPersonal Endpoint return FutureDated PerPersonal using query parameter (?futureDated=true).
- Supports new endpoints FutureDatedPerPersonals and FutureDatedPositions to handle the PerPersonal and Position records respectively which are having future effective dates.
- Supports new endpoint EmpJobRelationships.

Features available exclusively in SuccessFactors HR v10.1

- Added a flag ”Use base 64 encoded id in synchronization” which when enabled, makes all the endpoints to return one new attribute “targetId”.
- The "id" in the SCIM response will be base 64 encoded.

Features available exclusively in SuccessFactors HR v10.2

- In v10.2 onwards, the id of all resources (except custom objects) containin single quote (') in the id will be bypassed using another the single quote for correct usage in the SuccessFactors API requests. For example, id "test'd" will be changed as "test''d".

Support for Filter Condition

SuccessFactorsHR connector supports the filter condition for all the objects (i.e., endpoints). We could apply the filter condition and take the filtered records from SuccessFactorsHR target system.

- The connector **supports** filter conditions for all the objects.
- The connector **supports** filter condition in all the Versions.
- Supports only **AND**, **OR**, and **NOT** logical operators.
- Supports only parenthesis **()** for grouping the condition.
- The connector **supports only single quotes (‘) with filter condition value** (ex: phoneType co '10101')
- Filter conditions should be applied on those attributes that can be filtered. For more information, refer List of Attributes for Filter Condition.
- **Complex attributes are not supported in the filter condition** (example: name, email). **Only sub-attributes are supported**. (email.value, name.familyName)
- Filter condition should follow the syntax

  For example:

  1. <attribute_name><space><operator><space>'<string_value or date_value>'

  2.<attribute_name><space><operators><space><int_value or bool_value>
- Filter condition values **should NOT have single quotes or percentage with the filter condition value** example: (userName co 'O'Malley') or (userName co 'O%Malley%')
- Filter condition is **NOT supported** by the connector for **Custom attributes**.
- Supports the following operators to filter the values with example should apply in OneIM.

S.No	Operators	OneIM System filters	OneIM Select Objects
1	eq → equal to	phoneType eq '00000'	phoneType = '00000'
2	ne → not equal to	phoneType ne '00000'	phoneType <> '00000'
3	co → contains	phoneType co '00000'	phoneType like '%00000%'
4	sw → starts with	phoneType sw '00000'	phoneType like '00000%'
5	ew → ends with	phoneType ew	phoneType like '%00000'

		'00000'	
6	gt → greater than	phoneType gt 100	phoneType > 100
7	lt → less than	phoneType lt 100	phoneType < 100
8	ge → greater than or equal to	phoneType ge 500	phoneType >= 500
9	le → less than or equal to	phoneType le 500	phoneType <= 500

Some of the example filter conditions (Should be applied at OneIM):

- phoneType co '1'
- phoneType eq '00000'
- emails.value co 'someone.may' or emails.value co 'test.user'
- not areaCode co '1' and not ((not countryCode sw '1' or phoneType ew '6') and is Primary eq true)

List of Attributes for Filter Condition

The endpoints exposed by the SuccessFactorsHR connector supports filtering of target system data from One Identity Manager. Here is the detailed list of endpoints with both Filterable and non-filterable attributes, used in filter conditions.

Table 118: Employees

Section	Attributes
Table	EmpJob
Filterable	userId, timezone, department, businessUnit, division, location, costCenter, company, startDate, seqNumber, workingTimeDirective, emplStatus, event, eventReason, endDate, timeTypeProfileCode, timeRecordingVariant, employmentType, workscheduleCode, regularTemp, payScaleGroup, probationPeriodEndDate, payScaleType, managerId, jobCode, createdBy, position, retired, employeeClass, familyRelationshipWithEmployer, isCompetitionClauseActive, standardHours, jobTitle, countryOfCompany, hazard, travelDistance, isSideLineJobAllowed,

Section	Attributes
	payScaleArea, holidayCalendarCode, contractType, payGrade, workLocation, workingDaysPerWeek, empRelationship, isFulltimeEmployee, laborProtection, pensionProtection, payScaleLevel, worker-Category
Non filterable	NONE

Table 119: BusinessUnits

Section	Attributes
Table	FOBusinessUnit
Filterable	externalCode, name, description, createdBy, status, createdOn, lastModi-fiedBy, startDate, endDate, headOfUnit, description_de_DE, name_de_DE, lastModi-fiedOn
Non filterable	NONE

Table 120: Companies

Section	Attributes
Table	FOCompany
Filterable	externalCode, name, description, currency, createdBy, status, startDate, endDate, defaultLocation, country, standardHours, defaultPayGroup, createdOn, lastModi-fiedOn
Non filterable	NONE

Table 121: Department

Section	Attributes
Table	FODepartment
Filterable	externalCode, name, description, createdBy, costCenter, headOfUnit, status, startDate, endDate, lastModi-fiedDateTime, parent, createdOn, lastModi-

Section	Attributes
	fiedBy, lastModifiedOn
Non filterable	NONE

Table 122: Locations

Section	Attributes
Table	FOLocation
Filterable	externalCode, name, createdBy, createdOn, createdDateTime, lastModifiedBy, lastModi-fiedOn, lastModi-fiedDateTime, startDate, endDate, status
Non filterable	description, timezone, geozoneFlx, locationGroup, locationGroupFlx, standardHours

Table 123: CostCenters

Section	Attributes
Table	FOCostCenter
Filterable	externalCode, name, description, createdBy, costcenterManager, startDate, endDate, createdOn, lastModifiedBy, parent, status, lastModifiedOn
Non filterable	NONE

Table 124: Divisions

Section	Attributes
Table	FODivision
Filterable	externalCode, name, description, createdBy, status, startDate, endDate, lastModifiedDateTime, parent, createdOn, lastModifiedBy, createdDateTime, headOfUnit, lastModifiedOn
Non filterable	NONE

Table 125: EmpEmployments

Section	Attributes
Table	EmpEmployment
Filterable	personIdExternal, startDate, createdBy, createdOn, lastModifiedBy, lastModifiedOn
Non filterable	firstDateWorked, lastDateWorked

Table 126: EventReasons

Section	Attributes
Table	FOEventReason
Filterable	externalCode, name, status, startDate, lastModifiedBy, createdBy, createdOn, lastModifiedOn
Non filterable	event emplStatus, description

Table 127: JobCodes

Section	Attributes
Table	JobCode
Filterable	externalCode, name, status, description, startDate, endDate, lastModifiedBy, createdBy, createdOn, parentJobCode, supervisorLevel, defaultSupervisorLevel, standardHours, workerCompCode, grade, isFulltimeEmployee, jobFunction, regularTemporary, employeeClass, defaultJobLevel, isRegular, jobLevel, defaultEmployeeClass, lastModifiedOn
Non filterable	NONE

Table 128: PerEmails

Section	Attributes
Table	PerEmail
Filterable	personIdExternal, emailAddress, emailType, lastModifiedDateTime, createdBy, isPrimary, lastModifiedBy, createdDateTime, createdOn, lastModi-fiedOn
Non filterable	NONE

Table 129: PerPersonals

Section	Attributes
Table	PerPersonal
Filterable	personIdExternal, firstName, lastName, gender, startDate, createdBy, createdOn, lastModifiedBy, lastModifiedOn
Non filterable	preferredName

Table 130: PerPhones

Section	Attributes
Table	PerPhone
Filterable	personIdExternal, phoneNumber, phoneType, createdBy, createdOn, areaCode, countryCode, isPrimary, lastModifiedBy, lastModifiedOn
Non filterable	NONE

Table 131: PicklistLabels

Section	Attributes
Table	PicklistLabel
Filterable	id, locale, label, optionId
Non filterable	NONE

Table 132: PicklistOptions

Section	Attributes
Table	PicklistOption
Filterable	id, status, externalCode
Non filterable	NONE

Table 133: Positions

Section	Attributes
Table	Position
Filterable	code, description, effectiveStartDate, effectiveEndDate, effectiveStatus, standardHours, department, businessUnit,

Section	Attributes
	division, location, costCenter, jobTitle, employeeClass, jobCode, company, payGrade, jobLevel, positionTitle, vacant, regularTemporary, createdBy, createdDate, lastModifiedBy, lastModifiedDate, lastModifiedDateTime, externalName_defaultValue
Non filterable	payRange

Configuring changes in One Identity Manager to support filter conditions

1. Open the **Synchronization Editor** tool.
2. Select **SCIM connector** and the Target system
3. Navigate to **Schema Classes**.
4. Add a new schema class for the perphone.
5. Add the **System filter** and **Select Object** condition. Click **Commit to Database**.
6. In PerPhones mappings, edit the **Target** system schema class with the recently created schema and click **Commit to Database**.
7. Run the synchronization.

   The Filter conditions will be created.

Conditions on "Fetch Effective Dated Records Only" & "Separate Effective And Future Dated Employees Endpoints" flags based on different use cases (for version v.5.0 and above)

- Use Case #1: Get effective or future dated(if effective record does not exist) employee records in the employees endpoint response
  - "Fetch Effective Dated Records Only" - OFF
  - "Separate Effective And FutureDated Employees Endpoints" - OFF
- Use Case #2: Get only effective employee records in the employees endpoint response and no separate endpoint for future dated employee records

    - "Fetch Effective Dated Records Only" - ON
    - "Separate Effective And FutureDated Employees Endpoints" - OFF
- Use Case #3: Get only effective employee records in the employees endpoint response and get a separate endpoint for future dated employee records
    - "Fetch Effective Dated Records Only" - ON
    - "Separate Effective And FutureDated Employees Endpoints" - ON

22

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
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details)

Supported objects and operations

Users

Table 134: Supported operations for Users

Operation	VERB
Create	POST
Update	PUT
Delete	DELETE

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

Groups

Table 135: Supported operations for Groups

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

Mandatory fields

Users

- emails.value

Groups

- displayName

User and Group mapping

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

Table 136: User mapping

SCIM parameter	NutShell parameter
id	id
userName	email
name.familyName	lastName
name.givenName	firstName
displayName	name
emails[0].value	email
active	isEnabled
groups	teams
meta.created	createdTime
meta.lastModified	modifiedTime

Table 137: Group mapping

SCIM parameter	NutShell parameter
id	id
displayName	name
enterpriseExtension.division	division
meta.created	createdTime
meta.lastModified	modifiedTime

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.

23

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)
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details).

Supported objects and operations

Users

Table 138: Supported operations for Users

Operation	VERB
Get user by Id	GET
Get all users	GET

Groups

Table 139: 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

User and Group mapping

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

Table 140: User Mapping

SCIM Parameter	Insightly Parameter
Id	USER_ID
emails[0].value	EMAIL_ADDRESS
DisplayName	FIRST_NAME + LAST_NAME
name.FirstName	FIRST_NAME

SCIM Parameter	Insightly Parameter
name.LastName	LAST_NAME
name.Formatted	FIRST_NAME + LAST_NAME
active	ACTIVE
timezone	TIMEZONE_ID
meta.created	DATE_CREATED_UTC
userName	EMAIL_ADDRESS
meta.lastModified	DATE_UPDATED_UTC

Table 141: Group mapping

SCIM parameter	Insightly parameter
id	TEAM_ID
displayName	TEAM_NAME
created	DATE_CREATED_UTC
lastModified	DATE_UPDATED_UTC
members[].value	TEAMMEMBERS[].MEMBER_USER_ID

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.

NOTE: If the version of One Identity Manager is 8.0.2 , an error is returned, if the Group objects are more than four. If the version of One Identity Manager is 7.1.4, the display names of few groups would be missing in the Manager console of One Identity Manager, if the Group objects are more than twenty. The cause for the above mentioned irregularities is that, the Insightly cloud application can handle only five requests per second, if the account is a trial version.

24

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)
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details).

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 142: Supported operations for Users

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

Groups

Table 143: 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

User and Group mapping

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

Table 144: User mapping

SCIM parameter	Egnyte parameter
Id	Id
externalId	externalId
userName	userName
Name.FamilyName	name.FamilyName
Name.givenName	name.givenName
Name.Formatted	name.Formatted
DisplayName	name.Formatted
email.value	email
Active	active
userType	userType
EnterpriseExtension.authType	authType
Groups.DisplayName	groups.DisplayName
Groups.Value	groups.Value
Created	createdDate
LastModified	lastModificationDate

Table 145: Group mapping

SCIM parameter	Egnyte parameter
Id	id
displayName	displayName
members.value	members.value
members.display	members.display

Connector limitations

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

25

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)
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details).

Supported objects and operations

Users

Table 146: Supported operations for Users

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

Groups

Table 147: Supported operations for Groups

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

Mandatory fields

Users

- UserName

Groups

- Not Applicable

User and Group mapping

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

Table 148: User mapping

SCIM parameter	SugarCRM parameter
Id	id
UserName	user_name
Title	title
PreferredLanguage	preferred_language
name.FirstName	first_name
name.LastName	last_name
name.Formatted	full_name
Address.StreetAddress	address_street
Address.Region	address_city
Address.Country	address_country
Address.PostalCode	address_postalcode
Emails.value	email[0].email_address
Active	status.Value == "Active"
Groups[].display	team_name[].name
Groups[].value	team_name[].id
PhoneNumbers[].Value	phone_home
PhoneNumbers[].Value	phone_mobile
PhoneNumbers[].Value	phone_work
Meta.Created	date_entered
Meta.LastModified	date_modified

Table 149: Group mapping

SCIM parameter	SugarCRM parameter
id	id
displayName	name
Meta.created	date_entered
Meta.lastModified	date_modified

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.

26

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)
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details)

Supported objects and operations

Users

Table 150: 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 151: 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

User and Group mapping

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

Table 152: User mapping

SCIM Parameter	Oracle IDCS parameter
Id	id
userName	userName
externalId	externalId
name.givenName	name.givenName
name.familyName	name.familyName
name.middleName	name.middleName
name.formatted	name.formatted
name.honorificPrefix	name.honorificPrefix
name.honorificSuffix	name.honorificSuffix
displayName	displayName
nickName	nickName
emails.value	email.value
emails.type	email.type
emails.primary	email.primary
addresses.formatted	addresses.formatted
addresses.streetAddress	addresses.streetAddress
addresses.locality	addresses.locality
addresses.region	addresses.region
addresses.postalCode	addresses.postalCode
addresses.country	addresses.country
addresses.type	addresses.type

SCIM Parameter	Oracle IDCS parameter
phoneNumbers.value	phoneNumbers.value
phoneNumbers.type	phoneNumbers.type
phoneNumbers.primary	phoneNumbers.primary
password	password
profileUrl	profileUrl
title	title
userType	userType
preferredLanguage	preferredLanguage
locale	locale
timezone	timeZone
active	active
entitlements.value	entitlements.value
entitlements.display	entitlements.display
entitlements.type	entitlements.type
roles.value	roles.value
roles.display	roles.display
roles.type	roles.type
groups.value	groups.value
groups.display	groups.display
extension.organization	extension.organization
extension.division	extension.division
extension.department	extension.department
extension.manager.value	extension.manager.value
extension.manager.displayName	extension.manager.displayName
extension.costCenter	extension.costCenter
extension.employeeNumber	extension.employeeNumber
meta.created	meta.created
meta.lastModified	meta.lastModified

Table 153: Group mapping

SCIM parameter	Oracle IDCS parameter
id	id
displayName	displayName
Members.value	members.value
Members.display	members.display
extension.externalId	extension.externalId
extension.description	extension.description
meta.created	meta.created
meta.lastModified	meta.lastModified

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.

27

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
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details).

Supported objects and operations

Users

Table 154: Supported operations for Users

Operation	VERB
Create User	POST
Delete User	DELETE

Operation	VERB
Get User	GET
Get All Users	GET

Groups

Not Applicable

Mandatory fields

Users

- emails.value
- password

Groups

Not Applicable

User and Group mapping

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

Table 155: User mapping

SCIM parameter	Statuspage parameter
Id	id
UserName	email
last_name	name.familyName
first_name	name.givenName
first_namelast_name	name.formatted

SCIM parameter	Statuspage parameter
first_namelast_name	displayName
email	emails[0].value
created_at	meta.created
updated_at	meta.lastModified

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.

28

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)
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details)

Supported objects and operations

Users

Table 156: Supported operations for Users

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

Groups

Not Applicable

Mandatory fields

Users

Not Applicable

Groups

Not Applicable

NOTE: Additional features supported: Zendesk Sell connector supports attribute selection for the response based on the attributes mentioned in the query parameters ?attributes=.

User and Group mapping

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

Table 157: User mapping

SCIM parameter	Zendesk Sell parameter
Id	id
userName	email
name.Formatted	name
DisplayName	name
email.value	email
PhoneNumbers.value	phone_number
Active	status

SCIM parameter	Zendesk Sell parameter
Timezone	timeZone
Groups.Value	group.id
Groups.display	group.name
Extension.manager.value	reports_to
Created	created_at
LastModified	updated_at

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.

29

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
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details).

Supported objects and operations

Users

Table 158: Supported operations for Users

Operation	VERB
Get User	GET
Get All Users	GET

Groups

Not Applicable

Mandatory fields

Users

Not Applicable

Groups

Not Applicable

NOTE: Additional features supported: Workbooks connector supports attribute selection for the response based on the attributes mentioned in the query parameters ?attributes=.

User and Group mapping

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

Table 159: User mapping

SCIM parameter	Workbooks parameter
Id	id
userName	login_name
name.Formatted	person_name
displayName	person_name
emails[0].value	login_name
timezone	timezone
locale	date_time_locale

SCIM parameter	Workbooks parameter
active	is_enabled
meta.created	created_at
meta.lastModified	updated_at

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.

30

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. Refer section Configuring integration application for detailed instructions.

- Connector name
- Admin User Id
- Client Id
- Private Key
- Auth Server (account-d.docusign.com for developer environments and account.docusign.com for production environments)
- Account ID
- Target URL (Cloud application's instance URL used as targetURI in payload)
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details)

Supported objects and operations

Users

Table 160: Supported operations for Users

Operation	VERB
Create User	POST
Update User	PUT
Delete User	DELETE
Get User	GET
Get All Users	GET
Get All Users with Pagination	GET

Groups

Table 161: Supported operations for Groups

Operation	VERB
Create Group	POST
Update Group	PUT
Delete Group	DELETE
Get Group	GET
Get All Groups	GET
Get All Groups with Pagination	GET
Update Membership	PUT

Mandatory fields

Users

- UserName
- Email

Groups

- DisplayName

User and Group mapping

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

Table 162: User mapping

SCIM parameter	DocuSign parameter
Id	userId
UserName	userName
UserType	userType
DisplayName	userName
Title	jobTitle
name.GivenName	firstName
name.FamilyName	lastName
Addresses.StreetAddress	workAddress.address1
Addresses.Locality	workAddress.address2
Addresses.Region	workAddress.city
Addresses.Country	workAddress.country
Addresses.postalCode	workAddress.postalCode
PhoneNumbers.Value	workAddress.phone

SCIM parameter	DocuSign parameter
Emails.Value	email
Active	userStatus
Groups	groupList
Meta.Created	createdDateTime

Table 163: Group mapping

SCIM parameter	DocuSign parameter
id	groupId
displayName	groupName

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.

31

Citrix 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)
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details).

Supported objects and operations

Users

Table 164: Supported operations for Users

Operation	VERB
Create User	POST

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

Groups

Table 165: Supported operations for Groups

Operation	VERB
Create Group	POST
Update Group	PATCH
Delete Group	DELETE
Get Group	GET
Get Group Members	GET
Add Group Members	POST
Remove Group Members	DELETE
Get All Groups	GET

Mandatory fields

Users

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

Groups

Not Applicable

User and Group mapping

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

Table 166: User mapping

SCIM Parameter	Citrix ShareFile parameter
Id	id
userName	email
name.Formatted	FullName
Name.FamilyName	LastName
Name.GivenName	FirstName
Password	Password
DisplayName	FullName
email.value	email
Active	IsDeleted
Extension.Organization	Company
Created	DateCreated

Groups

Table 167: User mapping

SCIM parameter	Citrix ShareFile parameter
Id	id
DisplayName	Name
members.value	User.Id
members.display	User.FirstName+User.LastName

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.

32

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)
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details)

Supported objects and operations

Users

Table 168: Supported operations for Users

Operation	VERB
Create User	POST
Update User	PUT
Delete User	DELETE

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

Groups

Table 169: Supported operations for Users

Operation	VERB
Create Group	POST
Update Group	PUT
Delete Group	DELETE
Get Groups	GET
Get All Groups	GET
Get All Users with Pagination	GET
Update Membership	PUT

Mandatory fields

Users

- DisplayName
- Email

Groups

DisplayName

NOTE: Additional features supported: Zendesk connector supports attribute selection for the response based on the attributes mentioned in the query parameters ?attributes=.

User and Group mapping

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

Table 170: User mapping

SCIM parameter	Zendesk parameter
Id	id
UserName	email
DisplayName	name
Timezone	time_zone
Locale	locale
PhoneNumbers[].Value	phone
Emails[].Value	email
Active	active
Meta.Created	created_at
Meta.LastModified	updated_at

Groups

Table 171: Groups mapping

SCIM parameter	Zendesk parameter
Id	id
DisplayName	name
Meta.Created	created_at
Meta.LastModified	updated_at

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.
- APIs are rate limited and for more details refer Usage limits.

33

Azure AD

Azure AD 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.

Azure AD connectors are available for use with One Identity Safeguard for Privileged Passwords.

NOTE: Update the synchronization shell or create a new synchronization shell in One Identity Manager as changes are introduced in the schema.

Connector Configuration

Azure AD connector requires customer consent to retrieve resource details using the REST APIs. The Azure AD connector supports the configuration of both single tenant and multi tenant connectors. You can switch from a single tenant connector to a multi tenant connector while configuring the connector in Starling Connect UI.

NOTE:

- To provide consent, use an account with **Global administrator** or **Privileged role administrator** role in the Azure Active Directory tenant.
- For more information, see
  - Registering the application, providing necessary permissions, retrieving Client Id and Client Secret from the Azure AD tenant
  - Configuring a connector that uses the consent feature
- Safeguard for Privileged Passwords only allows for a single tenant connector configuration.

Supervisor configuration parameters for single tenant connector

To configure the single tenant 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).
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details).

Supervisor configuration parameters for multi tenant connector

To configure the multi tenant connector, following parameters are required:

- 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).
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details).

Supported objects and operations

Users

Table 172: Supported operations for Users

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

Groups

Table 173: Supported operations for Groups

Operation	VERB
Create Group	POST
Update Group	PATCH
Delete Group	DELETE
Get Group	GET
Get All Groups	GET

Application

Table 174: Supported operations for Application

Operation	VERB
Get Application	GET
Get All Applications	GET

Mandatory fields

Create/Update User

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

Groups

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

Invite User

- redirectUrl
- emails[].value
- userType

User Group and Application mapping

The user, group and application mappings are listed in the tables below:

Table 175: User mapping

SCIM parameter	Azure AD parameter
active	accountEnabled
addresses[0].country	country
addresses[0].locality	city
addresses[0].postalCode	postalcode
addresses[0].region	state
addresses[0].streetAddress	streetAddress
displayName	displayName
emails[0].value	userPrincipalName
groups[].display	memberOf[].displayName
groups[].value	memberOf[].id
Id	id
meta.created	createdDateTime
name.familyName	surname

SCIM parameter	Azure AD parameter
name.givenName	givenName
nickName	mailNickname
phoneNumbers[0].value	businessPhones[0]
preferredLanguage	preferredLanguage
redemptionUrl	inviteRedeemUrl
redirectUrl	inviteRedirectUrl
title	jobTitle
userExtension.applications[].display	applications[].displayName
userExtension.applications[].principalId	applications[].principalId
userExtension.applications[].principalType	applications[].principalType
userExtension.applications[].value	applications[].appId
userExtension.department	department
userExtension.employeeNumber	employeeId
userExtension.manager.displayName	manager.displayName
userExtension.manager.value	manager.id
userExtension.organization	companyName
userName	userPrincipalName
userType	userType

Groups

Table 176: Group mapping

SCIM parameter	Azure AD parameter
enterpriseExtension.applications[].value	applications[].appId
enterpriseExtension.applications[].display	applications[].displayName
enterpriseExtension.applications[].principalId	applications[].principalId
enterpriseExtension.applications[].principalType	applications[].principalType
displayName	displayName

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

Application

Table 177: Application Mapping

SCIM parameter	Azure AD parameter
appId	appId
displayName	displayName
Id	id
meta.created	createdDateTime
publisherDomain	publisherDomain

Connector limitations

- **lastModified** is not provided along with the **Users**, **Groups** and **Applications**.
- 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.
- If an appRole is assigned to a group, then only the direct user members of that group will also have these appRoles assigned to them, but not group members of that group.
- 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.

Azure AD connector for Safeguard for Privileged Passwords

- For Safeguard for Privileged Passwords, you must assign at least the **Helpdesk Administrator** role for the application created, but should assign a higher role if you want to manage special accounts (for example, **Billing Administrator** or **Global Administrator**).
- For Safeguard for Privileged Passwords, the Azure AD application registration must be public.
- Safeguard for Privileged Passwords only allows for a single tenant connector configuration.

34

Google Workspace

Google Workspace (formerly GSuite) 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 Google Workspace services. For information on creating a service account, see Creating a service account in Google Workspace.

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, for example: https://www.googleapis.com/admin/directory/v1)
- Customer Id
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details).

Supported objects and operations

Users

Table 178: Supported operations for Users

Operation	VERB
Create User	POST
Update User	PUT
Delete User	DELETE
Get User	GET
Get All Users	GET
Get All Users with Pagination	GET

Groups

Table 179: Supported operations for Groups

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

Mandatory fields

Users

- FirstName
- LastName
- Password

Groups

Email

User and Group mapping

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

Table 180: User mapping

SCIM parameter	Google Workspace parameter
Id	id
userName	primaryEmail
Name.GivenName	name.givenName
Name.FamilyName	name.familyName
Name.Formatted	name.fullName
DisplayName	name.fullName
Emails[0].value	primaryEmail
Addresses[0].StreetAddress	streetAddress
Addresses[0].Locality	locality
Addresses[0].Region	region
Addresses[0].PostalCode	postalcode
PhoneNumbers[0].Value	phones[0].value
PhoneNumbers[0].Type	phones[0].type
Active	suspended
ExternalId	externalIds.value
Extension.Organization	organizations.name
Extension.Department	organizations.department
Extension.Division	organizations.location
Created	creationTime

Groups

Table 181: User mapping

SCIM parameter	Google Workspace parameter
Id	id
displayName	name
members.value	groupMembers.id
members.type	groupMembers.type
groupExtension.Email	email
groupExtension.Description	description

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.

Google Workspace connector for Safeguard for Privileged Passwords

- The following OAuth scopes need to be authorized:
  - https://www.googleapis.com/auth/admin.directory.user
  - https://www.googleapis.com/auth/admin.directory.group
  - https://www.googleapis.com/auth/admin.directory.group.member
  - https://www.googleapis.com/auth/admin.directory.domain
  - https://www.googleapis.com/auth/admin.directory.rolemanagement

35

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 (in v.1.0)
- Password (in v.1.0)
- Geolocation (in v.1.0)
- RefreshToken (in v.2.0)
- Target URL (Cloud application's instance URL used as targetURI in payload)
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details).

Supported objects and operations

Users

Table 182: Supported operations for Users (for v1.0)

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

Table 183: Supported operations for Users (for v2.0)

Operation	VERB
Get User	GET
Get All Users	GET
Get All Users with Pagination	GET
Create User	POST
Update User	PUT

Groups

NA

Mandatory fields

Users (v1.0)

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

Users (v2.0)

- userName
- name.givenName
- name.familyName
- emails[].value
- emails[].type
- active
- enterpriseUserExtension.companyId
- enterpriseUserExtension.startDate
- entitlements[].value
- roles[].value
- enterpriseUserExtension.employeeNumber

Groups

NA

User and Group mapping

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

Table 184: User mapping

SCIM parameter	Concur parameter
Id	LoginId
userName	LoginId
Name.GivenName	FirstName
name.MiddleName	Mi
Name.FamilyName	LastName
DisplayName	FirstName+LastName
Emails[0].value	EmailAddress
Active	Active
Locale	LocaleName
Extension.EmpId	EmpId
Extension.LedgerKe	LedgerName
Extension.CtryCode	CtryCode
Extension.CrnKey	CrnKey
Extension.ExpenseApprover	ExpenseApprover
Extension.Custom1	Custom1
Extension.Custom2	Custom2
Extension.Custom3	Custom3
Extension.Custom4	Custom4
Extension.Custom5	Custom5
Extension.Custom6	Custom6
Extension.Custom7	Custom7
Extension.Custom8	Custom8
Extension.Custom9	Custom9
Extension.Custom10	Custom10
Extension.Custom11	Custom11

SCIM parameter	Concur parameter
Extension.Custom12	Custom12
Extension.Custom13	Custom13
Extension.Custom14	Custom14
Extension.Custom15	Custom15
Extension.Custom16	Custom16
Extension.Custom17	Custom17
Extension.Custom18	Custom18
Extension.Custom19	Custom19
Extension.Custom20	Custom20
Extension.Custom21	Custom21
Extension.OrgUnit1	OrgUnit1
Extension.OrgUnit2	OrgUnit2
Extension.OrgUnit3	OrgUnit3
Extension.OrgUnit4	OrgUnit4
Extension.OrgUnit5	OrgUnit5
Extension.OrgUnit6	OrgUnit6

Table 185: User v2 mapping

SCIM parameter	Concur parameter
Active	active
Addresses	addresses
DisplayName	displayName
Emails[].value	emails[].value
Extension.CompanyId	extension.companyId
Extension.CostCenter	extension.costCenter
Extension.Department	extension.department
Extension.Division	extension.division
Extension.EmployeeNumber	extension.employeeNumber
Extension.Manager.value	extension.manager.value
Extension.Organization	extension.organization

SCIM parameter	Concur parameter
Extension.StartDate	extension.startDate
Extension.TerminationDate	extension.terminationDate
externalId	externalId
Id	id
Meta.Created	meta.created
Meta.LastModified	meta.lastModified
Name.FamilyName	name.familyName
Name.GivenName	name.givenName
name.MiddleName	name.middleName
NickName	nickName
PhoneNumbers	phoneNumbers
PreferredLanguage	preferredLanguage
TimeZone	timezone
Title	title
UserName	userName
Roles[].value	spendExtensionRole.roles[].roleName
Roles[].display	spendExtensionRole.roles[].roleName
Entitlements[].value	entitlements[]
Entitlements[].display	entitlements[]
Extension.SpendReimbursementCurrency	spendExtensionUser.reimbursementCurrency
Extension.SpendLocale	spendExtensionUser.locale
Extension.SpendCountry	spendExtensionUser.country
Extension.SpendLedgerCode	spendExtensionUser.ledgerCode
extension.primaryApprover.id	SpendApprover.report[].approver.value
extension.primaryApprover.userName	UserName
extension.primaryApprover.employeeNumber	Extension.EmployeeNumber

NOTE: Attributes extension.primaryApprover.userName and extension.primaryApprover.employeeNumber are mapped from a different Get API.

Groups

NA

Connector limitations

- Connector will not return inactive users in the Get All Users response and return 404 Not Found for Get User by Id. (returned in version v.2.0)
- Meta data information with **created** and **lastModified** dates are not supported. (Supported in version v.2.0)
- Create User with the details of an existing User will return the same User details with '201 Created'. (returns 409 conflict in version v.2.0)
- Update of **givenName** and **familyName** are not supported. (Supported in version v.2.0)
- It is required to pass the values in specific format for the custom fields which depends on the target instance.
- To perform a successful integration, the enabled mandatory custom attributes need to be configured in One IM and all the values should be passed accordingly.

> **NOTE**:
>
> - As the connector does not support PATCH, it will accept all the write-able attributes in update request. If attributes are not specified in the request, system default values will be provisioned.
> - Default values for some attributes used in connectors are: Under "urn:i-etf:params:scim:schemas:extension:spend:2.0:User" :
> - reimbursement Currency: USD
> - country: US
> - locale: en-US

Connector versions and features

The following subsections describe the different connector version(s) and features available with them.

Features available exclusively in Concur v.2.0

Following are the features that are available exclusively in **Concur v.2.0**:

- v.2.0 of Concur connector leverages v4 APIs of target system.

Connector SCIM configuration

- The Concur connector is enhanced to support the configuration of SCIM connector with custom attributes.
- Disabling the attributes is not supported as this feature is not available in Concur.
- The supported custom attributes are custom 1 through 21 and orgUnit 1 through 6, which are string types.
- Only the "Users" resource type has support for configuring custom attributes via SCIM configuration.

  NOTE: Supported only for v.2.0.

Support for filter condition

- The connector supports filter condition on externalId, companyId, employeeNumber and userName.
- The only filter operator supported is eq.
- Supports AND logical operator only with the attribute combination employeeNumber + companyId and externalId + companyId.
- For OR logical operator, and for any other combination of attributes, the target API returns error message.
- The connector supports only the double quotes in the filter value (ex. userName eq "testUser").

  NOTE: Filter is supported only for v.2.0.

36

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 186: Supported operations for Users

Operation	VERB
Create User	POST
Update User	PUT
Delete User	DELETE

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

Groups

Table 187: Supported operations for Groups

Operation	VERB
Create Group	POST
Update Group	PUT
Get Group	GET
Get Groups	GET
Get All Groups with Pagination	GET
Update Membership	PUT

Mandatory fields

Users

Email

Groups

displayName

User and Group mapping

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

Table 188: User mapping

SCIM parameter	Tableau parameter
Id	LoginId
userName	name
name.formatted	fullName
displayName	fullName
emails[0].value	name
roles[0].value	siteRole

Groups

Table 189: Group mapping

SCIM parameter	Tableau parameter
Id	LoginId
displayName	name
members[].value	members[].id

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 .

37

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 190: Supported operations for Users

Operation	VERB
Create User	POST
Update User	PUT
Delete User	DELETE
Get User	GET
Get Users	GET
Get All Users with Pagination	GET

Groups

Table 191: Supported operations for Groups

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

Mandatory fields

Users

- Email
- givenName

- familyName

Groups

displayName

User and Group mapping

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

Table 192: User mapping

SCIM parameter	GoToMeeting parameter
Id	key
UserName	email
Name.givenName	firstName
Name.familyName	lastName
Name.formatted	firstName+""+lastName
DisplayName	firstName+""+lastName
emails[0].value	email
locale	locale
Timezone	timeZone
Groups[].Value	groupKey
Groups[].display	groupName

Groups

Table 193: Group mapping

SCIM parameter	GoToMeeting parameter
Id	key
DisplayName	name
members[].value	userKeys[]

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.

38

Coupa

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 for Coupa v.1.0

To configure the connector, the following parameters are required:

- Connector name
- API key
- Custom Properties (List of custom properties, if any, to be mapped).
  For more information, see Configuring custom attributes for Coupa v.1.0.
- Target URL (Cloud application's instance URL used as target URI in payload)
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details).

Configuring custom attributes for Coupa v.1.0

You can configure custom attributes for the **Coupa v.1.0** connector when you configure the connector in Starling Connect by adding the custom attributes in the **Custom Properties** field in the defined format.

NOTE: For more information about how to configure custom attributes in **Coupa v.1.0** , see Configuring custom attributes for Coupa v.1.0.

Supervisor configuration parameters for Coupa v.1.1

For more information, refer Refer Creating integration Connect Client in Coupa.

- Connector name
- Client ID
- Client Secret
- Custom Properties (List of custom properties, if any, to be mapped).
  For more information, see Configuring custom attributes for Coupa v.1.0.
- Target URL (Cloud application's instance URL used as target URI in payload)
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details).

You can configure custom attributes for the **Coupa v.1.1** connector similar to configuring the **Coupa v1.0**, in Starling Connect by adding the custom attributes in the **Custom Properties** field in the defined format.

NOTE: For more information about how to configure custom attributes in **Coupa v.1.1** , see Configuring custom attributes for Coupa v.1.0.

Supervisor configuration parameters for Coupa v.2.0

To configure the connector, the following parameters are required:

- Connector name
- Client ID
- Client Secret
- Target URL (Cloud application's instance URL used as target URI in payload)
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details)

Configuring custom attributes for Coupa v.2.0

You can configure custom attributes for the **Coupav.2.0** connector in Starling Connect for the **User** object in the **Custom Attributes** section in **Schema Configuration**.

NOTE:

- Coupa cloud application allows you to create custom attributes only for **User** objects.
- For more information about how to configure custom attributes in **Coupa v.2.0** , see Configuring custom attributes in connectors.

Supported objects and operations

Users

Table 194: Supported operations for Users

Operation	VERB
Create User	POST
Update User	PUT
Get User by id	GET
Get All Users	GET
Get All Users with Pagination	GET
Update Role Membership	PUT
Update Group Membership	PUT
Update UserGroups Membership	PUT
Update AccountGroups Membership	PUT

NOTE: The membership operations are user based operations according to target system behavior from Coupa.

Groups

Table 195: Supported operations for Groups

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

Roles

Table 196: Supported operations for Roles

Operation	VERB
Get Roles by id	GET
Get All Roles	GET
Get All Roles with Pagination	GET

UserGroups

Table 197:

Operation	VERB
Get UserGroups by id	GET
Get All UserGroups	GET
Get All UserGroups with pagination	GET

AccountGroups

Table 198:

Operation	VERB
Get AccountGroups by id	GET
Get All AccountGroups	GET
Get All AccountGroups with pagination	GET

Mandatory fields

Users

- Username
- Email

- FirstName
- LastName

Groups

NA

User and Group mapping

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

Table 199: User mapping

SCIM parameter	Coupa parameter
Id	id
UserName	login
Name.GivenName	firstname
Name.FamilyName	lastame
Name.Formatted	fullname
DisplayName	fullname
Emails[0].value	email
Photos	avatar-thumb-url
Addresses.StreetAddress	default-address[0].street1
Addresses.Locality	default-address[0].city
Addresses.Region	default-address[0].state
Addresses.PostalCode	default-address[0].postal-code
Addresses.Country	default-address[0].country[0].name
Groups.value	content-groups[x].id
Groups.display	content-groups[x].name
Roles.value	roles.id
Roles.display	roles.name
Active	active

SCIM parameter	Coupa parameter
Locale	default-locale
PreferredLanguage	default-locale
Extension.Manager.value	manager.id
Extension.EmployeeNumber	employee-number
Extension.CostCenter	custom-fields.default-user-cost-center
Extension.AuthenticationMethod	authentication-method
Extension.SsoIdentifier	sso-identifier
Extension.PurchasingUser	purchasing-user
Extension.ExpenseUser	expense-user
Extension.SourcingUser	sourcing-user
Extension.InventoryUser	inventory-user
Extension.ContractsUser	contracts-user
Extension.AnalyticsUser	analytics-user
Extension.invoiceApprovalLimit	invoice-approval-limit
Extension.invoiceSelfApprovalLimit	invoice-self-approval-limit
Extension.requisitionApprovalLimit	Requisition-approval-limit
Extension.requisitionSelfApprovalLimit	Requisition-self-approval-limit
Extension.contractApprovalLimit	Contract-approval-limit
Extension.contractSelfApprovalLimit	Contract-self-approval-limit
Extension.workConfirmationApprovalLimit	work-confirmation-approval-limit
Extension.defaultChartOfAccountsName	default-account.name
Extension.defaultAccountCode	default-account.code
Extension.defaultAccountCodeSegment1	default-account.segment1
Extension.defaultAccountCodeSegment2	default-account.segment2
Extension.defaultCurrency	default-currency
Extension.defaultAddressLocationCode	default-address.location-code
Extension.accountSecurityType	account-security-type
Extension.businessGroupSecurityType	business-group-security-type

SCIM parameter	Coupa parameter
Extension.mentionName	mention-name
Extension.AccountGroups	account-groups[]
Extension.ApprovalGroups	approval-groups[]
Created	created-at
LastModified	updated-at
Extension.expenseSelfApprovalLimit	expense-self-approval-limit
Extension.expenseApprovalLimit	expense-approval-limit

Groups

Table 200: Group mapping

SCIM parameter	Coupa parameter
Id	id
DisplayName	name
Created	created-at
LastModified	updated-at

Roles

Table 201: Roles mapping

SCIM parameter	Coupa parameter
Id	id
DisplayName	name
Created	created-at
LastModified	updated-at

UserGroups

Table 202: UserGroups (or ApprovalGroups) mapping

SCIM parameter	Coupa parameter
Id	id
DisplayName	name
Created	created-at
LastModified	updated-at

AccountGroups

Table 203: AccountGroups mapping

SCIM parameter	Coupa parameter
Id	id
DisplayName	name
Created	created-at
LastModified	updated-at

Coupa Connector has the capability of performing granular data update of Users object type and it is available exclusively with version 3.0. This allows customers to modify the User object by passing only the selected attribute and the value to be modified. This has been implemented by enabling the PATCH operation recommended by SCIM standard. This change can be witnessed on One Identity Manager by using any debug tool to capture the request sent. However, the prior versions of the connector continue to work with PUT without any change.

Connector versions and features

The following subsections describe the different connector version(s) and features available with them.

Supported Versions

The supported versions of **Coupa** connector are:

- v.1.0
- v.1.1
- v.2.0

NOTE: For more information, see Connector versions.

Features available exclusively in Coupa v.1.1

- Support for Oauth Authentication that is based out of v.1.0.

Features available exclusively in Coupa v.2.0

- Support for OAuth Authentication
- Support for schema configuration by adding custom attributes

Connector limitations

- The SCIM Pagination Parameter (rfc: https://tools.ietf.org/html/rfc7644#section-3.4.2.4) **Total Results** is not returned due to the **GetAllUsers** API Limitation of COUPA target system, which returns only 50 objects per request. The impact of this is that One Identity Manager SCIM synchronization works on INDEX based logic for the pagination.
- COUPA target system supports only Soft Delete of the **User** Object type. Because of this the **GET All Users** API returns both active and inactive users objects.
- Starling COUPA connector facilitates two new SCIM endpoints namely **Account-Groups** and **User-Groups**. These endpoints support **GET** and **GETALL** operations only. This is in line with COUPA target API behavior where the **CREATE**, **UPDATE**, and **DELETE** operations are not allowed.
- To accommodate modification of COUPA user object attributes **default-account.segment-1** and **default-account.segment-2**, the **User** object type update operation is carried out in two steps:
  - Step -1: Updates values for all the attributes except **default-account.segment-1** and **default-account.segment-2**.
  - Step -2: Updates values for **default-account.segment-1** and **default-account.segment-2** attributes.

  NOTE: As per the COUPA documentation, to set the attribute values of **default-account.segment-1** and **default-account.segment-2**, **values of account-security-type** and **default-account-type.name** attributes should already be

set.

- While Provisioning or Update **USER** object, the value of attribute **account-security-type** of **User** Object is calculated using the values of **default-account-type.name** and **account-groups** attributes. This is inline with the COUPA target system documentation and per the customer requirements.

  For example:

  - **account-security-type** would be modified to value **2** if **default-account-type.name** has value and **account-groups** is not empty.
  - **account-security-type** would be modified to value **1** if **default-account-type.name** has value and **account-groups** is empty.
  - **account-security-type** would not be modified if **default-account-type.name** does not have value.

Synchronization and integration of Roles object type with One Identity Manager

For more information, see Synchronization and integration of Roles object type with One Identity Manager

User centric membership configuration for Coupa

For more information, see User centric membership.

39

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)
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details).

Supported objects and operations

Users

Table 204: Supported operations for Users

Operation	VERB
Create User	POST
Update User	PUT
Delete User	DELETE
Get User	GET
Get All Users	GET
Get All Users with Pagination	GET

Groups

Table 205: Supported operations for Groups

Operation	VERB
Create Group	POST
Update Group	PUT
Delete Group	DELETE
Get Group	GET
Get All Groups	GET
Get All Users with Pagination	GET
Update Membership	PUT

Mandatory fields

Users

- Username
- Email

Groups

DisplayName

User and Group mapping

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

Table 206: User mapping

SCIM parameter	AWS Cognito parameter
Id	Username
userName	Username
Name.Formatted	Username
DisplayName	Username
Emails[0].value	UserAttributes.email
Active	UserStatus.CONFIRMED
PhoneNumbers[0].Value	phone_number
Password	Password
Extension.IsPasswordPermanent	Permanent
Extension.DesiredDeliveryMediums	DesiredDeliveryMediums
Extension.email_verified	UserAttributes.email_verified
Extension.phone_number_verified	UserAttributes.phone_number_verified
Created_at	UserCreateDate
lastModified_at	UserLastModifiedDate

Groups

Table 207: Group mapping

SCIM parameter	AWS Cognito parameter
Id	GroupName
displayName	GroupName
members[].value	Users[].Username
members[].display	Users[].Username
Extension.Precedence	Precedence
Extension.RoleArn	RoleArn
Created_at	CreationDate
lastModified_at	LastModifiedDate

Connector limitations

- Creating or updating the User or a Group happens 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.

40

Okta

The Okta connector allows you to connect Okta with One Identity Starling Connect enabling you to take advantage of the features and products available in Starling Connect that complement and enhance the services provided by Okta.

Okta provides single sign-on, multi-factor authentication and Platform Services, which is a set of modular components that can be used to address requirements that are specific to an organization.

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)
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details)
- Request Delay (in ms)

  NOTE: To handle the Okta rate limit issue, the Okta connector has been enabled with user configurable delay in milliseconds so that the each request to the target API would wait for the specific amount of time to help the connector to prevent the throttling of the Okta APIs. The default value for the configuration is 1000 (milliseconds) and OneIdentity recommends to keep the value below 2000 (milliseconds).

Configuring custom attributes for Okta

You can configure custom attributes for the Okta connector in Starling Connect for Users and Groups in the Custom Attributes section in Schema Configuration.

NOTE: For more information about how to configure custom attributes in Okta, see Configuring custom attributes in connectors.

Support for MultiValued Custom attributes

- In connector schema, only String datatype corresponds to the multivalued custom attribute.
- Connector output format for multivalued custom attributes will be as shown below:
  - "**MultivaluedAttributeName**" : "[abcd;; efgh;; xyzw;; uvty]"
- As per the connector output format, the values will be double semicolon separated (;;) and will be enclosed inside opening and closing square brackets.
- Opening and closing square brackets help to ensure that the attribute is of multivalued type.

Supported objects and operations

Users

Table 208: Supported operations for Users

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

Groups

Table 209: Supported operations for Groups

Operation	VERB
Create Group	POST

Operation	VERB
Update Group	PUT
Delete Group	DELETE
Get Group	GET
Get All Groups	GET
Get All Groups with pagination	GET
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 210: User mapping

SCIM parameter	Okta parameter
Id	id
UserName	login
DisplayName	displayName
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	tatus == "ACTIVE"
Extension.EmployeeNumber	employeeNumber
Extension.Division	division
Extension.Department	department
Extension.CostCenter	costCenter

SCIM parameter	Okta parameter
Extension.Organization	organization
Extension.Manager.value	managerId
Extension.Manager.DisplayName	manager
Meta.Created	created
Meta.LastModified	lastUpdated

Groups

Table 211: Group mapping

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

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.
- **Inactivated 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**.
- The connector deletes a user permanently from the target system irrespective of its status. When you perform a **DELETE** operation on:

    - a deprovisioned user, the user is deleted permanently.
    - an active user, the user is, first, deprovisioned and then deleted permanently. This process is taken care internally.
- 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. user who hav not been deactivated, the user gets deactivated.
- After activating a user, the active value will still be false until the user verifies or changes their password through the mail sent by Okta while activating the user.

41

DataDog

The Datadog connector allows you to connect Datadog with One Identity Starling enabling you to take advantage of the features and products available with Starling Connect that complement and enhance Datadog's real-time interactive dashboards and monitoring services.

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 212: 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 213: 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.

Synchronization and integration of Roles object type with One Identity Manager

For more information, see Synchronization and integration of Roles object type with One Identity Manager

42

Hideez

The Hideez connector allows you to connect Hideez with One Identity Starling enabling you to take advantage of the features and products available with Starling Connect that complement and enhance Hideez's wireless security key for passwordless user authentication and centralized password management.

Supervisor configuration parameters

To configure the connector, following parameters are required:

- Connector name
- Username
- Password
- Target URL
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details)

Supported objects and operations

AccessProfile

Table 214: Supported operations for AccessProfile

Operation	VERB
Create AccessProfile	POST
Update AccessProfile	PUT

Operation	VERB
Delete AccessProfile	DELETE
Get AccessProfile	GET
Get All AccessProfiles	GET

Companies

Table 215: Supported operations for Companies

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

Departments

Table 216: Supported operations for Departments

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

Devices

Table 217: Supported operations for Devices

Operation	VERB
Update Devices	PUT

Operation	VERB
Get Devices	GET
Get All Devices	GET

Positions

Table 218: Supported operations for Positions

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

Workstations

Table 219: Supported operations for Workstations

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

Employees

Table 220: 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 221: 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)

- RFId

Positions

- Name

Workstations (Update)

- DepartmentId
- RFId

Employees

- FirstName
- LastName
- Email
- DepartmentId
- PositionId

Mappings

The mappings are listed in the tables below.

Table 222: Employee mapping

SCIM parameter	Hideez parameter
Id	id
UserName	UserName
firstName	firstName
lastName	lastName
email	email
phoneNumber	phoneNumber
departmentId	departmentId
positionId	positionId

SCIM parameter	Hideez parameter
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
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

SCIM parameter	Hideez parameter
	nel
device.deviceAccessProfile.masterKeyBonding	device.deviceAccessProfile.pinBonding
device.deviceAccessProfile.masterKeyConnection	device.deviceAccessProfile.pinConnection
device.deviceAccessProfile.masterKeyNewChannel	device.deviceAccessProfile.pinNewChannel
device.deviceAccessProfile.pinExpiration	device.deviceAccessProfile.pinExpiration
device.deviceAccessProfile.pinLength	device.deviceAccessProfile.pinLength
device.deviceAccessProfile.pinTryCount	device.deviceAccessProfile.pinTryCount
device.deviceAccessProfile.pinExpirationConverted	device.deviceAccessProfile.pinExpirationConverted
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 223: AccessProfile mapping

SCIM parameter	Hideez parameter
Id	Id
name	name

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

SCIM parameter	Hideez parameter
device.importedAt	device.importedAt
device.isOnline	device.isOnline

Table 224: Company mapping

SCIM parameter	Hideez parameter
id	id
name	name

Table 225: Department mapping

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

Table 226: Device mapping

SCIM parameter	Hideez parameter
Id	Id
mac	mac
model	model
rfid	rfid
battery	battery
firmware	firmware
state	state
lastSynced	lastSynced
employeeId	employeeId

SCIM parameter	Hideez parameter
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
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 227: Position mapping

SCIM parameter	Hideez parameter
id	id
name	name

Table 228: Workstation mapping

SCIM parameter	Hideez parameter
Id	Id
name	name
domain	domain
clientVersion	clientVersion
departmentId	departmentId
departmentName	departmentName
os	os
ip	ip
lastSeen	lastSeen
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.
- When you use **http** in the target URL for the **POST**, **DELETE** and **Login** operations, the cloud APIs return an error. Hence, it is recommended that you use **https** for the target URL parameter for all operations.

One Identity Manager E2E integration needs

For more information, see One Identity Manager E2E integration needs for Hideez connector.

43

Opsgenie

The Opsgenie connector allows you to connect Opsgenie with One Identity Starling enabling you to take advantage of the features and products available with Starling Connect that complement and enhance Opsgenie's incident management platform that allows collaboration among the required stakeholders to stay in control during service disruptions.

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)
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details)

Supported objects and operations

Users

Table 229: Supported operations for Users

Operation	VERB
Create User	POST

Operation	VERB
Get User	GET
Get Users	GET
Update User	PUT
Delete User	DELETE

Groups

Table 230: Supported operations for Groups

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

Roles

Table 231: 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 232: 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

SCIM parameter	Opsgenie parameter
role.id	roles[].value
user teams[].id	groups[].value
skypeUsername	userExtension.skypeUsername
createdAt	meta.created

Groups

Table 233: Group mapping

SCIM parameter	Opsgenie parameter
id	id
name	displayName
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.

Synchronization and integration of Roles object type with One Identity Manager

For more information, see Synchronization and integration of Roles object type with One Identity Manager

Informatica Cloud Services

The Informatica Cloud Services connector allows you to connect Informatica Cloud Services with One Identity Starling enabling you to take advantage of the features and products available with Starling Connect that complement and enhance the services provided by Informatica Cloud Services.

Informatica Cloud Services is an Integration Platform as a Service (iPaaS) that allows you to integrate and synchronize data and applications in a hybrid environments.

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)
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details)

Supported objects and operations

Users

Table 234: Supported operations for Users

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

Groups

Table 235: Supported operations for Groups

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

Roles

Table 236: 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 237: 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

SCIM Parameter	Informatica parameter
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 238: 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 239: 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.

45

AppDynamics

The AppDynamics connector allows you to connect AppDynamics with One Identity Starling enabling you to take advantage of the features and products available with Starling Connect that complement and enhance the services provided by AppDynamics.

AppDynamics is a real-time business and application performance management and monitoring platform that provides a complete view of the application environment, allowing you to monitor and fix issues quickly.

Supervisor configuration parameters

To configure the connector, following parameters are required:

- Connector name
- Client Secret
- API Client Name
- Account Name

Supported objects and operations

Users

Table 240: Supported operations for Users

Operation	VERB
Create User	POST
Update User	PUT

Operation	VERB
Delete User	DELETE
Get User	GET
Get All Users	GET

Groups

Table 241: Supported operations for Groups

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

Roles

Table 242: Supported operations for Roles

Operation	VERB
Get Role	GET
Get All Roles	GET

Mandatory fields

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

Users

- UserName
- DisplayName

- Security_provider_type
- Password

Groups

- DisplayName
- Security_provider_type

Mappings

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

Table 243: User mapping

SCIM parameter	AppDynamics parameter
Id	id
UserName	name
DisplayName	displayName
password	password
Groups[].value	groups[].id
Groups[].display	groups[].name
Roles[].value	roles[].id
Roles[].display	roles[].name
Extension.security_provider_type	security_provider_type

Groups

Table 244: Group mapping

SCIM parameter	AppDynamics parameter
Id	id
displayName	name
Extension.Description	description

SCIM parameter	AppDynamics parameter
Extension.security_provider_type	security_provider_type
Extension.Roles[].value	roles[].id
Extension.Roles[].display	roles[].name

Roles

Table 245: Roles mapping

SCIM parameter	AppDynamics parameter
Id	id
displayName	name
description	description

Connector limitations

- **Groups members** information will not be retrieved in response to **GET specific Group**. The reason for this is the **Groups API** of the target system does not support it. However, the same is done at **Users API**. To overcome this deviation from standard behavior (rfc: https://tools.ietf.org/html/rfc7643#section-4.2), the connector is designed in such a way that all membership operations are done at Users endpoint. Hence, **GET specific User** response will retrieve the membership associations of respective **User**.
- A performance impact is expected in the assignment operation of **Roles** and **Group** memberships when the **User** belongs to multiple **Roles** and **Groups**. The reason for this is that separate API calls are made for each and every **Roles** or **Group** membership association.
- AppDynamics target system returns the **error code 500** for most of the error scenarios except for very specific errors such as **401 Unauthorized**. However, the connector handles few of those generic errors and responds appropriately.
- Most error messages returned by the target system are neither sufficiently informative nor available. The connector follows the same behavior, wherever custom error messages are not possible.
- Due to target system limitations, **password update** of **User** is not supported by the connector. However, the password can be set at the time of creation.

Synchronization and integration of Roles object type with One Identity Manager

For more information, see Synchronization and integration of Roles object type with One Identity Manager

User centric membership configuration for AppDynamics

For more information, see only the following sections in User centric membership:

- Creating a new schema class using Synchronization Editor
- Configuring User centric membership for Groups
- Creating a new column in UCIUser table and CSMUser table using Extension Tool
- Creating custom process using Designer

46

Marketo

The Marketo connector allows you to connect Marketo with One Identity Starling enabling you to take advantage of the features and products available with Starling Connect that complement and enhance the services provided by Marketo.

Marketo provides marketing automation software for all types of digital marketing. It provides services to capture the interaction with each customer, enabling users to identify the most profitable channels and campaigns.

Supervisor configuration parameters

To configure the connector, following parameters are required:

- Connector name
- Client Id
- Client Secret
- Target URI
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details)

Supported objects and operations

Users

Table 246: Supported operations for Users

Operation	VERB
Create(Invite) User	POST

Operation	VERB
Update User	PUT
Delete User	DELETE
Get User	GET
Get All Users	GET
Add RoleAndWorkspace to User	PUT
Remove RoleAndWorkspace from User	PUT

Roles

Table 247: Supported operations for Roles

Operation	VERB
Get all Roles	GET

Workspaces

Table 248: Supported operations for Workspaces

Operation	VERB
Get all Workspaces	GET

Mandatory fields

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

Users

- FirstName
- LastName
- EmailAddress
- accessRoleId
- WorkspaceId

Mappings

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

Table 249: User mapping

SCIM Parameter	Marketo parameter
Id	userid
UserName	userid
DisplayName	firstName + lastName
name.GivenName	firstName
name.FamilyName	lastName
emails[].value	emailAddress
Active	isLocked == false
Extension.rolesAndWorkspaces[].accessRoleId	userRoleWorkspaces[].accessRoleId
Extension.rolesAndWorkspaces[].accessRoleName	userRoleWorkspaces[].accessRoleName
Extension.rolesAndWorkspaces[].workspaceId	userRoleWorkspaces[].workspaceId
Extension.rolesAndWorkspaces[].workspaceName	userRoleWorkspaces[].workspaceName

Roles

Table 250: Roles mapping

SCIM parameter	Marketo parameter
id	id
name	name
description	description
Type	type
Meta.Created	createdAt
Meta.LastModified	updatedAt

Workspaces

Table 251: Workspaces mapping

SCIM parameter	Marketo parameter
id	id
name	name
description	description
Status	Status
Meta.Created	createdAt
Meta.LastModified	updatedAt

Connector limitations

1. Create User is a multiple steps operation.
    a. Once the Create User request is successfully submitted to One Identity Manager, the user will receive an email on the email ID mentioned in the request.
    b. User must click on the link provided in the email and set a password.
    c. User is now activated and will be available at the target instance.
2. To Create a User, at least one pair of **accessRoleId** and **WorkspaceId** must be provided.
3. One Identity Manager must have multi-value arrays of string type to hold the values of the User properties: **accessRoleId**, **accessRoleName**, **WorkspaceId** and **WorkspaceName**.
4. Update User is a multiple steps operation.
    a. Only confirmed Users can be updated.
    b. One round of full synchronization is required before submitting the UPDATE request on a newly created User. This must be done to synchronize the User details after activation. This applies to newly created Users only, however existing User UPDATE will work as usual.
5. **Roles** and **Workspaces** endpoints are used only to retrieve data from target and store it in One Identity Manager and can not to be used to assign or unassign **Roles** and **Workspaces** to a User.
6. Connector supports cursor pagination and hence **TotalResults** are not returned.
7. Duplicate User CREATE request will return Internal Server Error: 500 with the message **System Error: This userid is in use. Choose another email** for

already existing activated User. However, error 409 is returned if the User is not activated.

8. The pagination scenarios are not tested for Marketo Connector due to unavailability of adequate target system instance.

Synchronization and integration of Roles object type with One Identity Manager

For more information, see Synchronization and integration of Roles object type with One Identity Manager.

Synchronization and integration of Workspaces object type with One Identity Manager

For more information, see Synchronization and integration of Workspaces object type with One Identity Manager.

Add Roles ID and Workspaces ID to create and update users for Marketo connector

To create a user successfully using Marketo connector, you must provide valid values for mandatory properties such as **Roles ID** and **Workspaces ID** in the request. **Roles ID** and **Workspaces ID** are the sub-attributes of the main attribute **RolesAndWorkspaces**, which is a complex multi-valued string attribute defined under User extensions in the connector schema.

One Identity Manager must have fields where you can enter complex multi-value array values but it does not display such fields by default. However, it is possible to create custom multi-value array fields. For more information, see Creating multi-valued custom fields in One Identity Manager.

> NOTE: The above example of creating multi-valued custom fields is one of the various ways to achieve the configuration required for adding **Roles ID** and **Workspaces ID** to create and update Users. There may be other ways to achieve this integration based on the customization options that One Identity Manager provides.

47

Workday HR

The WorkdayHR connector allows you to connect WorkdayHR with One Identity Starling enabling you to take advantage of the features and products available with Starling Connect that complement and enhance WorkdayHR's cloud-based human resource management services.

Supervisor configuration parameters

To configure the connector, following parameters are required:

- Connector name
- Tenant
- API Version
- Username (Refer Workday permissions needed to integrate via the Starling Connector)
- Password (Refer Workday permissions needed to integrate via the Starling Connector)
- WorkdayHR instance URL (Cloud application's instance URL used as target URI in the payload)
- Customer-specific configuration parameters must be configured based on the Workday HR instance.
    - OrganizationTypeID for Department
    - OrganizationTypeID for Division
    - OrganizationTypeID for Desk
    - OrganizationTypeID for CostCenter
    - OrganizationTypeID for Company
    - OrganizationTypeID for Region
    - OrganizationTypeID for Personal Assistant
    - OrganizationTypeID for Asset Class

- OrganizationTypeID for DepartmentHead
- OrganizationSubTypeID for Department
- OrganizationSubTypeID for Division
- OrganizationSubTypeID for Desk
- OrganizationSubTypeID for CostCenter
- OrganizationSubTypeID for Company
- OrganizationSubTypeID for Region
- OrganizationSubTypeID for Personal Assistant
- OrganizationSubTypeID for Asset Class
- OrganizationRoleID for Department Head
- CustomIDTypeID for Date Joined Industry
- CustomIDTypeID for Code Of Conduct
- CustomIDTypeID for External ID
- Certification Names
- Additional Names Types
- OrganizationType reference ID for Location Hierarchy
- SAMAccount ID Type
- Mobile Device Type ID
- Landline Device Type ID
- OrgTypeID for Custom Organizations
- OrgSubTypeID for Custom Organizations
- OrganizationTypeID for Matrix
- OrganizationSubTypeID for Matrix
- Future Hire Interval
- Business Process Types

- Retry Server Call

  IMPORTANT:

  - Retry Server Call is used to make a retry request to WorkdayHR target instance in-case of failures related to the instance being unreachable at a given point in time.
  - By Default the value is set to false. The customer can enable it in-case such failures are encountered.

- Increase Request Time out

  IMPORTANT:The default request time out is 100 seconds, please enable this option if time out exception occurs.

- Use Change Contact Information API for Update.

  IMPORTANT:

  - This configuration defines which update API will be used to update the contact details including email, cell phone and business phone. When the configuration is enabled the Change_Work_Contact_Information API and Change_Home_Contact_Information API would be used to update the work and home contact information respectively.
  - By default, the configuration would be disabled and the update will use Maintain_Contact_Information API.
  - For additional information on update configurations in One Identity Manager, refer Additional configuration for update.

- Field Override Integration System ID
- OrganizationTypeID for Cost Center Hierarchy
- OrganizationSubTypeID for Cost Center Hierarchy
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details)

NOTE:

- **Username** should be entered in the format : **<username>@<tenantname>**.
- The **API version** supported by the connector is **v34.0**.
- To know more about configuring the values for customer specific parameters, refer Values for customer-specific configuration parameters.

Supported objects and operations

Employees

Table 252: Supported operations for Employees

Operation	VERB
Get Employee	GET
Get All Employees	GET
Update Employee	PUT

NOTE:

- The **Get Employee** endpoint fetches the primary work email, primary cellphone and landline for home and work. The **Update Employee** endpoint sets the default

value for email to type work and public to false, when the values for type and public flag are not provided. **IsPrimary** is always set to true.

- Available until v3.1.

Locations

Table 253: Supported operations for Locations

Operation	VERB
Get Location	GET
Get All Locations	GET

CustomOrgs

Table 254: Supported operations for CustomOrgs

Operation	VERB
Get CustomOrg	GET
Get All CustomOrgs	GET

NOTE:

- **CustomOrgs** is a single endpoint that provides information on Departments, SubDivisions, Divisions, Desks, LegalEntities and CostCenters.
- To extract specific entities from **CustomOrgs** you must create the mappings, workflow steps and set up the filter.
- For more information, see *OneIM_CloudHRSystems_Administration* guide on the Support site.

JobClassifications

Table 255: Supported operations for JobClassifications

Operation	VERB
Get JobClassification	GET
Get All JobClassifications	GET

JobProfiles

Table 256: Supported operations for JobProfiles

Operation	VERB
Get JobProfile	GET
Get All JobProfiles	GET

FutureDatedEmployees

Table 257: Supported operations for FutureDatedEmployees

Operation	VERB
Get FutureDatedEmployees	GET
Get All FutureDatedEmployees	GET

NOTE:

- The Get All FutureDatedEmployees endpoint is dependent on the Starling UI config parameters Business process type and Future Hire Interval.
- The FutureDatedEmployees endpoint does not support any filters.

DeltaSyncEmployees

Table 258: Supported operations for DeltaSyncEmployees

Operation	VERB
Get DeltaSyncEmployees	GET
Get All DeltaSyncEmployees GET	GET

NOTE: This endpoint is only for supporting the delta sync.

Positions

Table 259: Supported operations for Positions

Operation	VERB
Get Position	GET
Get All Position	GET

NOTE: This Endpoint requires additional permission for the API.

Mappings

Endpoint Mapping

Table 260: Target system objects mapping

Target system objects	SCIM endpoints
Workers	Employees
Locations	Locations
Organizations	CustomOrgs
Job Classification Groups	JobClassifications
Positions	Positions
Job Profiles	JobProfiles

Attributes Mapping

Different mappings associated with this connector are listed in the tables below:

Table 261: Employees mapping

SCIM parameter	WorkDayHR parameter
AdditionalNames.details[]	Additional_Name_Type_ID;First_Name;Last_Name
Addresses.country	Worker/Worker_Data/Personal_Data/Contact_Data/Address_Data

SCIM parameter	WorkDayHR parameter
	[@Defaul ted_Business_Site_ Address=1]/Country_Reference/ID [@wd:type='ISO_31 66-1_Alpha-3_ Code']/text()
Addresses.countryCode2	wd:Worker/Worker_Data/Personal_ Data/Contact_Data/Address_Data [@Defaulted_Business_Site_ Address=1]/Country_Reference/ID [@wd:type='ISO_31 66-1_Alpha-2_ Code']/text()
Addresses.locality	wd:Worker/wd:Worker_ Data/wd:Personal_Data/wd:Contact_ Data/wd:Addre ss_Data [@wd:Defaulted_Business_Site_ Address=1]/wd:Municipality/text()
Addresses.postalCode	wd:Worker/wd:Worker_ Data/wd:Personal_Data/wd:Contact_ Data/Address_ Data[@Defaulted_ Business_Site_Address=1]/Postal_ Code/text()
Addresses.region	wd:Worker/wd:Worker_ Data/wd:Personal_Data/wd:Contact_ Data/wd:Addre ss_Data [@wd:Defaulted_Business_Site_ Address=1]/wd:Country_Region_ Descriptor/text()
Addresses.streetAddress	wd:Worker/wd:Worker_ Data/wd:Personal_Data/wd:Contact_ Data/wd:Addre ss_Data [@wd:Defaulted_Business_Site_ Address=1]/@wd:Formatted_Address
assetClass	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_Data [@wd:Primary_Job=1]/wd:Position_ Organizations_Data/wd:Position_ Organization_Data[string (wd:Organization_ Data/wd:Organization_Type_ Reference/wd:ID [@wd:type='Organization_Type_

SCIM parameter	WorkDayHR parameter
	ID']/text())='<OrganizationTypeID_For_AssetClass>'] and string (wd:Organization_Data/wd:Organization_Subtype_Reference/wd:ID [@wd:type='Organization_Subtype_ID']/text ())='<OrganizationSubTypeID_For_AssetClass>']/wd:Organization_Reference/wd:ID [@wd:type='WID']/text()
assetClassReferenceId (Available from v3.2) (Not available in LIST response)	wd:Worker/wd:Worker_Data/wd:Employment_Data/wd:Worker_Job_Data [@wd:Primary_Job=1]/wd:Position_Organizations_Data/wd:Position_Organization_Data[string (wd:Organization_Data/wd:Organization_Type_Reference/wd:ID [@wd:type='Organization_Type_ID']/text())='<OrganizationTypeID_For_AssetClass>'] and string (wd:Organization_Data/wd:Organization_Subtype_Reference/wd:ID [@wd:type='Organization_Subtype_ID']/text ())='<OrganizationSubTypeID_For_AssetClass>']/wd:Organization_Reference/wd:ID [@wd:type='Organization_Reference_ID']/text()
businessUnitWID	wd:Worker/wd:Worker_Data/wd:Organization_Data/wd:Worker_Organization_Data/wd:Organization_Data/wd:Organization_Type_Reference/wd:ID [@wd:type='Organization_Type_ID']/text()='Business_Unit'/ID [@type='WID']/text()
Certificates.certificateDetails[]	Certification_Name;Certification_ID;Certification_Skill_ID;Issued_

SCIM parameter	WorkDayHR parameter
	Date;Expiry_Date
codeOfConduct	wd:Worker/wd:Worker_ Data/wd:Personal_ Data/wd:Identification_ Data/wd:Custom_ID/wd:Custom_ID_ Data[string(wd:ID_Type_ Reference/wd:ID/@wd:type)='Custo m_ID_Type_ID' and string(wd:ID_ Type_Reference/wd:ID [@wd:type='Custom_ID_Type_ ID']/text ())='<CodeOfConductValue>']/wd:ID /text()
company	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_Data [@wd:Primary_Job=1]/wd:Position_ Organizations_Data/wd:Position_ Organiz ation_Data[string(wd:Organization_ Data/wd:Organization_Type_ Reference/wd:ID [@wd:type='Organization_Type_ ID']/text())='<OrganizationTypeID_ For_Company>'] and string (wd:Organization_ Data/wd:Organization_Subtype_ Reference/wd:ID [@type='Organization_Subtype_ ID']/text ())='<OrganizationSubTypeID_For_ Company>']/Organization_ Reference/ID[@type='WID']/text()
companyReferenceId (Available from v3.2) (Not available in LIST response)	Data/wd:Employment_ Data/wd:Worker_Job_Data [@wd:Primary_Job=1]/wd:Position_ Organizations_Data/wd:Position_ Organization_Data[string (wd:Organization_ Data/wd:Organization_Type_ Reference/wd:ID [@wd:type='Organization_Type_ ID']/text())='<OrganizationTypeID_

SCIM parameter	WorkDayHR parameter
	For_Company>'] and string (wd:Organization_ Data/wd:Organization_Subtype_ Reference/wd:ID [@type='Organization_Subtype_ ID']/text ())='<OrganizationSubTypeID_For_ Company>']/Organization_ Reference/ID[@type='Organization_ Reference_ID']/text()
costCenter	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_Data [@wd:Primary_Job=1]/wd:Position_ Organizations_Data/wd:Position_ Organization_Data[string (wd:Organization_ Data/wd:Organization_Type_ Reference/wd:ID [@wd:type='Organization_Type_ ID']/text())='<OrganizationTypeID_ For_CostCenter>'] and string (wd:Organization_ Data/wd:Organization_Subtype_ Reference/wd:ID [@type='Organization_Subtype_ ID']/text ())='<OrganizationSubTypeID_For_ CostCenter>']/Organization_ Reference/ID[@type='WID']/text()
costCenterHierarchyReferenceId (Available from v3.2) (Not available in LIST response)	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_Data [@wd:Primary_Job=1]/wd:Position_ Organizations_Data/wd:Position_ Organization_Data[string (wd:Organization_ Data/wd:Organization_Type_ Reference/wd:ID [@wd:type='Organization_Type_ ID']/text())='<OrganizationTypeID_ For_CostCenterHierarchy>'] and string(wd:Organization_ Data/wd:Organization_Subtype_

SCIM parameter	WorkDayHR parameter
	Reference/wd:ID [@type='Organization_Subtype_ ID']/text ())='<OrganizationSubTypeID_For_ CostCenterHierarachy>']/Organizatio n_Reference/ID [@type='Organization_Reference_ ID']/text()
costCenterReferenceId (Available from v3.2) (Not available in LIST response)	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_Data [@wd:Primary_Job=1]/wd:Position_ Organizations_Data/wd:Position_ Organization_Data[string (wd:Organization_ Data/wd:Organization_Type_ Reference/wd:ID [@wd:type='Organization_Type_ ID']/text())='<OrganizationTypeID_ For_CostCenter>'] and string (wd:Organization_ Data/wd:Organization_Subtype_ Reference/wd:ID [@type='Organization_Subtype_ ID']/text ())='<OrganizationSubTypeID_For_ CostCenter>']/Organization_ Reference/ID[@type='Organization_ Reference_ID']/text()
countryIsoCode	NA
countryPhoneCode	NA
dateJoinedIndustry	wd:Worker/wd:Worker_ Data/wd:Personal_ Data/wd:Identification_ Data/wd:Custom_ID/wd:Custom_ID_ Data[string(wd:ID_Type_ Reference/wd:ID/@wd:type)='Custo m_ID_Type_ID' and string(wd:ID_ Type_Reference/wd:ID [@wd:type='Custom_ID_Type_ ID']/text ())='<DateJoinedIndustryValue>']/w d:ID/text()

SCIM parameter	WorkDayHR parameter
dateOfBirth	wd:Worker/wd:Worker_ Data/wd:Personal_Data/wd:Birth_ Date/text()
daysUnemployed	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Status_ Data/daysUnemployed/text()
department	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_Data [@wd:Primary_Job=1]/wd:Position_ Organizations_Data/wd:Position_ Organization_Data[string(string (wd:Organization_ Data/wd:Organization_Type_ Reference/wd:ID [@wd:type='Organization_Type_ ID']/text())='<OrganizationTypeID_ for_Department>'] and string (wd:Organization_ Data/wd:Organization_Subtype_ Reference/wd:ID [@type='Organization_Subtype_ ID']/text ())='<OrganizationSubTypeID_For_ Department>']/Organization_ Reference/ID[@type='WID']/text()
departmentHeadID	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_Data [@wd:Primary_Job=1]/wd:Position_ Organizations_Data/wd:Position_ Organization_Data/wd:Organization_ Data[string(wd:Organization_Type_ Reference/wd:ID [@wd:type='Organization_Type_ ID']/text())='<OrganizationTypeID_ For_DepartmentHead>' and string (wd:Organization_Support_Role_ Data/wd:Organization_Support_ Role/wd:Organization_Role_ Reference/wd:ID [@wd:type='Organization_Role_

SCIM parameter	WorkDayHR parameter
	ID']/text())='<OrganizationRoleID_For_DepartmentHead>' and string (wd:Organization_Support_Role_Data/wd:Organization_Support_Role/Organization_Role_Data/Assignment_From/text ())='assigned']/wd:Organization_Support_Role_Data/wd:Organization_Support_Role/wd:Organization_Role_Data/Worker_Reference/ID [@wd:type='WID']/text()
departmentHeadReferenceId (Available from v3.2) (Not available in LIST response)	wd:Worker/wd:Worker_Data/wd:Employment_Data/wd:Worker_Job_Data [@wd:Primary_Job=1]/wd:Position_Organizations_Data/wd:Position_Organization_Data/wd:Organization_Data[string(wd:Organization_Type_Reference/wd:ID [@wd:type='Organization_Type_ID']/text())='<OrganizationTypeID_For_DepartmentHead>' and string (wd:Organization_Support_Role_Data/wd:Organization_Support_Role/wd:Organization_Role_Reference/wd:ID [@wd:type='Organization_Role_ID']/text())='<OrganizationRoleID_For_DepartmentHead>' and string (wd:Organization_Support_Role_Data/wd:Organization_Support_Role/Organization_Role_Data/Assignment_From/text ())='assigned']/wd:Organization_Support_Role_Data/wd:Organization_Support_Role/wd:Organization_Role_Data/Worker_Reference/ID [@wd:type='Organization_Reference_ID']/text()
departmentReferenceId (Available from v3.2) (Not available in LIST response)	wd:Worker/wd:Worker_Data/wd:Employment_Data/wd:Worker_Job_Data [@wd:Primary_Job=1]/wd:Position_Organizations_Data/wd:Position_

SCIM parameter	WorkDayHR parameter
	Organization_Data[string(string (wd:Organization_ Data/wd:Organization_Type_ Reference/wd:ID [@wd:type='Organization_Type_ ID']/text())='<OrganizationTypeID_ for_Department>'] and string (wd:Organization_ Data/wd:Organization_Subtype_ Reference/wd:ID [@type='Organization_Subtype_ ID']/text ())='<OrganizationSubTypeID_For_ Department>']/Organization_ Reference/ID[@type='Organization_ Reference_ID']/text()
desk	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_Data [@wd:Primary_Job=1]/wd:Position_ Organizations_Data/wd:Position_ Organization_Data[string (wd:Organization_ Data/wd:Organization_Type_ Reference/wd:ID [@wd:type='Organization_Type_ ID']/text())='<OrganizationTypeID_ For_Desk>'] and string (wd:Organization_ Data/wd:Organization_Subtype_ Reference/wd:ID [@type='Organization_Subtype_ ID']/text ())='<OrganizationSubTypeID_For_ Desk>']/Organization_Reference/ID [@type='WID']/text()
deskReferenceId (Available from v3.2) (Not available in LIST response)	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_Data [@wd:Primary_Job=1]/wd:Position_ Organizations_Data/wd:Position_ Organization_Data[string (wd:Organization_ Data/wd:Organization_Type_

SCIM parameter	WorkDayHR parameter
	Reference/wd:ID [@wd:type='Organization_Type_ ID']/text())='<OrganizationTypeID_ For_Desk>'] and string (wd:Organization_ Data/wd:Organization_Subtype_ Reference/wd:ID [@type='Organization_Subtype_ ID']/text ())='<OrganizationSubTypeID_For_ Desk>']/Organization_Reference/ID [@type='Organization_Reference_ ID']/text()
DisplayName	wd:Worker/wd:Worker_ Descriptor/text()
division	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_Data [@wd:Primary_Job=1]/wd:Position_ Organizations_Data/wd:Position_ Organization_Data[string (wd:Organization_ Data/wd:Organization_Type_ Reference/wd:ID [@wd:type='Organization_Type_ ID']/text())='<OrganizationTypeID_ for_Division>'] and string (wd:Organization_ Data/wd:Organization_Subtype_ Reference/wd:ID [@type='Organization_Subtype_ ID']/text ())='<OrganizationSubTypeID_For_ Division>']/Organization_ Reference/ID[@type='WID']/text()
divisionReferenceId (Available from v3.2) (Not available in LIST response)	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_Data [@wd:Primary_Job=1]/wd:Position_ Organizations_Data/wd:Position_ Organization_Data[string (wd:Organization_ Data/wd:Organization_Type_

SCIM parameter	WorkDayHR parameter
	Reference/wd:ID [@wd:type='Organization_Type_ ID']/text())='<OrganizationTypeID_ for_Division>'] and string (wd:Organization_ Data/wd:Organization_Subtype_ Reference/wd:ID [@type='Organization_Subtype_ ID']/text ())='<OrganizationSubTypeID_For_ Division>']/Organization_ Reference/ID[@type='Organization_ Reference_ID']/text()
Emails.value	wd:Worker/wd:Worker_Data/wd:Per-sonal_Data/wd:Contact_Data/wd:E-mail _Address_Data/wd:Email_ Address/text()
endDate	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_Data [@wd:Primary_Job=1]/wd:Position_ Data/wd:End_Date/text()
endEmploymentDate	wd:Worker/wd:Worker_ Data/wd:Employment_Data[string (wd:Worker_Job_Data [@wd:Primary_Job=1]/wd:Position_ Data/wd:Worker_Type_ Reference/wd:ID/@wd:type)='Emplo yee_Type_ID']/wd:Worker_Status_ Data/End_Employment_Date/text()
estimatedLeaveEndDate	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Status_ Data/wd:Leave_Status_Data[wd:On_ Leave='1']/wd:Estimated_Leave_ End_Date/text()
externalID	wd:Worker/wd:Worker_ Data/wd:Personal_ Data/wd:Identification_ Data/wd:Custom_ID/wd:Custom_ID_ Data[string(wd:ID_Type_ Reference/wd:ID/@wd:type)='Custo

SCIM parameter	WorkDayHR parameter
	m_ID_Type_ID' and string(wd:ID_ Type_Reference/wd:ID [@wd:type='Custom_ID_Type_ ID']/text ())='<ExternalIDValue>']/wd:ID/text ()
externalIDDescription	wd:Worker/wd:Worker_ Data/wd:Personal_ Data/wd:Identification_ Data/wd:Custom_ID/wd:Custom_ID_ Data[string(wd:ID_Type_ Reference/wd:ID/@wd:type)='Custo m_ID_Type_ID' and string(wd:ID_ Type_Reference/wd:ID [@wd:type='Custom_ID_Type_ ID']/text ())='<ExternalIDValue>']/wd:Custo m_Description/text()
externalIDType	wd:Worker/wd:Worker_ Data/wd:Personal_ Data/wd:Identification_ Data/wd:Custom_ID/wd:Custom_ID_ Data/wd:ID_Type_Reference[string (wd:ID/@wd:type)='Custom_ID_ Type_ID' and string(wd:ID [@wd:type='Custom_ID_Type_ ID']/text ())='<ExternalIDValue>']/wd:ID [@wd:type='Custom_ID_Type_ ID']/text()
fullTimeEquivalentPercentage	/wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_ Data/wd:Position_Data/wd:Full_ Time_Equivalent_Percentage/text()
Gender	wd:Worker/wd:Worker_ Data/wd:Personal_Data/wd:Gender_ Reference/wd:ID [@wd:type="Gender_Code"]/text()
hireDate	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Status_ Data/wd:Hire_Date/text()

SCIM parameter	WorkDayHR parameter
hireReason	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Status_ Data/wd:Hire_Reason_ Reference/wd:ID/ [@wd:type='General_Event_ Subcategory_ID']/text()
hireRescinded	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Status_ Data/hireRescinded/text()
Id	wd:Worker/wd:Worker_ Reference/wd:ID [@wd:type='WID']/text()
isContingentWorker	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_Data[@wd :Primary_Job=1]/wd:Position_ Data/wd:Worker_Type_ Reference/wd:ID/@w d:type='Contingent_Worker_Type_ ID'
isEmployee	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_Data[@wd :Primary_Job=1]/wd:Position_ Data/wd:Worker_Type_ Reference/wd:ID/@w d:type='Employee_Type_ID'
jobCategoryID (Available from v3.2)	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_ Data/wd:Position_Data/wd:Job_ Profile_Summary_Data/wd:Job_ Category_Reference/wd:ID [@wd:type='Job_Category_ID']
jobClassificationReference.id	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_Data [@wd:Primary_Job=1]/wd:Position_ Data/wd:Job_Classification_ Summary_Data/wd:Job_

SCIM parameter	WorkDayHR parameter
	Classification_Reference/wd:ID [@wd:type='WID']
jobClassificationReference.referenceID	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_Data [@wd:Primary_Job=1]/wd:Position_ Data/wd:Job_Classification_ Summary_Data/wd:Job_ Classification_Reference/wd:ID [@wd:type='Job_Classification_ Reference_ID']
jobClassifications.id	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_Data [@wd:Primary_Job=1]/wd:Position_ Data/wd:Job_Classification_ Summary_Data/wd:Job_Group_ Reference/wd:ID[@wd:type='WID']
jobExempt (Available from v3.2)	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_ Data/wd:Position_Data/Job_ Exempt/text()
jobFamilyID	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_ Data/wd:Position_Data/wd:Job_ Profile_Summary_Data/wd:Job_ Family_Reference/wd:ID [@wd:type='Job_Family_ID']/text()
jobProfileID	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_Data [@wd:Primary_Job=1]/wd:Position_ Data/wd:Job_Profile_Summary_ Data/wd:Job_Profile_ Reference/wd:ID[wd:type='Job_ Profile_ID']/text()
jobProfileWID	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_ Job_Data [@wd:Primary_ Job=1]/wd:Position_

SCIM parameter	WorkDayHR parameter
	Data/wd:Job_Profile_ Summary_ Data/wd:Job_Profile_ Reference/wd:ID [wd:type='WID']/text()
jobTitle	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_Data [@wd:Primary_Job=1]/wd:Position_ Data/wd:Business_Title/text()
lastHierarchicalManagerWID	wd:Worker/wd:Worker_ Data/wd:Management_Chain_ Data/wd:Worker_Supervisory_ Management_Chain_ Data/wd:Management_Chain_ Data/wd:Manager/wd:Worker_ Reference/wd:ID [@wd:type='WID']/text()
leaveAbsenceType	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Status_ Data/wd:Leave_Status_Data[wd:On_ Leave='1']/wd:Leave_of_Absence_ Type_Reference/wd:ID [@wd:type='Leave_of_Absence_ Type_ID']/text()
leaveEndDate	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Status_ Data/wd:Leave_Status_Data[wd:On_ Leave='1']/wd:Leave_End_Date/text ()
leaveStartDate	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Status_ Data/wd:Leave_Status_Data[wd:On_ Leave='1']/wd:Leave_Start_ Date/text()
localFirstName	wd:Worker/wd:Worker_ Data/wd:Personal_Data/wd:Name_ Data/wd:Preferred_Name_ Data/wd:Name_Detail_ Data/wd:Local_Name_Detail_

SCIM parameter	WorkDayHR parameter
	Data/wd:First_Name/text()
localLastName	wd:Worker/wd:Worker_ Data/wd:Personal_Data/wd:Name_ Data/wd:Preferred_Name_ Data/wd:Name_Detail_ Data/wd:Local_Name_Detail_ Data/wd:Last_Name/text()
localTerminationReasonID	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Status_ Data/wd:Local_Termination_Reason_ Reference/wd:ID/[@wd:type='Local_ Termination_Reason_ID']/text()
managementLevelID	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_Data [@wd:Primary_Job=1]/wd:Position_ Data/wd:Job_Profile_Summary_ Data/wd:Management_Level_ Reference/wd:ID [wd:type='Management_Level_ ID']/text()
managerEmployeeID	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_ Job_Data [@wd:Primary_ Job=1]/wd:Position_ Data/wd:Manager_as_ of_last_ detected_manager_change_ Reference/wd:ID [@wd:type='Employee_ID']/text()
managerId	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_Data [@wd:Primary_Job=1]/wd:Position_ Data/wd:Manager_as_of_last_ detected_manager_change_ Reference/wd:ID [@wd:type='WID']/text()
matrixReferenceId (Available from v3.2) (Not available in LIST response)	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_Data

SCIM parameter	WorkDayHR parameter
	[@wd:Primary_Job=1]/wd:Position_ Organizations_Data/wd:Position_ Organization_Data[string (wd:Organization_ Data/wd:Organization_Type_ Reference/wd:ID [@wd:type='Organization_Type_ ID']/text())='<OrganizationTypeID_ For_Matrix>'] and string (wd:Organization_ Data/wd:Organization_Subtype_ Reference/wd:ID [@wd:type='Organization_Subtype_ ID']/text ())='<OrganizationSubTypeID_For_ Matrix>']/wd:Organization_ Reference/wd:ID [@wd:type='Organization_ Reference_ID']/text()
Name.FamilyName	wd:Worker/wd:Worker_ Data/wd:Personal_Data/wd:Name_ Data/wd:Legal_Na me_ Data/wd:Name_Detail_ Data/wd:Last_Name /text()
Name.Formatted	wd:Worker/wd:Worker_ Data/wd:Personal_Data/wd:Name_ Data/wd:Legal_Na me_ Data/wd:Name_Detail_ Dat/@wd:Formatted_Name
Name.GivenName	wd:Worker/wd:Worker_ Data/wd:Personal_Data/wd:Name_ Data/wd:Legal_Na me_ Data/wd:Name_Detail_ Data/wd:First_Name/text()
notReturning	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Status_ Data/notReturning/text()
onLeave	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Status_ Data/wd:Leave_Status_Data/wd:On_ Leave

SCIM parameter	WorkDayHR parameter
OrganizationSubTypeID for Cost Center Hierarchy	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_ Data/wd:Position_Organizations_ Data/wd:Position_Organization_ Data/wd:Organization_Data[string (wd:Organization_Type_ Reference/wd:ID/@type\)='Organization_Type_ID' and string (wd:Organization_Subtype_ Reference/wd:ID/@type\)='Organization_Subtype_ID' and string (wd:Organization_Subtype_ Reference/wd:ID [@type='Organization_Subtype_ ID'])/text()='{value_for_the_UI_ config_field_OrganizationSubTypeID for Cost Center Hierarchy}']/Organization_Type_ Reference/wd:ID [@type='Organization_subType_ ID']/text()
OrganizationSubTypeID for Matrix	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_ Data/wd:Position_Organizations_ Data/wd:Position_Organization_ Data/wd:Organization_Data[string (wd:Organization_Type_ Reference/wd:ID/@type\)='Organization_Type_ID' and string (wd:Organization_Subtype_ Reference/wd:ID/@type\)='Organization_Subtype_ID' and string (wd:Organization_Type_ Reference/wd:ID [@type='Organization_Type_ ID'])/text()='{value_for_the_UI_ config_field_OrganizationTypeID for Matrix}']/Organization_Subtype_ Reference/wd:ID [@type='Organization_Subtype_ ID']/text()

SCIM parameter	WorkDayHR parameter
OrganizationTypeID for Cost Center Hierarchy	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_ Data/wd:Position_Organizations_ Data/wd:Position_Organization_ Data/wd:Organization_Data[string (wd:Organization_Type_ Reference/wd:ID/@type\)='Organization_Type_ID' and string (wd:Organization_Subtype_ Reference/wd:ID/@type\)='Organization_Subtype_ID' and string (wd:Organization_Subtype_ Reference/wd:ID [@type='Organization_type_ ID'])/text()='{value_for_the_UI_ config_field_OrganizationTypeID for Cost Center Hierarchy}']/Organization_Type_ Reference/wd:ID [@type='Organization_Type_ID']/text ()
OrganizationTypeID for Matrix	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_ Data/wd:Position_Organizations_ Data/wd:Position_Organization_ Data/wd:Organization_Data[string (wd:Organization_Type_ Reference/wd:ID/@type\)='Organization_Type_ID' and string (wd:Organization_Subtype_ Reference/wd:ID/@type\)='Organization_Subtype_ID' and string (wd:Organization_Subtype_ Reference/wd:ID [@type='Organization_Subtype_ ID'])/text()='{value_for_the_UI_ config_field_OrganizationSubTypeID for Matrix}']/Organization_Type_ Reference/wd:ID [@type='Organization_Type_ID']/text ()

SCIM parameter	WorkDayHR parameter
OrgSubTypeID for Custom Organizations	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_ Data/wd:Position_Organizations_ Data/wd:Position_Organization_ Data/wd:Organization_Data[string (wd:Organization_Type_ Reference/wd:ID/@type\)='Organization_Type_ID' and string (wd:Organization_Subtype_ Reference/wd:ID/@type\)='Organization_Subtype_ID' and string (wd:Organization_Subtype_ Reference/wd:ID [@type='Organization_Subtype_ ID'])/text()='{value_for_the_UI_ config_field_OrgSubTypeID for Custom Organizations}']/Organization_Type_ Reference/wd:ID [@type='Organization_Type_ID']/text ()
OrgTypeID for Custom Organizations	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_ Data/wd:Position_Organizations_ Data/wd:Position_Organization_ Data/wd:Organization_Data[string (wd:Organization_Type_ Reference/wd:ID/@type\)='Organization_Type_ID' and string (wd:Organization_Subtype_ Reference/wd:ID/@type\)='Organization_Subtype_ID' and string (wd:Organization_Type_ Reference/wd:ID [@type='Organization_Type_ ID'])/text()='{value_for_the_UI_ config_field_OrgTypeID for Custom Organizations}']/Organization_ Subtype_Reference/wd:ID [@type='Organization_Subtype_ ID']/text()
originalHireDate	wd:Worker/wd:Worker_

SCIM parameter	WorkDayHR parameter
	Data/wd:Employment_ Data/wd:Worker_Status_ Data/wd:Orignial_Hire_Date/text(
personalAssistantID	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_Data [@wd:Primary_Job=1]/wd:Position_ Organizations_Data/wd:Position_ Organization_Data[string (wd:Organization_ Data/wd:Organization_Type_ Reference/wd:ID [@wd:type='Organization_Type_ ID']/text())='<OrganizationTypeID_ For_PersonalAssistant>'] and string (wd:Organization_ Data/wd:Organization_Subtype_ Reference/wd:ID [@wd:type='Organization_Subtype_ ID']/text ())='<OrganizationSubTypeID_For_ PersonalAssistant>']/wd:Organizatio n_Reference/wd:ID [@wd:type='WID']/text()
personalAssistantReferenceId (Available from v3.2) (Not available in LIST response)	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_Data [@wd:Primary_Job=1]/wd:Position_ Organizations_Data/wd:Position_ Organization_Data[string (wd:Organization_ Data/wd:Organization_Type_ Reference/wd:ID [@wd:type='Organization_Type_ ID']/text())='<OrganizationTypeID_ For_PersonalAssistant>'] and string (wd:Organization_ Data/wd:Organization_Subtype_ Reference/wd:ID [@wd:type='Organization_Subtype_ ID']/text ())='<OrganizationSubTypeID_For_ PersonalAssistant>']/wd:Organizatio n_Reference/wd:ID

SCIM parameter	WorkDayHR parameter
	[@wd:type='Organization_ Reference_ID']/text()
PhoneNumbers.businessPhone (available until v3.1)	wd:Worker/wd:Worker_ Data/wd:Personal_Data/wd:Contact_ Data/wd:Phone_Data[string (wd:Phone_Device_Type_ID/wd:ID [@wd:type='Phone_Device_Type_ ID'])=<Landline_ Device_Type_ ID>]/wd:Phone_Number/text() wd:Worker/wd:Worker_ Data/wd:Personal_Data/wd:Contact_ Data/wd:Phone_Data/wd:Usage_ Data/wd:Type_Data/wd:Type_ Reference/wd:ID [@wd:type='Communication_Usage_ Type_ID'])='Home']
PhoneNumbers.cellPhone (available until v3.1)	wd:Worker/wd:Worker_ Data/wd:Personal_Data/wd:Contact_ Data/wd:Phone_Data[string (wd:Phone_Device_Type_ID/wd:ID [@wd:type='Phone_Device_Type_ ID'])=<Mobile_ Device_Type_ ID>]/wd:Phone_Number /text() wd:Worker/wd:Worker_ Data/wd:Personal_Data/wd:Contact_ Data/wd:Phone_Data/wd:Usage_ Data/wd:Type_Data/wd:Type_ Reference/wd:ID [@wd:type='Communication_Usage_ Type_ID'])='Home']
PhoneNumbersWork.businessPhone (available until v3.1)	wd:Worker/wd:Worker_ Data/wd:Personal_Data/wd:Contact_ Data/wd:Phone_Data[string (wd:Phone_Device_Type_ID/wd:ID [@wd:type='Phone_Device_Type_ ID'])=<Landline_ Device_Type_ ID>]/wd:Phone_Number/text() wd:Worker/wd:Worker_ Data/wd:Personal_Data/wd:Contact_ Data/wd:Phone_Data/wd:Usage_ Data/wd:Type_Data/wd:Type_ Reference/wd:ID [@wd:type='Communication_Usage_ Type_ID'])='Work']

SCIM parameter	WorkDayHR parameter
PhoneNumbersWork.cellPhone (available until v3.1)	wd:Worker/wd:Worker_Data/wd:Personal_Data/wd:Contact_Data/wd:Phone_Data[string(wd:Phone_Device_Type_ID/wd:ID[@wd:type='Phone_Device_Type_ID'])=<Mobile_Device_Type_ID>]/wd:Phone_Number/text() wd:Worker/wd:Worker_Data/wd:Personal_Data/wd:Contact_Data/wd:Phone_Data/wd:Usage_Data/wd:Type_Data/wd:Type_Reference/wd:ID[@wd:type='Communication_Usage_Type_ID'])='Work']
positionReferenceWID	wd:Worker/wd:Worker_Data/wd:Employment_Data/wd:Worker_Job_Data[@wd:Primary_Job=1]/wd:Position_Data/wd:Position_Reference/wd:ID[@wd:type='WID']
preferredCommunicationLanguageReference	/wd:Worker/wd:Worker_Data/wd:User_Account_Data/wd:Preferred_Communication_Language_Reference/text()
preferredFirstName	wd:Worker/wd:Worker_Data/wd:Personal_Data/wd:Name_Data/wd:Preferred_Name_Data/wd:Name_Detail_Data/wd:First_Name/text()
preferredLastName	wd:Worker/wd:Worker_Data/wd:Personal_Data/wd:Name_Data/wd:Preferred_Name_Data/wd:Name_Detail_Data/wd:Last_Name/text()
preferredLastNameSuffix	wd:Worker/wd:Worker_Data/wd:Personal_Data/wd:Name_Data/wd:Preferred_Name_Data/wd:Name_Detail_Data/wd:Suffix_Data/wd:Hereditary_Suffix_Reference/wd:Descriptor/text()

SCIM parameter	WorkDayHR parameter
preferredMiddleName	wd:Worker/wd:Worker_ Data/wd:Personal_Data/wd:Name_ Data/wd:Preferred_Name_ Data/wd:Name_Detail_ Data/wd:Middle_Name/text()
primaryDeviceType	wd:Worker/wd:Worker_ Data/wd:Personal_Data/wd:Contact_ Data/wd:Phone_Data[string (wd:Phone_Device_Type_ID/wd:ID [@wd:type='Phone_Device_Type_ ID'])=<Mobile_Device_Type_ ID>]/wd:Phone_Device_Type_ Reference/wd:Phone_Device_Type_ ID/text() wd:Worker/wd:Worker_ Data/wd:Personal_Data/wd:Contact_ Data/wd:Phone_Data/wd:Usage_ Data/wd:Type_Data/wd:Type_ Reference/wd:ID [@wd:type='Communication_Usage_ Type_ID'])='Work']
primaryTerminationCategoryID	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Status_ Data/wd:Primary_Termination_ Category_Reference/wd:ID/ [@wd:type='Termination_Category_ ID']/text()
primaryTerminationSubCategoryID	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Status_ Data/wd:Primary_Termination_ Reason_Reference/wd:ID/ [@wd:type='Termination_ Subcategory_ID']/text()
pronounID (Available from v3.2)	wd:Worker/wd:Worker_ Data/wd:Personal_ Data/wd:Personal_Information_ Data/wd:Pronoun_Reference/wd:ID [@wd:type='Pronoun_ID']
region	wd:Worker/wd:Worker_ Data/wd:Employment_

SCIM parameter	WorkDayHR parameter
	Data/wd:Worker_Job_Data [@wd:Primary_Job=1]/wd:Position_ Organizations_Data/wd:Position_ Organization_Data[string (wd:Organization_ Data/wd:Organization_Type_ Reference/wd:ID [@wd:type='Organization_Type_ ID']/text())='<OrganizationTypeID_ For_Region>'] and string (wd:Organization_ Data/wd:Organization_Subtype_ Reference/wd:ID [@wd:type='Organization_Subtype_ ID']/text ())='<OrganizationSubTypeID_For_ Region>']/wd:Organization_ Reference/wd:ID [@wd:type='WID']/text()
regionReferenceId (Available from v3.2) (Not available in LIST response)	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_Data [@wd:Primary_Job=1]/wd:Position_ Organizations_Data/wd:Position_ Organization_Data[string (wd:Organization_ Data/wd:Organization_Type_ Reference/wd:ID [@wd:type='Organization_Type_ ID']/text())='<OrganizationTypeID_ For_Region>'] and string (wd:Organization_ Data/wd:Organization_Subtype_ Reference/wd:ID [@wd:type='Organization_Subtype_ ID']/text ())='<OrganizationSubTypeID_For_ Region>']/wd:Organization_ Reference/wd:ID [@wd:type='Organization_ Reference_ID']/text()
rehire	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Status_ Data/rehire/text()

SCIM parameter	WorkDayHR parameter
retired	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Status_ Data/Retired/text()
returnUnknown	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Status_ Data/returnUnknown/text()
samAccountName	wd:Worker/wd:Worker_ Data/wd:Personal_ Data/wd:Identification_ Data/wd:Custom_ID/wd:Custom_ID_ Data[string(wd:ID_Type_ Reference/wd:ID/@wd:type)='Custo m_ID_Type_ID' and string(wd:ID_ Type_Reference/wd:ID [@wd:type='Custom_ID_Type_ ID']/text ())='<SAMAccountID>']/wd:ID/text()
startDate	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_Data [@wd:Primary_Job=1]/wd:Position_ Data/wd:Start_Date/text()
status	Active (A): wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Status_ Data/Active/text()='1' Or Terminated (L): wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Status_ Data/Terminated/text()='1'
supervisorManagementChainData~managerDes criptor (Available from v3.2)	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_ Data/wd:Position_Management_ Chains_Data/wd:Position_ Supervisory_Management_Chain_ Data/wd:Management_Chain_ Data/wd:Manager/Worker_ Descriptor/text()
supervisorManagementChainData~managerId	wd:Worker/wd:Worker_

SCIM parameter	WorkDayHR parameter
(Available from v3.2)	Data/wd:Employment_ Data/wd:Worker_Job_ Data/wd:Position_Management_ Chains_Data/wd:Position_ Supervisory_Management_Chain_ Data/wd:Management_Chain_ Data/wd:Manager/wd:Worker_ Reference/wd:ID[@wd:type='WID']
supervisorManagementChainData~organization ReferenceId (Available from v3.2)	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_ Data/wd:Position_Management_ Chains_Data/wd:Position_ Supervisory_Management_Chain_ Data/wd:Management_Chain_ Data/wd:Organization_ Reference/wd:ID [@wd:type='Organization_ Reference_ID']
supplierReferenceID (Available from v3.2)	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Contract_ Data/wd:Supplier_Reference/wd:ID [@wd:type='Supplier_Reference_ID']
terminationDate	wd:Worker/wd:Worker_ Data/wd:Employment_Data[string (wd:Worker_Job_Data [@wd:Primary_Job=1]/wd:Position_ Data/wd:Worker_Type_ Reference/wd:ID/@wd:type)='Employee_Type_ID']/wd:Worker_Status_ Data/Termination_Date/text() or wd:Worker/wd:Worker_ Data/wd:Employment_Data[string (wd:Worker_Job_Data [@wd:Primary_Job=1]/wd:Position_ Data/wd:Worker_Type_ Reference/wd:ID/@wd:type)='Contingent_Worker_Type_ID']/wd:Worker_ Contract_Data/Contract_End_ Date/text()
terminationLastDayOfWork	wd:Worker/wd:Worker_ Data/wd:Employment_

SCIM parameter	WorkDayHR parameter
	Data/wd:Worker_Status_ Data/Termination_Last_Day_Of_ Work/text()
title	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_Data [@wd:Primary_Job=1]/wd:Position_ Data/wd:Position_Title/text()
userId	wd:Worker/wd:Worker_ Data/wd:User_ID/text()
userLanguageReference	/wd:Worker/wd:Worker_ Data/wd:User_Account_ Data/wd:User_Language__ Reference/text()
UserName	wd:Worker/wd:Worker_ Data/wd:User_ID/text()
workerId	wd:Worker/wd:Worker_ Data/wd:Worker_ID/text()
workerType	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_Data[@wd :Primary_Job=1]/wd:Position_ Data/wd:Worker_Type_ Reference/wd:ID[@w d:type='Employee_Type_ID' Or @wd:type='Contingent_Worker_ Type_ID']/text()
workPhoneLandline (Available until v3.1)	wd:Worker/wd:Worker_ Data/wd:Personal_Data/wd:Contact_ Data/wd:Phone_Data[string (wd:Phone_Device_Type_ID/wd:ID [@wd:type='Phone_Device_Type_ ID'])=<Landline_ Device_Type_ ID>]/wd:Phone_Number/text ()wd:Worker/wd:Worker_ Data/wd:Personal_Data/wd:Contact_ Data/wd:Phone_Data/wd:Usage_ Data/wd:Type_Data [@wd:primary='0']/wd:Type_ Reference/wd:ID [@wd:type='Communication_Usage_

SCIM parameter	WorkDayHR parameter
	Type_ID'])='Work']
workPhoneLandline~countryIsoCode (Available from v3.2)	wd:Worker/wd:Worker_ Data/wd:Personal_Data/wd:Contact_ Data/wd:Phone_Data[string (wd:Phone_Device_Type_ Reference/wd:ID[@wd:type='Phone_ Device_Type_ID'])=<Landline_ Device_Type_ID> AND string (wd:Usage_Data/wd:Type_Data [@wd:primary='0']/wd:Type_ Reference/wd:ID [@wd:type='Communication_Usage_ Type_ID'])='Work']/wd:Country_ ISO_Code/text()
workPhoneLandline~countryPhoneCode (Available from v3.2)	wd:Worker/wd:Worker_ Data/wd:Personal_Data/wd:Contact_ Data/wd:Phone_Data[string (wd:Phone_Device_Type_ Reference/wd:ID[@wd:type='Phone_ Device_Type_ID'])=<Landline_ Device_Type_ID> AND string (wd:Usage_Data/wd:Type_Data [@wd:primary='0']/wd:Type_ Reference/wd:ID [@wd:type='Communication_Usage_ Type_ ID'])='Work']/wd:International_ Phone_Code/text()
workPhoneLandline~number (Available from v3.2)	wd:Worker/wd:Worker_ Data/wd:Personal_Data/wd:Contact_ Data/wd:Phone_Data[string (wd:Phone_Device_Type_ Reference/wd:ID[@wd:type='Phone_ Device_Type_ID'])=<Landline_ Device_Type_ID> AND string (wd:Usage_Data/wd:Type_Data [@wd:primary='0']/wd:Type_ Reference/wd:ID [@wd:type='Communication_Usage_ Type_ID'])='Work')]/@wd:E164_ Formatted_Phone
workPhoneMobile (Available until v3.1)	wd:Worker/wd:Worker_ Data/wd:Personal_Data/wd:Contact_

SCIM parameter	WorkDayHR parameter
	Data/wd:Phone_Data[string (wd:Phone_Device_Type_ID/wd:ID [@wd:type='Phone_Device_Type_ ID'])=<Mobile_ Device_Type_ ID>]/wd:Phone_Number/text ()wd:Worker/wd:Worker_ Data/wd:Personal_Data/wd:Contact_ Data/wd:Phone_Data/wd:Usage_ Data/wd:Type_Data [@wd:primary='0']/wd:Type_ Reference/wd:ID [@wd:type='Communication_Usage_ Type_ID'])='Work']
workPhoneMobile~countryIsoCode (Available from v3.2)	wd:Worker/wd:Worker_ Data/wd:Personal_Data/wd:Contact_ Data/wd:Phone_Data[string (wd:Phone_Device_Type_ Reference/wd:ID[@wd:type='Phone_ Device_Type_ID'])=<Mobile_Device_ Type_ID> AND string(wd:Usage_ Data/wd:Type_Data [@wd:primary='0']/wd:Type_ Reference/wd:ID [@wd:type='Communication_Usage_ Type_ID'])='Work']/wd:Country_ ISO_Code/text()
workPhoneMobile~countryPhoneCode (Available from v3.2)	wd:Worker/wd:Worker_ Data/wd:Personal_Data/wd:Contact_ Data/wd:Phone_Data[string (wd:Phone_Device_Type_ Reference/wd:ID[@wd:type='Phone_ Device_Type_ID'])=<Mobile_ Device_ Type_ID> AND string(wd:Usage_ Data/wd:Type_Data [@wd:primary='0']/wd:Type_ Reference/wd:ID [@wd:type='Communication_Usage_ Type_ ID'])='Work']/wd:International_ Phone_Code/text()
workPhoneMobile~number (Available from v3.2)	wd:Worker/wd:Worker_ Data/wd:Personal_Data/wd:Contact_ Data/wd:Phone_Data[string

SCIM parameter	WorkDayHR parameter
	(wd:Phone_Device_Type_ Reference/wd:ID[@wd:type='Phone_ Device_Type_ID'])=<Mobile_ Device_ Type_ID> AND string(wd:Usage_ Data/wd:Type_Data [@wd:primary='0']/wd:Type_ Reference/wd:ID [@wd:type='Communication_Usage_ Type_ID'])='Work')]/@wd:E164_ Formatted_Phone
workPhoneMobilePrimary~countryIsoCode (Available from v3.2)	wd:Worker/wd:Worker_ Data/wd:Personal_Data/wd:Contact_ Data/wd:Phone_Data[string (wd:Phone_Device_Type_ Reference/wd:ID[@wd:type='Phone_ Device_Type_ID'])=<Mobile_ Device_ Type_ID> AND string(wd:Usage_ Data/wd:Type_Data [@wd:primary='1']/wd:Type_ Reference/wd:ID [@wd:type='Communication_Usage_ Type_ID'])='Work']/wd:Country_ ISO_Code/text()
workPhoneMobilePrimary~countryPhoneCode (Available from v3.2)	wd:Worker/wd:Worker_ Data/wd:Personal_Data/wd:Contact_ Data/wd:Phone_Data[string (wd:Phone_Device_Type_ Reference/wd:ID[@wd:type='Phone_ Device_Type_ID'])=<Mobile_ Device_ Type_ID> AND string(wd:Usage_ Data/wd:Type_Data [@wd:primary='1']/wd:Type_ Reference/wd:ID [@wd:type='Communication_Usage_ Type_ ID'])='Work']/wd:International_ Phone_Code/text()
workPhoneMobilePrimary~number (Available from v3.2)	wd:Worker/wd:Worker_ Data/wd:Personal_Data/wd:Contact_ Data/wd:Phone_Data[string (wd:Phone_Device_Type_ Reference/wd:ID[@wd:type='Phone_ Device_Type_ID'])=<Mobile_ Device_ Type_ID> AND string(wd:Usage_

SCIM parameter	WorkDayHR parameter
	Data/wd:Type_Data [@wd:primary='1']/wd:Type_ Reference/wd:ID [@wd:type='Communication_Usage_ Type_ID'])='Work']/@wd:E164_ Formatted_Phone
workPhonePrimary (Available until v3.1)	wd:Worker/wd:Worker_ Data/wd:Personal_Data/wd:Contact_ Data/wd:Phone_Data[string (wd:Phone_Device_Type_ID/wd:ID [@wd:type='Phone_Device_Type_ ID'])=<Any_ Device_Type_ ID>]/wd:Phone_Number/text ()wd:Worker/wd:Worker_ Data/wd:Personal_Data/wd:Contact_ Data/wd:Phone_Data/wd:Usage_ Data/wd:Type_Data [@wd:primary='1']/wd:Type_ Reference/wd:ID [@wd:type='Communication_Usage_ Type_ID'])='Work']
workPhonePrimary~countryIsoCode (Available from v3.2)	wd:Worker/wd:Worker_ Data/wd:Personal_Data/wd:Contact_ Data/wd:Phone_Data[string (wd:Phone_Device_Type_ Reference/wd:ID[@wd:type='Phone_ Device_Type_ID'])=<Landline_ Device_Type_ID> AND string (wd:Usage_Data/wd:Type_Data [@wd:primary='1']/wd:Type_ Reference/wd:ID [@wd:type='Communication_Usage_ Type_ID'])='Work']/wd:Country_ ISO_Code/text()
workPhonePrimary~countryPhoneCode (Available from v3.2)	wd:Worker/wd:Worker_ Data/wd:Personal_Data/wd:Contact_ Data/wd:Phone_Data[string (wd:Phone_Device_Type_ Reference/wd:ID[@wd:type='Phone_ Device_Type_ID'])=<Landline_ Device_Type_ID> AND string (wd:Usage_Data/wd:Type_Data [@wd:primary='1']/wd:Type_ Reference/wd:ID

SCIM parameter	WorkDayHR parameter
	[@wd:type='Communication_Usage_Type_ID']='Work']/wd:International_Phone_Code/text()
workPhonePrimary~number (Available from v3.2)	wd:Worker/wd:Worker_Data/wd:Personal_Data/wd:Contact_Data/wd:Phone_Data[string (wd:Phone_Device_Type_Reference/wd:ID[@wd:type='Phone_Device_Type_ID'])=<Landline_Device_Type_ID> AND string (wd:Usage_Data/wd:Type_Data [@wd:primary='1']/wd:Type_Reference/wd:ID [@wd:type='Communication_Usage_Type_ID'])='Work')]/@wd:E164_Formatted_Phone

Table 262: FutureDatedEmployees Mapping

SCIM Parameter	WorkDayHR Parameter
managerID	wd:Worker/wd:Worker_Data/wd:Employment_Data/wd:Worker_Job_Data/wd:Position_Organizations_Data/wd:Position_Organization_Data/wd:Organization_Data/wd:Organization_Support_Role_Data/wd:Organization_Support_Role/wd:Organization_Role_Data/wd:Worker_Reference/wd:ID[@wd:type='WID']
continuousServiceDate	wd:Worker/wd:Worker_Data/wd:Employment_Data/wd:Worker_Status_Data/wd:Continuous_Service_Date/text()
rehireDate	wd:Worker/wd:Worker_Data/wd:Transaction_Log_Entry_Data/wd:Transaction_Log_Entry/wd:Transaction_Log_Data/wd:Transaction_Effective_Moment/text() WHERE wd:Worker/wd:Worker_Data/wd:Transaction_Log_Entry_Data/wd:Transaction_Log_Entry/wd:Transaction_Log_Data/wd:Transaction_Log_Type_Reference/wd:ID [@wd:type="Business_Process_Type"]/text() = Hire Employee

SCIM Parameter	WorkDayHR Parameter
businessProcessTransactionLogs []~businessProcessType [Mapped only if the corresponding Business Process Type is configured in the Starling Connect portal]	wd:Worker/wd:Worker_Data/wd:Transaction_Log_Entry_Data/wd:Transaction_Log_Entry/wd:Transaction_Log_Data/wd:Transaction_Log_Type_Reference/wd:ID [@wd:type="Business_Process_Type"]/text()
businessProcessTransactionLogs []~businessProcessEffectiveMoment [Mapped only if the corresponding Business Process Type is configured in the Starling Connect portal]	wd:Worker/wd:Worker_Data/wd:Transaction_Log_Entry_Data/wd:Transaction_Log_Entry/wd:Transaction_Log_Data/wd:Transaction_Effective_Moment/text()
businessProcessTransactionLogs []~businessProcessXML [Mapped only if the corresponding Business Process Type is configured in the Starling Connect portal]	wd:Worker/wd:Worker_Data/wd:Transaction_Log_Entry_Data/wd:Transaction_Log_Entry/xml()

NOTE:

- All the other SCIM Parameter mapping is same as the Employees Mapping.

Table 263: DeltaSyncEmployees Mapping

NOTE:

- All the SCIM Parameter mapping is same as the Employees Mapping.

Table 264: Locations Mapping

SCIM Parameter	WorkDayHR Parameter
Addresses.country	wd:Location/wd:Location_Data/wd:Contact_Data/wd:Address_Data/wd:Country_Refer ence/ID [@type='ISO_3166-1_Alpha-3_Code']/text()
Addresses.countryCode2	wd:Location/wd:Location_Data/wd:Contact_Data/wd:Address_Data/wd:Country_Reference/ID [@type='ISO_3166-1_Alpha-2_Code']/text()
Addresses.locality	wd:Location/wd:Location_

SCIM Parameter	WorkDayHR Parameter
	Data/wd:Contact_Data/wd:Address_ Data/wd:Municipality/ text()
Addresses.postalCode	wd:Location/wd:Location_ Data/wd:Contact_Data/wd:Address_ Data/wd:Postal_Code/t ext()
Addresses.region	wd:Location/wd:Location_ Data/wd:Contact_Data/wd:Address_ Data/wd:Country_Region_ Descriptor/text()
Addresses.streetAddress	wd:Location/wd:Location_ Data/wd:Contact_Data/wd:Address_ Data/@Formatted_Addre ss
addressLineData.addressData	wd:Location/wd:Location_ Data/wd:Contact_Data/wd:Address_ Data/wd:Address_Line_Data/text()
countryRegionCode2	wd:Location/wd:Location_ Data/wd:Contact_Data/wd:Address_ Data/wd:Country_Region_ Reference/wd:ID[@wd:type='ISO_ 3166-2_Code']
countryRegionCode	wd:Location/wd:Location_ Data/wd:Contact_Data/wd:Address_ Data/wd:Country_Region_ Reference/wd:ID[@wd:type='ISO_ 3166-2_Country-Region_Code']
citySubDivisionData.citySubdivisionData	wd:Location/wd:Location_ Data/wd:Contact_Data/wd:Address_ Data/wd:Submunicipality_Data/text()
Emails.value	wd:Location/wd:Location_ Data/wd:Contact_Data/wd:Email_ Address_Data/wd:Email_A ddress/text()
fax	wd:Location/wd:Location_ Data/wd:Contact_Data/wd:Phone_ Data[string(Phone_Devic e_Type_ Reference/ID[@wd:type='Phone_ Device_Type_ID']/text ())='Fax']/wd:Phone_ Number/text()

SCIM Parameter	WorkDayHR Parameter
Id	wd:Location/Location_Reference/ID [@type='WID']/text()
locationID	wd:Location/wd:Location_ Data/wd:Location_ID/text()
name	wd:Location/wd:Location_ Data/wd:Location_Name/text()
regionSubDivisionData.regionSubdivisionData	wd:Location/wd:Location_ Data/wd:Contact_Data/wd:Address_ Data/wd:Subregion_Data/text()
status	wd:Location/wd:Location_ Data/wd:Inactive/text()
telephone	wd:Location/wd:Location_ Data/wd:Contact_Data/wd:Phone_ Data[string(Phone_Devic e_Type_ Reference/ID[@wd:type='Phone_ Device_Type_ID']/text ())='Landline']/wd:P hone_ Number/text()

Table 265: CustomOrgs Mapping

SCIM Parameter	WorkDayHR Parameter
companyReferenceID	wd:Organization/wd:Organization_ Data/wd:Supervisory_Data/wd:Organization_ Assignments_Data[string(wd:Organization_ Type_Reference/wd:ID [@wd:type='Organization_Type_ID']/text ())='<OrganizationTypeID_For_ Company>']/Organization_Reference/ID [@wd:type='WID']/text()
costCenterID	wd:Organization/wd:Organization_ Data/wd:Supervisory_Data/wd:Organization_ Assignments_Data[string(wd:Organization_ Type_Reference/wd:ID [@wd:type='Organization_Type_ID']/text ())='<OrganizationTypeID_For_ CostCenter>']/Organization_Reference/ID [@wd:type='WID']/text()
Id	wd:Organization/Organization_Reference/ID [@type='WID']/text()
lastModifiedOn	wd:Organization/wd:Organization_Data/Last_ Updated_DateTime/text()

SCIM Parameter	WorkDayHR Parameter
locationID	wd:Organization/wd:Organization_Data/Supervisory_Data/Location_Reference/ID[@type='WID']/text()
managerReferenceID	wd:Organization/wd:Organization_Data/wd:Manager_Reference/wd:ID[@wd:type='WID']/text()
Meta.LastModified	wd:Organization/wd:Organization_Data/Last_Updated_DateTime/text()
name	wd:Organization/wd:Organization_Data/wd:Name/text()
organizationCode	wd:Organization/wd:Organization_Data/wd:Organization_Code/text()
organizationOwnerID	wd:Organization/wd:Organization_Data/Organization_Owner_Reference/ID[@type='WID']/text()
organizationTypeReferenceID	wd:Organization/wd:Organization_Data/Organization_Type_Reference/ID[@type='Organization_Type_ID']/text()
referenceID	wd:Organization/wd:Organization_Data/wd:Reference_ID/text()
regionReferenceID	wd:Organization/wd:Organization_Data/wd:Supervisory_Data/wd:Organization_Assignments_Data[string(wd:Organization_Type_Reference/wd:ID[@wd:type='Organization_Type_ID']/text())='<OrganizationTypeID_For_Region>']/Organization_Reference/ID[@wd:type='WID']/text()
status	wd:Organization/wd:Organization_Data/wd:Inactive/text()
type	wd:Organization/wd:Organization_Data/wd:Organization_Subtype_Reference/wd:ID[@type='Organization_Subtype_ID']/text()
includedInOrganizationReferenceWID	wd:Worker/wd:Worker_Data/wd:Employment_Data/wd:Worker_Job_Data[@wd:Primary_Job=1]/wd:Position_Data/wd:Position_Reference/wd:ID[@wd:type='WID']

SCIM Parameter	WorkDayHR Parameter
leadershipReferences~id	wd:Organization/wd:Organization_Data/wd:Leadership_Reference/wd:ID [@type='WID']/text()
leadershipReferences~empId	wd:Organization/wd:Organization_Data/wd:Leadership_Reference/wd:ID [@type='Employee_ID']/text()

Table 266: JobClassifications

SCIM Parameter	WorkDayHR Parameter
groupId	Job_Classification_Group/Job_Classification_Group_Data/ID/text()
groupName	Job_Classification_Group/Job_Classification_Group_Name_Data/ Job_Classification_Group_Name/text()
Id	Job_Classification_Group/Job_Classification_Group_Reference/ID[@type='WID']/text()
inActive	Job_Classification_Group/Job_Classification_Group_Data/Inactive/text()

Table 267: Positions

SCIM Parameter	WorkDayHR Parameter
ID	wd:Position/wd:Position_Reference/wd:Employment_Data/ID [@type='WID']/text()
jobPostingTitle	wd:Position/wd:Position_Data/wd:Position_Definition_Data/wd:Job_Posting_Title/text()
jobDescriptionSummary	wd:Position/wd:Position_Data/wd:Position_Definition_Data/wd:Job_Description_Summary/text()
positionID	wd:Position/wd:Position_Data/wd:Position_Definition_Data/wd:Position_ID/text()

Table 268: Jobprofiles

SCIM Parameter	WorkDayHR Parameter
ID	wd:Job_Profile/Job_Profile_Reference/ID [@type='WID']/text()
jobCode	wd:Job_Profile/Job_Profile_Data/Job_Code/text()

SCIM Parameter	WorkDayHR Parameter
jobTitle	wd:Job_Profile/Job_Profile_Data/Job_Profile_Basic_Data/Job_Title/text()
inActive	true - wd:Job_Profile/Job_Profile_Data/Job_Profile_Basic_Data/Inactive/text() = '1' or false - wd:Job_Profile/Job_Profile_Data/Job_Profile_Basic_Data/Inactive/text() = '0'
includeJobCodeInName	true - wd:Job_Profile/Job_Profile_Data/Job_Profile_Basic_Data/Include_Job_Code_in_Name/text() = '1' or false - wd:Job_Profile/Job_Profile_Data/Job_Profile_Basic_Data/Include_Job_Code_in_Name/text() = '0'
criticalJob	true - wd:Job_Profile/Job_Profile_Data/Job_Profile_Basic_Data/Critical_Job/text() = '1' or false - wd:Job_Profile/Job_Profile_Data/Job_Profile_Basic_Data/Critical_Job/text() = '0'

Filter Resource

Workday Employee resource response does not provide '**meta.lastModified**' in the response. This makes impossible to get the revision filtered employees list. The full employee list without revision filters will be too slow for frequent synchronizations. As a work-around for this the Workday HR connector has been modified to support filtering only on the **Employees** endpoint. Even though the intension to support filtering is only on '**meta.lastModified**', the connector has been modified to support some more attributes for filtering. Below are the details on the supported attributes and operations on filter functionality on the Employee resource on the SCIM connector.

NOTE:

WorkdayHR supports two kind of updates -

- Manual update- when an employee record is updated manually on workdayHR.
- effective update - when an employee is updated manually with an effective date and workdayHR updates the record as the effective date is reached

A new endpoint DeltaSyncEmployees has been added to support these two updates using combination of two filters - meta.lastModified and manualupdate

Supported attributes for Filtering Employee Resource

Table 269: Supported attributes for Filtering Employee Resource

Attribute	Supported Operations
addresses.country	eq (equal to)
assetClass	eq
company	eq
costCenter	eq
department	eq
desk	eq
division	eq
id	eq
futurehire	eq
meta.lastModified	gt (greater than) ge (greater than or equal to)
personalAssistantID	eq
region	eq
status	eq
manualUpdate	eq

NOTE: As the WorkDayHR API supports only filtering of Active Employees, Status filter has been implemented to support only Active employees. Filtering of inactive employees is not supported. Valid values for Status filter is 'A' for active Employees.

NOTE: manualUpdate is only applicable for DeltaSyncEmployees endpoint

More information about Filtering Resource

- As the Workday API supports only AND conditions in the request filter criteria, the connector has been implemented to support only AND in SCIM filter condition.
- In the connector filter functionality, any invalid or non-supported filter criteria will be ignored in the filter. If no valid criteria found, then normal LIST employees will be carried out.

- Due to timezone differences there is a considerable difference in the Workday returned date time data and the local date time date. Since the Workday documentation do not mention on the supported timezone, as a work around, 1 day is subtracted from current date time while implementing the filter in the Workday HR connector for meta.lastModified. Similarly 1 day is subtracted from the meta.lastModified value in the filter criteria while making a request to the target system.
- The filter functionality searches generously for the filter condition and values instead of performing a greedy and strict match. For example: the meta.lastModified with below are some of the valid formats:

  filter=meta.lastModified gt xxxx-xx-xxTxx:xx:xx

  filter=meta.lastModified gt xxxx-xx-xx xx:xx:xx

  filter=meta.lastModified gt xxxx-xx-xxTxx:xx:xx.xxx

  filter=meta.lastModified gt "xxxx-xx-xxTxx:xx:xx"

  filter=meta.lastModified gt xxxx-xx-xx xx:xx:xxZ

  filter=meta.lastModified gt xxxx-xx-xxTxx:xx:xx.xxxZ

  filter=meta.lastModified gt 'xxxx-xx-xxTxx:xx:xx'
- The Filter expressions will only accept OR with ID attributes and individual filter expressions on various attributes are combined using AND only.
- Only OR is supported within individual id filter expressions
- All OR expressions of ID should be placed together, out-of-order OR expressions are considered invalid. The collection of OR expressions on IDs can be at the start or at the end.

For more information about Filter Resource, see Workday documentation of filtering on Workers endpoints.

One IM Configuration for Delta Synchronization

Modifying the FullProjection process

1. In **Designer**, locate the '**DPR_DPRProjectionStartInfo_Run_Synchronization**' process click to edit it. Under '**Pre-script for generating**' add the script as mentioned below:

   ```
   'Starling Delta Sync Handling (search sync project variables with their
   names staring with dprRevisionDate and put the corresponding revision
   data value in)
   ```

```
Dim f = session.SqlFormatter
Dim nameSchema as String
Dim nameVariable as String
Dim variableValue as String
values("OverrideVariables") = ""

'search project variables dprRevisionDate*
Dim qVariables = Query _
.From("DPRSystemVariable") _
.Orderby("UID_DPRSystemVariable") _
.Where( f.AndRelation( _
f.Comparison("Name", "dprRevisionDate%", ValType.String,
CompareOperator.Like, FormatterOptions.IgnoreCase), _
f.UidComparison("UID_DPRSystemVariableSet", $UID_DPRSystemVariableSet$,
CompareOperator.Equal))) _
.Select("Name")
Dim colVariables = Session.Source.GetCollection(qVariables)

If colVariables.Count > 0 then
'fetching revision data from last synchronization of that sync project
configuration
Dim qRevStore = Query _
.From("DPRRevisionStore") _
.Where( f.AndRelation( _
f.UidComparison("UID_DPRProjectionConfig", $UID_DPRProjectionConfig$,
CompareOperator.Equal), _
f.UidComparison("UID_DPRSystemVariableSet", $UID_DPRSystemVariableSet$,
CompareOperator.Equal))) _
.Select("Value", "SchemaTypeKey")

Dim colRevStore = Session.Source.GetCollection(qRevStore)
Dim dictRevStore = new System.Collections.Generic.Dictionary(of String,
String)()

For Each elemRevStore As IEntity In colRevStore
```

```
nameSchema = elemRevStore.GetValue("SchemaTypeKey").String 'Schema
[FTP#C04A6567-9EAE-4121-973E-AF1EE514D728].Type[Employees]
If string.IsNullOrEmpty(nameSchema) OrElse not nameSchema.Contains(".") then
Continue For
End If
nameSchema = nameSchema.Split("."c)(1)

dictRevStore.Add(nameSchema, elemRevStore.GetValue("Value").String)
Next

'put the revision date into the variables if available, else provide the
revision data as 1900-01-01
Dim lstVariables = new System.Collections.Generic.List(of String)()
For Each elemVariable As IEntity In colVariables
nameVariable = elemVariable.GetValue("Name").String 'e.g.
dprRevisionDateEmployees
nameSchema = string.Format("Type[{0}]", nameVariable.Trim().Substring(15))
'e.g. Type[Employees]

If dictRevStore.TryGetValue(nameSchema, variableValue) then
values(nameVariable) = variableValue.Replace(" ", "T")
Else
values(nameVariable) = "1900-01-01"
End If
lstVariables.Add(nameVariable)
Next
values("OverrideVariables") = string.Join(";", lstVariables.ToArray())
End If
```

2. Under '**Run Synchronization**' select '**Parameters**' tab and provide the below script under '**OverrideVariables**'.

```
If not String.IsNullOrEmpty(values("OverrideVariables").ToString()) then
Imports System.Data.Common
Dim sb as DbConnectionStringBuilder = new DbConnectionStringBuilder(false)
For each varName as String in values("OverrideVariables").ToString
().Split(";"c)
sb.Add(varName, values(varName).ToString())
```

```
Next
Value = sb.ConnectionString
End if
```

3. '**Commit to database**' and then '**Compile database**'.

Modifying the synchronization project

1. Make sure that the local cache is turned off for the Synchronization project.

   NOTE: This is applicable for employees and DeltaSyncEmployees endpoint.

2. Select the SCIM synchronization project and select 'Variables' to add a new variable similar to 'dprRevisionDateEmployees' (the variable name should be **dprRevisionDate<*schema name*>**).
3. Create a new 'Schema Class' from the supported endpoints in the 'Target system'. For example: "Employees for Delta Sync".
4. On the Schema Class set the System Filter: meta.LastModified gt $dprRevisionDate<Schema name>$. Under 'Select Objects' tab, use 'meta_lastModified' as the attribute, '>' as the operator and $dprRevisionDate<Schema name>$ as the text field value.

   NOTE:

   To get the all the updates from DeltaSyncEmployee Endpoint, please follow the additional step

   - Create two new 'Schema Class' from Employee in the 'Target system'. For example:

     "Manual Update Employees for Delta Sync" & "Effective Update Employees for Delta Sync"

   - On the respective Schema Classes set the System Filter: meta.LastModified gt

     $dprRevisionDateDeltaSyncEmployees$ and manualUpdate eq 'true' for manualUpdate, meta.LastModified gt

     $dprRevisionDateDeltaSyncEmployees$ and manualUpdate eq 'false' for effective update.

     Under 'Select Objects' tab, use 'meta_lastModified' as the attribute, '>' as the operator and $dprRevisionDateDeltaSyncEmployees$ as the text field value.

5. As required, other supported attributes also can be added under filters.
6. Create a new Mapping using the new Schema Class dialog box.
7. Create a new Workflow using the new mapping. This workflow updates the existing records based on the revision filter.
8. To improve the syncs performance, remove the update steps from the existing default Initial sync Work Flow.

9. Create a new Startup Config using the new workflow. Select 'One Identity Manager' for the 'Synchronization in direction'. Use 'default variable set' for the 'Variable Set'.
10. Use hotfix #33601 on One Identity Manager version 8.1.2 and 8.1.4.

Connector limitations

- It supports **GET** operation.
- Currently, **Update** functionality is available only for the following attributes of the **Employees** object:
  - Work phone and mobile numbers
  - email
  - username
  - SAMAccount ID (Custom ID for SAMAccount Name)

    NOTE: Update of phone information supports work and home based on the attribute being updated, phoneNumbersWork and phoneNumbers respectively until v2.0 and only work phone and mobile numbers are updatable in from v3.0 onwards.
- **CREATE** and **DELETE** operations are not supported by any object.
- Any changes to the *updatable employee* attributes for contact information listed above will be performed effective immediately (EffectiveDate = today). Updates will only be successful if no future dated event is pending, that may conflict with the attribute update.
- There is no **meta.LastModified** attribute available for **Employees** and **Location** endpoint. Delta sync could be performed by following the steps in One IM Configuration for Delta Synchronization.
- When using futurehire filter, delta sync cannot be used as it will affect the future hire results returned from WorkdayHR API.
- The target system WorkdayHR API supports:-
  - OR operation only within the same filter type.
  - AND operation only across different filter type.

  For example, costCenter and region belongs to Organization type. WorkdayHR API will perform OR operation and return employees that belong to either of the Organization. Conversely, in case of costCenter and country, WorkdayHR will perform AND operation and return employees that belong to Costcenter and Country.

  NOTE: The Get Employee endpoint fetches the primary work email, primary cellphone and landline for home and work. The Update Employee endpoint sets the default value for email to type work and public to false, when the values for type and public flag are not provided. IsPrimary is always set to true (until version 2.0).

- Due to impact in the performance, the below listed attributes are not returned in the LIST response of Employees and FutureDatedEmployees (in v3.2). These attributes are available in GET by Id response.
    - departmentReferenceId
    - divisionReferenceId
    - deskReferenceId
    - costCenterReferenceId
    - companyReferenceId
    - regionReferenceId
    - personalAssistantReferenceId
    - assetClassReferenceId
    - departmentHeadReferenceId
    - costCenterHierarchyReferenceId
    - matrixReferenceId
    - customOrgReferences[].OrgReferenceID

Connector versions and features

The following subsections describe the different connector version(s) and features available with them.

Features available exclusively in Workday HR v.2.0

Following are the features that are available exclusively in **Workday HRv.2.0**:

- The Employee endpoint is enhanced to support the **PATCH** operation to update the Employee details.

  NOTE:The supported attributes for Employee **PATCH** operation will be same as the **UPDATE**.

- The Employee endpoint is enhanced to support the **DELETE** functionality for following attributes:
    - SamAccountName
    - Email
    - PhoneNumbers

> NOTE: Set the supported attributes value to blank in One Identity Manager to delete them from target system.

Features available exclusively in Workday HR v.3.0

Following are the features that are available exclusively in **Workday HRv.3.0**:

- The Employee endpoint is enhanced to support non primary work phone numbers.
- The Create, Update and Delete operations are supported for non primary work phone numbers along with other previously supported attributes.

  > NOTE: Please check the section Values for customer-specific configuration parameters for more details.

Features available exclusively in Workday HR v.3.1

- This version does not support PATCH for modifying the resources, instead supports PUT for updating.

  > NOTE: The supported attributes for updating an Employee are userName, emails and samAccountName.

Features available exclusively in Workday HR v.3.2

- This version supports updating work phone numbers of employees. Schema properties related to employee phone numbers have been modified.
- New attributes added:
  - workPhoneMobilePrimary
  - pronounID
  - jobCategoryID
  - supplierReferenceID
  - jobExempt
  - supervisorManagementChainData~organizationReferenceId
  - supervisorManagementChainData~managerId

    - supervisorManagementChainData~managerDescriptor
    - departmentReferenceId
    - divisionReferenceId
    - deskReferenceId
    - costCenterReferenceId
    - companyReferenceId
    - regionReferenceId
    - personalAssistantReferenceId
    - assetClassReferenceId
    - departmentHeadReferenceId
    - costCenterHierarchyReferenceId
    - matrixReferenceId
    - customOrgReferences[].OrgReferenceID (Not available in LIST response)
- Attributes removed:
    - phoneNumbers
    - phoneNumbersWork
- This version supports updating work phone numbers of employees following PUT. Schemas related to phone numbers have been modified and couple of schema attributes available in lower version have been removed in this version. The obsolete schema attributes are phoneNumbers and phoneNumbersWork (including sub attributes).

> NOTE:
>
> - The schema attributes phoneNumbers, phoneNumbers~businessPhone, phoneNumbers~cellPhone, phoneNumbers~isBusinessPhonePublic, phoneNumbers~countryPhoneISOCode, phoneNumbers~internationalPhoneCode, phoneNumbers~isCellPhonePublic, phoneNumbers~type are deprecated and will not return data any longer.
> - These attributes are still available in schemas to gracefully allow the creation of synchronization project in Identity Manager using the Workday HR template.
> - These attributes will be removed when updating the Synchronization Templates.

48

OneLogin

The OneLogin connector allows you to connect OneLogin with One Identity Starling enabling you to take advantage of the features and products available with Starling Connect that complement and enhance the services provided by OneLogin.

OneLogin is a Unified Access Management (UAM) platform that provides several products and solutions, such as single sign-on, user provisioning and management and multi-factor authentication to manage identities.

OneLogin connectors are available for use with One Identity Safeguard for Privileged Passwords.

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.)
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details)
- Request Delay (in ms)

> NOTE: To handle the OneLogin rate limit issue, the OneLogin connector has been enabled with user configurable delay in milliseconds so that the each request to the target API would wait for the specific amount of time to help the connector to prevent the throttling of the OneLogin APIs. The default value for the configuration is 500(milliseconds) and OneIdentity recommends to keep the value below 2000 (milliseconds).

Supported objects and operations

Users

Table 270: Supported operations for Users

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

Groups

Table 271: Supported operations for Groups

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

Roles

Table 272: Supported operations for Roles

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

Application

Table 273: Supported operations for Application

Operation	VERB
Get an App	GET
List Apps	GET
List Apps with pagination	GET

Mandatory fields

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

Users - Create (in v.1.0)

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

Users - Create (in v.2.0)

- userName
- emails.value

Users - Update

userName or emails.value

Roles - Update

roleName

Set Role Apps - update

application id

Mappings

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

Table 274: 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
Locale	locale_code(in v1),preferred_locale_code (in v2)
Password (only in v2.0)	password
Extension.Manager.Value	manager_user_id
Extension.Organization	company
Extension.Department	department
Extension.OpenIdName	openid_name
Extension.DistinguishedName	distinguished_name
Extension.SamAccountName	samaccountname

SCIM Parameter	OneLogin parameter
Extension.UserPrincipalName	userprincipalname
Extension.MemberOf	member_of
Extension.DirectoryId	directory_id
Extension.UserStatus	status
Extension.LastLogin	last_login
Meta.Created	created_at
Meta.LastModified	updated_at

Groups

Table 275: Group mapping

SCIM parameter	OneLogin parameter
Id	id
DisplayName	name

Roles

Table 276: Role mapping

SCIM parameter	OneLogin parameter
Id	id
Name	name
Applications[].value	apps[].id
Applications[].name	apps[].name
users[].value	users[].id
users[].name	users[].name

Application

Table 277: Role mapping

SCIM parameter	OneLogin parameter
Id	id
Name	name
Description	description
Auth_Method	auth_method
Visible	visible
Meta.Created	created_at
Meta.LastModified	updated_at

NOTE: OneLogin API for Users accepts two letter values for locale, for example: "en", "es" and so on.

Connector SCIM configuration

You can configure custom attributes for the OneLogin SCIM connector in Starling Connect for Users in the Custom Attributes section in Schema Configuration.

NOTE:

- For more information about how to configure custom attributes in OneLogin, see Configuring custom attributes in connectors.
- As the OneLogin target system does not support disabling of attributes, the OneLogin connector is enhanced only to support the configuration of custom attributes in the SCIM connector.
- The target supports only simple attributes that are grouped under the object custom_attributes in the target API response. Hence, the connector supports only simple custom attributes.

Connector limitations

- Target cloud application supports below given integer value for Status field. OneIdentity has created 'userStatus' integer type attribute in User extension schema and mapped with 'status' and it needs to be taken care in OneIM mapping:

- (in v.1.0):
    - Can set through Api → Unactivated: 0, Active: 1, Suspended: 2, Locked: 3, Password expired: 4
    - Cannot set through Api → Awaiting password reset: 5, Pending password: 7, Security questions required: 8
- (in v.2.0):
    - Can set through Api → Unactivated: 0, Active: 1, Suspended: 2, Locked: 3, Password expired: 4, Awaiting password reset: 5, Pending password: 7
    - Cannot set through Api → Security questions required: 8

- Adding or removing a Group can be achieved by using the **User update** operation. Only one group can be assigned to a User.
- For the User object, when NULL value is updated to **openid_name**, the cloud application considers the first part of the email Id as **openid_name**. For example, for the email id, **email123@test.com** , **openIdname** value will be **email123**.
- API does not support the assignment of applications under users what it support is assigning application under roles and assigning roles under user.
- In pagination, records are returned in multiples of 50 only.

Connector versions and features

The following subsections describe the different connector version(s) and features available with them.

Features available exclusively in OneLogin v.2.0

Following are the features that are available exclusively in **OneLogin v.2.0**:

- Creation and updation of user password.
- v.2.0 of OneLogin connector leverages v2 APIs of target system.
- Support for filter condition
    - The filter is supported in Users, Roles and Applications.
    - The filter supported is eq.
    - For attributes meta.Created, meta.LastModified and lastLogin the filter supported is ge,le,gt and lt, but in lt and gt the response will be similar to ge and le.

    - The AND logical operator is supported in the target system.
    - The OR logical operator neither returns any data nor returns any error message.
    - In some cases of roles endpoint, the partial match of data is also working.
- List of attributes supported for filter condition.

Table 278: List of attributes supported for filter condition

Users	Applications	Roles
userName, emails.Value, givenName, familyName, directoryId, externalId, meta.LastModified, meta.Created, lastLogin, CustomAttributes	name	name
	auth_method	applications.Value
		applications.name

OneLogin connector for Safeguard for Privileged Passwords

When creating a OneLogin connector for use with Safeguard for Privileged Passwords, you need to use the following OneLogin API credentials configuration:

- Client Id
- Client secret
- SCIM URL (The base URL of the REST API of the Cloud application.)
- Manage All type of client id/secret must be selected.

In addition, the default URL needs to be changed in order to support check/change/discover (for example, <domain>.onelogin.com).

For more information, see https://developers.onelogin.com/api-docs/1/getting-started/working-with-api-credentials.

User centric membership configuration for OneLogin

For more information, see only the following sections in User centric membership:

- Creating a new schema class using Synchronization Editor
- Configuring User centric membership for Groups
- Creating a new column in UCIUser table and CSMUser table using Extension Tool
- Creating custom process using Designer

49

PingOne

The PingOne connector allows you to connect PingOne with One Identity Starling enabling you to take advantage of the features and products available with Starling Connect that complement and enhance the services provided by PingOne.

PingOne is a hybrid Identity-as-a-Service (IDaaS) based product that allows users to use single sign-on across different applications.

Supervisor configuration parameters

To configure the connector, following parameters are required:

- Connector name
- Client Id
- API Key
- Target URL (based on the region)

Supported objects and operations

Users

Table 279: Supported operations for Users

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

Groups

Table 280: Supported operations for Groups

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

Mandatory fields

Users

- email[].value
- userName

Groups

displayName

User and Group mapping

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

Table 281: User mapping

SCIM Parameter	PingOne Parameter
id	id
userName	userName
externalId	externalId
name.givenName	name.givenName
name.familyName	name.familyName
name.middleName	name.middleName

SCIM Parameter	PingOne Parameter
name.formatted	name.formatted
name.honorificPrefix	name.honorificPrefix
name.honorificSuffix	name.honorificSuffix
displayName	displayName
nickName	nickName
email.value	email.value
email.type	email.type
email.primary	email.primary
addresses.formatted	addresses.formatted
addresses.streetAddress	addresses.streetAddress
addresses.locality	addresses.locality
addresses.region	addresses.region
addresses.postalCode	addresses.postalCode
addresses.country	addresses.country
addresses.type	addresses.type
phoneNumbers.value	phoneNumbers.value
phoneNumbers.type	phoneNumbers.type
password	password
profileUrl	profileUrl
title	title
userType	userType
preferredLanguage	preferredLanguage
locale	locale
timeZone	timeZone
active	active
entitlements.value	entitlements.value
roles.value	roles.value
ims.value	ims.value
ims.type	ims.type

SCIM Parameter	PingOne Parameter
groups.value	groups.value
groups.display	groups.display
x509Certificates.value	x509Certificates.value
extension.accountId	extension.accountId
extension.directoryId	extension.directoryId
extension.state	extension.state
extension.passwordExpired	extension.passwordExpired
meta.created	meta.created
meta.lastModified	meta.lastModified

Groups

Table 282: Group mapping

SCIM parameter	PingOne parameter
id	id
displayName	displayName
members.value	members.value
members.display	members.display
members.type	members.type
extension.accountId	extension.accountId
extension.directoryId	extension.directoryId
meta.created	meta.created
meta.lastModified	meta.lastModified

Connector limitations

- PingOne supports addresses of type **home**, **work**, and **other**. Similarly, it supports phone numbers of types **work**, **mobile**, **home**, **fax**, **pager**, and **other**. However the connector supports only one type of address and phone number.
  The connector first looks for type **work**. If type **work** is not found, the connector looks for type **home**.
  Else, it looks for the address and phone number of any type. If **type** value is not present, then the connector assigns the value of **work** to **type**.

50

Aha!

The Aha! connector allows you to connect Aha! with One Identity Starling enabling you to take advantage of the features and products available with Starling Connect that complement and enhance the services provided by Aha!

Aha! is a product management software that enables software companies to collaborate across cross functional teams.

Supervisor configuration parameters

To configure the connector, following parameters are required:

- Connector name
- Api Key
- Target URI
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details).

Supported objects and operations

Users

Table 283: Supported operations for Users

Operation	VERB
Create User	POST
Update User	PUT

Operation	VERB
Delete User (soft delete)	DELETE
Get User	GET
Get All users	GET
Get All Users with Pagination	GET

Roles

Table 284: Supported operations for Roles

Operation	VERB
Get Role by Id	GET
Get all Roles	GET

Products

Table 285: Supported operations for Products

Operation	VERB
Get Product by Id	GET
Get all Products	GET
GET All Products with Pagination	GET

Mandatory fields

Users

- Name.GivenName
- Name.FamilyName
- EmailAddress
- role
- product_id

Groups

Not Applicable

Mappings

Table 286: User mapping

SCIM Parameter	Aha parameter
Id	id
UserName	email
DisplayName	name
emails[].value	email
Active	enabled
name.givenName	first_name (not returned, only writable)
name.familyName	last_name (not returned, only writable)
Extension.productRoles[].role	product_roles[].role
Extension.productRoles[].productId	product_roles[].product_id
Extension.productRoles[].productName	product_roles[].product_name
Meta.Created	created_at
Meta.LastModified	updated_at

Roles

Table 287: Roles mapping

SCIM parameter	Aha parameter
id	id
name	name

Products

Table 288: Products mapping

SCIM parameter	Aha parameter
id	id
name	name
referencePrefix	reference_prefix
productLine	product_line
productLineType	product_line_type
url	url
resource	resource
children[].id	children[].id
children[].referencePrefix	children[].reference_prefix
children[].name	children[].name
children[].productLine	children[].product_line
capacityPlanningEnabled	capacity_planning_enabled
defaultCapacityUnits	default_capacity_units
Meta.Created	created_at
Meta.LastModified	updated_at

Connector limitations

1. Aha accepts **Role** and **Product** assignment of **Users** in a combined form and they cannot be assigned separately.
2. Aha accepts an invalid target URL and returns the results when the API key provided is valid. Due to this behavior, the Test Connection on Starling Connect UI will be successful even without a valid target URI.
3. **Teams** and **Groups** are not supported because Aha does not provide APIs to create or manage them.
4. Connector supports cursor pagination for the object types **Users** and **Products**. It does not support cursor pagination for the **Roles** object type. However, the records returned are in multiples of 100. For example, if 255 records are requested, connector returns 300 records (next nearest multiple of 100s of the count).

5. Aha supports only soft delete of **Users**. **Users** are set to **inactive** when the **Delete** operation is performed. The same **User** can be reactivated by passing active flag set to **True**. However, the deleted **User** can be retrieved in the list of **Users** as well as individually, irrespective of the status.
6. No error is returned when a nonexistent **Role** is specified in the **Create** and **Update** request. However, the operation would be completed with a default **Role** assigned to the **User**.
7. Invalid Product ID specified in **User Create** and **User Update** request would return Error 404 with message 'Not Found'.

Synchronization and integration of Roles object type with One Identity Manager

For more information, see Synchronization and integration of Roles object type with One Identity Manager.

Synchronization and integration of Products object type with One Identity Manager

For more information, see Synchronization and integration of Products object type with One Identity Manager.

Add Roles ID and Product ID to create and update users for Aha connector

To create a user successfully using Aha connector, you must provide valid values for mandatory properties such as **Roles** and **Products ID** in the request. **Roles** and **Products ID** are the sub-attributes of the main attribute **ProductRoles**, which is a complex multi-valued string attribute defined under User extensions in the connector schema.

One Identity Manager must have fields where you can enter complex multi-value array values but it does not display such fields by default. However, it is possible to create

custom multi-value array fields. For more information, see Creating multi-valued custom fields in One Identity Manager.

> NOTE: The above example of creating multi-valued custom fields is one of the various ways to achieve the configuration required for adding **Roles** and **Products ID** to create and update Users. There may be other ways to achieve this integration based on the customization options that One Identity Manager provides.

51

SAP Litmos

The SAP Litmos connector allows you to connect SAP Litmos with One Identity Starling enabling you to take advantage of the features and products available with Starling Connect that complement and enhance the services provided by SAP Litmos.

SAP Litmos is an online learning platform that caters to the training requirements of an organization, capable of providing continuous and targeted training for all business segments.

Supervisor configuration parameters

To configure the connector, following parameters are required:

- Connector name
- Api Key
- Target URI
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details).

Supported objects and operations

Users

Table 289: Supported operations for Users

Operation	VERB
Create User	POST
Update User	PUT

Operation	VERB
Get User by Id	GET
Get All users with pagination	GET
Delete User	DELETE

Groups

Table 290: Supported operations for Groups

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

Mandatory fields

Users

- Name.GivenName
- Name.FamilyName
- UserName

Groups

DisplayName

User and Group mapping

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

Table 291: User mapping

SCIM Parameter	SAP Litmos parameter
Id	id
UserName	UserName
DisplayName	FirstName + LastName
Name.GivenName	FirstName
Name.FamilyName	LastName
Name.Formatted	FullName
Emails.Value	Email
Active	Active
Groups[].value	(UserGroupsResponse) Id
Groups[].display	(UserGroupsResponse) Name
Addresses[].streetAddress	Street1
Addresses[].region	City
Addresses[].locality	State
Addresses[].postalCode	PostalCode
Addresses[].country	Country
PhoneNumbers[].value (work)	PhoneWork
PhoneNumbers[].value (mobile)	PhoneMobile
Timezone	Timezone
Title	JobTitle
Locale	Culture
userExtension.AccessLevel	AccessLevel
userExtension.OriginalId	OriginalId
userExtension.CompanyName	CompanyName
userExtension.Manager.value	ManagerId
userExtension.Manager.displayName	ManagerName
Meta.Created	CreatedDate
Password	Password

Groups

Table 292: Groups mapping

SCIM parameter	SAP Litmos parameter
Id	Id
displayName	Name
members[].value	(groupMembersResponse) Id
members[].display	(groupMembersResponse) UserName
groupExtension.Description	Description
groupExtension.ParentTeamId	ParentTeamId

Connector limitations

- There is a difference in the way the legacy and non legacy custom attributes of the **User** object are supported in the connector.
  - Legacy custom attributes are supported as part of core custom user schema attributes

    (*urn:starling:custom:urn:ietf:params:scim:schemas:core:2.0:User*)
  - Non legacy custom attributes are supported as part of custom user extension schema attributes

    (*urn:starling:custom:urn:ietf:params:scim:schemas:extension:enterprise:2.0:User*)
- The user name provided while performing the **Create User** operation will be considered for both the username and email at the target system side .
- **AddGroupMembers** with an invalid userid does not display any exception.
- Multiple groups with the same display name can be created.
- While configuring custom attributes of a core user in Starling Connect, all the custom attributes must be of type string. However, user extension custom attributes can be of one among the supported data types - integer, string, decimal and DateTime.
- Parent Group id cannot be un-assigned from a group.
- A group can be created with or without a parent group.
- **Created date** and **last modified date** are not returned by the cloud application for both **Users** and **Groups**.
- When a user is created or updated with a password through the connector, the user is prompted to change the password in next login to the target application.

- An attempt to update a **User** that has been deleted, the target application will return error 500: *The server encountered an error processing the request. Please see the server logs for more details*.

52

HackerRank

The HackerRank connector allows you to connect HackerRank with One Identity Starling enabling you to take advantage of the features and products available with Starling Connect that complement and enhance the services provided by HackerRank .

HackerRank provides remote hiring solutions for companies, interview preparation solutions for developers, and also provides a platform to bring the two together.

Supervisor configuration parameters

To configure the connector, following parameters are required:

- Connector name
- API Key
- Target URL
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details).

Supported objects and operations

Users

Table 293: Supported operations for Users

Operation	VERB
Create User	POST
Get User	GET

Operation	VERB
Update User	PUT
Delete User	DELETE

Groups

Table 294: Supported operations for Groups

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

Roles

Table 295: Supported operations for Groups

Operation	VERB
Get roles	GET
Get role by id	GET

Mandatory fields

Users

- email {SCIM - emails[].value}
- firstname {SCIM - name.givenName}
- role {SCIM - roles[].value}
- teams.id {SCIM - extension.groupIds}

Groups

name {SCIM - displayName}

User and Group mapping

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

Users

Table 296: User mapping

SCIM Parameter	HackerRank parameter
id	id
email	userName
firstname	name.givenName
lastname	name.familyName
firstname + " " + lastname	name.formatted
firstname + " " + lastname	displayName
email	emails[].value
country	addresses[].country
phone	phoneNumbers[].value
timezone	timezone
status	active
role	roles[].value
teams[]	groups[].value (Only for read operation)
questions_permission	extension.questionsPermission
tests_permission	extension.candidatesPermission
interviews_permission	extension.interviewsPermission
candidates_permission	extension.candidatesPermission
shared_questions_permission	extension.sharedQuestionsPermission

SCIM Parameter	HackerRank parameter
shared_tests_permission	extension.sharedTestsPermission
shared_interviews_permission	extension.sharedInterviewsPermission
company_admin	extension.companyAdmin
team_admin	extension.teamAdmin
activated	extension.userEmailActivated
send_email	extension.sendEmail
teams[].id	extension.groupIds (Only for write operation)
created_at	meta.created
last_activity_time	meta.lastModified

Groups

Table 297: Group mapping

SCIM parameter	HackerRank parameter
id	id
name	displayName
members[].value	TeamMembers[].user
invite_as	extension.inviteAs
recruiter_cap	extension.recruiterCap
developer_cap	extension.developerCap
interviewer_cap	extension.interviewerCap
recruiter_count	extension.recruiterCount
developer_count	extension.developerCount
interviewer_count	extension.interviewerCount
owner	extension.owner
locations	extension.locations
departments	extension.departments
meta.created	meta.created

Connector limitations

- The connector supports the HackerRank REST APIs v3 only.

53

Slack

The Slack connector allows you to connect Slack with One Identity Starling enabling you to take advantage of the features and products available with Starling Connect that complement and enhance the services provided by Slack.

Slack is a cloud-based platform, where users can create and maintain multiple dedicated and organized spaces to allow team members to effectively communicate with each other in a seamless manner.

Connector Configuration

Slack connector requires customer consent to retrieve resource details using REST APIs. Currently, the Slack connector supports the configuration of a single tenant connector only.

NOTE:

- To provide consent, use an account with administrative privileges.
- For more information, see
  - Creating an app for using SCIM on Slack Enterprise Grid Organization
  - Configuring a connector that uses the consent feature.

Supervisor configuration parameters

To configure the connector, following parameters are required:

- Connector name
- Client Id for the app
- Client Secret of the app
- Target URL (Cloud application's instance URL used as target URI in payload - Example: https://api.slack.com/scim/v1/)

- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details).

Supported objects and operations

Users

Table 298: Supported operations for Users

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

Groups

Table 299: Supported operations for Groups

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

Mandatory fields

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

User

- userName
- emails.value

Group

- displayName

User and Group mapping

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

Table 300: User mapping

SCIM Parameter	Slack parameter
id	id
userName	userName
name.givenName	name.givenName
name.familyName	name.familyName
name.honorificPrefix	name.honorificPrefix
displayName	displayName
nickName	nickName
emails[].value	emails[].value
emails[].primary	emails[].primary
addresses[].streetAddress	addresses[].streetAddress
addresses[].locality	addresses[].locality
addresses[].region	addresses[].region
addresses[].postalCode	addresses[].postalCode
addresses[].country	addresses[].country
phoneNumbers[].value	phoneNumbers[].value
phoneNumbers[].type	phoneNumbers[].type

SCIM Parameter	Slack parameter
phoneNumbers[].primary	phoneNumbers[].primary
profileUrl	profileUrl
title	title
userType	userType
password	password (Write-only and never returned)
preferredLanguage	preferredLanguage
locale	locale
timezone	timezone
active	active
groups[].value	groups[].value
groups[].display	groups[].display
roles[].value	roles[].value
roles[].primary	roles[].primary
photos[].value	photos[].value
photos[].type	photos[].type
extension.costCenter	extension.costCenter
extension.department	extension.department
extension.division	extension.division
extension.employeeNumber	extension.employeeNumber
extension.organization	extension.organization
extension.manager.managerId	extension.manager.value
meta.created	meta.created

Groups

Table 301: Groups mapping

SCIM parameter	Slack parameter
id	id
displayName	displayName
members[].value	members[].value

SCIM parameter	Slack parameter
members[].display	members[].display
meta.created	meta.created

Connector limitations

- **Create User** operation can create only **Active** users in the target application. **Update User** operation can be used to make the user **Inactive**.
- You cannot create a new user or update the name of an existing user using the name of an existing user or channel.
- The **email id** provided in the **user name** field during the **User Create** operation will automatically be converted to a **user name** according to the target application standard.
- There is no endpoint available for **Roles** and any string value can be assigned as a **Role** of a **User**. However, the number of strings that can be assigned as a **Role** of a **User** has been limited to maximum one.
- **Last Modified Date** is not returned in meta of **Users** and **Groups**.
- Target system supports only soft delete of users. **Users** deleted using soft delete will still be accessible to read, update and delete.
- **Error 429** occurs when the requests from a SCIM client exceed the **SCIM API rate limit** of the Slack target application.
- The special characters used in **userName** are converted to underscore in **Create User** and **Update User** operations.
- **User Name** is replaced by the **Nick Name** when it is passed in a **Create User** and **Update User** request.

54

ActiveCampaign

The ActiveCampaign connector allows you to connect ActiveCampaign with One Identity Starling enabling you to take advantage of the features and products available with Starling Connect that complement and enhance ActiveCampaign's wide range of marketing services and solutions.

Supervisor configuration parameters

To configure the connector, following parameters are required:

- Connector name
- Api Key
- Target URI
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details)

Supported objects and operations

Users

Table 302: Supported operations for Users

Operation	VERB
Create User	POST
Update User	PUT
Delete User	DELETE

Operation	VERB
Get User	GET
Get All users	GET

Groups

Table 303: Supported operations for Groups

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

Mandatory fields

This section lists the mandatory fields required to create Users and Groups.

Users

- Name.GivenName
- Name.FamilyName
- Email
- Username
- password
- GroupId

Groups

DisplayName

User and Group mapping

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

Users

Table 304: User mapping

SCIM parameter	ActiveCampaign parameter
Id	id
UserName	username
DisplayName	firstName+ lastName
Name.GivenName	firstName
Name.FamilyName	lastName
Emails.Value	email
Groups[].value (readOnly)	groupid
PhoneNumbers[].value	phone
Meta.Created	cdate
Meta.LastModified	udate
Password	Password
userExtension.groupId (WriteOnly)	groupid

Table 305: Group mapping

SCIM Parameter	ActiveCampaign parameter
Id	Id
displayName	title
members[].value	(groupMembersResponse) userid
groupExtension.Description	Descript

Connector limitations

- **GroupId** is a **writeOnly** mandatory extension property while creating or updating a **User**.
- **Membership** operations are not implemented due to the unavailability of APIs.
- The **Groups** property in the schema of the **User** is an on-demand attribute, which will not be fetched during the operation **GET User by Id** unless the request has an attribute for groups.

55

Webex

The **Webex** connector allows you to connect Webex with One Identity Starling enabling you to take advantage of the features and products available with Starling Connect that complement and enhance Webex's real-time video conferencing and communication services. With features such as file sharing, screen sharing, the Webex application enables teams to collaborate without interruption over any device such as mac, PC, or mobile.

Connector configuration

Webex connector requires customer consent to retrieve resource details using REST APIs. Currently, the Webex connector supports the configuration of a single tenant connector only.

NOTE:

- To provide consent, use an account with administrative privileges.
- For more information, see
  - Creating a Webex integration application, providing necessary scopes, retrieving Client Id and Client Secret
  - Configuring a connector that uses the consent feature

Supervisor configuration parameters

To configure the connector, following parameters are required:

- Connector name
- Client Id for the integration app
- Client Secret of the integration app
- Target URL (Cloud application's instance URL used as target URI in payload. The value needs to be *https://webexapis.com/v1*)

- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details).

Supported objects and operations

Users

Table 306: Supported operations for Users

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

Groups

Table 307: Supported operations for Groups

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

Roles

Table 308: Supported operations for Roles

Operation	Operation
Get Role	GET
Get Roles	GET

Profiles

Table 309: Supported operations for Profiles

Operation	Operation
Get Profile	GET
Get Profiles	GET

Mandatory fields

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

Users

- emails.value
- displayName

Groups

displayName

User and Group mapping

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

Table 310: User mapping

SCIM Parameter	Webex parameter
id	id
userName	emails[0]
name.familyName	lastName
name.givenName	firstName

SCIM Parameter	Webex parameter
name.formatted	firstName lastName
displayName	displayName
nickName	nickName
emails[0].value	emails[0]
timezone	timezone
active	loginEnabled
userType	type
roles[].value	roles[]
entitlements[].value	licenses[]
photos[].value	avatar
userExtension.organization	orgId
userExtension.status	status
meta.created	created
meta.lastModified	lastModified

Groups

Table 311: Groups mapping

SCIM Parameter	Webex parameter
id	id
displayName	name
members[].value	members[].personId
members[].display	members[].personDisplayName
meta.created	created

Connector limitations

- If the wrong cursor is passed in the request, the cloud instance does not validate it as an error. Hence the SCIM response will contain only the schema URN and the

previous cursor.

- Sometimes, even though the wrong cursor is passed in the request, the cloud instance returns the resources.
- Webex User creation requires you to pass either of one of the following attributes as a mandatory attribute
    - displayName
    - givenName
    - familyName

      NOTE: The attribute **displayName** is considered as a mandatory attribute for user creation in the connector.
- Multiple groups with the same name can be created due to target system behavior.
- The last moderator of a group can leave the group or can be unassigned from the group only if there are no members in the group. This happens due to target system behavior.
- When you update a group, removing the last member of the group removes the entire group due to target system behavior. In this scenario, the WebEx connector returns error 404 as the update operation internally is carried out internally as
    a. update group name
    b. manage members
    c. retrieve updated group details
- When a group member, who is a moderator of the group and whose credentials are used while providing consent for the Webex integration app, gets removed from the Webex connector group update operations or has been assigned as a normal member but not a moderator through the Webex Teams User Interface, then the Webex connector fails to update the group due to insufficient privileges on that particular the group.
- Deleting or updating a deleted user results in error 403 due to target system behavior.

56

Apigee

The **Apigee** connector allows you to connect Apigee with One Identity Starling enabling you to take advantage of the features and products available with Starling Connect that complement and enhance Apigee's platform that allows you to design, secure, analyze, scale, publish, monitor, and manage the APIs.

Supervisor configuration parameters

To configure the connector, following parameters are required:

- Connector name
- UserName
- Password
- Organization
- Target URL (Cloud application's instance URL used as target URI in payload)

Supported objects and operations

Users

Table 312: 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

Roles

Table 313: Supported operations for Roles

Operation	Operation
Get Role by id	GET
Get All Roles	GET

Mandatory fields

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

Users

- Name.GivenName
- Name.FamilyName
- Emails.Value
- Password

User and Group mapping

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

Table 314: User mapping

SCIM Parameter	Apigee parameter
id	emailId
userName	emailId

SCIM Parameter	Apigee parameter
DisplayName	firstName+lastName
Name.GivenName	firstName
Name.FamilyName	lastName
Emails.Value	emailId
Roles[].value	(userRolesResponse)role[].name
Password	Password

Role

Table 315: Role mapping

SCIM Parameter	Apigee parameter
id	name
name	name

Connector limitations

- At least one role must be assigned to the created user. If the role is not assigned to the user, the particular user is not visible on the User management dashboard of the target instance due to the limitation of the target system.
- **Get All Users** does not return the **displayName** as it is not available in the target system. However, **Get User by ID** returns the display name with the other available attributes of the User.
- Create User operation fails intermittently and an Internal Server Error 500 is displayed due to the Target system API behavior.
- The **Get All** and **Create User** operations may occasionally take more time to respond for requests.
- Apigee Connector does not support pagination for **Users** and **Roles** object types due to API limitation in the target system.
- The connector does not support special characters in the object ID. For more information, see Connectors that do not support special characters in the object ID.

Synchronization and integration of Roles object type with One Identity Manager

For more information, see Synchronization and integration of Roles object type with One Identity Manager.

57

Databricks

The **Databricks** connector allows you to connect Databricks with One Identity Starling enabling you to take advantage of the features and products available with Starling Connect that complement and enhance Databricks' unified platform for data and Artificial Intelligence (AI). Databricks provides services that allow you to migrate complex and expensive on-premises data systems to cloud data platforms.

Supervisor configuration parameters

To configure the connector, following parameters are required:

- Connector name
- Access Token
- Target URL (Format:- https://databricks_instance/api/2.0/preview/scim/v2)

Supported objects and operations

Users

Table 316: Supported operations for Users

Operation	VERB
Create User	POST
Get User	GET
List Users	GET
Update User	PUT
Delete User	DELETE

Groups

Table 317: Supported operations for Groups

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

Mandatory fields

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

Users

- userName

Groups

- displayName

User and Group mapping

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

Table 318: User mapping

SCIM Parameter	Databricks parameter
id	id
userName	userName
name.familyName	name.familyName

SCIM Parameter	Databricks parameter
name.givenName	name.givenName
displayName	displayName
emails[0].value	emails[0].value
emails[0].type	emails[0].type
emails[0].primary	emails[0].primary
active	active
groups[].value	groups[].value
groups[].display	groups[].display
entitlements[].value	entitlements[].value

Group

Table 319: Group mapping

SCIM Parameter	Databricks parameter
id	id
displayName	displayName
members[].value	members[].value
members[].display	members[].display
extension.parentGroups[].value	groups[].value
extension.parentGroups[].display	groups[].display
extension.entitlements[].value	entitlements[].value

Connector limitations

- If User's **displayName** attribute is present in the request, then the **name** attributes are not considered. If **displayName** is not provided, the values from the **name** attributes would be considered.
- The connector doesn't implement roles for **Users**. **Roles** endpoints are not supported at target system and the user can not be assigned with random text to the roles.
- The connector does not implement modifying the entitlements for Users or Groups. Entitlements endpoints are not supported at target system. The **User** or **Group** can

not be assigned with random text to the entitlements.

- **Create User** operation can create only **Active** users in the target application. However, **Update User** operation can be used to make the user **InActive**.
- When a user create operation is tried with **userName** of a deleted user, the target system re-activates the deleted user and returns the details of that deleted user (with any updated values for attributes from the create request) instead of creating a new user with new user id.
- The Databricks REST API supports a maximum of 30 requests per second per workspace. A 429 response status code is displayed if the requests exceed the rate limit.
- A Databricks admin user whose Personal Access Token is used to authorize the target endpoints and who is managed by the Identity Provider (IdP) can be deprovisioned using the IdP, which may cause the SCIM provisioning integration to be disabled.
- No meta information is retrieved for users and groups.
- Target system follows soft delete of resources. Inactivating a user by updating 'active' to 'false' soft-deletes the user and that user cannot be retrieved.
- Group's members will not contain 'type' attribute with values 'User' / 'Group' as the target system does not return the type of the members. Groups in target system can have users and groups as members.
- Delete group request with invalid id returns 204 because of the target API behavior. The target API returns success when a deleted group is tried deleting again.
- List users and list groups APIs are relatively slow. Hence used very minimal set of attributes in the query attributes on these endpoint.

58

Hive

The Hive connector allows you to connect Hive with One Identity Starling enabling you to take advantage of the features and products available with Starling Connect that complement and enhance Hive's services as a collaborative tool used for project planning.

Supervisor configuration parameters

To configure the connector, following parameters are required:

- Connector name
- Workspace Id
- API Key
- User Id
- Target URL (Cloud application's instance URL used as target URI in payload)

Supported objects and operations

Users

Table 320: Supported operations for Users

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

Groups

Table 321: Supported operations for Groups

Operation	VERB
GET Group by Id	GET
Get All Groups	GET

Mandatory fields

Users

- email

Groups

- Create Group is not supported by the target system.

User and Group mapping

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

Table 322: User mapping

SCIM Parameter	Hive parameter
Id	id
UserName	email
Name.GivenName	profile.firstname
Name.FamilyName	profile.lastname
Name.Formatted	fullname
DisplayName	fullname
Emails[0].value	email

Groups

Table 323: Groups mapping

SCIM parameter	Hive parameter
Id	id
DisplayName	name
Members.value	members[]

Connector limitations

- Connector gets All the Groups and filters the group from the list for **GET Group By Id** operation since the target system does not have an API to support **Get Group by Id**.
- **Update User** operation supports only to update **GivenName** and **FamilyName** due to target system limitation.
- Connector does not support the meta information **created** and **lastModified** as these are not supported by the target system.

59

PagerDuty

PagerDuty is an incident response platform solution for IT departments. It is the leading market based product of a SaaS specialized organization that allows its customers to have an effective real-time operations platform ensuring lesser downtime and fewer outages. It is generally used for incident response, on-call management, analytics and event intelligence .

The PagerDuty connector allows you to connect PagerDutywith One Identity Starling enabling you to take advantage of the features and products available with Starling Connect that complement and enhance PagerDuty's real-time operations platfrom services.

Supervisor configuration parameters

To configure the connector, following parameters are required:

- Connector name
- API Key
- Target URL (https://api.pagerduty.com)

Supported objects and operations

Users

Table 324: Supported operations for Users

Operation	VERB
Create User	POST
Get a user	GET

Operation	VERB
Get All Users	GET
Update a user	PUT
Delete a user	DELETE

Groups

Table 325: Supported operations for Groups

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

Mandatory fields

Users

- email.value
- name.displayName

Groups

- displayName

User and Group mapping

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

Table 326: User mapping

PagerDuty parameter	SCIM Parameter
id	id
summary	extension.summary
html_url	profileUrl
name	displayName
email	emails[].value
time_zone	timezone
role	roles[].value
avatar_url	photos[].value
description	extension.description
job_title	title
teams[].id	groups[].value

Groups

Table 327: Groups mapping

PagerDuty parameter	SCIM parameter
id	id
summary	extension.summary
name	displayName
description	extension.description
parent[].type	extension.parent[].type
parent[].id	extension.parent[].id
groupMembersResponse.user.id	members[].value
groupMembersResponse.user.type	members[].type

Connector limitations

- PagerDuty Target System does not return important meta information like created and lastModified.

60

Dayforce

Dayforce is an HCM software platform that helps in data unification across each phase of employee lifecycle enabling better reasoning and decision-making. It offers a vantage point view and control from a single platform covering benefits, HR, payroll, workforce and talent management.

Supervisor configuration parameters

To configure the connector, following parameters are required:

- Connector name
- Username for the cloud account
- Password for the cloud account
- Target URL (Format:- https://{instance_name}.dayforcehcm.com/Api/{clientNamespace}/V1)
- Request Delay (in ms)
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details)

NOTE:

- To handle the Dayforce rate limit issue, the Dayforce connector has been enabled with user configurable delay in milliseconds so that the each request to the target API would wait for the specific amount of time to help the connector to prevent the throttling of the Dayforce APIs. The default value for the configuration is 500 (milliseconds) and it would be advisable to keep the value below 2000 (milliseconds).
- The connector has been tested against Service Versions 59 and 60 of the Dayforce instance.

Supported objects and operations

Employees

Table 328: Supported operations for Employees

Operation	VERB
Get Employee Details	GET
Get all employees	GET
Update employee	PUT

Departments

Table 329: Supported operations for Departments

Operation	VERB
Get departments	GET
Get department by id	GET

Locations

Table 330: Supported operations for Locations

Operation	VERB
Get all locations	GET
Get location by id	GET

Organizations

Table 331: Supported operations for Organizations

Get all organizations	GET
Ger Organization Details	GET

Mappings

The mappings are listed in the tables below.

Table 332: Dayforce to SCIM Employee mapping

Dayforce properties	SCIM properties
Addresses.Items[].Address1	address.streetAddress
Addresses.Items[].City	address.locality
Addresses.Items[].Country.Name	address.country
Addresses.Items[].PostalCode	address.postalCode
Addresses.Items[].State.Name	address.region
BirthDate	birthDate
CommonName	commonName
Contacts.Items[].ContactNumber (Contacts.Items[].ContactInformationType.XRefCode = "BusinessPhone")	phoneNumbers.businessPhone
Contacts.Items[].ContactNumber (Contacts.Items[].ContactInformationType.XRefCode = "Mobile")	phoneNumbers.cellPhone
Contacts.Items[].ElectronicAddress (Contacts.Items[].ContactInformationType.XRefCode = "BusinessEmail")	emails.businessEmail
Contacts.Items[].ElectronicAddress (Contacts.Items[].ContactInformationType.XRefCode = "PersonalEmail")	emails.personalEmail
DisplayName	displayName
EmployeeBadge.BadgeNumber	employeeBadge.badgeNumber
EmployeeBadge.EffectiveEnd	employeeBadge.effectiveEnd
EmployeeBadge.EffectiveStart	employeeBadge.effectiveStart
EmployeeManagers.Items[].ManagerFirstName EmployeeManagers.Items[].ManagerLastName	employeeManager.displayName
EmployeeManagers.Items[].ManagerXRefCode	employeeManager.value
EmployeeNumber	employeeNumber
EmploymentStatuses.Items[].EmploymentStatus.EffectiveEnd	employmentStatus.effectiveEnd

Dayforce properties	SCIM properties
EmploymentStatuses.Items[].EmploymentStatus.EffectiveStart	employmentStatus.effectiveStart
EmploymentStatuses.Items[].EmploymentStatus.LongName	employmentStatus.longName
EmploymentStatuses.Items[].EmploymentStatus.ShortName	employmentStatus.shortName
EmploymentStatuses.Items[].EmploymentStatus.XRefCode	employmentStatus.value
EmploymentStatuses.Items[].EmploymentStatusGroup.XRefCode	employmentStatusGroup.value
EmploymentStatuses.Items[].EmploymentStatusGroup.ShortName	employmentStatusGroup.shortName
EmploymentStatuses.Items[].EmploymentStatusGroup.LongName	employmentStatusGroup.longName
EmploymentStatuses.Items[].PayGroup.LongName	payGroup.longName
EmploymentStatuses.Items[].PayGroup.ShortName	payGroup.shortName
EmploymentStatuses.Items[].PayGroup.XRefCode	payGroup.value
FederatedId	federatedId
FirstName	name.givenName
Gender	gender
HireDate	hireDate
HomeOrganization.LongName	homeOrganization.displayName
HomeOrganization.XRefCode	homeOrganization.value
LastName	name.familyName
Locations.Items[].Location.LongName	location.displayName
Locations.Items[].Location.XRefCode	location.value
LoginId	userName
LoginId	loginId
NewHireApprovalDate	newHireApprovalDate

Dayforce properties	SCIM properties
NewHireApproved	newHireApproved
NewHireApprovedBy	newHireApprovedBy
OrgUnitInfos.Items[].Department.LongName	department.longName
OrgUnitInfos.Items[].Department.ShortName	department.shortName
OrgUnitInfos.Items[].Department.XRefCode	department.value
OriginalHireDate	originalHireDate
PhotoExempt	photoExempt
RegisteredDisabled	registeredDisabled
RequiresExitInterview	requiresExitInterview
SeniorityDate	seniorityDate
SocialSecurityNumber	socialSecurityNumber
StartDate	startDate
TaxExempt	taxExempt
TerminationDate	terminationDate
Title	title
WorkAssignments.Items[].Position.Job.LongName	jobs[].longName
WorkAssignments.Items[].Position.Job.ShortName	jobs[].shortName
WorkAssignments.Items[].Position.Job.XRefCode	jobs[].value
XRefCode	id
GenderIdentity.XRefCode	genderIdentity.value
GenderIdentity.ShortName	genderIdentity.shortName
GenderIdentity.LongName	genderIdentity.longName
Contacts.Items[].ContactNumber (Contacts.Items[].ContactInformationType.XRefCode = "HomePhone")	phoneNumbers.homePhone
SSOAccounts.Items[].LoginName	loginNames[].loginName
WorkAssignments.Items[].Location.XRefCode	locations[].value

Dayforce properties	SCIM properties
WorkAssignments.Items[].Location.LongName	locations[].longName
WorkAssignments.Items [].Location.ShortName	locations[].shortName
EmploymentStatuses.Items [].PayClass.XRefCode	payClass.value
EmploymentStatuses.Items [].PayClass.ShortName	payClass.shortName
EmploymentStatuses.Items [].PayClass.LongName	payClass.longName
EmploymentStatuses.Items [].EmploymentStatusReason.LongName	employmentStatusReason.longName
EmploymentStatuses.Items [].EmploymentStatusReason.ShortName	employmentStatusReason.shortName
EmploymentStatuses.Items [].EmploymentStatusReason.XRefCode	employmentStatusReason.value
Contacts.Items[].ContactNumber(Contact- s.Items[].ContactInformationType.XRefCode = "BusinessMobile")	phoneNumbers.businessMobile
Contacts.Items[].ContactNumber(Contact- s.Items[].ContactInformationType.XRefCode = "BusinessFax")	phoneNumbers.businessFax
Contacts.Items[].ContactNumber(Contact- s.Items[].ContactInformationType.XRefCode = "Pager")	phoneNumbers.pager
Culture.XRefCode	culture.value
Culture.ShortName	culture.displayName
PreferredLastName	preferredLastName
Addresses.Items[].State.ShortName (Addresse- s.Items[].ContactInformationType.XRefCode = "PrimaryResidence")	address.shortName
Addresses.Items[].State.XRefCode (Addresse- s.Items[].ContactInformationType.XRefCode = "PrimaryResidence")	address.valueState

Dayforce properties	SCIM properties
Addresses.Items[].Country.XRefCode (Addresse- s.Items[].ContactInformationType.XRefCode = "PrimaryResidence")	address.valueCountry
WorkAssignments.Items [].Position.Job.JobUDFString2	jobs[].jobUDFString2
WorkAssignments.Items[].Position.XRefCode	position.value
WorkAssignments.Items[].Position.ShortName	position.shortName

Table 333: Dayforce Employee to SCIM Employee mapping

Dayforce properties	SCIM properties
XRefCode	id
LoginId	userName
FederatedId	federatedId
Gender	gender
BirthDate	birthDate
EmployeeNumber	employeeNumber
CommonName	commonName
DisplayName	displayName
LastName	name.familyName
FirstName	name.givenName
MiddleName	name.middleName
OrgUnitInfos.Items[].OrgUnitDetail.XRefCode (OrgUnitInfos.Items [].OrgUnitDetail.OrgLevel.XRefCode = "Corp")	corporate.value
OrgUnitInfos.Items[].OrgUnitDetail.ShortName (OrgUnitInfos.Items [].OrgUnitDetail.OrgLevel.XRefCode = "Corp")	corporate.shortName
OrgUnitInfos.Items[].OrgUnitDetail.LongName (OrgUnitInfos.Items [].OrgUnitDetail.OrgLevel.XRefCode = "Corp")	corporate.longName
Contacts.Items[].ElectronicAddress (Contacts.Items [].ContactInformationType.XRefCode = "BusinessE-mail")	emails.businessEmail

Dayforce properties	SCIM properties
Contacts.Items[].ElectronicAddress (Contacts.Items[].ContactInformationType.XRefCode = "PersonalEmail")	emails.personalEmail
Contacts.Items[].ContactNumber (Contacts.Items[].ContactInformationType.XRefCode = "BusinessPhone")	phoneNumbers.businessPhone
Contacts.Items[].ContactNumber (Contacts.Items[].ContactInformationType.XRefCode = "Mobile")	phoneNumbers.cellPhone
Addresses.Items[].Address1	address.streetAddress
Addresses.Items[].City	address.locality
Addresses.Items[].State.Name	address.region
Addresses.Items[].PostalCode	address.postalCode
Addresses.Items[].Country.Name	address.country
LoginId	loginId
HireDate	hireDate
NewHireApprovalDate	newHireApprovalDate
NewHireApproved	newHireApproved
NewHireApprovedBy	newHireApprovedBy
OriginalHireDate	originalHireDate
SeniorityDate	seniorityDate
StartDate	startDate
PhotoExempt	photoExempt
OrgUnitInfos.Items[].OrgUnitDetail.XRefCode (OrgUnitInfos.Items[].OrgUnitDetail.OrgLevel.XRefCode = "Region")	region.value
OrgUnitInfos.Items[].OrgUnitDetail.ShortName (OrgUnitInfos.Items[].OrgUnitDetail.OrgLevel.XRefCode = "Region")	region.shortName
OrgUnitInfos.Items[].OrgUnitDetail.LongName (OrgUnitInfos.Items[].OrgUnitDetail.OrgLevel.XRefCode = "Region")	region.longName
OrgUnitInfos.Items[].OrgUnitDetail.XRefCode (OrgUnitInfos.Items[].OrgUnitDetail.OrgLevel.XRefCode = "District")	district.value

Dayforce properties	SCIM properties
OrgUnitInfos.Items[].OrgUnitDetail.ShortName (OrgUnitInfos.Items [].OrgUnitDetail.OrgLevel.XRefCode = "District")	district.shortName
OrgUnitInfos.Items[].OrgUnitDetail.LongName (OrgUnitInfos.Items [].OrgUnitDetail.OrgLevel.XRefCode = "District")	district.longName
OrgUnitInfos.Items[].OrgUnitDetail.XRefCode (OrgUnitInfos.Items [].OrgUnitDetail.OrgLevel.XRefCode = "Site")	site.value
OrgUnitInfos.Items[].OrgUnitDetail.ShortName (OrgUnitInfos.Items [].OrgUnitDetail.OrgLevel.XRefCode = "Site")	site.shortName
OrgUnitInfos.Items[].OrgUnitDetail.LongName (OrgUnitInfos.Items [].OrgUnitDetail.OrgLevel.XRefCode = "Site")	site.longName
OrgUnitInfos.Items[].OrgUnitDetail.ShortName (OrgUnitInfos.Items [].OrgUnitDetail.OrgLevel.XRefCode = "OnSiteDepartment")	onSiteDepartment.shortName
OrgUnitInfos.Items[].OrgUnitDetail.LongName (OrgUnitInfos.Items [].OrgUnitDetail.OrgLevel.XRefCode = "OnSiteDepartment")	onSiteDepartment.longName
OrgUnitInfos.Items[].OrgUnitDetail.XRefCode (OrgUnitInfos.Items [].OrgUnitDetail.OrgLevel.XRefCode = "OnSiteDepartment")	onSiteDepartment.value
RegisteredDisabled	registeredDisabled
RequiresExitInterview	requiresExitInterview
SocialSecurityNumber	socialSecurityNumber
TaxExempt	taxExempt
EmployeeBadge.BadgeNumber	employeeBadge.badgeNumber
EmployeeBadge.EffectiveStart	employeeBadge.effectiveStart
EmployeeBadge.EffectiveEnd	employeeBadge.effectiveEnd
EmployeeManagers.Items[].ManagerXRefCode	employeeManager.value
EmployeeManagers.Items[].ManagerFirstName	employeeManager.displayName

Dayforce properties	SCIM properties
EmployeeManagers.Items[].ManagerLastName	
Locations.Items[].Location.XRefCode	location.value
Locations.Items[].Location.LongName	location.displayName
OrgUnitInfos.Items[].Department.XRefCode	department.value
OrgUnitInfos.Items[].Department.LongName	department.displayName
HomeOrganization.XRefCode	homeOrganization.value
HomeOrganization.LongName	homeOrganization.displayName

Table 334: Dayforce Department to SCIM Department mapping

Dayforce properties	SCIM properties
XRefCode	id
ShortName	shortName
LongName	longName
LastModifiedTimestamp	meta.lastModified

Table 335: Dayforce Location to SCIM Locations mapping

Dayforce properties	SCIM properties
Address	address
AddressLineTwo	addressLineTwo
City	city
CountryCode	countryCode
CountryName	countryName
County	county
Description	description
IsTaxation	isTaxation
ShortName	shortName
StateProvince	stateProvince
StateProvinceCode	stateProvinceCode
XRefCode	id
ZipPostalCode	zipPostalCode

Table 336: Dayforce OrgUnits to SCIM Organizations mapping

Dayforce properties	SCIM properties
XRefCode	id
PhysicalLocation	physicalLocation
OpeningDate	openingDate
IsMobileOrg	isMobileOrg
ShortName	shortName
LongName	longName
OrgLevel.XRefCode	orgLevel.value
OrgLevel.ShortName	orgLevel.shortName
OrgLevel.LongName	orgLevel.longName
OrgUnitParents.Items [].ParentOrgUnit.XRefCode	orgUnitParents.value
OrgUnitParents.Items [].ParentOrgUnit.ShortName	orgUnitParents.shortName
OrgUnitParents.Items [].ParentOrgUnit.LongName	orgUnitParents.longName

Filter Resource

Dayforce target APIs supports filtering on employees and hence the Starling Connector for Dayforce has the filter feature implemented in employees endpoint. Below are the details on the supported attributes and operations on filter functionality on the Employee resource on the SCIM connector.

Supported attributes for Dayforce

Table 337: Supported attributes for Dayforce

Attribute	Supported Operations
meta.lastModified	gt (greater than) ge (greater than or equal to) lt (less than) le (less than or equal to)

	eq (equal to)
hireDate	gt ge lt le eq
originalHireDate	gt ge lt le eq
seniorityDate	gt ge lt le eq
employeeNumber	co (contains)
displayName	co
socialSecurityNumber	co
homeOrganization.value	eq
department.value	eq

More information about Filtering Resource

- As the Dayforce API support only AND conditions in the request filter criteria, the connector has implemented to support only AND in SCIM filter condition.
- In the connector filter functionality any invalid or non-supported filter criteria will be ignored in the filter. If no valid criteria found then normal LIST employees will be carried out.
- When 'meta.lastModified' is used with 'lt' | 'le' as the filter criteria then the target APIs demands filter condition on 'meta.lastModified' with 'gt' | 'ge' | 'eq' since a date range is expected by the target APIs. When 'meta.lastModified' is applied with 'gt' | 'ge' | 'eq' but no 'meta.lastModified' with 'lt' | 'le' criteria is provided, then the current date time will be used within the connector logic to acomplish the date range requirement.

- The filter functionality looks generously for the filter condition and values instead of performing a greedy and strict match. For example: the 'meta.lastModified' with below are some of the valid formats:

  filter=meta.lastModified gt xxxx-xx-xxTxx:xx:xx

  filter=meta.lastModified gt xxxx-xx-xx xx:xx:xx

  filter=meta.lastModified gt xxxx-xx-xxTxx:xx:xx.xxx

  filter=meta.lastModified gt "xxxx-xx-xxTxx:xx:xx"

  filter=meta.lastModified gt xxxx-xx-xx xx:xx:xxZ

  filter=meta.lastModified gt xxxx-xx-xxTxx:xx:xx.xxxZ

  filter=meta.lastModified gt 'xxxx-xx-xxTxx:xx:xx'

For more information about Filter Resource, see Documentation of filtering on Dayforce endpoints.

Connector SCIM Configuration

The Dayforce connector supports configuring custom attributes for Employee object type. Supported data types are integer, decimal, string, datetime, boolean and binary.

NOTE:

- The custom attributes are available under the "EmployeeProperties" attribute in Dayforce Employee schema. If the necessary permissions are not provided on the Dayforce instance to let "EmployeeProperties" attribute be retrivable along with the GET Employee details request, then the connector makes an extra request to retrieve the "EmployeeProperties" alone which would introduce additional delay in completing the Identity Manager synchronization.
- The complex type of EmployeeProperties would not be processed in the Dayforce Connect.
- The "OptionValue" EmployeeProperties would be considered as string and if multiple occurrences of such values are there then the individual values would be combined using a delimiter "$$". For example: "Option Value 1$$ Option Value 2".
- While configuring custom attribute in Starling Connect Portal the attribute name to be used would be like "EmployeePropertyXrefCodeXXX" which would be available under the "EmployeeProperty". Refer the sample date for "EmployeeProperties" (custom attributes) below:

Request: GET {instance_base_url}/Employees/{employee_XRefCode}/EmployeeProperties

```
{
"Data":
[
{
"EmployeeProperty":
{
"XRefCode": "EmployeePropertyXrefCode1",
"ShortName": "Short_Name",
"LongName": "Long_Name"
},
"StringValue": "String_Value"
}
]
}
```

Request: GET {instance_base_url}/Employees/{employee_XRefCode}?expand=Addresses,Contacts,EmployeeManagers,Locations,OrgUnitInfos,EmployeeProperties,EmploymentStatuses,WorkAssignments

```
{
"Data":
{
.....,
.....,
```

```
"EmployeeProperties":
{
"Items":
[
{
"EffectiveStart": "2000-01-01T00:00:00",
"EmployeeProperty":
{
"XRefCode": "EmployeePropertyXrefCode1",
"ShortName": "Short_Name",
"LongName": "Long_Name"
},
"NumberValue": 11
},
{
"EffectiveStart": "2000-01-01T00:00:00",
"EmployeeProperty":
{
"XRefCode": "EmployeePropertyXrefCode2",
"ShortName": "Short_Name",
"LongName": "Long_Name"
},
"StringValue": "String_Value"
}
]
},
.....,
.....
}
}
```


One IM Configuration for Delta Synchronization

Modifying the FullProjection process

1. In **Designer**, locate the '**DPR_DPRProjectionStartInfo_Run_Synchronization**' process click to edit it. Under '**Pre-script for generating**' add the script as mentioned below:

```
'Starling Delta Sync Handling (search sync project variables with their names staring with dprRevisionDate and put the corresponding revision data value in)
Dim f = session.SqlFormatter
Dim nameSchema as String
Dim nameVariable as String
Dim variableValue as String
values("OverrideVariables") = ""

'search project variables dprRevisionDate*
Dim qVariables = Query _
.From("DPRSystemVariable") _
.Orderby("UID_DPRSystemVariable") _
.Where( f.AndRelation( _
f.Comparison("Name", "dprRevisionDate%", ValType.String, CompareOperator.Like, FormatterOptions.IgnoreCase), _
f.UidComparison("UID_DPRSystemVariableSet", $UID_DPRSystemVariableSet$, CompareOperator.Equal))) _
.Select("Name")
Dim colVariables = Session.Source.GetCollection(qVariables)

If colVariables.Count > 0 then
'fetching revision data from last synchronization of that sync project configuration
Dim qRevStore = Query _
.From("DPRRevisionStore") _
.Where( f.AndRelation( _
f.UidComparison("UID_DPRProjectionConfig", $UID_DPRProjectionConfig$, CompareOperator.Equal), _
f.UidComparison("UID_DPRSystemVariableSet", $UID_DPRSystemVariableSet$, CompareOperator.Equal))) _
.Select("Value", "SchemaTypeKey")

Dim colRevStore = Session.Source.GetCollection(qRevStore)
```

```
Dim dictRevStore = new System.Collections.Generic.Dictionary(of String, String)()

For Each elemRevStore As IEntity In colRevStore
nameSchema = elemRevStore.GetValue("SchemaTypeKey").String 'Schema [FTP#C04A6567-9EAE-4121-973E-AF1EE514D728].Type[Employees]
If string.IsNullOrEmpty(nameSchema) OrElse not nameSchema.Contains(".") then
Continue For
End If
nameSchema = nameSchema.Split("."c)(1)

dictRevStore.Add(nameSchema, elemRevStore.GetValue("Value").String)
Next

'put the revision date into the variables if available, else provide the revision data as 1900-01-01
Dim lstVariables = new System.Collections.Generic.List(of String)()
For Each elemVariable As IEntity In colVariables
nameVariable = elemVariable.GetValue("Name").String 'e.g. dprRevisionDateEmployees
nameSchema = string.Format("Type[{0}]", nameVariable.Trim().Substring(15)) 'e.g. Type[Employees]

If dictRevStore.TryGetValue(nameSchema, variableValue) then
values(nameVariable) = variableValue.Replace(" ", "T")
Else
values(nameVariable) = "1900-01-01"
End If
lstVariables.Add(nameVariable)
Next
values("OverrideVariables") = string.Join(";", lstVariables.ToArray())
End If
```

2. Under '**Run Synchronization**' select '**Parameters**' tab and provide the below script under '**OverrideVariables**'.

```
If not String.IsNullOrEmpty(values("OverrideVariables").ToString()) then
Imports System.Data.Common
```

```
Dim sb as DbConnectionStringBuilder = new DbConnectionStringBuilder(false)
For each varName as String in values("OverrideVariables").ToString
().Split(";"c)
sb.Add(varName, values(varName).ToString())
Next
Value = sb.ConnectionString
End if
```

3. '**Commit to database**' and then '**Compile database**'.

Modifying the synchronization project

1. Make sure that the local cache is turned off for the Synchronization project.
2. Select the SCIM synchronization project and select 'Variables' to add a new variable 'dprRevisionDateEmployees' (the variable name should be **dprRevisionDate<*schema name*>**).
3. Create a new 'Schema Class' from Employee in the 'Target system'. For example: "Employees for Delta Sync".
4. On the Schema Class set the System Filter: **meta.LastModified gt $dprRevisionDateEmployees$**. Under 'Select Objects' tab, use 'meta_lastModified' as the attribute, '>' as the operator and $dprRevisionDateEmployees$ as the text field value.
5. As required, other supported attributes also can be added under filters.
6. Create a new Mapping using the new Schema Class dialog box.
7. Create a new Workflow using the new mapping. This workflow updates the existing records based on the revision filter.
8. To improve the syncs performance, remove the update steps from the existing default Initial sync Work Flow.
9. Create a new Startup Config using the new workflow. Select 'One Identity Manager' for the 'Synchronization in direction'. Use 'default variable set' for the 'Variable Set'.
10. Use hotfix #33601 for One Identity Manager version 8.1.2 and 8.1.4.

Connector limitations

- Pagination is not supported for Employees, Departments, LocationAddresses and OrgUnits resources.
- List response for Employees, Departments and OrgUnits return only xRefCode (ID).

- Meta attributes are not retrieved for Employees, Departments, LocationAddresses and OrgUnits resources.
- In absence of necessary access rights for the employee attributes **EmployeeProperties** and **OrgUnitInfos** at the Dayforce target instance, the Dayforce connector would need to make additional requests to retrieve these attributes which impact the Identity Manager synchronization performance.
- Dayforce generally applies rate limiting to the API requests. If a request exceeds the defined rate limit, the request is rejected with the `HTTP status 429 - Quota exceeded for number of requests` response.

61

Smartsheet

Smartsheet is a software that offers enhanced collaboration and work management. It uses a tabular user interface to assign tasks, track project progress, manage calendars, documents. It is an enterprise platform for dynamic work that aligns technology and people resulting in an efficient work environment.

Supervisor Configuration Parameters

- Connector name
- API Key
- Target URL (https://api.smartsheet.com/2.0/)
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details).

Supported objects and operations

Users

Table 338: Supported operations for Users

Operation	VERB
Create User	POST
Get a User	GET
List Users	GET
Update a user	PUT
Delete a user	DELETE

Groups

Table 339: Supported operations for Groups

Operation	VERB
Create a group	POST
Delete a group	DELETE
Get a group	GET
List groups	GET
Update a group	PUT

Mandatory Fields

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

Users

- extension.admin
- emails[].value
- extension.licensedSheetCreator

Groups

- displayName

Mappings

The mappings are listed in the tables below.

Table 340: Smartsheet User to SCIM user mapping

SCIM properties	Smartsheet Properties
id	id
extension.admin	admin
emails[].value	email
name.givenName	firstName
extension.groupAdmin	groupAdmin
extension.lastLogin	lastLogin
name.familyName	lastName
extension.licensedSheetCreator	licensedSheetCreator
displayName	name
photos[].value	profileImage.id
extension.resourceViewer	resourceViewer
extension.sheetCount	sheetCount
active	status
title	title
timeZone	timeZone

Table 341: Smartsheet group to SCIM group mapping

SCIM properties	Smartsheet Properties
id	id
extension.ownerId	ownerId
meta.created	createdAt
extension.description	description
members[].value	members[]
meta.lastModified	modifiedAt
displayName	name
extension.ownerEmail	owner

Connector limitations

- Connector does not return important meta information like created and lastModified for users.
- While trying to create a user with already used details, the connector returns the existing user details.
- While creating or updating a group, the members attribute is sometimes available with all members, sometimes it doesn't.
- For larger page(cursor) values than the present number of pages in list response, the connector returns last page(cursor) response.

62

Pingboard

Pingboard is real-time organizational chart software that makes it easy to build professional looking org charts. It keeps company org charts in sync with HRMS software automatically, thus replacing the manual need to make the org charts using flow charting applications like Microsoft Visio or Lucidchart. Pingboard was designed to help companies organize their employees and departments, develop hiring and succession plans, and share this information on the corporate org chart.

Supervisor configuration parameters

To configure the connector, following parameters are required:

- Connector name
- Client Id for the service account
- Client Secret for the service account
- Target URL (https://app.pingboard.com/api/v2)
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details).

Supported objects and operations

Users

Table 342: Supported operations for Users

Operation	VERB
Create User	POST

Operation	VERB
Update User	PUT
Delete User	DELETE
Get User by Id	POST
List Users	POST

Groups

Table 343: Supported operations for Groups

Operation	VERB
Create Group	POST
Update Group	PUT
List Groups	POST
Get Group by Id	POST
Delete Group	DELETE

Mandatory fields

Users

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

Groups

- displayName
- extension.groupType

User and Group mapping

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

Table 344: Pingboard user to SCIM mapping

SCIM parameter	Pingboard parameter
id	id
userName	email
name.givenName	first_name
name.familyName	last_name
name.formatted	first_name + " " + last_name
displayName	first_name + " " + last_name
nickName	nickname
emails[].value	email
phoneNumbers[].value	office_phone
photos[].value	avatar_urls.original
timezone	time_zone
locale	locale
title	job_title
groups[].value (Only for read operation)	links.groups[] & links.locations[]
extension.description	bio
extension.manager.value	reports_to_id
meta.created	created_at
meta.lastModified	updated_at

Table 345: Pingboard group to SCIM group mapping

SCIM parameter	Pingboard parameter
id	id
displayName	name
members[].value	links.users[]

SCIM parameter	Pingboard parameter
extension.description	description
extension.type	type
meta.created	created_at
meta.lastModified	updated_at

Connector limitations

- If all of the member IDs used in the create group request are invalid, an error with status 500 and no message will be returned but the group gets created. Even with at least one valid member ID, the group write operation gets successful.
- Even though the **Pingboard API** supports custom attributes for user resource, the **Pingboard** connector does not support custom attributes for users. The reason being is to avoid the unnecessary overhead in retrieving the names of the custom attributes by making additional request as the target API returns custom attribute IDs instead of the attribute name for **GET** user details response.
- An Admin user can also be deleted using APIs in which case the connector functionality will not work.
- Random string value for user's locale gets saved due to the target API behavior.

63

SAP Cloud for Customer

SAP Cloud for Customer (C4C) is a cloud solution to manage customer sales, customer service and marketing activities efficiently and is one of the key SAP solution to manage customer relationship.

Supervisor configuration parameters

To configure the connector, following parameters are required:

- Connector name
- Username
- Password
- Target URL (https://{tenant_id}.crm.ondemand.com/sap/c4c/odata/v1/)
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details)

Supported objects and operations

Users

Table 346: Supported operations for Users

Operation	VERB
Create User	POST
Get a User	GET
List Users	GET

Operation	VERB
Update a User	PUT
Delete User	DELETE

Roles

Table 347: Supported operations for Roles

Operation	VERB
Get a Role	GET
List Roles	GET

Mandatory fields

Users

- name.givenName
- name.familyName

Mappings

Table 348: SAPC4CEmployee,BusinessUser to SCIM User mapping

SCIM properties	SAPC4C properties
active	EmployeeValidityEndDate
addresses[].country	CountryCode
addresses[].postalCode	PostalCode
addresses[].region	RegionCode
addresses[].streetAddress	Street
displayName	FirstName + " " + LastName
emails[].value	Email

SCIM properties	SAPC4C properties
exten-sion.businessUserLanguageCode	LogonLanguageCode
extension.businessUserLanguage	LogonLanguageCodeText
extension.companyName	CompanyName
extension.dateFormat	DateFormat
extension.dateFormatCode	DateFormatCode
extension.decimalFormatCode	DecimalFormatCode
extension.department	Department
extension.employeeId	EmployeeID
extension.gender	GenderCodeText
extension.genderCode	GenderCode
extension.employeeLanguage	LanguageCodeText
extension.employeeLanguageCode	LanguageCode
extension.managerName	ManagerName
extension.maritalStatus	MaritalStatusCodeText
extension.maritalStatusCode	MaritalStatusCode
extension.passwordPolicyCode	PasswordPolicyCode
extension.timeFormat	TimeFormat
extension.timeFormatCode	TimeFormatCode
extension.titleCode	TitleCode
extension.titleCodeText	TitleCodeText
extension.userId	UserID
extension.userLockedIndicator	UserLockedIndicator
extension.validityEndDate	UserValidityEndDate
extension.validityStartDate	UserValidityStartDate
id	ObjectID
meta.created	CreatedOn
meta.lastModified	EntityLastChangedOn
name.familyName	LastName

SCIM properties	SAPC4C properties
name.givenName	FirstName
name.middleName	MiddleName
nickName	NickName
phoneNumbers[].value	MobilePhoneNumber
roles.value	Employ-eeUserBusinessRoleAssignment.BusinessRoleID
timezone	TimeZoneCode
userName	UserID

Table 349: SAPC4CIdentityBusinessRoles to SCIM Role mapping

SCIM properties	SAPC4C properties
id	ObjectID
name	Name
meta.created	CreationDateTime
meta.lastModified	EntityLastChangedOn

Connector limitations

- Update is not supported for attributes like **ManagerName**, **CompanyName** and **Department**, as they come under **Organization** endpoints.
- Deleting a User, will inactivate it. But the user will still be present in the list of users.
- Due to the target API behavior, any text value can be used as the value for **phoneNumbers**.
- For most of the error scenarios, the status code returned is 500.
- While user creation, the user will still be created if there is an error while user role assignments.
- Due to One IM limitation on DateTime attributes, value having 'YEAR' less than 1753 could not be shown in One IM user interface.

64

Azure Infrastructure

AzureInfrastructure is an alias for Azure Resource Manager. Azure Resource Manager is the deployment and management service for Azure. It provides a management layer that enables you to create, update, and delete resources in your Azure account. You use management features, like access control, locks, and tags, to secure and organize your resources after deployment.

Supervisor configuration parameters

To configure the connector, following parameters are required. For more information, refer How to create Service Principal to authenticate the resource management REST APIs:

- Connector name
- Client Id of 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 - Example:https://management.azure.com)
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details).

Supported objects and operations

ManagementGroups

Table 350: Supported operations for ManagementGroups

Operation	VERB
Get ManagementGroup By Id	GET
List ManagementGroups	GET

Subscriptions

Table 351: Supported operations for Subscriptions

Operation	VERB
Get Subscription By Id	GET
List Subscriptions	GET
Get Subscriptions with Pagination	GET

ResourceGroups

Table 352: Supported operations for ResourceGroups

Operation	VERB
Get ResourceGroup By Id	GET
List ResourceGroups	GET
Get ResourceGroups with Pagination	GET

AzResource

Table 353: Supported operations for AzResource

Operation	VERB
List Azresources	GET
Get AzResource by id	GET
Get AzResource with Pagination	GET

AzResourceTypes

Table 354: Supported operations for AzResourceTypes

Operation	VERB
List AzresourcesTypes	GET
Get AzResourceTypes by id	GET

Locations

Table 355: Supported operations for Locations

Operation	VERB
List Locations	GET
Get Location By Id	GET

Roles

Table 356: Supported operations for Divisions

Operation	VERB
Get Role By Id	GET
List Roles	GET

RoleAssignments

Table 357: Supported operations for RoleAssignments

Operation	VERB
Get RoleAssignment By Id	GET
List RoleAssignments	GET
Create RoleAssignments	POST
Delete RoleAssignments	DELETE

Mandatory fields

This section lists the mandatory field required to CREATE.

RoleAssignments

- roleDefinitionId
- principalId
- scope

Attributes Mappings

Different mappings associated with this connector are listed in the tables below.

Table 358: AzureInfrastructure managementGroup to SCIM managementGroup mapping

Azure Infrastructure properties	SCIM properties
id.Replace("/", "$$")	id
name	name
Properties.displayName	displayName
Properties.details.updatedBy	updatedBy
Properties.tenantId	tenantId

Azure Infrastructure properties	SCIM properties
properties.details.parent.id	parentManagementGroupId
id	resourceId
role[].value.name	role[].value
role[].value.properties.principalId	role[].principalId
role[].value.properties.principalType	role[].principalType
role[].value.properties.roleDefinitionId	role[].azRoleReference
properties.details.updatedTime	meta.LastModified

Table 359: AzureInfrastructure subscription to SCIM subscription mapping

Azure Infrastructure properties	SCIM properties
id.Replace("/", "$$")	id
name	name
name	subscriptionId
Properties.displayName	displayName
properties.state	state
properties.tenant	tenantId
id	resourceId
properties.parent.id.Split('/')[4]	managementGroupName
properties.parent.id	managementGroupId
role[].value.name	role[].value
role[].value.properties.principalId	role[].principalId
role[].value.properties.principalType	role[].principalType
role[].value.properties.roleDefinitionId	role[].azRoleReference

Table 360: AzureInfrastructure resourceGroup to SCIM resourceGroup mapping

Azure Infrastructure properties	SCIM properties
id.Replace("/", "$$")	id
name	name
name	displayName
location	location

Azure Infrastructure properties	SCIM properties
properties.provisioningState	provisioningState
id.Split('/')[2]	subscriptionName
/subscriptions/{id.Split('/')[2]}	subscriptionId
id	resourceId
role[].value.name	role[].value
role[].value.properties.principalId	role[].principalId
role[].value.properties.principalType	role[].principalType
role[].value.properties.roleDefinitionId	role[].azRoleReference

Table 361: AzureInfrastructure resources to SCIM AzResources mapping

Azure Infrastructure properties	SCIM properties
id.Replace("/", "$$")	id
name	name
name	displayName
type	resourceType
location	location
id	resourceId
id.Split('/')[2]	subscriptionName
/subscriptions/{id.Split('/')[2]}	subscriptionId
id.Split('/')[4]	resourceGroupName
/subscriptions/{id.Split('/')[2]}/resourceGroups/{id.Split('/')[4]}	resourceGroupId
tags[].Name	tags[].name
tags[].Value	tags[].value
role[].value.name	role[].value
role[].value.properties.principalId	role[].principalId
role[].value.properties.principalType	role[].principalType
role[].value.properties.roleDefinitionId	role[].azRoleReference

Table 362: AzureInfrastructure roleAssignments to SCIM roleAssignments mapping

Azure Infrastructure properties	SCIM properties
id.Replace("/", "$$")	id
properties.description	description
properties.roleDefinitionId	roleDefinitionId
properties.principalId	principalId
properties.principalType	principalType
properties.scope	scope
id	resourceId
properties.createdOn	meta.Created
properties.updatedOn	meta.LastModified

Table 363: AzureInfrastructure resourceTypes to SCIM AzResourceTypes mapping

Azure Infrastructure properties	SCIM properties
Namespace + '$$' + resourceTypes.resourceType	id
namespace + '/' + resourceTypes.resourceType	displayName

Table 364: AzureInfrastructure locations to SCIM locations mapping

Azure Infrastructure properties	SCIM properties
id.Replace("/", "$$")	id
name	name
displayName	displayName
regionalDisplayName	regionalDisplayName
id	resourceId

Table 365: AzureInfrastructure roles to SCIM roles mapping

Azure Infrastructure properties	SCIM properties
id	id
properties.roleName	displayName

Azure Infrastructure properties	SCIM properties
id	resourceId
properties.roleName	name
properties.description	description
properties.type	type
properties.createdOn	meta.Created
properties.updatedOn	meta.LastModified
properties.assignableScopes	assignableScopes

Connector limitations

- Pagination is not supported for **ManagementGroups**, **AzResourceTypes**, **Locations** and **Roles** endpoints.

65

Oracle Fusion Cloud

The **Oracle Fusion Cloud** is a next-generation service-oriented platform and applications suite that caters to the enterprise technologies, applications, and services, including Oracle Fusion Applications and Oracle Fusion Middleware, to change the dynamics in the applications marketplace and revolutionize business.

Supervisor configuration parameters

To configure the connector, following parameters are required:

- Connector Name
- Username
- Password
- Target URL (https://<instance>.oraclecloud.com/)
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details).

Supported objects and operations

Users

Table 366: Supported operations for users

Operation	VERB
Create User	POST
Get a User	GET

Operation	VERB
Get all Users	GET
Get all Users with Pagination	GET
Update Users	PUT
Delete User	DELETE

Roles

Table 367: Supported operations for roles

Operation	VERB
Get a Role	GET
Get all Roles	GET
Get all Roles with pagination	GET
Update Role	PUT

Employees

Table 368: Supported operations for Employees

Operation	VERB
Create Employee	POST
Get an Employee	GET
Get All Employees	GET
Update Employee	PUT

Data Securitiees

Table 369: Supported operations for Data Securities

Operation	VERB
List Data Securities	GET
Get Data Security	GET

Operation	VERB
Create Data Security	POST
Update Data Security	PUT

NOTE: Data Securities feature is still in beta.

Mandatory Fields

This section lists the mandatory fields required to **CREATE**.

Users

- userName

Employees

- names[].LastName
- names[].LegislationCode
- workRelationships[].LegalEmployerName
- workRelationships[].assignments[].ActionCode
- workRelationships[].assignments[].BusinessUnitName

NOTE: While creating employee, if emails attribute is present then EmailAddress and EmailType is mandatory. If phones attribute is present then PhoneNumber and PhoneType is mandatory and if addresses attribute is present then AddressType and Country is mandatory.

Data Securities

- securityContext
- securityContextValue
- roleNameCr
- userName

Mappings

Attributes mapping

Different mappings associated with this connector are listed in the tables below.

Table 370: User mapping

SCIM User	OracleFusion User
active	active
displayName	displayName
emails[].primary	emails[].primary
emails[].type	emails[].type
emails[].value	emails[].value
id	id
meta.created	meta.created
meta.lastModified	meta.lastModified
name.familyName	name.familyName
name.givenName	name.givenName
roles[].display	roles [].displayName
roles[].value	roles[].id
userName	userName

Table 371: Role mapping

SCIM Role	OracleFusion Role
category	category
description	description
displayName	displayName
id	id
Meta.Created	meta.created

SCIM Role	OracleFusion Role
meta.lastModified	meta.lastModified
name	name
members[].value	members[].value

Table 372: Employeemapping

SCIM Employee	OracleFusion Employee
id	PersonId
personId	PersonId
personNumber	PersonNumber
name.legislationCode	names[].LegislationCode
name.firstName	names[].FirstName
name.lastName	names[].LastName
name.displayName	names[].DisplayName
name.fullName	names[].FullName
name.honors	names[].Honors
name.knownAs	names[].KnownAs
name.listName	names[].ListName
name.middleNames	names[].MiddleNames
name.orderName	names[].OrderName
name.suffix	names[].Suffix
name.title	names[].Title
name.preNameAdjunct	names[].PreNameAdjunct
name.previousLastName	names[].PreviousLastName
name.localSuffix	names[].LocalSuffix
name.localTitle	names[].LocalTitle
name.localDisplayName	names[].LocalDisplayName
name.localFirstName	names[].LocalFirstName
name.localFullName	names[].LocalFullName
name.localHonors	names[].LocalHonors
name.localKnownAs	names[].LocalKnownAs

SCIM Employee	OracleFusion Employee
name.localLastName	names[].LocalLastName
name.localListName	names[].LocalListName
name.localMiddleNames	names[].LocalMiddleNames
name.localOrderName	names[].LocalOrderName
name.localPreNameAdjunct	names[].LocalPreNameAd-junct
name.localPreviousLastName	names[].LocalPre-viousLastName
name.nameInformation1	names[].NameInformation1
name.nameInformation2	names[].NameInformation2
name.nameInformation3	names[].NameInformation3
name.nameInformation4	names[].NameInformation4
name.nameInformation5	names[].NameInformation5
name.nameInformation6	names[].NameInformation6
name.nameInformation7	names[].NameInformation7
name.nameInformation8	names[].NameInformation8
name.nameInformation9	names[].NameInformation9
name.nameInformation10	names[].NameIn-formation10
name.nameInformation11	names[].NameIn-formation11
name.nameInformation12	names[].NameIn-formation12
name.nameInformation13	names[].NameIn-formation13
name.nameInformation14	names[].NameIn-formation14
name.nameInformation15	names[].NameIn-formation15
name.nameInformation16	names[].NameIn-formation16
name.nameInformation17	names[].NameIn-formation17

SCIM Employee	OracleFusion Employee
name.nameInformation18	names[].NameInformation18
name.nameInformation19	names[].NameInformation19
name.nameInformation20	names[].NameInformation20
name.nameInformation21	names[].NameInformation21
name.nameInformation22	names[].NameInformation22
name.nameInformation23	names[].NameInformation23
name.nameInformation24	names[].NameInformation24
name.nameInformation25	names[].NameInformation25
name.nameInformation26	names[].NameInformation26
name.nameInformation27	names[].NameInformation27
name.nameInformation28	names[].NameInformation28
name.nameInformation29	names[].NameInformation29
name.nameInformation30	names[].NameInformation30
name.localNameInformation1	names[].LocalNameInformation1
name.localNameInformation2	names[].LocalNameInformation2
name.localNameInformation3	names[].LocalNameInformation3
name.localNameInformation4	names[].LocalNameInformation4
name.localNameInformation5	names[].LocalNameInformation5

SCIM Employee	OracleFusion Employee
name.localNameInformation6	names[].LocalNameIn-formation6
name.localNameInformation7	names[].LocalNameIn-formation7
name.localNameInformation8	names[].LocalNameIn-formation8
name.localNameInformation9	names[].LocalNameIn-formation9
name.localNameInformation10	names[].LocalNameIn-formation10
name.localNameInformation11	names[].LocalNameIn-formation11
name.localNameInformation12	names[].LocalNameIn-formation12
name.localNameInformation13	names[].LocalNameIn-formation13
name.localNameInformation14	names[].LocalNameIn-formation14
name.localNameInformation15	names[].LocalNameIn-formation15
name.localNameInformation16	names[].LocalNameIn-formation16
name.localNameInformation17	names[].LocalNameIn-formation17
name.localNameInformation18	names[].LocalNameIn-formation18
name.localNameInformation19	names[].LocalNameIn-formation19
name.localNameInformation20	names[].LocalNameIn-formation20
name.localNameInformation21	names[].LocalNameIn-formation21
name.localNameInformation22	names[].LocalNameIn-formation22
name.localNameInformation23	names[].LocalNameIn-formation23

SCIM Employee	OracleFusion Employee
name.localNameInformation24	names[].LocalNameIn-formation24
name.localNameInformation25	names[].LocalNameIn-formation25
name.localNameInformation26	names[].LocalNameIn-formation26
name.localNameInformation27	names[].LocalNameIn-formation27
name.localNameInformation28	names[].LocalNameIn-formation28
name.localNameInformation29	names[].LocalNameIn-formation29
name.localNameInformation30	names[].LocalNameIn-formation30
emails[].emailAddress	emails[].EmailAddress
emails[].emailType	emails[].EmailType
emails[].primaryFlag	emails[].PrimaryFlag
addresses[].addressLine1	addresses[].AddressLine1
addresses[].addressLine2	addresses[].AddressLine2
addresses[].addressLine3	addresses[].AddressLine3
addresses[].addressLine4	addresses[].AddressLine4
addresses[].addressType	addresses[].AddressType
addresses[].building	addresses[].Building
addresses[].floorNumber	addresses[].FloorNumber
addresses[].country	addresses[].Country
addresses[].primaryFlag	addresses[].PrimaryFlag
addresses[].postalCode	addresses[].PostalCode
addresses[].longPostalCode	addresses [].LongPostalCode
addresses[].townOrCity	addresses[].TownOrCity
addresses[].region1	addresses[].Region1
addresses[].region2	addresses[].Region2

SCIM Employee	OracleFusion Employee
addresses[].region3	addresses[].Region3
addresses[].addlAddressAttribute1	addresses[].AddlAddressAttribute1
addresses[].addlAddressAttribute2	addresses[].AddlAddressAttribute2
addresses[].addlAddressAttribute3	addresses[].AddlAddressAttribute3
addresses[].addlAddressAttribute4	addresses[].AddlAddressAttribute4
addresses[].addlAddressAttribute5	addresses[].AddlAddressAttribute5
phones[].phoneNumber	phones[].PhoneNumber
phones[].phoneType	phones[].PhoneType
phones[].areaCode	phones[].AreaCode
phones[].countryCodeNumber	phones[].CountryCodeNumber
phones[].primaryFlag	phones[].PrimaryFlag
workRelationships[].LegalEntityId	workRelationships[].LegalEntityId
workRelationships[].legalEmployerName	workRelationships[].LegalEmployerName
workRelationships[].workerType	workRelationships[].WorkerType
workRelationships[].legislationCode	workRelationships[].LegislationCode
workRelationships[].startDate	workRelationships[].StartDate
workRelationships[].assignments[].actionCode	workRelationships[].assignments[].ActionCode
workRelationships[].assignments[].businessUnitName	workRelationships[].assignments[].BusinessUnitName
dateOfBirth	DateOfBirth
townOfBirth	TownOfBirth

SCIM Employee	OracleFusion Employee
countryOfBirth	CountryOfBirth
meta.created	CreationDate
meta.lastModified	LastUpdateDate
userId	userId

NOTE:

- The nameInformation1 is not considered for some of the legislationCode for Create Employee.
- Supported Updation of first object of Emails, Phones and Addresses.
- If Phones, Emails, Addresses does not exist for an Employee so for creating a new one we have some mandatory fields
    - For Addresses : AddressType and Country are mandatory.
    - For Phones : PhoneNumber and PhoneType are mandatory.
    - For Emails : EmailAddress and EmailType are mandatory.

Table 373: Data Securities mapping

SCIM Security	OracleFusion Data Security
id	UserRoleDataAssignmentId
userName	UserName
roleNameCr	RoleNameCr
securityContext	SecurityContext
securityContextValue	SecurityContextValue
active	ActiveFlag
meta.Created	CreationDate
Meta.LastModified	LastUpdateDate

Steps to sync the roles in OracleFusionCloud

User and Employee Objects are available and synced by default, but not Roles. To sync Roles, follow the below steps:

1. Log in to the instance.
2. Navigate to: **My Enterprise** > **Setup and Maintenance** > **Initial Users** > **Run User and Roles Synchronization process**.

OneIM E2E Integration Needs

The OracleFusionCloud connector has Employees endpoints along with Users and Roles which is different when compared to the other Starling connectors. None of the existing OneIM Synchronization templates available for SCIM Connector or CHS modules template work with OracleFusionCloud connector.

Here is more explanation on the same:

- The regular "SCIM Synchronization" and "One Identity Starling Connect Synchronization" template cannot be used while the synchronization project is created since the addition endpoint Employees is there along with Users and Roles.
- The "One Identity Starling Connect HR" template cannot be used because there are no costcenter and location endpoint available in OracleFusionCloud, is mandatory for the One Identity Starling Connect HR template to be used.

Recommended Approach

- Use a blank project template and the do the manual mappings.

Connector Limitations

- List response of users would be relatively slow as the connector makes additional requests to exclude the system users and reserved users since these users are not retrievable using GET request but are retrievable in LIST request.
- Update Employee will only done when values for some attributes (LastName , LegislationCode , EmailType, EmailAddress, PhoneType, PhoneNumber, AddressType, Country, CountryOfBirth) are provided , otherwise it will take the existing value.

66

Majesco

Majesco is the leading software partner to both the P&C and L&A insurance markets for modernization and optimization of their businesses.

Supervisor configuration parameters

To configure the connector, following parameters are required:

- Connector name
- Client Id for the API client
- Client Secret for the API client
- Customer Key
- Target URL (https://instance_name.majesco.com)
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details)

Supported objects and operations

Users

Table 374: Supported operations for Users

Operation	VERB
Create User	POST
Get User by Id	GET
List Users	GET
Update User	PUT

Roles

Table 375: Supported operations for Roles

Operation	VERB
Get Role by Id	GET
Create Roles	POST
List Roles	GET
Update Role	PUT

Mandatory fields

Users

- userName
- displayName
- emails[].value

Roles

- name

User and Role mapping

The user mappings are listed in the tables below.

Table 376: User mapping

SCIM User	Majesco User
Id	id
userName	userid
name.Formatted	name

SCIM User	Majesco User
displayName	name
active	status
emails[].value	email
extension.customerCode	customercode
phoneNumbers[].value	phoneno
extension.domain	domain
extension.isExternalUser	isexternaluser
extension.isServiceUser	isserviceuser
extension.isUnlock	isunlock
extension.linkedUserId	linkeduserid
extension.sourceIdentityStoreName	sourceidentitystorename
extension.suspended	suspended
meta.Created	createdate
meta.LastModified	modifieddate
roles[].value	userRoles[].id
roles[].display	userRoles[].rolename
extension.applications	userRoles[].rolename

Table 377: Role mapping

SCIM Role	Majesco Role
Id	id
name	rolename
roleType	roletype
description	roledescription
parentRoles[].value	parentroleslist[].id
parentRoles[].display	parentroleslist[].rolename
childRoles[].value	childroleslist[].id
childRoles[].display	childroleslist[].rolename
meta.Created	createddate
meta.LastModified	modifieddate

SCIM Role	Majesco Role
members[].value	roleMembers[].id
members[].display	roleMembers[].name

Connector limitations

- Unless modified explicitly, the User resource will not have lastModified value under meta.
- Due to target behavior, it is not possible to disassociate parent roles from a role, however, more roles can be assigned as parent roles.
- DELETE is not supported in the connector, instead UPDATE can be used for inactivating a user. Delete is not supported because the inactivated user at target is still returned in the LIST APIs, which would make data inconsistent at the SCIM client.
- The assignment operations under roles or users would consider only integer valued data due to target API behavior.
- Target API follows PUT REPLACE for update, and hence attributes not passed will get removed from the resource.
- Due to the target behavior, it is not possible to remove all roles associated with a user as well as to remove all users under a role.

67

LuccaHR

LuccaHR provides solutions to optimize administrative and HR processes.

Supervisor configuration parameters

To configure the connector, following parameters are required:

- Connector name
- API Key
- Target URL (https://{instance}.ilucca-demo.net/)

Supported objects and operations

Users

Table 378: Supported operations for Users

Operation	VERB
Create User	POST
Get a user	GET
List Users	GET
Update a user	PUT

Departments

Table 379: Supported operations for Departments

Operation	VERB
Create a department	POST
Delete a department	DELETE
Get a department	GET
List department	GET
Update a department	PUT

Mandatory fields

Users

- name.firstName
- name.lastName
- userName
- email.value
- extension.legalEntityId
- extension. departmentId

Departments

- name

User and Department mapping

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

Table 380: User mapping

SCIM parameter	LuccaHR parameter
displayName	displayName
Emails.Value	mail
Extension.birthDate	birthDate
Extension.contractEnd	dtContractEnd
Extension.contractStart	dtContractStart
Extension.department.name	department.name
Extension.department.value	departmentID
Extension.employeeNumber	employeeNumber
Extension.gender	gender
Extension.legalEntity.name	legalEntity.name
Extension.legalEntity.value	legalEntityID
Extension.manager.name	manager.name
Extension.Manager.Value	managerID
Extension.rolePrincipal.name	rolePrincipal.name
Extension.rolePrincipal.value	rolePrincipalId
Id	id
meta.Created	createdOn
meta.LastModified	modifiedOn
Name.FamilyName	lastName
Name.Formatted	name
Name.GivenName	firstName
Roles[].display	habilitedRoles[].name
Roles[].value	habilitedRoles[].id
Title	jobTitle
UserName	login

Table 381: Department mapping

SCIM parameter	LuccaHR parameter
id	id
name	name
code	code
Active	isActive
head.value	headID
head.name	head.name
members[].value	users[].id
members[].display	users[].name
meta.Created	createdOn
meta.LastModified	modifiedOn

Connector limitations

- A user once created cannot be deleted, but it can be terminated using the PUT API.
- Multiple departments with same name can be created.
- Departments with one or more active users cannot be deleted.

68

OpenText

OpenText provides a complete and integrated Information Management platform, allowing companies to organize, integrate and protect data and content as it flows through business processes inside and outside the organization.

Supervisor configuration parameters

To configure the connector, following parameters are required:

- Connector name
- Client Id
- Client Secret
- Directory Id
- Target URL (https://<instance>.opentext.com)
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details)

Supported objects and operations

Users

Table 382: Supported operations for Users

Operation	VERB
Create User	POST
Get a user	GET

Operation	VERB
Update a user	PUT
Get all Users	GET
Delete a User	DELETE

Group

Table 383: Supported operations for Groups

Operation	VERB
Create Group	POST
Get a Group	DELETE
Get all Group	GET
Update a Group	PUT
Delete a Group	DELETE

Mandatory fields

Users

- userName

Groups

- displayName

User and Groups mapping

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

Table 384: User mapping

SCIM User	OpenText User
id	id
externalId	externalId
userName	userName
name.givenName	name.givenName
name.formatted	name.formatted
name.familyName	name.familyName
displayName	displayName
title	title
userType	userType
locale	locale
timezone	timezone
preferredLanguage	preferredLanguage
emails[].value	emails[].value
emails[].type	emails[].type
phoneNumbers[].value	phoneNumbers[].value
phoneNumbers[].type	phoneNumbers[].type
addresses[].formatted	addresses[].formatted
addresses[].streetAddress	addresses[].streetAddress
addresses[].locality	addresses[].locality
addresses[].region	addresses[].region
addresses[].postalCode	addresses[].postalCode
addresses[].country	addresses[].country
addresses[].type	addresses[].type
userExtension.employeeNumber	userExtension.employeeNumber
userExtension.costCenter	userExtension.costCenter
userExtension.organization	userExtension.organization
userExtension.division	userExtension.division
userExtension.department	userExtension.department

SCIM User	OpenText User
userExtension.manager.value	userExtension.manager.value
userExtension.manager.location	userExtension.manager.$ref
password	password
active	active
meta.created	meta.created
meta.lastModified	meta.lastModified

Table 385: Group mapping

SCIM Group	OpenText Group
id	id
displayName	displayName
GroupExtension.externalId	externalId
GroupExtension.emails[].value	emails[].value
GroupExtension.emails[].type	emails[].type
members[].value	members[].value
members[].type	members[].type
members[].display	members[].display
meta.created	meta.created
meta.lastModified	meta.lastModified

Connector limitations

- Most of the attributes like phoneNumber, addresses, preferredLanguage, timezone, locale takes any junk value due to target API behavior.

69

JFrog Artifactory

JFrog Artifactory is the single solution for housing and managing all the artifacts, binaries, packages, files, containers, and components for use throughout your software supply chain. JFrog Artifactory serves as your central hub for DevOps, integrating with your tools and processes to improve automation, increase integrity, and incorporate best practices along the way.

Supervisor Configuration Parameters

- Connector name
- User Name
- Password
- Target URL (https://<Artifactory_Server_HostName.jfrog.io/artifactory/)

Supported objects and operations

Users

Table 386: Supported operations for Users

Operation	VERB
Create User	POST
Get User by Id	GET
List Users	GET
Update user	PUT
Delete user	DELETE

Groups

Table 387: Supported operations for Groups

Operation	VERB
Create a group	POST
Delete a group	DELETE
Get Group by Id	GET
List groups	GET
Update Group	PUT

Mandatory Fields

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

Users

- userName
- emails[].value
- password

Groups

- displayName

Mappings

The mappings are listed in the tables below.

Table 388: JFrog Artifactory User to SCIM user mapping

JFrog Artifactory properties	SCIM properties
name	id
name	UserName
group	groups[].value
realm	extension.realm
status	active
email	emails[].value

Table 389: JFrog Artifactory Group to SCIM group mapping

JFrog Artifactory properties	SCIM Properties
name	id
name	displayName
usernames[]	members[]
description	extension.description
realm	extension.realm

Connector limitations

- Pagination is not supported in both users and groups endpoints.
- When list of users or groups are retrieved from connector we get limited number of attributes, so not all the attributes in get user by id is supported in get a list of users. Only id, userName, realm, meta are supported in list of users and id, displayName, meta are supported in list of groups, this is because the target system also return limited number of attributes.
- The resources do not have the important meta informations created date and lastModified date.

70

xMatters

xMatters is a service reliability platform that helps DevOps, SRES, and operations teams automate workflows, ensure infrastructure and applications are always working, and rapidly deliver products at scale. Our code-free workflow builder, adaptive approach to incident management, and real-time performance analytics all support a single goal: the happiness of your customers.

Supervisor Configuration Parameters

- Connector name
- User Name
- Password
- Target URL(https://{organization}.xmatters.com/api/xm/1)
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details).

Supported objects and operations

Users

Table 390: Supported operations for Users

Operation	VERB
Create	POST
Get User by Id	GET

Operation	VERB
List Users	GET
Update user	PUT
Delete user	DELETE

Groups

Table 391: Supported operations for Groups

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

Roles

Table 392: Supported operations for Roles

Operation	VERB
Get Role By Id	GET
List Roles	GET

Mandatory Fields

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

Users

- userName
- name.familyName

- name.givenName
- roles[].value

Groups

- displayName

Mappings

The mappings are listed in the tables below.

Table 393: xMatters User to SCIM user mapping

xMatters properties	SCIM properties
id	id
links.self	profileUrl
targetName	userName
firstName	name.givenName
firstName lastName	name.formatted
lastName	name.familyName
firstName lastName	displayName
roles[].name	roles[].display
status	active
recipentType	userType
timezone	timezone
language	preferredLanguage
whenCreated	meta.created
whenUpdated	meta.lastModified

Table 394: xMatters Group to SCIM group mapping

xMatters properties	SCIM Properties
id	id

xMatters properties	SCIM Properties
targetName	displayName
status	extension.active
description	extension.description
members[].id	members[].value
createTime	meta.created
members[].targetName	members[].display

Table 395: xMatters Role to SCIM role mapping

xMatters properties	SCIM Properties
id	id
name	role[].name

Connector limitations

- List Groups do not support the members Attribute in query attributes.
- Roles do not support query attribute feature.
- If invalid Id value is used while deleting Users and Groups, the response has status code 204 due to target behavior.

71

Discourse

Discourse is the 100% open source discussion platform built for the next decade of the Internet. Use it as a mailing list, discussion forum, long-form chat room, and more! Discourse is a from-scratch reboot, an attempt to reimagine what a modern Internet discussion forum should be today, in a world of ubiquitous smartphones, tablets, Facebook, and Twitter.

Supervisor Configuration Parameters

- Connector name
- Api Key
- Target URL (https://instance_name.discourse.group)
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details).

Supported objects and operations

Users

Table 396: Supported operations for Users

Operation	VERB
Create User	POST
Get User by Id	GET
List Users	GET

Operation	VERB
Update user	PUT
Delete user	DELETE

Groups

Table 397: Supported operations for Groups

Operation	VERB
Create a group	POST
Delete a group	DELETE
Get Group by Id	GET
List groups	GET
Update Group	PUT

Mandatory Fields

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

Users

- userName
- emails[].value
- displayName
- password

Groups

- displayName

Mappings

The mappings are listed in the tables below.

Table 398: Discourse User to SCIM user mapping

Discourse properties	SCIM properties
id	id
username	UserName
name	displayName
active	active
admin	extension.admin
created_at	meta.Created
name	name.formatted
emails	emails[].value

Table 399: Discourse Group to SCIM group mapping

Discourse properties	SCIM Properties
name	id
name	displayName
members[].id	members[].value

Connector limitations

- Discourse Target System does not return important meta information lastModified for users and created and lastModified for groups.
- In pagination, the records can be returned in multiples of 100 only.
- Modifying the displayName of a group would change its id.
- Specifying the attribute 'members' in Groups LIST will not return the members as getting the members would slow down the LIST request processing as there would be as many number of additional membership requests as the number of groups in the list response are needed due to a target API behavior.
- StartIndex value is ignored in this connector due to the target API behavior (page based).

- Without passing anything in update request body, the update API runs and give the old data.
- In Users/Get user by id, target behaviour which ignores some characters from id. "1cc1" is considered as "1" itself.
- While giving invalid API key, target gives 404 (not found) instead of 401 (unauthorized).

72

Testrail

TestRail is a web-based test case management tool. It is used by QA engineers, developers, and team leads to manage, track, and organize software testing efforts. TestRail allows team members to design test cases, organize test suites, execute test runs, and track their results, all from a modern and easy-to-use web interface. This article will give you an overview of the core features and workflows in TestRail that you can use to streamline your testing and deliver high-quality releases.

Supervisor Configuration Parameters

- Connector name
- User Name
- Password
- Target URL (https://instance_name.testrail.io)

Supported objects and operations

Users

Table 400: Supported operations for Users

Operation	VERB
Create User	POST
Get User by Id	GET
List Users	GET
Update user	PUT

Groups

Table 401: Supported operations for Groups

Operation	VERB
Create a group	POST
Delete a group	DELETE
Get Group by Id	GET
List groups	GET
Update Group	PUT

Mandatory Fields

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

Users

- userName
- emails[].value

Groups

- displayName

Mappings

The mappings are listed in the tables below.

Table 402: TestRail User to SCIM user mapping

TestRail properties	SCIM properties
id	id

TestRail properties	SCIM properties
name	UserName
group_ids	groups
is_admin	extension.admin
is_active	active
email	emails[].value

Table 403: TestRail Group to SCIM group mapping

TestRail properties	SCIM Properties
id	id
name	displayName
user_ids	members[].value

Connector limitations

- Deleting of User is not supported.

73

ChipSoft

ChipSoft contributes to greater patient safety and more efficiency by develops cutting-edge software for healthcare professionals.

Offering fully integrated EMR/EHR solution for both individual organisations as well as organisations operating within the entire chain of care, ChipSoft is the market leader in Netherlands and in expansion across Europe.

Supervisor Configuration Parameters

- Connector name
- Target URL

Supported objects and operations

Users

Table 404: Supported operations for Users

Operation	VERB
Create User	POST
Get User by Id	GET
List Users	GET
Update user	PUT

Login Groups

Table 405: Supported operations for Login Groups

Operation	VERB
Get Login Group by Id	GET
List users	GET

User Groups

Table 406: Supported operations for User Groups

Operation	VERB
Get User Group by Id	GET
List User Groups	GET

Mandatory Fields

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

Users

- ldap
- userName
- displayName
- active
- startDate
- endDate

Mappings

The mappings are listed in the tables below.

Table 407: ChipSoft to SCIM user mapping

ChipSoft properties (Dutch and English)	SCIM properties
Ldap	ldap
Ldapdomain	ldapDomain
Gebruikersnaam	id or userName
Gebruikersomschrijving	displayName
Geblokkeerd	active
Startdate	startDate
Enddate	endDate
Afdeling	department
Functie	position
Soort	kind
Uzinr	uzinNo
Rolecode	roles { value = RoleCode display = RoleCode type = blankValue }
Bedrijf	company
Email	emails { value = emailValue, primary = 'true, type = 'work' }
Laatsteinlogdatum	lastLoginDate
Laatsteinlogtijdstip	lastLoginTime
Login Groups	
Inloggroepcode	value
Inloggroepzoekcode	searchCode
User Group	
Groepcode	value
Zoekcode	searchCode

Table 408: ChipSoft to SCIM user group mapping

ChipSoft properties (Dutch and English)	SCIM Properties
groepcode	id

ChipSoft properties (Dutch and English)	SCIM Properties
zoekcode	searchCode
groepomschrijving	displayName
soortcode	typeCode
soortomschrijving	speciesDescription

Table 409: ChipSoft to SCIM login group mapping

ChipSoft properties (Dutch and English)	SCIM Properties
inloggroepcode	id
inloggroepzoekcode	searchCode
inloggroepomschrijving	displayName
inloggroepactief	active

Connector limitations

Due to target behavior, following has been observed:

- User Groups and Login Groups result don't support pagination.
- Memberships are not managed under Groups. Instead Groups are managed under Users.
- For any junk value in cursor, it fetches records from target. It returns last login date as "0001-01-01T00:00:00Z" and time "12:00:00" for some of the records.
- Email is not available for any user, target also does not accept new user with email.
- Delete is not available for any user.
- Some of the fields are not created during create user request.
- System throws an error when it is trying to create an existing user. It displays the value of "ldap" in error description instead of "userName".
- userName (Gebruikersnaam) fields only accept 8 characters. Any string more than 8 characters will be truncated and only first 8 characters are saved.

74

PingOne Platform

PingOne is a cloud-based identity as a service (IDaaS) framework for secure identity access management that uses an organization based model to define tenant accounts and their related entities within the PingOne platform.

Supervisor configuration parameters

To configure the connector, following parameters are required:

- PingOne Platform
- Client Id of the API client
- Client Secret of the API client
- Environment Id
- Target URL (https://api.pingone.{instance_region})
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details)

Supported objects and operations

Users

Table 410: Supported operations for Users

Operation	VERB
Create User	POST
Get User by Id	GET

Operation	VERB
List Users	GET
Update User	PUT
Delete User	DELETE

Groups

Table 411: Supported operations for Groups

Create Group	POST
Get Group	GET
Get Groups	GET
Update Group	PUT

Populations

Table 412: Supported operations for Populations

Get Populations by Id	GET
List Populations	GET

Mandatory fields

Users

- userName
- population

Groups

displayName

User mapping

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

Table 413: User mapping

SCIM Parameter	PingOne Parameter
id	id
userName	username
name.givenName	name.given
name.middleName	name.middle
name.formatted	name.formatted
name.honorificSuffix	name.honorificSuffix
name.honorificPrefix	name.honorificPrefix
title	title
displayName	name.given name.family
emails[].value	email
active	enabled
locale	locale
preferredLanguage	preferredLanguage
timezone	timezone
groups[].value	memberOfGroupIDs
externalId	externalId
userType	type
nickName	nickname
photos[].value	photo.href
addresses[].streetAddress	address.streetAddress
addresses[].region	address.region
addresses[].locality	address.locality
addresses[].countryCode	address.country
addresses[].postalCode	address.postalCode
phoneNumbers[].value	primaryPhone

SCIM Parameter	PingOne Parameter
phoneNumbers[].Value	mobilePhone
enterpriseExtension.accountId	accountId
enterpriseExtension.population	population.id
enterpriseExtension.environment	environment.id
enterpriseExtension.identityProvider	identityProvider.type
enterpriseExtension.mfaEnabled	mfaEnabled
createdAt	meta.created
updatedAt	meta.lastModified

Groups

Table 414: Group mapping

SCIM parameter	PingOne parameter
id	id
displayName	name
members[].value	members[].id
externalId	externalId
enterpriseExtension.population	population.id
enterpriseExtension.description	description
enterpriseExtension.environment	environment.id
enterpriseExtension.checkSum	checkSum
enterpriseExtension.customData.securityGroup	customData.securityGroup
enterpriseExtension.customData.groupOwner	customData.groupOwner
meta.lastModified	updatedAt
meta.created	createdAt

Population mapping

Table 415: Population mapping

SCIM Parameter	PingOne Parameter
id	id
displayName	name
userCount	userCount
description	description
environment	environment.id
passwordPolicy	passwordPolicy.id
isDefault	default
updatedAt	meta.lastModified
createdAt	meta.created

Connector SCIM configuration

The PingOne Platform connector is enhanced to support the configuration of SCIM connector with custom attributes and disabling of attributes. 'Users' resources in PingOne Platform connector have the support for configuring custom attributes and disabling of attributes.

NOTE:

- In connector schema, datatype corresponding to multivalued custom attribute is of type string and JSON only.
- Connector output format for multivalued custom attributes will be as shown below:

  ```
  "MultivaluedAttributeName" : "[abcd;; efgh;; xyzw;; uvty]"
  ```

- As per the connector output format, the values will be double semicolon separated (;;) and will be enclosed inside opening and closing square brackets.
- Opening and closing square brackets helps to ensure that the attribute is of multivalued type.

Connector limitations

- In pagination, records are returned in multiples of 100 only due to target behaviour.
- Custom attributes and disabling attributes are only supported in users due to target behaviour.
- Custom attributes are supported for string and JSON attributes due to target behaviour.
- While updating a group that was created at the population level, it should contain the same population id in the update body that was given while creating the group, while groups created at the environment level should not contain the population attribute in the update body due to target behaviour, else the target will throw the error message.

75

Azure DevOps

Azure DevOps is methodology that supports cohesiveness between development and operations into a smooth sailing event allowing organizations to create and improve products at a faster pace than they can with traditional software development approaches.

Supervisor configuration parameters

To configure the connector, following parameters are required.

- Connector name
- PAT (Personal Access Token)

  NOTE: For more information related to generating a PAT, see Retrieving Personal Access Token.
- Target URL (https://vsaex.dev.azure.com/{ORGANIZATION_NAME})
- Project Target URL (https://dev.azure.com/{ORGANIZATION_NAME})
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details).

Supported objects and operations

Users

Table 416: Supported operations for Users (for v1.0 & v2.0)

Operation	VERB
Create User	POST

Operation	VERB
Get User by Id	GET
List Users	GET
Update User	PUT
Delete User	DELETE

Groups

Table 417: Supported operations for Groups (for v1.0 & v2.0)

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

Projects

Table 418: Supported operations for Projects (for v1.0 & v2.0)

Operation	VERB
Create Project	POST
Get Project by Id	GET
List Projects	GET
Update Project	PUT
Delete Project	DELETE

Mandatory fields

This section lists the mandatory field required to CREATE a user.

Users (for v1.0 & v2.0)

- userName

Groups (for v1.0 & v2.0)

- displayName
- enterpriseExtension.licenseRule.accountLicenseType
- enterpriseExtension.licenseRule.licensingSource
- enterpriseExtension.licenseRule.msdnLicenseType

Projects (for v1.0 & v2.0)

- displayName
- capabilities.processTemplateTypeId
- capabilities.versionSourceControlType

Attributes Mappings

Different mappings associated with this connector are listed in the tables below.

Table 419: User mapping (for v1.0)

SCIM User	Azure DevOps Parameter
id	id
userName	user.principalName
displayName	user.displayName
emails[].value	user.mailAddress
enterpriseExtension.accessLevel.licensingSource	accessLevel.licensingSource
enterpriseExtension.accessLevel.accountLicenseType	accessLevel.accountLicenseType
enterpriseExtension.accessLevel.msdnLicenseType	accessLevel.msdnLicenseType
enter-	accessLevel.licenseDisplayName

SCIM User	Azure DevOps Parameter
priseExtension.accessLevel.licenseDisplayName	
enterpriseExtension.accessLevel.status	accessLevel.status
enterpriseExtension.accessLevel.statusMessage	accessLevel.statusMessage
enterpriseExtension.accessLevel.assignmentSource	accessLevel.assignmentSource
enterpriseExtension.originId	user.originId
enterpriseExtension.origin	user.origin
enterpriseExtension.descriptor	user.descriptor
enterpriseExtension.subjectKind	user.subjectKind
enterpriseExtension.metaType	user.metaType
enterpriseExtension.domain	user.domain
enterpriseExtension.directoryAlias	user.directoryAlias
enterpriseExtension.projectEntitlements[].assignmentSource	projectEntitlements[].assignmentSource
enterpriseExtension.projectEntitlements[].isProjectPermissionInherited	projectEntitlements[].projectPermissionInherited
enterpriseExtension.projectEntitlements[].projectRefId	projectEntitlements[].projectRef.id
enterpriseExtension.projectEntitlements[].projectRefName	projectEntitlements[].projectRef.name
enterpriseExtension.projectEntitlements[].projectGroupType	projectEntitlements[].group.groupType
enterpriseExtension.projectEntitlements[].projectGroupDisplayName	projectEntitlements[].group.displayName
enterpriseExtension.groupAssignments[].groupId	groupAssignments[].id
enterpriseExtension.groupAssignments[].groupDescription	groupAssignments[].group.description
enterpriseExtension.groupAssignments[].groupDescriptor	groupAssignments[].group.descriptor
enterpriseExtension.groupAssignments[].groupDisplayName	groupAssignments[].group.displayName
enterpriseExtension.groupAssignments[].groupDomain	groupAssignments[].group.domain
enterpriseExtension.groupAssignments	groupAssignments[].group.-

SCIM User	Azure DevOps Parameter
[].groupMailAddress	mailAddress
enterpriseExtension.groupAssignments[].groupOrigin	groupAssignments[].group.origin
enterpriseExtension.groupAssignments[].groupOriginId	groupAssignments[].group.originId
enterpriseExtension.groupAssignments[].groupPrincipalName	groupAssignments[].group.principalName
enterpriseExtension.groupAssignments[].groupSubjectkind	groupAssignments[].group.subjectKind
enterpriseExtension.groupAssignments[].status	groupAssignments[].status
enterpriseExtension.groupAssignments[].groupLicensingSource	groupAssignments[].licenseRule.licensingSource
enterpriseExtension.groupAssignments[].groupAccountLicenseType	groupAssignments[].licenseRule.accountLicenseType
enterpriseExtension.groupAssignments[].groupMsdnLicenseType	groupAssignments[].licenseRule.msdnLicenseType
enterpriseExtension.groupAssignments[].groupLicenseDisplayName	groupAssignments[].licenseRule.licenseDisplayName
enterpriseExtension.groupAssignments[].groupLicensingRuleStatus	groupAssignments[].licenseRule.status
enterpriseExtension.groupAssignments[].groupLicensingRuleStatusMessage	groupAssignments[].licenseRule.statusMessage
enterpriseExtension.groupAssignments[].groupLicensingRuleAssignmentSource	groupAssignments[].licenseRuleAssignmentSource
meta.created	dateCreated

Table 420: User mapping (for v2.0)

SCIM User	Azure DevOps Parameter
id	user.descriptor
userName	user.principalName
displayName	user.displayName
emails[].value	user.mailAddress
enterpriseExtension.originId	user.originId
enterpriseExtension.origin	user.origin

SCIM User	Azure DevOps Parameter
enterpriseExtension.subjectKind	user.subjectKind
enterpriseExtension.metaType	user.metaType
enterpriseExtension.domain	user.domain
enterpriseExtension.directoryAlias	user.directoryAlias
enterpriseExtension.projectEntitlements[].assignmentSource	projectEntitlements[].assignmentSource
enterpriseExtension.projectEntitlements[].isProjectPermissionInherited	projectEntitlements[].projectPermissionInherited
enterpriseExtension.projectEntitlements[].projectRefId	projectEntitlements[].projectRef.id
enterpriseExtension.projectEntitlements[].projectRefName	projectEntitlements[].projectRef.name
enterpriseExtension.projectEntitlements[].projectGroupType	projectEntitlements[].group.groupType
enterpriseExtension.projectEntitlements[].projectGroupDisplayName	projectEntitlements[].group.displayName
enterpriseExtension.accessLevel.licensingSource	accessLevel.licensingSource
enterpriseExtension.accessLevel.accountLicenseType	accessLevel.accountLicenseType
enterpriseExtension.accessLevel.msdnLicenseType	accessLevel.msdnLicenseType
enterpriseExtension.accessLevel.licenseDisplayName	accessLevel.licenseDisplayName
enterpriseExtension.accessLevel.status	accessLevel.status
enterpriseExtension.accessLevel.statusMessage	accessLevel.statusMessage
enterpriseExtension.accessLevel.assignmentSource	accessLevel.assignmentSource

Table 421: Group mapping (for v1.0)

SCIM Group	Azure DevOps Parameter
id	id
displayName	group.displayName
members[].value	members[].id
enterpriseExtension.licenseRule.licensingSource	licenseRule.licensingSource
enterpriseExtension.licenseRule.accountLicenseType	licenseRule.accountLicenseType
enterpriseExtension.licenseRule.msdnLicenseType	licenseRule.msdnLicenseType

SCIM Group	Azure DevOps Parameter
enterpriseExtension.licenseRule.licenseDisplayName	licenseRule.licenseDisplayName
enterpriseExtension.licenseRule.status	licenseRule.status
enterpriseExtension.licenseRule.statusMessage	licenseRule.statusMessage
enterpriseExtension.licenseRule.assignmentSource	licenseRule.assignmentSource
enterpriseExtension.originId	group.originId
enterpriseExtension.origin	group.origin
enterpriseExtension.descriptor	group.descriptor
enterpriseExtension.subjectKind	group.subjectKind
enterpriseExtension.description	group.description
enterpriseExtension.domain	group.domain
enterpriseExtension.status	group.status
enterpriseExtension.principalName	group.principalName
enterpriseExtension.projectEntitlements[].assignmentSource	projectEntitlements[].assignmentSource
enterpriseExtension.projectEntitlements[].isProjectPermissionInherited	projectEntitlements[].projectPermissionInherited
enterpriseExtension.projectEntitlements[].projectRefId	projectEntitlements[].projectRef.id
enterpriseExtension.projectEntitlements[].projectRefName	projectEntitlements[].projectRef.name
enterpriseExtension.projectEntitlements[].projectGroupType	projectEntitlements[].group.groupType
enterpriseExtension.projectEntitlements[].projectGroupDisplayName	projectEntitlements[].group.displayName

Table 422: Group mapping (for v2.0)

SCIM Group	Azure DevOps Parameter
id	group.descriptor
displayName	group.displayName
members[].value	members[].id
enterpriseExtension.licenseRule.licensingSource	licenseRule.licensingSource
enterpriseExtension.licenseRule.accountLicenseType	licenseRule.accountLicenseType

SCIM Group	Azure DevOps Parameter
enterpriseExtension.licenseRule.msdnLicenseType	licenseRule.msdnLicenseType
enterpriseExtension.licenseRule.licenseDisplayName	licenseRule.licenseDisplayName
enterpriseExtension.licenseRule.status	licenseRule.status
enterpriseExtension.licenseRule.statusMessage	licenseRule.statusMessage
enterpriseExtension.licenseRule.assignmentSource	licenseRule.assignmentSource
enterpriseExtension.originId	group.originId
enterpriseExtension.origin	group.origin
enterpriseExtension.subjectKind	group.subjectKind
enterpriseExtension.description	group.description
enterpriseExtension.domain	group.domain
enterpriseExtension.status	group.status
enterpriseExtension.principalName	group.principalName
enterpriseExtension.projectEntitlements[].assignmentSource	projectEntitlements[].assignmentSource
enterpriseExtension.projectEntitlements[].isProjectPermissionInherited	projectEntitlements[].projectPermissionInherited
enterpriseExtension.projectEntitlements[].projectRefId	projectEntitlements[].projectRef.id
enterpriseExtension.projectEntitlements[].projectRefName	projectEntitlements[].projectRef.name
enterpriseExtension.projectEntitlements[].projectGroupType	projectEntitlements[].group.groupType
enterpriseExtension.projectEntitlements[].projectGroupDisplayName	projectEntitlements[].group.displayName

Table 423: Projects mapping (for v1.0 & v2.0)

SCIM Projects	Azure DevOps Parameter
id	id
displayName	name
description	description
state	state
visibility	visibility

SCIM Projects	Azure DevOps Parameter
revision	revision
capabilities.processTemplateName	capabilities.processTemplate.templateName
capabilities.processTemplateTypeId	capabilities.processTemplate.templateTypeId
capabilities.versionSourceControlType	capabilities.versioncontrol.sourceControlType
capabilities.versionControlGitEnabled	capabilities.versioncontrol.gitEnabled
capabilities.versionControlTfvcEnabled	capabilities.versioncontrol.tfvcEnabled
defaultTeam.id	defaultTeam.id
defaultTeam.name	defaultTeam.name
meta.lastModified	lastUpdatedTime

Connector limitations

- The userName should be in the format of the email address (The email address of the user which has to be added to the organization).
- If we use the username that is already existing, the system will not throw a conflict error; instead, it will update that user or return the existing data.
- Extensions[] are not mapped because the data is not returning from the target in response.
- If we add a user that already exists in the organisation but is deleted, that user will have the same user ID as it had previously.
- Only one email per user is supported by target system.
- Azure DevOps Target System does not return important meta information lastModified for users, lastModified & created for groups and created for projects.
- At least one writable attribute should be provided while updating a user, group and project.
- Projects and access levels added indirectly when groups are associated for users are not updatable.
- Providing an already used display name to a group will return error even though the old group is deleted in target instance.
- The create or update of a group will be successful even though the target API fails with errors during the membership management operations on the group. This is because the create or update of a group in connector internally handles create/update and membership management.
- Adding a project with different group types is not supported currently.

- Pagination in users and projects returns records in multiples of 100.
- Pagination is not supported in groups.

76

UKG PRO

UKG PRO is a comprehensive HRMS that allows the organizations to efficiently manage the personnel data, handle robust payroll tasks, boost scheduling efficiency, and attract, nurture, and grow talent.

Supervisor configuration parameters

To configure the connector, following parameters are required.

- Connector name
- Login Username
- Login Password
- User API Key for web services
- Customer API Key for web services
- Target URL (https://{service_name}.ultipro.com)
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details)

> NOTE:
>
> Retrieving credentials to generate token:
>
> 1. Login to Pro portal
> 2. Access Web Services under System Configuration > Security
> 3. Note the "User API Key", "Customer API Key" and base URL of the web services listed

Supported objects and operations

Employees

Table 424: Supported operations for Employee

Operation	VERB
Get Employee by Id	GET
List Employees	GET

EmpJobs

Table 425: Supported operations for EmpJobs

Operation	VERB
Get EmpJob by Id	GET
List EmpJobs	GET

EmpEmployments

Table 426: Supported operations for EmpEmployments

Operation	VERB
Get EmpEmployment by Id	GET
List Employments	GET

Attributes Mappings

Different mappings associated with this connector are listed in the tables below.

Table 427: Employee mapping

SCIM Properties	SCIM UKG Pro Employee Properties
id	Person/EmployeeIdentifier/EmployeeNumber/text

SCIM Properties	SCIM UKG Pro Employee Properties
	(), Person/EmployeeIdentifier/CompanyCode/text()
userName	Person/EmployeeIdentifier/EmployeeNumber/text()
name.familyName	Person/LastName/Text()
name.givenName	Person/FirstName/Text()
name.middleName	Person/MiddleName/Text()
name.honorificPrefix	Person/Prefix/Text()
name.honorificSuffix	Person/Suffix/Text()
name.preferredFirstName	Person/PreferredFirstName/Text()
name.formerLastName	Person/FormerLastName/Text()
emails.email	Person/EmailAddress/Text()
emails.alternateEmail	Person/AlternateEmailAddress/Text()
companyCode	Person/EmployeeIdentifier/CompanyCode/text()
ssn	Person/SSN/Text()
supressSsn	Person/SuppressSSN/Text()

Table 428: EmpJob mappings

SCIM Properties	SCIM UKG Pro EmpJob Properties
id	Job/EmployeeIdentifier/EmployeeNumber/text (),Job/EmployeeIdentifier/CompanyCode/text()
agricultural	Job/Agricultural/text()
alternateTitle	Job/AlternateTitle/text()
dateInJob	Job/DateInJob/text()
directLabor	Job/DirectLabor/text()
effectiveDate	Job/EffectiveDate/text()
companyCode	Job/EmployeeIdentifier/CompanyCode/text()
employeeNumber	Job/EmployeeIdentifier/EmployeeNumber/text()
employeeType	Job/EmployeeType/text()
fullOrPartTime	Job/FullOrPartTime/text()
hourlyOrSalaried	Job/HourlyOrSalaried/text()
jobCode	Job/JobCode/text()
jobGroup	Job/JobGroup/text()

SCIM Properties	SCIM UKG Pro EmpJob Properties
localUnion	Job/LocalUnion/text()
nationalUnion	Job/NationalUnion/text()
orgLevel1	Job/OrgLevel1/text()
orgLevel2	Job/OrgLevel2/text()
orgLevel3	Job/OrgLevel3/text()
orgLevel4	Job/OrgLevel4/text()
payFrequency	Job/PayFrequency/text()
payGroup	Job/PayGroup/text()
payScaleCode	Job/PayScaleCode/text()
project	Job/Project/text()
promotion	Job/Promotion/text()
reasonCode	Job/ReasonCode/text()
scheduledHours	Job/ScheduledHours/text()
seasonal	Job/Seasonal/text()
shiftCode	Job/ShiftCode/text()
shiftGroup	Job/ShiftGroup/text()
stepNo	Job/StepNo/text()
supervisorCompanyCode	Job/Supervisor/CompanyCode/text()
supervisorEmployeeNumber	Job/Supervisor/EmployeeNumber/text()
timeClock	Job/TimeClock/text()
transfer	Job/Transfer/text()
youthTraining	Job/YouthTraining/text()

Table 429: EmpEmployment mappings

SCIM Properties	SCIM UKG Pro EmpEmployment Properties
id	EmploymentInformation/EmployeeIdentifier/EmployeeNumber/text(),EmploymentInformation/EmployeeIdentifier/CompanyCode/text()
arrearsSuspendedFrom	EmploymentInformation/ArrearsSuspendedFrom/text()

SCIM Properties	SCIM UKG Pro EmpEmployment Properties
arrearsSuspendedTo	EmploymentInformation/ArrearsSuspendedTo/text()
beneSeniority	EmploymentInformation/BeneSeniority/text()
deceased	EmploymentInformation/Deceased/text()
deceasedDate	EmploymentInformation/DeceasedDate/text()
earlyRetirement	EmploymentInformation/EarlyRetirement/text()
companyCode	Employ-mentInformation/EmployeeIdentifier/CompanyCode/text()
employeeNumber	Employ-mentInformation/EmployeeIdentifier/EmployeeNumber/text()
employmentStatus	EmploymentInformation/EmploymentStatus/text()
fmlaCode	EmploymentInformation/FMLA_Code/text()
hcsoEndDate	EmploymentInformation/HCSOEndDate/text()
hcsoNotCovered	EmploymentInformation/HCSONotCovered/text()
hcsoStartDate	EmploymentInformation/HCSOStartDate/text()
job	EmploymentInformation/Job/text()
jobStart	EmploymentInformation/JobStart/text()
lastHire	EmploymentInformation/LastHire/text()
lastPerfReview	EmploymentInformation/LastPerfReview/text()
lastSalaryReview	EmploymentInformation/LastSalaryReview/text()
leaveReason	EmploymentInformation/LeaveReason/text()
nextPerfReview	EmploymentInformation/NextPerfReview/text()
nextSalaryReview	EmploymentInformation/NextSalaryReview/text()
originalHire	EmploymentInformation/OriginalHire/text()
ptoSuspendedFrom	EmploymentInformation/PTOSuspendedFrom/text()
ptoSuspendedTo	EmploymentInformation/PTOSuspendedTo/text()
payAutomatically	EmploymentInformation/PayAutomatically/text()
paySuspendedFrom	EmploymentInformation/PaySuspendedFrom/text()
paySuspendedTo	EmploymentInformation/PaySuspendedTo/text()
roeIssueReason	EmploymentInformation/ROEIssueReason/text()

SCIM Properties	SCIM UKG Pro EmpEmployment Properties
regularRetirement	EmploymentInformation/RegularRetirement/text()
seniority	EmploymentInformation/Seniority/text()
statusAnticipatedEnd	EmploymentInformation/StatusAnticipatedEnd/text()
statusStartDate	EmploymentInformation/StatusStartDate/text()
weeks	EmploymentInformation/Weeks/text()

Connector SCIM configurations

While UKG Pro system does not support disabling attributes feature, the Starling Connector for UKG Pro does supports disabling attributes by removing the SCIM mapping in the object GET response.

Connector limitations

- Target APIs do not support created date and last modified date for employees.
- The target API does not exactly validate the Id, the results are returned even when some additional characters are added to the end of a valid resource Id.

77

Atlassian Cloud

Atlassian cloud lets you automate user provisioning from your identity provider to Atlassian Cloud thus ensuring a smooth provisioning/de-provisioning users and groups from an identity provider to Confluence and Jira Cloud. With this, you can write your own integration with an external identity provider using the SCIM 2.0 protocol to manage your Atlassian Cloud users and groups.

Supervisor configuration parameters

To configure the connector, the following parameters are required:

- Connector name
- API key

  NOTE: For more information related to generating an API key, see Retrieving Atlassian Cloud API Key and Directory Id.
- Directory Id

  NOTE: For more information related to generating a Directory ID, see Retrieving Atlassian Cloud API Key and Directory Id.
- Target URL (https://api.atlassian.com/)
- Instance DateTime Offset (refer Configuring additional datetime offset in connectors for more details).

Supported objects and operations

Users

Table 430: Supported operations for Users

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

Groups

Table 431: Supported operations for Groups

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

Mandatory fields

Users

- userName
- emails[].value
- emails[].primary = true

Groups

- displayName

User mapping

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

Table 432: User mapping

SCIM parameter	Atlassian Cloud parameter
id	id
userName	userName
name.formatted	name.formatted
name.givenName	name.givenName
name.familyName	name.familyName
name.middleName	name.middleName
name.honorificSuffix	name.honorificSuffix
name.honorificPrefix	name.honorificPrefix
emails[].value	emails[].value
emails[].type	emails[].type
emails[].primary	emails[].primary
phoneNumbers[].value	phoneNumbers[].value
phoneNumbers[].type	phoneNumbers[].type
phoneNumbers[].primary	phoneNumbers[].primary
active	active
externalId	externalId
timezone	timezone
title	title
preferredLanguage	preferredLanguage
nickname	nickName
displayName	displayName

SCIM parameter	Atlassian Cloud parameter
enterpriseExtension.organization	enterpriseExtension.organization
enterpriseExtension.department	enterpriseExtension.department
atlassianExtension.atlassianAccountId	enterpriseExtension.atlassianAccountId
meta.created	meta.created
meta.lastModified	meta.lastModified

Groups

Table 433: Group mapping

SCIM parameter	Atlassian Cloud parameter
id	id
displayName	displayName
externalId	externalId
members[].value	members[].value
members[].type	members[].type
members[].display	members[].display
meta.created	meta.created
meta.lastModified	meta.lastModified

Connector limitations

- While the displayName in Groups, is immutable, it is set as a readWrite attribute since it is a mandatory attribute during update.

Appendix A

Creating a service account in Google Workspace

You must obtain a JSON file with Private Key to authorize the APIs to access data on Google Workspace 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 Google workspace 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
   - https://www.googleapis.com/auth/admin.directory.group.member
   - https://www.googleapis.com/auth/admin.directory.domain
   - https://www.googleapis.com/auth/admin.directory.domain.readonly
   - https://www.googleapis.com/auth/admin.directory.rolemanagement

   For more information on API scopes, see https://developers.google.com/identity/protocols/googlescopes

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

   The unique Id and the scopes added is displayed.

Appendix B

Setting a trial account on Salesforce

To login to the Saleforce application, you must create a trial 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 trial account is created and an instance is assigned.
3. Switch the view to Saleforce 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 url text **https://app.getpostman.com/oauth2/callback** in the **Callback URL** text field.

   NOTE: This url must be used just to configure the trial account and not as a browsing link.
10. From the **Selected OAuth Scopes** drop-down menu, select **Access and manage your data(api)**.
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:

- 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.

Appendix C

Registering the application, providing necessary permissions, retrieving Client Id and Client Secret from the Azure AD tenant

This section provides the details about registering the application, providing necessary permissions, retrieving Client Id and Client Secret from the Azure AD tenant, for both single tenant and multi-tenant connector configuration.

NOTE: Safeguard for Privileged Passwords only allows for a single tenant connector configuration..

To register application, provide appropriate permissions, retrieve client ID, and client secret from the Azure AD tenant

1. Login to Azure portal and select **Azure Active Directory**.
2. Select **App registrations**.

   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**
   - **Redirect URL**: *https://connect-supervisor.cloud.oneidentity.com/v1/consent*.
4. Select the created application and click **View API Permissions**.
5. From **API permission**, add the required permissions for Microsoft Graph API (delegated and application permissions).

   The registered application must have the following permissions:

   - Directory.ReadWrite.All
   - Group.ReadWrite.All

- User.ManageIdentities. All
- User.ReadWrite.All

6. Create a user under **Azure Active Directory** and assign **Privileged role administrator** role under the user's **Assigned roles**.

   NOTE: A **Global administrator** would also be able to provide consent.

7. For the **Azure Active Directory**, assign **User administrator** role for the application created.

   NOTE: For Safeguard for Privileged Passwords, you must assign at least the **Helpdesk Administrator** role for the application created, but should assign a higher role if you want to manage special accounts (for example, **Billing Administrator** or **Global Administrator**).

   To assign **User administrator** role for the application created:

   a. Select **Roles and administrators**.

   b. Click **+ Add Assignments**, and search the name of the application created.

8. Gather the following details from the corresponding pages of the application given in the table below.

Table 434: Application details

Details	Page
Application (client) ID Azure Active Directory's **Directory (tenant) ID**	Overview
Client Secret	Certificates & secrets

More details on Azure AD

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

Table 435: More details on Azure AD

More details on Azure AD	Link
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	https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-configure-app-expose-web-apis

APIs	
To modify the accounts supported by an application	https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-modify-supported-accounts

Appendix D

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.

Appendix E

Configuring Amazon S3 AWS connector to support entitlements for User and Group

This section gives the details of the configuration changes to be made to the Amazon (S3 and AWS) connector to support entitlements for **User** and **Group**. The **Designer** tool and the **Synchronization Editor** tool are used to configure the **Amazon S3 AWS** connector to support entitlements for **User** and **Group**.

For more information, see:

Configuring Amazon S3 AWS connector to support entitlements for User

Configuring Amazon S3 AWS connector to support entitlements for Group

- Configuring Amazon S3 AWS connector to support entitlements for User
  - Viewing the default custom process for User
  - Configuring Amazon S3 AWS connector to support entitlements for User using the Synchronization Editor
- Configuring Amazon S3 AWS connector to support entitlements for Group
  - Creating a custom process for Amazon S3 AWS connector to support entitlements for Group using the Designer tool
  - Configuring Amazon S3 AWS connector to support entitlements for Group using the Synchronization Editor

Configuring Amazon S3 AWS connector to support entitlements for User

To configure the **Amazon S3 AWS** connector to support entitlements for **User**, use the **Synchronization Editor**.

For more information, see:

- Viewing the default custom process for User
- Configuring Amazon S3 AWS connector to support entitlements for User using the Synchronization Editor

Viewing the default custom process for User

To view the default custom process for User:

1. Open the **Designer** tool.
2. In the **Navigation** pane, select **Process Orchestration**| **Process**| **UCIUserHasItem**| **UCI_UCIUserHasItem_Update**.
3. In the **Tasks** pane, under the **Edit Process** option, click **Edit process**| **UCI_ UCIUserHasItem_Update**.
   The **Process properties** window is displayed.

   NOTE: Refer to the values in the **Process properties** window for **User** when you create a custom process for **Group**. For more information about how to create a custom process for **Group**, see Creating a custom process for Amazon S3 AWS connector to support entitlements for Group using the Designer tool

Configuring Amazon S3 AWS connector to support entitlements for User using the Synchronization Editor

The **Synchronization Editor** tool is used to configure the Amazon (S3 and AWS) connector to support entitlements for **User**.

To configure Amazon S3 AWS connector to support entitlements for User:

1. Open the **Synchronization Editor**.
2. Open the specific synchronization project.
3. Navigate to the **Mappings** tab and select **User**.
4. Remove **vrtEntitlements** from the One Identity Manager side in the **Mapping** window.
5. In the **Property mapping rules** section, add the new mapping rule **Value Comparison Rule**, with the value **vrtProfiles <--> Entitlements~value**.
6. Run the synchronization.

   The users and entitlements that exist on the target system instance are synchronized with One Identity Manager.

Configuring Amazon S3 AWS connector to support entitlements for Group

To configure the Amazon (S3 and AWS) connector to support entitlements for **Group**, create a custom process using the **Designer** tool and then configure the connector using the **Synchronization Editor**.

To configure the Amazon S3 AWS Connector to support entitlements for Group, do the following:

- Creating a custom process for Amazon S3 AWS connector to support entitlements for Group using the Designer tool
- Configuring Amazon S3 AWS connector to support entitlements for Group using the Synchronization Editor

Creating a custom process for Amazon S3 AWS connector to support entitlements for Group using the Designer tool

The **Designer** tool is used to create a custom process for **Group**.

NOTE: Refer to the default custom process for **User**. For more information, see Viewing the default custom process for User.

To create a custom process for Amazon S3 AWS connector to support entitlements for Group:

1. Open the **Designer** tool.
2. In the **Navigation** pane, select **Process Orchestration** |**Custom process**| **Navigation**| **Process Editor**| **Create a new process**.
   The **Process properties** window is displayed.
3. In the **General** tab, enter the following values:

Table 436: Values for creating custom process for Group

Process properties	Value
Name	UCI_UCIGroupHasItem_Update
Table	UCIGroupHasItem

Process properties	Value

Pre-script for generating	`If Not CBool(Connection.Variables("FULLSYNC")) AndAlso _`
	`Not CBool(Connection.Variables("PendingChangeReady")) AndAlso _`
	`Not $FK(UID_UCIGroup).FK(UID_UCIRoot).IsManualProvisioning:Bool$`
	`Then`
	`Imports System.Collections.Generic`
	`Dim data As IDictionary(Of String,string) = Nothing`
	`values("AdHocDataFound") = False`
	`values("NeedExecute") = true`
	`' try to get UCI data`
	`Try`
	`Dim myUCIGroup As ISingleDbObject = Connection.CreateSingle("UCIGroup",$UID_UCIGroup$)`
	`data = DPR_GetAdHocData($FK(UID_UCIGroup).FK(UID_UCIRoot).XObjectKey$,"SCIM","","Update",myUCIGroup.GetEntity())`
	`Catch ex As AdHocDataException`
	`End Try`
	`If Not data is Nothing`
	`values("AdHocDataFound") = True`
	`values("ObjectKey") = New DbObjectKey("UCIGroup",$UID_UCIGroup$).ToXmlString()`
	`values("UID_DPRSystemVariableSet") = data("VariableSetUID")`
	`values("UID_DPRProjectionConfiguration") = data("ProjectionConfigUID")`
	`values("UID_QBMServer") = data("ExecutionServerUID")`
	`End if`
	`End If`

Generating condition	`Value = Not CBool(Connection.Variables("FULLSYNC")) AndAlso _`
	`Not CBool(Connection.Variables("PendingChangeReady")) AndAlso _`
	`Not $FK(UID_UCIGroup).FK(UID_UCIRoot).IsManualProvisioning:Bool$ AndAlso _`

Process properties	Value
	`CBool(values("AdHocDataFound")) Andalso _` `UCI_TargetUsesProfiles($FK(UID_UCIGroup).UID_UCIRoot$)`

4. In the **Events** tab, at the bottom of the page, click **+**.
   The **Edit event** window is displayed.
5. In the **Edit event** window, click **+** next to the **Object Event** field.

   The **Edit object event** window is displayed.
6. In the **Edit object event**, select **Delete** and then **Insert** from the list. Click **OK**.
   The **Process step properties** window is displayed.
7. In the **Process step properties** window, select the values as follows:
   a. In the **General tab**, in the **Name** field, enter the value PUT/PATCH Group.
   b. Select **ProjectorComponent – AdHocProjectionSingle** from the **Process Task** drop down list.
   c. In the **Generation** tab, enter the script for server selection: `Value = values ("UID_QBMServer").ToString()`.
   d. In the **Error Handling** tab, select **Stop on Error**.
8. In the **Parameters** tab at the bottom, add the values for **ForceSyncOf**.
9. Set the parameter **CausingEntityPatch** to the following value:
   ```
   Dim myUCIGroup As ISingleDbObject =
   Connection.CreateSingle("UCIGroup",$UID_UCIGroup$)
   Value = DPR_WrapObjectForProjection(myUCIGroup.GetEntity())
   ```
   The custom process **UCI_UCIGroupHasItem_Update** is created for **Group**.
10. Click **Commit to Database**.
11. Select **Database**| **Compile Database** in the **Designer** tool.
12. Use the **Synchronization Editor Tool** to create a new mapping for **Group**. For more information, see Configuring Amazon S3 AWS connector to support entitlements for Group using the Synchronization Editor

Configuring Amazon S3 AWS connector to support entitlements for Group using the Synchronization Editor

The **Synchronization Editor** tool is used to configure the Amazon (S3 and AWS) connector to support entitlements for **Group**.

NOTE: Create a multivalued array property to hold entitlements for **Group**.

To configure Amazon S3 AWS connector to support entitlements for Group:

1. Open the **Synchronization Editor** tool.
2. Open the specific synchronization project.
3. Navigate to **Configuration** | **One Identity Manager Connection** |**Update Schema**.
4. Activate the project.
5. Navigate to the **Mappings** tab and select **Group**.
6. In the **Property** pane, select **UID_UCIGroup**.
7. Click **Add** under **UID_UCIGroup**.
   The **Edit property** window is displayed.
8. Enter the **Name** and **Display name** for the property to be created. For example, vrtProfilesArr.
9. Select the options in the check boxes below the **Display name** field according to your requirements.
10. Click the **+** button to add the schema type.
11. Select the **Member key properties** for **Group** as listed in the table below:

Table 437: Member key properties

Entity	Value
M:N schema type	UCIGroupHasItem
	UID_UCIGroup
	UID_UCIItem
Primary key property	OjectGUID

12. Click **OK**.
13. Add a new mapping rule **Value Comparison Rule** with **vrtProfiles <--> Entitlements~value**.
14. Run the synchronization.

    The groups and entitlements that exist on target system instance are synchronized with One Identity Manager.

Appendix F

Configuring Box connector to support additional email IDs for users

This section describes the configuration changes to be made to the Box connector to support additional email IDs for Users- **CSMUser** and **UCIUser**.

The **Schema Extension** tool, **Designer** tool and the **Synchronization Editor** tool are used to configure the **Box** connector to support additional email IDs for users.

To configure the Box connector to support additional email IDs for Users:

1. Add new columns to an existing table using the **Schema Extension** tool . For more information, see Adding new columns for Users using the Schema Extension Tool.
2. Create a custom property using the **Designer** tool. For more information, seeCreating a custom property using Designer tool.
3. Map the newly created custom property using **Synchronization Editor**. For more information, see Mapping custom properties using the Synchronization Editor.

Adding new columns for Users using the Schema Extension Tool

This section describes the procedure to add new columns to an existing table for **CSMUser**.

To add new columns using the Schema Extension Tool for a CSMUser:

1. Open **Schema Extension** tool.

   The **Select method** window is displayed.
2. In the **Select method** window, select **Extend Table** and click **Next**.

   The **Extend Table** window is displayed.

3. In the **Extend Table** window, select **CSMUser** from the **Table** dropdown list and click **Next**.

   The **Configure columns** window is displayed.
4. In the **Configure columns** window, create a new column. Name the column appropriately and click **Next**.
   The **Access permissions** window is displayed.
5. In the **Access permissions** window, define access rights using the options available in the dropdown list and click **Next**.
6. **Compile database**.
   A new column is added.

This section describes the procedure to add new columns to an existing table for **UCIUser**.

To add new columns using the Schema Extension Tool for a UCIUser:

1. Open **Schema Extension** tool.

   The **Select method** window is displayed.
2. In the **Select method** window, select **Extend Table** and click **Next**.

   The **Extend Table** window is displayed.
3. In the **Extend Table** window, select **UCIUser** from the **Table** dropdown list and click **Next**.

   The **Configure columns** window is displayed.
4. In the **Configure columns** window, create a new column.

   > NOTE: To name the column, use the same name that you used when you created a new column in step 4 of the procedure To add new columns using the Schema Extension Tool for a CSMUser:
5. Click **Next**.
   The **Access permissions** window is displayed.
6. In the **Access permissions** window, define access rights using the options available in the dropdown list and click **Next**.
7. **Compile database**.
   A new column is added.

Creating a custom property using Designer tool

The Designer tool is used to create a custom process for **CSMUSer** and **UCIUser**.

This section describes the procedure to create a custom process for **CSMUser**.

To create a custom property for a **CSMUser**:

1. Open **Designer**.
2. Select **One Identity Manager Schema**.
   The **One Identity Manager Schema** allows you to display and edit the database tables, columns and information.
3. Expand **Tables** and select **CSMUser**.
4. Select **Show table definition**.
5. Navigate to the **More** tab.
6. Select the custom property created.
7. Select multi-value column.
8. Run **Commit to Database**.
9. Compile the Database.
   A custom property is created.

To create a custom property for a **UCIUser**:

1. Open **Designer**.
2. Select **One Identity Manager Schema**.
   The **One Identity Manager Schema** allows you to display and edit the database tables, columns and information.
3. Expand **Tables** and select **UCIUser**.
4. Select **Show table definition**.
5. Navigate to the **More** tab.
6. Select the custom property created.
7. Select multi-value column.
8. Run **Commit to Database**.
9. Compile the Database.
   A custom property is created.

Mapping custom properties using the Synchronization Editor

The **Synchronization Editor** is used to map the newly custom created property from One Identity Manager to the target system.

To map the newly created custom property from One Identity Manager to the target system:

1. Open **Synchronization Editor**.
2. Create a synchronization project for **Box** connector.

3. Map the newly created custom property from One Identity Manager to **additionalEmails** under extensions at target system side.
4. Run the synchronization.
5. The additional emails IDs of users are synchronized with One Identity Manager. You can now create new users with additional email IDs or modify the existing users to add additional email IDs.

Appendix G

One Identity Manager E2E integration needs for Hideez connector

One Identity Manager Integration cannot use the existing synchronization templates for **Hideez** connector. The endpoints provided by **Hideez** are different when compared to that of other Starling connectors. And, none of the existing One Identity Manager Synchronization templates that are available for SCIM Connector or for CHS modules template would work with **Hideez** endpoints.

Here is more explanation about the same:

- The regular **SCIM Synchronization** and **One Identity Starling Connect Synchronization** template cannot be used while the synchronization project is created, since the endpoints do not match.
- The **One Identity Starling Connect HR** template also cannot be used because **Hideez** does not have the **costcenter** and **location** endpoints. It is mandatory for a connector to have the **costcenter** and **location** endpoints if you want to use the One Identity Starling Connect HR template.
- The recommended approach would to create a blank project template and then map the endpoints manually.

Appendix H

Configuring custom attributes for ServiceNow v.1.0

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 the One Identity Manager provide the values for these custom attributes.

NOTE: While configuring **ServiceNow v.1.0** connector, if you do not want to configure any custom attributes, then enter the value **None** in the **Custom Properties** field.

To configure custom attributes in ServiceNow v.1.0:

1. Create a Custom Attribute in ServiceNow.

   NOTE:The Starling Platform currently supports only the types **String**, **dateTime**, **True**/**False** and **Choice** in the **ServiceNow sys_user** table.

2. To configure the custom attributes in Starling UI, enter the **Custom Properties** in the specified format in the Starling Platform.
3. On the One Identity Manager, map the created custom attributes that were specified in the Starling Platform.
4. Perform a synchronization and verify if the custom attributes are available in the One Identity Manager.

   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

field_name = Column name in ServiceNow

data_type = string (or) boolean (or) datetime

- All custom attributes are mapped in the enterprise user extensions.
- The supported data types in the Starling Connect ServiceNow connector are **string**, **boolean** and **dataTime**.

  Choice type in the ServiceNow will become **string** type in OneIM with Canonical Values.
- Only simple json attributes are supported. Complex json attributes are not supported.
- All custom user attributes have **'mutability': 'readWrite'**, **'returned': 'default'**, **'caseExact': 'false'**, **'required': 'false'**, **'multiValued': 'false','uniqueness': 'none'**.

Appendix I

Configuring custom attributes for Coupa v.1.0

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 the One Identity Manager provide the values for these custom attributes.

NOTE:

- Only **String** and **Boolean** data types are supported currently by Coupa connector.
- While configuring **Coupa v.1.0** connector, if you do not want to configure any custom attributes, then enter the value **None** in the **Custom Properties** field.

To configure custom attributes:

1. Enter the **custom properties** in the mentioned format in Starling.
2. In the One Identity Manager, map the created custom attributes that were specified in Starling.
3. Perform a synchronization and verify if the custom attributes are available in the One Identity Manager.

   NOTE:

   - The Starling UI has default mapped attributes.
   - Apart from the default mapped attributes, the Starling UI used for registering a Coupa connector has an input field where you can provide the custom attributes that have to be mapped in the connector's **User resource** type.

     The format of the custom attributes in the **User resource** type must be as follows:

     `{field_name}|{data_type}`

     `Example: custom_attribute_name1|string;custom_attribute_name2|string;`

     `custom_attribute_name1 = name of the custom attribute`

     `data_type = string (or) boolean`
   - All custom attributes are mapped in the enterprise user extensions.

- All custom user attributes have **mutability**: **readWrite**, **returned**: **default**, **caseExact**: **false**, **required**: **false**, '**multiValued**: **false**, **uniqueness**: **none**.
- Only the data types **String**and **Boolean** are supported currently by Coupa connector.

Appendix J

Configuring custom attributes in connectors

This section describes the steps to configure custom attributes using Starling Connect for connectors.

NOTE:

- You must first configure custom attributes in the target system before configuring them in Starling Connect.
- When you are configure custom attributes in Starling Connect, make sure that you provide the custom attribute that you configured in the cloud application because Starling Connect does not perform any validation to check if you have provided a custom attribute that exists in the cloud application.
- This issue is common for all connectors that allow you to configure custom attributes in Starling Connect.

To configure a custom attribute:

1. Navigate to the configured connector in the **Active Connectors** section.
2. Click the connector tile.

   The **General Configuration** and **Schema Configuration** are displayed.
3. Click **EDIT**.

   The **Schema Configuration** displays the **Custom Attributes** section, where you can configure the custom attributes.

   NOTE: If you have already configured any custom attributes, they are displayed in the **Custom Attributes** section.
4. Select the object under which you want to create the custom attribute.
5. In the **Custom Attributes** section, enter the appropriate values in the following fields:
   - Data Type
   - Target System Attribute name
   - Description

NOTE:

Choose the required option from the available list of data types in the **Data Type** field

- Binary
- Boolean
- DateTime
- Decimal
- Integer
- String

6. Click **SAVE**.

NOTE:

- To configure another custom attribute, click **ADD ATTRIBUTE**.
- To remove a custom attribute, select the custom attribute and click **Remove**.
- To modify and existing custom attribute, click the custom attribute and enter new configuration details.

7. Enter the configuration details in the **General Configuration** section and click **Test Connection**.
8. Click **SAVE**.

   The newly created custom attribute is displayed in **Custom Attributes** section and is available in One Identity Manager.

NOTE:

- In SuccessFactors HR connector, if a custom attribute is a part of navigation, then you must enter it in the following format in Starling Connect: **<navigation>$$<custom_attribute>**. For example, you must enter **userNav/dateOfBirth** as **userNav$$dateOfBirth** in Starling Connect.
- The **SuccessFactors HR** connector supports single level of navigation only.

Appendix K

Disabling attributes

The **Disable attribute** feature can be used when you want to skip an attribute that exists in the target system.

NOTE: Mandatory attributes cannot be disabled.

This section describes the steps to disable an attribute using Starling Connect.

To disable an attribute:

1. Navigate to the configured connector in the **Active Connectors** section.
2. Click the connector tile.

   The **General Configuration** and **Schema Configuration** are displayed.
3. Click **EDIT**.

   The **Schema Configuration** highlights the attributes that can be disabled.

   NOTE: You cannot disable mandatory attributes. Mandatory attributes are suffixed with a *.
4. Toggle the attribute that you want to disable.

   NOTE: If you disable a parent attribute, all its child attributes are disabled.
5. Enter the configuration details in the **General Configuration** section and click **Test Connection**.
6. Click **SAVE**.

   The disabled attribute is removed from the SCHEMA responses and requests of the following operations:

Operation	From
GET Schema	Response
Get <object> by Id	Response
	Response
Create <object>	Request (which is sent from the connector to the cloud application)
	Response
Update <object>	Request (which is sent from the connector to the cloud application)

NOTE: In the above table, <object> represents a connector endpoint.

Configuring a connector that uses the consent feature

This section describes the procedure to configure a connector that uses the consent feature.

To configure a connector that uses the consent feature

1. Enter the configuration details in the **General Configuration**.

   NOTE:

   - Each connector requires a different set of configuration details. For more information about the configuration details for each connector, navigate to the section **Supervisor configuration parameters** for the connector that you want to configure, in this document.
   - Every connector license that you have, allows you to configure two different connections, one in the **Production** environment and the other in the **Development** environment. Hence, you can configure the connector to create a Starling Connect connector connection in your **Development** environment for testing, and then, configure it in your **Production** environment.

2. Click **Give Consent**.

   NOTE:

   - To provide consent, use an account with administrative privileges.
   - For more information about the necessary permissions required to configure each connector, navigate to the section **Connector configuration** for the connector that you want to configure, in this document.

3. Click **Test Connection**.
4. Click **Save**.

Appendix M

Synchronization and integration of Roles object type with One Identity Manager

This section describes the synchronization and integration of **Roles** object type with One Identity Manager.

To synchronize and integrate Roles object type with One Identity Manager:

1. Ensure that the **Roles** endpoint of Starling Connect Connector returns the list of **Roles** from the target instance.
2. Create a mapping for **Roles** endpoint.

   To create a mapping for **Roles** endpoint:

   a. Open **Synchronization Editor**.

   b. Select the project.

   c. Navigate to the **Navigation** pane.

   d. In the **Navigation** pane, click **Configuration**.

   e. In the **Navigation** pane, click **Target system**.

   f. Click **Update Schema** in the **General** section.

   g. In the **Navigation** pane, click **Mappings**.

   h. Create a new mapping named **Roles**.

   To create a new mapping, click **+** in the **Mappings** section.

   i. In the **Create map** window, enter the values for all the fields, including the display name, in the following sections :

   - General
   - Relation
3. Click **OK**.
4. Click **Next**.

5. In the **Mapping Wizard** window, in the **Select task** section, select the required template. For example, **Group template**.
6. Create a new **Fixed-value virtual attribute** at the target system side with the name **vrtRoles**, for example.

   To create a **Fixed-value virtual attribute**:

   a. Click **+** at the target system side in the **SCIM** section.

   b. In the **Create property** window, enter the values for all the fields.
   The value of the **Value** field must be **Profiles**.
7. Configure **Mappings**.
   To configure **Mappings**:

   a. Map **Item type <- vrtRoles**.

   b. Map **Ident_UCIItem <- name**.
8. Create Synchronization workflow for **Roles**.

   NOTE: The procedure to **Create Synchronization workflow for Roles** is similar to the procedure to **Create Synchronization workflow for Users** and to **Create Synchronization workflow for Groups**.
9. Create Provisioning workflows for **Roles**.

   NOTE: The procedure to **Create Provisioning workflow for Roles** is similar to the procedure to **Create Provisioning workflow for Users** and to **Create Provisioning workflow for Groups**.
10. Run Synchronization.
11. Perform **assign** or **unassign** of **Roles** at **Users** and **Groups**.

Appendix N

Synchronization and integration of Workspaces object type with One Identity Manager

This section describes the synchronization and integration of **Workspaces** object type with One Identity Manager.

To synchronize and integrate Workspaces object type with One Identity Manager:

1. Ensure that the **Workspaces** endpoint of Starling Connect Connector returns the list of **Workspaces** from the target instance.
2. Create a mapping for **Workspaces** endpoint.

   To create a mapping for **Workspaces** endpoint:

   a. Open **Synchronization Editor**.

   b. Select the project.

   c. Navigate to the **Navigation** pane.

   d. In the **Navigation** pane, click **Configuration**.

   e. In the **Navigation** pane, click **Target system**.

   f. Click **Update Schema** in the **General** section.

   g. In the **Navigation** pane, click **Mappings**.

   h. Create a new mapping named **Workspaces** .

   To create a new mapping, click **+** in the **Mappings** section.

   i. In the **Create map** window, enter the values for all the fields, including the display name, in the following sections :

   - General
   - Relation
3. Click **OK**.
4. Click **Next**.

5. In the **Mapping Wizard** window, in the **Select task** section, select the required template. For example, **Group template**.
6. Create a new **Fixed-value virtual attribute** at the target system side with the name **vrtWorkspaces**, for example.

   To create a **Fixed-value virtual attribute**:

   a. Click **+** at the target system side in the **SCIM** section.

   b. In the **Create property** window, enter the values for all the fields.
   The value of the **Value** field must be **Profiles**.
7. Configure **Mappings**.
   To configure **Mappings**:

   a. Map **Item type <- vrtWorkspaces**.

   b. Map **Ident_UCIItem <- name**.
8. Create Synchronization workflow for **Workspaces** .

   NOTE: The procedure to **Create Synchronization workflow for Workspaces** is similar to the procedure to **Create Synchronization workflow for Users** and to **Create Synchronization workflow for Groups**.
9. Create Provisioning workflows for **Workspaces** .

   NOTE: The procedure to **Create Provisioning workflow for Workspaces** is similar to the procedure to **Create Provisioning workflow for Users** and to **Create Provisioning workflow for Groups**.
10. Run Synchronization.
11. Perform **assign** or **unassign** of **Workspaces** at **Users** and **Groups**.

Appendix O

Synchronization and integration of Products object type with One Identity Manager

This section describes the synchronization and integration of **Products** object type with One Identity Manager.

To synchronize and integrate Products object type with One Identity Manager:

1. Ensure that the **Products** endpoint of Starling Connect Connector returns the list of **Products** from the target instance.
2. Create a mapping for **Products** endpoint.

   To create a mapping for **Products** endpoint:

   a. Open **Synchronization Editor**.

   b. Select the project.

   c. Navigate to the **Navigation** pane.

   d. In the **Navigation** pane, click **Configuration**.

   e. In the **Navigation** pane, click **Target system**.

   f. Click **Update Schema** in the **General** section.

   g. In the **Navigation** pane, click **Mappings**.

   h. Create a new mapping named **Products** .

   To create a new mapping, click **+** in the **Mappings** section.

   i. In the **Create map** window, enter the values for all the fields, including the display name, in the following sections :

   - General
   - Relation
3. Click **OK**.
4. Click **Next**.

5. In the **Mapping Wizard** window, in the **Select task** section, select the required template. For example, **Group template**.
6. Create a new **Fixed-value virtual attribute** at the target system side with the name **vrtProducts**, for example.

   To create a **Fixed-value virtual attribute**:

   a. Click **+** at the target system side in the **SCIM** section.

   b. In the **Create property** window, enter the values for all the fields.
   The value of the **Value** field must be **Profiles**.
7. Configure **Mappings**.
   To configure **Mappings**:

   a. Map **Item type <- vrtProducts**.

   b. Map **Ident_UCIItem <- name**.
8. Create Synchronization workflow for **Products** .

   NOTE: The procedure to **Create Synchronization workflow for Products** is similar to the procedure to **Create Synchronization workflow for Users**.
9. Create Provisioning workflows for **Products** .

   NOTE: The procedure to **Create Provisioning workflow for Products** is similar to the procedure to **Create Provisioning workflow for Users** .
10. Run Synchronization.
11. Perform **assign** or **unassign** of **Products** at **Users**.

Appendix P

User centric membership

This section describes the procedure to configure One Identity Manager to achieve User centric membership operation. The following tools are used to configure the configure One Identity Manager to achieve User centric membership: Synchronization Editor, Schema Extension, and Designer.

To to configure One Identity Manager to achieve User centric membership

1. Using Synchronization Editor.
   a. Creating a new schema class using Synchronization Editor
   b. Configuring User centric membership for Groups, UserGroups and AccountGroups using Synchronization Editor.
2. Using Schema Extension.
   - Creating a new column in UCIUser table and CSMUser table using Extension Tool
3. Using Designer.
   - Creating custom process using Designer

Creating a new schema class using Synchronization Editor

This section describes the procedure to create a new schema class. **Synchronization Editor** is used to create a new schema class.

This is an example of how to create a new schema class. In this example, a schema class named **UCIGroup(Group)** is created for the **Group** resource type.

To create a new schema class

1. Launch the **Synchronization Editor**.
2. Select **Configurations** | **One Identity Manager connection** | **Schema classes**.
3. Click **+** to create a new schema class.

4. In the **New schema class** window, select **UCIGroup** from **Schema type** list and enter the values of the other fields as shown in the table below

Table 438: New schema class UCIGroup(Group)Group for Group

Field	Value
Schema Type	UCIGroup
Display Name	UCIGroup(Group)
Class Name	UCIGroup_Group
Description	UCIGroup_Group
System Objects --> Condition	ResourceType = Group

NOTE: A similar table is available in the corresponding sections to create the other schema classes.

5. Click **Ok**.

NOTE: Similarly, you can create the other schema classes by referring to the values in the corresponding tables in the corresponding sections.

Configuring User centric membership for Groups, UserGroups and AccountGroups using Synchronization Editor

This section describes the procedures to configure User centric memberships for Groups, UserGroups and AccountGroups.

For more information see:

- Configuring User centric membership for Groups
- Configuring User centric membership for UserGroups
- Configuring User centric membership for AccountGroups

Configuring User centric membership for Groups

This section describes the procedure to configure User centric membership for Groups in **Synchronization Editor**.

To configure User centric membership for Groups

1. Create the new schema class **UCIGroup(Group)**, with **UCIGroup Schema type**, using the details provided in the table:

   Table 439: New schema class UCIGroup(Group)Group for Group

Field	Value
Schema Type	UCIGroup
Display Name	UCIGroup(Group)
Class Name	UCIGroup_Group
Description	UCIGroup_Group
System Objects --> Condition	ResourceType = Group

   NOTE: **Synchronization Editor** is used to create a new schema class. For more information, see Creating a new schema class using Synchronization Editor.

2. Create the new schema class **UCIUserInGroup(Group)**, with **Schema typeUCIUserInGroup**, using the details provided in the table:

   Table 440: New schema class UCIUserInGroup(Group) for Group

Field	Value
Schema Type	UCIUserInGroup
Display Name	UCIUserInGroup(Group)
Class Name	UCIUserInGroup_Group
Description	UCIUserInGroup_Group
System Objects --> Condition	UID_UCIGroup <> 'leave it as empty'
System filter	UID_UCIGroup in (select UID_UCIGroup from UCIGroup where ResourceType = 'Group')

3. Click **Commit to database** in the **Synchronization Editor**.

   The new schema classes are created and the changes are saved.

4. Navigate to **Target system** and click **Update schema** to perform a schema update.
5. Edit default mapping for **Group**.

   To edit default mapping for Group:

   a. In the **Navigation** pane, select **Mappings| Group**.
   b. In the **Mappings** section, click **Edit Map**.
   c. In the **Edit map...** window, in the **Relation** section, click **Edit**.

d. Select the values from the lists as shown in the following table and click **Ok**:

Table 441: Edit default mapping for Group

List	Value
One Identity Manager schema class	UCIGroup(Group)
Target system schema class	Group (all)

NOTE: Add the group members mapping under **User** object in **Synchronization Editor**.

6. Create **<vrtMembers>** property for **Groups**

   Add **vrtMembersGroup** parameter with **M:N type schema type** with the below configuration.

   To add the virtual parameters:

   a. Select **Mappings| User**.

   b. Select **+** in the **User** pane to create a property.

   c. In the **Create property** window, from the **Property type** list, select **Members of M:N schema types** .

   d. Enter the following values in the fields mentioned in the table, and select the options listed below:

   Table 442: Virtual parameters

Field/ Option	Value
Name	vrtMembersGroup
Display name	GroupMembers

   Select the following options:

   - Ignore case
   - Try to mark the objects for deletion (outstanding)

   e. In the **M:N schema types** section at the bottom of the window, select **UCIUserinGroup(Group)**, **UID_UCIUser**, and **UID_UCIGroup**.

   f. In the **Members UCIGroup** section, select **ObjectGUID** .

   NOTE: Select UCIUserInGroup(Group) schema type for vrtMembersGroup parameter.

   g. Click **Ok**.

7. Create mapping for **groups~value** as shown below with mapping direction.

   To create mappings:

a. Select **Mappings| User**.

b. Select **vrtMembersGroup** in the **User** pane.

c. Create mappings for **Groups** under **User** object.

> NOTE: You can create a mapping by dragging the property **vrtMembersGroup** in the **UCIUser** pane and dropping it to the property **groups~value** in the **SCIMUser** pane.

d. Click **Commit to database** to save the changes.

Configuring User centric membership for UserGroups

This section describes the procedure to configure User centric membership for **UserGroups** in the **Synchronization Editor**.

To configure User centric membership for UserGroups

1. Create the new schema class **UCIGroup(UserGroups)** , with **UCIGroup Schema type**, using the details provided in the table:

   Table 443: UserGroups

Field	Value
Schema Type	UCIGroup
Display Name	UCIGroup(UserGroups)
Class Name	UCIGroup_UserGroups
Description	UCIGroup_UserGroups
System Objects --> Condition	ResourceType = UserGroups

   > NOTE: **Synchronization Editor** is used to create a new schema class. For more information, see Creating a new schema class using Synchronization Editor.

2. Create the new schema class **UCIUserInGroup(UserGroups)**, with **Schema typeUCIUserInGroup**, using the details provided in the table:

   Table 444: New schema class UCIUserInGroup(UserGroups) for UserGroups

Field	Value
Schema Type	UCIUserInGroup

Display Name	UCIUserInGroup(UserGroups)
Class Name	UCIUserInGroup_UserGroups
Description	UCIUserInGroup_UserGroups
System Objects --> Condition	UID_UCIGroup <> 'leave it as empty'
System filter	UID_UCIGroup in (select UID_UCIGroup from UCIGroup where ResourceType = 'UserGroups')

3. Click **Commit to database** in the **Synchronization Editor**.

   The new schema classes are created and the changes are saved.

4. Navigate to **Target system** and click **Update schema** to perform a schema update (if **UserGroups** is not exposed).

5. Create mappings for **UserGroups**.

   To create mappings for **UserGroups**:

   a. In the **Navigation** pane, select **Mappings** | **User.**

   b. Click **+** to create a new mapping.

   c. In the **New mapping** window:

      i. In the **General** section, enter the values in fields as shown in the table

Table 445: Create new mapping for UserGroups - General section

Field	Value
Mapping name	UserGroups
Mapping direction	Both directions

NOTE: Select the option **Maps objects referenced by multiple references**.

ii. In the **Relation** section, enter the values in fields as shown in the table

Table 446: Create new mapping for UserGroups - Relation section

Field	Value
One Identity Manager schema class	UCIGroup(UserGroups)
Target system schema class	UserGroups (all)

iii. Click **Ok** and click **Next**.

d. In the **Mapping Wizard**:

i. In the **Select task** section, select the template **Create rules based on template**, click **Next** and click **Finish**.

ii. In the **Select source mapping** section, select **Group** and click **Next**.

iii. In the **Analysis result section**, select a new rule **ConanicalName <-> vrtcononicalName** from the suggestion list.

The new mapping rule **ConanicalName <-> vrtcononicalName** is displayed in the **Property mapping rules** section in the **Schema property in One Identity Manager** list.

6. Create **Initial Synchronization** workflow for **UserGroups**.

To create Initial Synchronization workflow for **UserGroups**.

a. In the **Navigation** pane, select **Workflow| Initial Synchronization**.

b. In the **Initial Synchronization** page, in the **Workflow** section, click **+** to add a new step.

c. In the **Create a new Synchronization step** window, in the **General** tab, select the values as shown in the table below:

Table 447: Create synchronization step

Field	Value
Name	UserGroups
Mapping	UserGroups
Synchronization direction	One Identity Manager
Revision filtering	Use revision filter
Exception handling	Use workflow default

d. In the **Processing** tab, select the values in the same way that they are set in the **Processing** tab for the **User** workflow and click **Ok**.

e. Click **Commit to database** and click **Ok**.

The **UserGroups** workflow is displayed in the **Workflow** section.

7. Create **Provisioning** workflow for **UserGroups**.

To create **Provisioning** workflows for **UserGroups**.

a. In the **Navigation** pane, select **Workflow| Provisioning**.

b. In the **Provisioning** page, in the **Workflow** section, click **+** to add a new step.

c. In the **Create a new Synchronization step** window, in the **General** tab, select the values as shown in the table below:

Table 448: Create synchronization step

Field	Value
Name	UserGroups
Mapping	UserGroups
Synchronization direction	Target system
Revision filtering	Use workflow default
Exception handling	Use workflow default

d. In the **Processing** tab, select the values in the same way that they are set in the **Processing** tab for the **User** workflow and click **Ok**.

e. Click **Commit to database** and click **Ok**.

The **UserGroups** workflow is displayed in the **Workflow** section.

8. Create **<vrtMembers>** property for **UserGroups**.

Add **vrtMembersUserGroups** parameter with **M:N type schema type** with the below configuration.

To add the virtual parameters:

a. Select **Mappings| User**.

b. Select **+** in the **User** pane to create a property.

c. In the **Create property** window, from the **Property type** list, select **Members of M:N schema types** .

d. Enter the following values in the fields mentioned in the table, and select the options listed below:

Table 449: Virtual parameters

Field/ Option	Value
Name	vrtMembersUserGroups
Display name	UserGroupMembers

Select the following options:

- Ignore case
- Try to mark the objects for deletion (outstanding)

e. In the **M:N schema types** section at the bottom of the window, select **UCIUserInGroup(UserGroups)**, **UID_UCIUser**, and **UID_UCIGroup**.

f. In the **Members UCIGroup** section, select **ObjectGUID** .

> NOTE: Select UCIUserInGroup(UserGroups) schema type for vrtMembersUserGroups parameter.

g. Click **Ok**.

9. Create mappings with **vrtMembersUserGroup** and SCIM extension **ApprovalGroups(~)value**.
10. Create mapping for **userGroups~value** as shown below with mapping direction.

    To create mappings:

    a. Select **Mappings| User**.

    b. Select **vrtMembersGroup** in the **User** pane.

    c. Create mappings for **UserGroups** under **User** object.

    > NOTE: You can create a mapping by dragging the property **vrtMembersUserGroups** in the **UCIUser** pane and dropping it to the property **userGroups~value** in the **SCIMUser** pane.

    d. Click **Commit to database** to save the changes.

Configuring User centric membership for AccountGroups

This section describes the procedure to configure User centric membership for Groups in **Synchronization Editor**.

To configure User centric membership for AccountGroups

1. Create the new schema class **UCIGroup(AccountGroups)**, with **UCIGroup Schema type**, using the details provided in the table:

Table 450: New Schema class UCIGroup(AccountGroups) for AccountGroups

Field	Value
Schema Type	UCIGroup
Display Name	UCIGroup(AccountGroups)

Class Name	UCIGroup_AccountGroups
Description	UCIGroup_AccountGroups
System Objects --> Condition	ResourceType = AccountGroups

NOTE: **Synchronization Editor** is used to create a new schema class. For more information, see Creating a new schema class using Synchronization Editor.

2. Create the new schema class **UCIUserInGroup(AccountGroups)**, with **Schema typeUCIUserInGroup**, using the details provided in the table:

Table 451: New schema class UCIUserInGroup(AccountGroups) for AccountGroups

Field	Value
Schema Type	UCIUserInGroup
Display Name	UCIUserInGroup(AccountGroups)
Class Name	UCIUserInGroup_AccountGroups
Description	UCIUserInGroup_AccountGroups
System Objects --> Condition	UID_UCIGroup <> 'leave it as empty'
System filter	UID_UCIGroup in (select UID_UCIGroup from UCIGroup where ResourceType = 'AccountGroups')

3. Click **Commit to database** in the **Synchronization Editor**.

   The new schema classes are created and the changes are saved.

4. Navigate to **Target system** and click **Update schema** to perform a schema update (if **AccountGroups** is not exposed).
5. Create mappings for **AccountGroups**.

   To create mappings for **AccountGroups**:

   a. In the **Navigation** pane, select **Mappings** | **User.**

   b. Click **+** to create a new mapping.

c. In the **New mapping** window:

i. In the **General** section, enter the values in fields as shown in the table

Table 452: Create new mapping for AccountGroups - General section

Field	Value
Mapping name	AccountGroups
Mapping direction	Both directions

NOTE: Select the option **Maps objects referenced by multiple references**.

ii. In the **Relation** section, enter the values in fields as shown in the table

Table 453: Create new mapping for AccountGroups - Relation section

Field	Value
One Identity Manager schema class	UCIGroup(AccountGroups)
Target system schema class	AccountGroups (all)

iii. Click **Ok** and click **Next**.

d. In the **Mapping Wizard**:

i. In the **Select task** section, select the template **Create rules based on template**, click **Next** and click **Finish**.

ii. In the **Select source mapping** section, select **Group** and click **Next**.

iii. In the **Analysis result section**, select a new rule **ConanicalName <-> vrtcononicalName** from the suggestion list.

The new mapping rule **ConanicalName <-> vrtcononicalName** is displayed in the **Property mapping rules** section in the **Schema property in One Identity Manager** list.

6. Create **Initial Synchronization** workflow for **AccountGroups**.

To create Initial Synchronization workflow for **AccountGroup**

a. In the **Navigation** pane, select **Workflow| Initial Synchronization**.

b. In the **Initial Synchronization** page, in the **Workflow** section, click **+** to add a new step.

c. In the **Create Synchronization step** window, in the **General** tab, select the values as shown in the table below:

Table 454: Create synchronization step

Field	Value
Name	UserGroups
Mapping	UserGroups
Synchronization direction	One Identity Manager
Revision filtering	Use revision filter
Exception handling	Use workflow default

d. In the **Processing** tab, select the values in the same way that they are set in the **Processing** tab for the **User** workflow and click **Ok**.

e. Click **Commit to database** and click **Ok**.

The **AccountGroups** workflow is displayed in the **Workflow** section.

7. Create **Provisioning** workflow for **AccountGroups**.

To create **Provisioning** workflows for **AccountGroups**.

a. In the **Navigation** pane, select **Workflow| Provisioning**.

b. In the **Provisioning** page, in the **Workflow** section, click **+** and click **Ok**.

c. In the **Create Synchronization step** window, in the **General** tab, select the values as shown in the table below:

Table 455: Create synchronization step

Field	Value
Name	AccountGroups
Mapping	AccountGroups
Synchronization direction	Target system
Revision filtering	Use workflow default
Exception handling	Use workflow default

d. In the **Processing** tab, select the values in the same way that they are set in the **Processing** tab for the **User** workflow and clcik **Ok**.

e. Click **Commit to database** and click **Ok**.

The **AccountGroups** workflow is displayed in the **Workflow** section.

8. Create **<vrtMembers>** property for **AccountGroups**

Add **vrtMembersAccountGroups** parameter with **M:N type schema type** with the below configuration.

To add the virtual parameters:

a. Select **Mappings| User**.

b. Select **+** in the **User** pane to create a property.

c. In the **Create property** window, from the **Property type** list, select **Members of M:N schema types** .

d. Enter the following values in the fields mentioned in the table, and select the options listed below:

Table 456: Virtual parameters

Field/ Option	Value
Name	vrtMembersAccountGroup
Display name	AccountGroupMembers

Select the following options:

- Ignore case
- Try to mark the objects for deletion (outstanding)

e. In the **M:N schema types** section at the bottom of the window, select select **UCIUserInGroup(AccountGroups)**, **UID_UCIUser**, and **UID_UCIGroup**.

f. In the **Members UCIGroup** section, select **ObjectGUID** .

> NOTE: Select UCIUserInGroup(AccountGroups) schema type for vrtMembersAccountGroups parameter.

g. Click **Ok**.

9. Create mapping for **accountGroups~value** as shown below with mapping direction.

To create mappings:

a. Select **Mappings| User**.

b. Select **vrtMembersGroup** in the **User** pane.

c. Create mappings for **AccountGroups** under **User** object.

> NOTE: You can create a mapping by dragging the property **vrtMembersAccountGroups** in the **UCIUser** pane and dropping it to the property **accountGroups~value** in the **SCIMUser** pane.

d. Click **Commit to database** to save the changes.

Creating a new column in UCIUser table and CSMUser table using Extension Tool

This section describes the steps that you must perform in **Schema Extension** tool to configure User centric membership. You must create a new column in the tables:

- UCIUser. For more information, see Creating a new column in UCIUser table.
- CSMUser. For more information, see Creating a new column in CSMUser table

Creating a new column in UCIUser table

To create a new column in UCIUser table

1. Launch **Schema Extension**.
2. Select **Extend Table**.
3. Select **UCIUser**.
4. Create a column named **CCC_XDateSubItem** of type **Date** in the **UCIUser** table.

   To create a column in the **UCIUser** table

   a. In the **Configure columns** window, click **+**.

   b. In the **Create new column** window, enter the details as required and click **Next**.

   c. In the **Date type** column, select **Date** and click **Next**.

   d. Select the required permissions and click **Next**

      - Read and write permissions
      - Read only permissions

   e. Select the option **No change label** and click **Next**.

      System changes are displayed in the **Systems modifications** window and you can export them to a file if required.

   f. Click **Next** and save the changes to the database and compile the database changes.

   g. Click **Finish** after compilation.

Creating a new column in CSMUser table

To create a new column in CSMUser table

1. Launch **Schema Extension**.
2. Select **Extend Table**.
3. Select **CSMUser**.

   NOTE:

   - Now, repeat step 4 from the procedure To configure User centric membership using Schema Extension for UCIUser. Replace all instances of **UCIUser** with **CSMUser**.

- To see the changes in **Synchronization Editor Mapping properties** of **User** object, navigate to **Synchronization Editor** -> Select SCIM project (which you created) -> **One Identity Manager Connection** -> **Update Schema** in **General Window** -> **Commit to database**.

NOTE: After you perform the above steps in Schema Extension, see Configuring User centric membership using Designer.

Creating custom process using Designer

This section describes the steps that you must perform in **Designer** to configure User centric membership. You must a custom process **UCI_UserInGroup_Custom** on the **UCIUserInGroup** table

To configure User centric membership using Designer

1. Launch **Designer**.
2. Create a custom process **UCI_UserInGroup_Custom** on the **UCIUserInGroup** table.

   To create a custom process

   a. In the **Navigation** pane, select **Process Orchestration** |**Custom process**| **Navigation**| **Process Editor**| **Create a new process**.
   The **Process properties** window is displayed.

   b. In the **General** tab of the **Process properties** window, enter the following values:

   Table 457: Values for creating custom process for Group

Process properties	Value
Name	UCI_UserInGroup_Custom
Table	UCIUserInGroup

3. Add **Insert** and **Delete** events for the process.
   To add **Insert** and **Delete** events for the process

   a. In the **Events** tab, at the bottom of the page, click **+**.
   The **Edit event** window is displayed.

   b. In the **Edit event** window, click **+** next to the **Object Event** field.
   The **Edit object event** window is displayed.

   c. In the **Edit object event**, select **Delete** and then select **Insert** from the list. Click **OK**.
   Delete and **Insert** are displayed in the **Events** window.

4. Create another process **Patch DPRMembershipaction**, which can run as sub process of **UCI_UserInGroup_Custom**.

   NOTE: To create a sub process, right click in the process window and clcik **New**.

5. In the **Process step properties** window, select the values as follows:
   a. In the **General tab**,
      i. in the **Name** field, enter the value **Patch DPRMembershipaction**.
      ii. in the **Process task** field, enter the value **SQLComponent - Execute SQL**.
   b. In the **Generation** tab, set server function value to **SQL processing server**.
   c. Navigate to the **Parameters tab** at the bottom of the window, and set the parameter **SQLStmt** to the following value using the **Edit parameters** window:
      ```
      Dim f As ISqlFormatter = Connection.SqlFormatter
      Value = "update DPRMemberShipAction set ObjectKeyBase =
      ObjectKeyMember, ObjectKeyMember = ObjectKeyBase where " & _
       f.Comparison("ObjectKeyMN",
      $XObjectKey$,ValType.String,CompareOperator.Equal)
      ```

6. Create a link between process **UCI_UserInGroup_Custom** to **Patch DPRMembershipaction**.

   NOTE: You can drag and drop from the parent process to the child process to create a link between the two processes.

7. Create another sub process for **Patch DPRMembershipaction**.

   In the **Process step properties** window, select the values as follows:
   a. In the **General tab**,
      i. in the **Name** field, enter the value **Set CCC_XDateSubItem**.
      ii. in the **Process task** field, enter the value **HandleObjectComponent - Update**.
      iii. in the **Priority** field, set the priority.
   b. In the **Generation** tab, set server function value to **SQL processing server**.
   c. Navigate to the **Parameters tab** at the bottom of the window, and
      i. set the parameter the following parameters to the values given below using the **Edit parameters** window:
         Object type: `Value = "UCIUser"`
         WhereClause:
         ```
         Dim f As ISqlFormatter = Connection.SqlFormatter
         Value = f.UidComparison("UID_UCIUser", $UID_UCIUser$)
         ```
      ii. enable any of the **val_Property*** by double-clicking it, and then rename the property name to **val_CCC_XDateSubItem and set Value = Now ()** using the **Edit paramaters** window.

8. Create a link between the processes **Patch DPRMembershipaction** and **Set CCC_XDateSubItem**.

   NOTE: You can drag and drop to create a link between the two processes.

9. a. Create a custom script to avoid running **UCI_UCIGroup_update** job chain for <connector_name> connector.

   To create a custom script, in the **Navigation** pane, select **Script Library** |**Custom script**|**Create a new script** using the following details:

   Name: UCI_TargetUsers<connector_name>_Custom

   Add below function with code

```
Public Function UCI_TargetUsers<connector_name>_Custom (UID_UCIRoot As
String) As Boolean

Dim f As ISqlFormatter = Connection.SqlFormatter

Dim UCIRoot<connector_name>Display = Connection.GetSingleProperty
("UCIRoot", "DisplayName", f.UidComparison("UID_UCIRoot", UID_UCIRoot,
CompareOperator.Equal))

If UCIRoot<connector_name>Display.ToString().ToLower().Contains
("<connector_name>") Then

Return True

End If

Return False

End Function
```

10. Navigate to **Process Orchestration| Process| UCI_UCIGroup_Update**.
11. In the **Process properties** window, in the **General** tab, add the condition `Not UCI_TargetUsers<connector_name>_Custom($UID_UCIRoot$) AndAlso _`
12. Click **Commit to database**.
13. Click **Compile the Database**.
14. In the **Compilation settings** window, select **script including all dependencies** and click **Next**.

Appendix Q

Creating multi-valued custom fields in One Identity Manager

This section describes the procedure to create multi-valued custom fields in One Identity Manager.

To create multi-valued custom fields in One Identity Manager

1. Create a custom column in the respective User tables in the database.
   a. Create a custom column in **CSMUser** table.

      To create a custom column in **CSMUser** table

      i. Open **SchemaExtension. exe**.
      ii. In the **Select Method** window, select **Extend table** and click **Next**.
      iii. In the **Extend table** window, select **CSMUser** table and click **Next**.
      iv. In the **Configure columns** window, click **Create New column** (**+**).
      v. In the **Create new column** window, enter a name for the column. For example: RolesID.
      vi. Enter a display name for the column to be displayed in **Manager.exe**.
      vii. In the **Configure columns** window, select the data type as **string** from the **Data type** list and click **Next**.
      viii. In the **Access permissions** window, add appropriate permissions and click **Next**.
      ix. Click **Finish** after the compilation is done.
      x. Repeat the steps for all custom columns that you have to create. For example: **RolesName**, **WorkspaceID**, and **WorkspaceName**.

   b. Create a custom column in **UCIUser** table.

      To create a custom column in **UCIUser** table

      i. Repeat the steps that you performed for creating a custom column in **CSMUser** table.

ii. Ensure that you use the same column name and other details used when you created a custom column in **CSMUser** table.

2. Change the created custom column to multi-value in both the tables.
   a. Change the created column in **CSMUser** table to multi-value.

      To change the created column in **CSMUser** table to multi-value

      i. Open **Designer.exe**.
      ii. Select **One Identity Manager Schema** in the left pane.
      iii. Click **Show Table Definition**.
      iv. Select **CSMUser**.
      v. Select the created custom column.
      vi. Select the **More** tab.
      vii. Select **multi-value** column and click **Finish**.
      viii. Select **Commit to database**.
      ix. Select **Compile Database**.

   b. Change the created column in **UCIUser** table to multi-value.

      To change the created column in **UCIUser** table to multi-value, repeat the steps that you performed for **CSMUser** table.

3. Create custom mappings and add directions accordingly.
   a. Add mappings for each custom field created.
   b. Add the mapping directions accordingly.

Appendix R

Synchronization and assignment of PermissionSets to Users with One Identity Manager

This section describes the synchronization and assignment of **PermissionSets** to Users with One Identity Manager.

To synchronize and assign PermissionSets to Users with One Identity Manager

For more information, see

1. Creating mapping for PermissionSets using Synchronization Editor
2. Creating a Process Chain using Designer

Creating mapping for PermissionSets using Synchronization Editor

This section describes the procedure to create mapping for **PermissionSets**.

To create mapping for PermissionSets

1. Open the **Synchronization Editor** tool.
2. Open the specific synchronization project.
3. Navigate to **Configuration** | **One Identity Manager Connection** |**Update Schema**.
4. Activate the project.
5. Navigate to the **Mappings** tab and click **+** to create a mapping.

6. In the **New mapping** window:
   a. In the **General** section, enter the values in the fields as shown in the table

Table 458: Create new mapping for PermissionSets - General section

Field	Value
Mapping name	PermissionSets
Mapping direction	Both directions

NOTE: Select the option **Maps objects referenced by multiple references**.

   b. In the **Relation** section, enter the values in the fields as shown in the table

Table 459: Create new mapping for PermissionSets - Relation section

Field	Value
One Identity Manager schema class	PermissionSets
Target system schema class	PermissionSets(all)

   c. Click **Ok** and click **Next**.
7. In the **Mapping Wizard**:
   a. In the **Select task** section, select the template **Create rules based on template**, click **Next**.
   b. In the **Select source mapping** section, select **Group** and click **Next**.
   c. Verify the **Analysis Result** and click **Next** and then click **Finish**.
8. To add the virtual parameter
   a. Select **Mappings| PermissionSets** .
   b. Select **+** to create a property.
   c. In the **Create property** window, from the **Property type** list, select **Members of M:N schema types** .
   d. Enter the following values, for example, in the fields mentioned in the table, and select the options listed below:

Table 460: Virtual parameters

Field/ Option	Value
Name	vrtUser
Display name	vrtUser

Select the following options, below the **Display name** field, according to your requirements:

- Ignore case
- Try to mark the objects for deletion (outstanding)

e. Click **+** to add the schema type.

f. Select the **Member key properties** for **Group** as listed in the table below

Table 461: Member key properties

Entity	Value
M:N schema type	UCIUserHasItem
	UID_UCIItem
	UID_UCIUser
Primary key property	OjectGUID

g. Click **Ok**.

h. Add a new mapping rule Value Comparison Rule with **vrtUser <--> members~value**.

i. Run the synchronization.

Creating a Process Chain using Designer

This section describes the procedure to create a Process Chain using **Designer**.

To create a Process Chain using Designer

1. Open the **Designer** tool.
2. In the **Navigation** pane, select **Process Orchestration** |**Custom process**| **Navigation**| **Process Editor**| **Create a new process**.
   The **Process properties** window is displayed.
3. In the **General** tab of the **Process properties** window, enter the following values:

Table 462: Values for creating custom process for PermssionSets

Process properties	Value
Name	UCI_UCIPermissionSethasItem_Update
Table	UCIUserHasItem

Process properties	Value

Pre-script for generating	`If Not CBool(Connection.Variables("FULLSYNC")) AndAlso _`
	`Not CBool(Connection.Variables("PendingChangeReady")) AndAlso _`
	`Not $FK(UID_UCIItem).FK(UID_UCIRoot).IsManualProvisioning:Bool$ Then`
	
	`Imports System.Collections.Generic`
	`Dim data As IDictionary(Of String,string) = Nothing`
	`values("AdHocDataFound") = False`
	`values("NeedExecute") = true`
	`' try to get UCI data`
	`Try`
	`Dim myUCIItem As ISingleDbObject = Connection.CreateSingle("UCIItem",$UID_UCIItem$)`
	`data = DPR_GetAdHocData($FK(UID_UCIItem).FK(UID_UCIRoot).XObjectKey$,"SCIM","","Update",myUCIItem.GetEntity())`
	`Catch ex As AdHocDataException`
	`End Try`
	`If Not data is Nothing`
	`values("AdHocDataFound") = True`
	`values("ObjectKey") = New DbObjectKey("UCIItem",$UID_UCIItem$).ToXmlString()`
	`values("UID_DPRSystemVariableSet") = data("VariableSetUID")`
	`values("UID_DPRProjectionConfiguration") = data("ProjectionConfigUID")`
	`values("UID_QBMServer") = UCI_GetProvisioningServer(data("ExecutionServerUID"), Entity, data("ExecutionServerTag"))`
	`End if`

Generating condition	`Value = Not CBool(Connection.Variables("FULLSYNC")) AndAlso _`
	`Not CBool(Connection.Variables("PendingChangeReady")) AndAlso _`
	`Not $FK(UID_UCIItem).FK(UID_`

Process properties	Value

	`UCIRoot).IsManualProvisioning:Bool$ AndAlso _`
	`CBool(values("AdHocDataFound")) Andalso _`
	`UCI_TargetUsesProfiles($FK(UID_UCIItem).UID_UCIRoot$)`

4. In the **Events** tab, at the bottom of the page, click **+**.
   The **Edit event** window is displayed.
5. In the **Edit event** window, click **+** next to the **Object Event** field.

   The **Edit object event** window is displayed.
6. In the **Edit object event**, select **Delete** and then **Insert** from the list. Click **OK**.
   The **Process step properties** window is displayed.
7. In the **Process step properties** window, select the values as follows:
   a. In the **General tab**, in the **Name** field, enter the value **PUT/PATCH Group**.
   b. Select **ProjectorComponent – AdHocProjectionSingle** from the **Process Task** drop down list.
   c. In the **Generation** tab, enter the script for server selection: `Value = values ("UID_QBMServer").ToString()`.
   d. In the **Error Handling** tab, select **Stop on Error**.
8. In the **Parameters** tab at the bottom, add the values for **ForceSyncOf**: `Value = "UID_UCIUser,vrtProfilesArr,vrtUser"`.
9. Set the parameter **CausingEntityPatch** to the following value:
   ```
   Dim myUCIItem As ISingleDbObject =
   Connection.CreateSingle("UCIItem",$UID_UCIItem$)
   Value = DPR_WrapObjectForProjection(myUCIItem.GetEntity())
   ```

   The custom process **UCI_UCIPermissionSethasItem_Update** is created for **PermissionSets**.
10. Click **Commit to Database**.
11. Select **Database**| **Compile Database** in the **Designer** tool.

Appendix S

Connectors that support password attribute in User object

The **password** attribute of **User** object is a **writeOnly** field for all the connectors.

Connectors that support the **password** attribute in the **User** object

- Amazon S3 AWS
- AppDynamics
- Atlassian JIRA
- AWS Cognito
- Citrix ShareFile
- Crowd
- JIRA
- Oracle IDCS
- PingOne
- Salesforce
- SAP Litmos
- ServiceNow

Appendix T

Connectors that do not support special characters in the object ID

Starling Connect does not support special characters with the exceptions of a few such as @, +, _, - and so on in the object ID, for example, **User ID** and **Group ID**.

According to SCIM standards (*RFC https://tools.ietf.org/html/rfc7643#section-3.1*), the object ID must be a stable, non-reassignable identifier that does not change when the same resource is returned in subsequent requests.

However, there are some exceptions with some applications and hence, the corresponding connectors do not have an ID assigned. In these connectors, the **username** is considered to be object ID. There is a possibility that special characters are contained in the **username**, which would eventually become a part of the ID of the object. This causes an issue while returning the object details through the connector.

The current design of connectors does not have the capability to process the ID passed at the URI of the endpoints. Hence, Starling Connect returns error 404 with the message *The resource you are looking for has been removed, had its name changed, or is temporarily unavailable*.

Connectors that do not support special characters in the object ID

The connectors that have this issue are

- AmazonS3AWS
- Crowd
- JiraServer
- Apigee

Appendix T

Creating an app for using SCIM on Slack Enterprise Grid Organization

On the **Enterprise Grid**, SCIM operations work across the entire organization and not an individual workspaces. A SCIM app can provision, de-provision, and update team members in just one place rather than having to do so across every workspace in an organization.

To achieve this, the **OAuth** token used for calling SCIM API methods must be obtained by installing the app on the organization and not just a workspace within the organization.

To get a SCIM app working on a grid organization

1. Ensure that the web service that is powering your application is able to handle a standard **OAuth 2** flow.
2. Create a new Slack app.
3. In the application settings, select **OAuth & Permissions** from the left navigation.
4. In the **Redirect URLs** section, save the URL *https://connect-supervisor.cloud.oneidentity.com/v1/consent.*
5. In the **Scopes** section, add the **admin** scope and click **Save Changes**.
6. In the application settings, select **Manage Distribution** from the left navigation.
7. In the **Share Your App with Other Workspaces** section, make sure all four sections have the green check.
8. Click **Activate Public Distribution**.
9. Collect the **Client Id** and **Client Secret** of the app.
10. While configuring this application for consent flow in Starling UI, provide the **Client Id** and **Client Secret**.
11. When the consent flow is initiated, the **OAuth** handshake will install the application on your organization.
    You must be logged in as an owner of your **Enterprise Grid organization** to install the application
12. Check the dropdown in the upper right corner of the installation screen to make sure you are installing the application on the **Enterprise Grid organization**, but not on an individual workspace within the organization.

13. Once the app completes the **OAuth** flow, it will grant an **OAuth** token that can be used for accessing all of the SCIM API methods for the **Slack enterprise organization**.

Appendix U

Creating a Webex integration application, providing necessary scopes, retrieving Client Id and Client Secret

This section describes the procedure to create an integration application, provide necessary scopes, retrieve Client Id and Client Secret

To creating an integration application, providing necessary scopes, retrieving Client Id and Client Secret

1. Create a new application of type **Integration** in https://developer.webex.com/my-apps.
2. Provide the redirect URL https://connect-supervisor.cloud.oneidentity.com/v1/consent for US data center and https://connect-supervisor.cloud.oneidentity.eu/v1/consent for EU data center of the Starling Connect.
3. Provide the below scopes
   - spark:team_memberships_read
   - spark:team_memberships_write
   - spark:teams_read
   - spark:teams_write
   - spark-admin:licenses_read
   - spark-admin:organizations_read
   - spark-admin:people_read
   - spark-admin:people_write
   - spark-admin:roles_read
4. Collect the client ID and client Secret of the integration application.

Appendix V

Retrieving the API key from Facebook Workplace

This section describes the procedure to retrieve the API key from Facebook Workplace that you must use when you configure the connector in Starling Connect.

To retrieve the API key from Facebook Workplace

1. In the admin account, go to "Admin Panel", select "Integrations".
2. Create a Custom Integration.
3. Go to the custom integration created and under "Details" menu, select the "Create Access Token" and copy the access token created.
    - This Access Token is to be used as the value for API Key in the Connector Configuration.
4. Under "Permissions" menu of the custom integration, select the permissions:
    - Read group membership
    - Manage accounts
    - Manage groups
    - Manage work profiles
    - Provision user accounts
    - Read group content
    - Read user email
    - Read work profile
5. Under the "Give integration access to groups" section of "Permissions" page, select the "Group permissions" to "All groups".

Appendix W

Outbound IP addresses

This section has the list of outbound IP Addresses for all the Starling Connect connectors. The outbound connection from a given Starling Connect connector uses one of the outbound IP addresses as the origin IP address. To white list the connector in firewall environments, administrators are recommended to open its firewall to all the possible outbound IP addresses listed against the each given connector.

NOTE:

- As Starling Connect connectors are SaaS based deployments, the outbound IP list may get added with new IP addresses. This happens very rarely and only after the given Additional Possible Outbound IP addresses are consumed.
- We recommend customers to check this list for latest IP addresses in case of failures in the communication.

Click the connector name in the list for the outbound IP addresses of the particular connector:

Salesforce

Facebook Workplace

SAP Cloud Platform

JIRA Server

RSA Archer

Successfactors

Amazon S3 AWS

ServiceNow

Dropbox

Crowd

Atlassian JIRA Confluence

Trello

Box

Pipedrive

SuccessFactors HR

NutShell

Insightly
Egnyte
SugarCRM
Oracle IDCS
Statuspage
Zendesk Sell
Workbooks
DocuSign
Citrix ShareFile
Zendesk
Azure AD
Google Workspace
Concur
Tableau
GoToMeeting
Coupa
AWS Cognito
Okta
Apigee
DataDog
Hideez
OpsGenie
Informatica Cloud Services
AppDynamics
OneLogin
Marketo
Workday HR
PingOne
Aha!
Hacker Rank
SAP Litmos
Slack
ActiveCampaign
WebEx
Databricks

Hive
PagerDuty
Dayforce
Smartsheet
Pingboard

Salesforce

West US	East US	North Europe
Possible Outbound IP Addresses	**Possible Outbound IP Addresses**	**Possible Outbound IP Addresses**
40.112.243.33	40.71.11.161	20.50.64.32
104.40.57.101	191.238.32.104	20.105.97.248
104.40.82.23	191.238.32.154	20.105.98.61
104.40.81.188	191.238.34.67	20.105.98.138
104.40.85.254	191.238.35.12	20.105.99.3
40.78.71.184	52.154.76.248	20.105.99.41
40.83.166.253	52.154.76.250	20.105.99.224
40.83.173.206	13.72.72.29	20.93.14.38
40.83.166.164	52.154.76.249	20.93.15.169
40.83.165.34	52.154.76.251	20.93.15.194
104.42.58.78	20.237.8.177	20.93.15.234
20.237.156.124	20.237.8.218	20.105.96.9
20.245.240.122	20.237.9.91	20.105.96.75
104.42.63.76	20.237.9.253	20.105.96.97
20.245.240.75	20.237.10.71	20.105.96.116
104.42.62.182	20.237.10.171	20.105.96.131
20.66.122.126	20.242.160.128	20.105.96.157
20.66.120.186	20.242.160.131	20.105.96.169
20.66.124.17	20.242.160.212	20.105.96.229
20.66.125.145	20.242.160.229	20.105.96.234

Possible Outbound IP Addresses	Possible Outbound IP Addresses	Possible Outbound IP Addresses
20.66.122.132	20.242.161.84	20.105.96.235
20.66.125.135	20.242.161.144	20.105.96.251
104.40.63.98	191.238.33.50	20.105.97.16
		20.67.164.71
		20.105.96.130
		20.105.97.17
		20.105.96.154
		20.67.209.167
		20.67.212.199
		20.82.169.132
		20.82.170.255
		20.50.64.32

Facebook Workplace

West US

Possible Outbound IP Addresses
40.112.243.33
104.40.57.101
104.40.82.23
104.40.81.188
104.40.85.254
40.78.71.184
40.83.166.253
40.83.173.206
40.83.166.164
40.83.165.34

East US

Possible Outbound IP Addresses
40.71.11.161
191.238.32.104
191.238.32.154
191.238.34.67
191.238.35.12
52.154.76.248
52.154.76.250
13.72.72.29
52.154.76.249
52.154.76.251

North Europe

Possible Outbound IP Addresses
20.50.64.32
20.105.97.248
20.105.98.61
20.105.98.138
20.105.99.3
20.105.99.41
20.105.99.224
20.93.14.38
20.93.15.169
20.93.15.194

Possible Outbound IP Addresses	Possible Outbound IP Addresses	Possible Outbound IP Addresses
104.42.58.78	20.237.8.177	20.93.15.234
20.237.156.124	20.237.8.218	20.105.96.9
20.245.240.122	20.237.9.91	20.105.96.75
104.42.63.76	20.237.9.253	20.105.96.97
20.245.240.75	20.237.10.71	20.105.96.116
104.42.62.182	20.237.10.171	20.105.96.131
20.66.122.126	20.242.160.128	20.105.96.157
20.66.120.186	20.242.160.131	20.105.96.169
20.66.124.17	20.242.160.212	20.105.96.229
20.66.125.145	20.242.160.229	20.105.96.234
20.66.122.132	20.242.161.84	20.105.96.235
20.66.125.135	20.242.161.144	20.105.96.251
104.40.63.98	191.238.33.50	20.105.97.16
		20.67.164.71
		20.105.96.130
		20.105.97.17
		20.105.96.154
		20.67.209.167
		20.67.212.199
		20.82.169.132
		20.82.170.255
		20.50.64.32

SAP Cloud Platform

West US	East US	North Europe

Possible Outbound IP Addresses	Possible Outbound IP Addresses	Possible Outbound IP Addresses
40.112.243.33	40.71.11.161	20.50.64.32
104.40.57.101	191.238.32.104	20.105.97.248
104.40.82.23	191.238.32.154	20.105.98.61
104.40.81.188	191.238.34.67	20.105.98.138
104.40.85.254	191.238.35.12	20.105.99.3
40.78.71.184	52.154.76.248	20.105.99.41
40.83.166.253	52.154.76.250	20.105.99.224
40.83.173.206	13.72.72.29	20.93.14.38
40.83.166.164	52.154.76.249	20.93.15.169
40.83.165.34	52.154.76.251	20.93.15.194
104.42.58.78	20.237.8.177	20.93.15.234
20.237.156.124	20.237.8.218	20.105.96.9
20.245.240.122	20.237.9.91	20.105.96.75
104.42.63.76	20.237.9.253	20.105.96.97
20.245.240.75	20.237.10.71	20.105.96.116
104.42.62.182	20.237.10.171	20.105.96.131
20.66.122.126	20.242.160.128	20.105.96.157
20.66.120.186	20.242.160.131	20.105.96.169
20.66.124.17	20.242.160.212	20.105.96.229
20.66.125.145	20.242.160.229	20.105.96.234
20.66.122.132	20.242.161.84	20.105.96.235
20.66.125.135	20.242.161.144	20.105.96.251
104.40.63.98	191.238.33.50	20.105.97.16
		20.67.164.71
		20.105.96.130
		20.105.97.17
		20.105.96.154
		20.67.209.167
		20.67.212.199
		20.82.169.132
		20.82.170.255
		20.50.64.32

JIRA Server

West US

Possible Outbound IP Addresses
40.112.243.33
104.40.57.101
104.40.82.23
104.40.81.188
104.40.85.254
40.78.71.184
40.83.166.253
40.83.173.206
40.83.166.164
40.83.165.34
104.42.58.78
20.237.156.124
20.245.240.122
104.42.63.76
20.245.240.75
104.42.62.182
20.66.122.126
20.66.120.186
20.66.124.17
20.66.125.145
20.66.122.132
20.66.125.135
104.40.63.98

East US

Possible Outbound IP Addresses
40.71.11.161
191.238.32.104
191.238.32.154
191.238.34.67
191.238.35.12
52.154.76.248
52.154.76.250
13.72.72.29
52.154.76.249
52.154.76.251
20.237.8.177
20.237.8.218
20.237.9.91
20.237.9.253
20.237.10.71
20.237.10.171
20.242.160.128
20.242.160.131
20.242.160.212
20.242.160.229
20.242.161.84
20.242.161.144
191.238.33.50

North Europe

Possible Outbound IP Addresses
20.50.64.32
20.105.97.248
20.105.98.61
20.105.98.138
20.105.99.3
20.105.99.41
20.105.99.224
20.93.14.38
20.93.15.169
20.93.15.194
20.93.15.234
20.105.96.9
20.105.96.75
20.105.96.97
20.105.96.116
20.105.96.131
20.105.96.157
20.105.96.169
20.105.96.229
20.105.96.234
20.105.96.235
20.105.96.251
20.105.97.16
20.67.164.71
20.105.96.130
20.105.97.17

Possible Outbound IP Addresses
20.105.96.154
20.67.209.167
20.67.212.199
20.82.169.132
20.82.170.255
20.50.64.32

RSA Archer

West US

Possible Outbound IP Addresses
40.112.243.33
104.40.57.101
104.40.82.23
104.40.81.188
104.40.85.254
40.78.71.184
40.83.166.253
40.83.173.206
40.83.166.164
40.83.165.34
104.42.58.78
20.237.156.124
20.245.240.122
104.42.63.76
20.245.240.75
104.42.62.182

East US

Possible Outbound IP Addresses
40.71.11.161
191.238.32.104
191.238.32.154
191.238.34.67
191.238.35.12
52.154.76.248
52.154.76.250
13.72.72.29
52.154.76.249
52.154.76.251
20.237.8.177
20.237.8.218
20.237.9.91
20.237.9.253
20.237.10.71
20.237.10.171

North Europe

Possible Outbound IP Addresses
20.50.64.32
20.105.97.248
20.105.98.61
20.105.98.138
20.105.99.3
20.105.99.41
20.105.99.224
20.93.14.38
20.93.15.169
20.93.15.194
20.93.15.234
20.105.96.9
20.105.96.75
20.105.96.97
20.105.96.116
20.105.96.131

Possible Outbound IP Addresses	Possible Outbound IP Addresses	Possible Outbound IP Addresses
20.66.122.126	20.242.160.128	20.105.96.157
20.66.120.186	20.242.160.131	20.105.96.169
20.66.124.17	20.242.160.212	20.105.96.229
20.66.125.145	20.242.160.229	20.105.96.234
20.66.122.132	20.242.161.84	20.105.96.235
20.66.125.135	20.242.161.144	20.105.96.251
104.40.63.98	191.238.33.50	20.105.97.16
		20.67.164.71
		20.105.96.130
		20.105.97.17
		20.105.96.154
		20.67.209.167
		20.67.212.199
		20.82.169.132
		20.82.170.255
		20.50.64.32

Successfactors

West US

Possible Outbound IP Addresses
40.112.243.33
104.40.57.101
104.40.82.23
104.40.81.188
104.40.85.254
40.78.71.184

East US

Possible Outbound IP Addresses
40.71.11.161
191.238.32.104
191.238.32.154
191.238.34.67
191.238.35.12
52.154.76.248

North Europe

Possible Outbound IP Addresses
20.50.64.32
20.105.97.248
20.105.98.61
20.105.98.138
20.105.99.3
20.105.99.41

Possible Outbound IP Addresses	Possible Outbound IP Addresses	Possible Outbound IP Addresses
40.83.166.253	52.154.76.250	20.105.99.224
40.83.173.206	13.72.72.29	20.93.14.38
40.83.166.164	52.154.76.249	20.93.15.169
40.83.165.34	52.154.76.251	20.93.15.194
104.42.58.78	20.237.8.177	20.93.15.234
20.237.156.124	20.237.8.218	20.105.96.9
20.245.240.122	20.237.9.91	20.105.96.75
104.42.63.76	20.237.9.253	20.105.96.97
20.245.240.75	20.237.10.71	20.105.96.116
104.42.62.182	20.237.10.171	20.105.96.131
20.66.122.126	20.242.160.128	20.105.96.157
20.66.120.186	20.242.160.131	20.105.96.169
20.66.124.17	20.242.160.212	20.105.96.229
20.66.125.145	20.242.160.229	20.105.96.234
20.66.122.132	20.242.161.84	20.105.96.235
20.66.125.135	20.242.161.144	20.105.96.251
104.40.63.98	191.238.33.50	20.105.97.16
		20.67.164.71
		20.105.96.130
		20.105.97.17
		20.105.96.154
		20.67.209.167
		20.67.212.199
		20.82.169.132
		20.82.170.255
		20.50.64.32

Amazon S3 AWS

West US	East US	North Europe

Possible Outbound IP Addresses	Possible Outbound IP Addresses	Possible Outbound IP Addresses
40.112.243.33	40.71.11.161	20.50.64.32
104.40.57.101	191.238.32.104	20.105.97.248
104.40.82.23	191.238.32.154	20.105.98.61
104.40.81.188	191.238.34.67	20.105.98.138
104.40.85.254	191.238.35.12	20.105.99.3
40.78.71.184	52.154.76.248	20.105.99.41
40.83.166.253	52.154.76.250	20.105.99.224
40.83.173.206	13.72.72.29	20.93.14.38
40.83.166.164	52.154.76.249	20.93.15.169
40.83.165.34	52.154.76.251	20.93.15.194
104.42.58.78	20.237.8.177	20.93.15.234
20.237.156.124	20.237.8.218	20.105.96.9
20.245.240.122	20.237.9.91	20.105.96.75
104.42.63.76	20.237.9.253	20.105.96.97
20.245.240.75	20.237.10.71	20.105.96.116
104.42.62.182	20.237.10.171	20.105.96.131
20.66.122.126	20.242.160.128	20.105.96.157
20.66.120.186	20.242.160.131	20.105.96.169
20.66.124.17	20.242.160.212	20.105.96.229
20.66.125.145	20.242.160.229	20.105.96.234
20.66.122.132	20.242.161.84	20.105.96.235
20.66.125.135	20.242.161.144	20.105.96.251
104.40.63.98	191.238.33.50	20.105.97.16
		20.67.164.71
		20.105.96.130
		20.105.97.17
		20.105.96.154
		20.67.209.167
		20.67.212.199
		20.82.169.132
		20.82.170.255
		20.50.64.32

ServiceNow

West US

Possible Outbound IP Addresses
40.112.243.33
104.40.57.101
104.40.82.23
104.40.81.188
104.40.85.254
40.78.71.184
40.83.166.253
40.83.173.206
40.83.166.164
40.83.165.34
104.42.58.78
20.237.156.124
20.245.240.122
104.42.63.76
20.245.240.75
104.42.62.182
20.66.122.126
20.66.120.186
20.66.124.17
20.66.125.145
20.66.122.132
20.66.125.135
104.40.63.98

East US

Possible Outbound IP Addresses
40.71.11.161
191.238.32.104
191.238.32.154
191.238.34.67
191.238.35.12
52.154.76.248
52.154.76.250
13.72.72.29
52.154.76.249
52.154.76.251
20.237.8.177
20.237.8.218
20.237.9.91
20.237.9.253
20.237.10.71
20.237.10.171
20.242.160.128
20.242.160.131
20.242.160.212
20.242.160.229
20.242.161.84
20.242.161.144
191.238.33.50

North Europe

Possible Outbound IP Addresses
20.50.64.32
20.105.97.248
20.105.98.61
20.105.98.138
20.105.99.3
20.105.99.41
20.105.99.224
20.93.14.38
20.93.15.169
20.93.15.194
20.93.15.234
20.105.96.9
20.105.96.75
20.105.96.97
20.105.96.116
20.105.96.131
20.105.96.157
20.105.96.169
20.105.96.229
20.105.96.234
20.105.96.235
20.105.96.251
20.105.97.16
20.67.164.71
20.105.96.130
20.105.97.17

Possible Outbound IP Addresses
20.105.96.154
20.67.209.167
20.67.212.199
20.82.169.132
20.82.170.255
20.50.64.32

Dropbox

West US

Possible Outbound IP Addresses
40.112.243.33
104.40.57.101
104.40.82.23
104.40.81.188
104.40.85.254
40.78.71.184
40.83.166.253
40.83.173.206
40.83.166.164
40.83.165.34
104.42.58.78
20.237.156.124
20.245.240.122
104.42.63.76
20.245.240.75
104.42.62.182

East US

Possible Outbound IP Addresses
40.71.11.161
191.238.32.104
191.238.32.154
191.238.34.67
191.238.35.12
52.154.76.248
52.154.76.250
13.72.72.29
52.154.76.249
52.154.76.251
20.237.8.177
20.237.8.218
20.237.9.91
20.237.9.253
20.237.10.71
20.237.10.171

North Europe

Possible Outbound IP Addresses
20.50.64.32
20.105.97.248
20.105.98.61
20.105.98.138
20.105.99.3
20.105.99.41
20.105.99.224
20.93.14.38
20.93.15.169
20.93.15.194
20.93.15.234
20.105.96.9
20.105.96.75
20.105.96.97
20.105.96.116
20.105.96.131

Possible Outbound IP Addresses	Possible Outbound IP Addresses	Possible Outbound IP Addresses
20.66.122.126	20.242.160.128	20.105.96.157
20.66.120.186	20.242.160.131	20.105.96.169
20.66.124.17	20.242.160.212	20.105.96.229
20.66.125.145	20.242.160.229	20.105.96.234
20.66.122.132	20.242.161.84	20.105.96.235
20.66.125.135	20.242.161.144	20.105.96.251
104.40.63.98	191.238.33.50	20.105.97.16
		20.67.164.71
		20.105.96.130
		20.105.97.17
		20.105.96.154
		20.67.209.167
		20.67.212.199
		20.82.169.132
		20.82.170.255
		20.50.64.32

Crowd

West US

Possible Outbound IP Addresses
40.112.243.33
104.40.57.101
104.40.82.23
104.40.81.188
104.40.85.254
40.78.71.184

East US

Possible Outbound IP Addresses
40.71.11.161
191.238.32.104
191.238.32.154
191.238.34.67
191.238.35.12
52.154.76.248

North Europe

Possible Outbound IP Addresses
20.50.64.32
20.105.97.248
20.105.98.61
20.105.98.138
20.105.99.3
20.105.99.41

Possible Outbound IP Addresses	Possible Outbound IP Addresses	Possible Outbound IP Addresses
40.83.166.253	52.154.76.250	20.105.99.224
40.83.173.206	13.72.72.29	20.93.14.38
40.83.166.164	52.154.76.249	20.93.15.169
40.83.165.34	52.154.76.251	20.93.15.194
104.42.58.78	20.237.8.177	20.93.15.234
20.237.156.124	20.237.8.218	20.105.96.9
20.245.240.122	20.237.9.91	20.105.96.75
104.42.63.76	20.237.9.253	20.105.96.97
20.245.240.75	20.237.10.71	20.105.96.116
104.42.62.182	20.237.10.171	20.105.96.131
20.66.122.126	20.242.160.128	20.105.96.157
20.66.120.186	20.242.160.131	20.105.96.169
20.66.124.17	20.242.160.212	20.105.96.229
20.66.125.145	20.242.160.229	20.105.96.234
20.66.122.132	20.242.161.84	20.105.96.235
20.66.125.135	20.242.161.144	20.105.96.251
104.40.63.98	191.238.33.50	20.105.97.16
		20.67.164.71
		20.105.96.130
		20.105.97.17
		20.105.96.154
		20.67.209.167
		20.67.212.199
		20.82.169.132
		20.82.170.255
		20.50.64.32

Atlassian JIRA Confluence

West US	East US	North Europe

Possible Outbound IP Addresses	Possible Outbound IP Addresses	Possible Outbound IP Addresses
40.112.243.33	40.71.11.161	20.50.64.32
104.40.57.101	191.238.32.104	20.105.97.248
104.40.82.23	191.238.32.154	20.105.98.61
104.40.81.188	191.238.34.67	20.105.98.138
104.40.85.254	191.238.35.12	20.105.99.3
40.78.71.184	52.154.76.248	20.105.99.41
40.83.166.253	52.154.76.250	20.105.99.224
40.83.173.206	13.72.72.29	20.93.14.38
40.83.166.164	52.154.76.249	20.93.15.169
40.83.165.34	52.154.76.251	20.93.15.194
104.42.58.78	20.237.8.177	20.93.15.234
20.237.156.124	20.237.8.218	20.105.96.9
20.245.240.122	20.237.9.91	20.105.96.75
104.42.63.76	20.237.9.253	20.105.96.97
20.245.240.75	20.237.10.71	20.105.96.116
104.42.62.182	20.237.10.171	20.105.96.131
20.66.122.126	20.242.160.128	20.105.96.157
20.66.120.186	20.242.160.131	20.105.96.169
20.66.124.17	20.242.160.212	20.105.96.229
20.66.125.145	20.242.160.229	20.105.96.234
20.66.122.132	20.242.161.84	20.105.96.235
20.66.125.135	20.242.161.144	20.105.96.251
104.40.63.98	191.238.33.50	20.105.97.16
		20.67.164.71
		20.105.96.130
		20.105.97.17
		20.105.96.154
		20.67.209.167
		20.67.212.199
		20.82.169.132
		20.82.170.255
		20.50.64.32

Trello

West US

Possible Outbound IP Addresses
40.112.243.33
104.40.57.101
104.40.82.23
104.40.81.188
104.40.85.254
40.78.71.184
40.83.166.253
40.83.173.206
40.83.166.164
40.83.165.34
104.42.58.78
20.237.156.124
20.245.240.122
104.42.63.76
20.245.240.75
104.42.62.182
20.66.122.126
20.66.120.186
20.66.124.17
20.66.125.145
20.66.122.132
20.66.125.135
104.40.63.98

East US

Possible Outbound IP Addresses
40.71.11.161
191.238.32.104
191.238.32.154
191.238.34.67
191.238.35.12
52.154.76.248
52.154.76.250
13.72.72.29
52.154.76.249
52.154.76.251
20.237.8.177
20.237.8.218
20.237.9.91
20.237.9.253
20.237.10.71
20.237.10.171
20.242.160.128
20.242.160.131
20.242.160.212
20.242.160.229
20.242.161.84
20.242.161.144
191.238.33.50

North Europe

Possible Outbound IP Addresses
20.50.64.32
20.105.97.248
20.105.98.61
20.105.98.138
20.105.99.3
20.105.99.41
20.105.99.224
20.93.14.38
20.93.15.169
20.93.15.194
20.93.15.234
20.105.96.9
20.105.96.75
20.105.96.97
20.105.96.116
20.105.96.131
20.105.96.157
20.105.96.169
20.105.96.229
20.105.96.234
20.105.96.235
20.105.96.251
20.105.97.16
20.67.164.71
20.105.96.130
20.105.97.17

Possible Outbound IP Addresses
20.105.96.154
20.67.209.167
20.67.212.199
20.82.169.132
20.82.170.255
20.50.64.32

Box

West US

Possible Outbound IP Addresses
40.112.243.33
104.40.57.101
104.40.82.23
104.40.81.188
104.40.85.254
40.78.71.184
40.83.166.253
40.83.173.206
40.83.166.164
40.83.165.34
104.42.58.78
20.237.156.124
20.245.240.122
104.42.63.76
20.245.240.75
104.42.62.182

East US

Possible Outbound IP Addresses
40.71.11.161
191.238.32.104
191.238.32.154
191.238.34.67
191.238.35.12
52.154.76.248
52.154.76.250
13.72.72.29
52.154.76.249
52.154.76.251
20.237.8.177
20.237.8.218
20.237.9.91
20.237.9.253
20.237.10.71
20.237.10.171

North Europe

Possible Outbound IP Addresses
20.50.64.32
20.105.97.248
20.105.98.61
20.105.98.138
20.105.99.3
20.105.99.41
20.105.99.224
20.93.14.38
20.93.15.169
20.93.15.194
20.93.15.234
20.105.96.9
20.105.96.75
20.105.96.97
20.105.96.116
20.105.96.131

Possible Outbound IP Addresses	Possible Outbound IP Addresses	Possible Outbound IP Addresses
20.66.122.126	20.242.160.128	20.105.96.157
20.66.120.186	20.242.160.131	20.105.96.169
20.66.124.17	20.242.160.212	20.105.96.229
20.66.125.145	20.242.160.229	20.105.96.234
20.66.122.132	20.242.161.84	20.105.96.235
20.66.125.135	20.242.161.144	20.105.96.251
104.40.63.98	191.238.33.50	20.105.97.16
		20.67.164.71
		20.105.96.130
		20.105.97.17
		20.105.96.154
		20.67.209.167
		20.67.212.199
		20.82.169.132
		20.82.170.255
		20.50.64.32

Pipedrive

West US	East US	North Europe
Possible Outbound IP Addresses	**Possible Outbound IP Addresses**	**Possible Outbound IP Addresses**
40.112.243.33	40.71.11.161	20.50.64.32
104.40.57.101	191.238.32.104	20.105.97.248
104.40.82.23	191.238.32.154	20.105.98.61
104.40.81.188	191.238.34.67	20.105.98.138
104.40.85.254	191.238.35.12	20.105.99.3
40.78.71.184	52.154.76.248	20.105.99.41

Possible Outbound IP Addresses	Possible Outbound IP Addresses	Possible Outbound IP Addresses
40.83.166.253	52.154.76.250	20.105.99.224
40.83.173.206	13.72.72.29	20.93.14.38
40.83.166.164	52.154.76.249	20.93.15.169
40.83.165.34	52.154.76.251	20.93.15.194
104.42.58.78	20.237.8.177	20.93.15.234
20.237.156.124	20.237.8.218	20.105.96.9
20.245.240.122	20.237.9.91	20.105.96.75
104.42.63.76	20.237.9.253	20.105.96.97
20.245.240.75	20.237.10.71	20.105.96.116
104.42.62.182	20.237.10.171	20.105.96.131
20.66.122.126	20.242.160.128	20.105.96.157
20.66.120.186	20.242.160.131	20.105.96.169
20.66.124.17	20.242.160.212	20.105.96.229
20.66.125.145	20.242.160.229	20.105.96.234
20.66.122.132	20.242.161.84	20.105.96.235
20.66.125.135	20.242.161.144	20.105.96.251
104.40.63.98	191.238.33.50	20.105.97.16
		20.67.164.71
		20.105.96.130
		20.105.97.17
		20.105.96.154
		20.67.209.167
		20.67.212.199
		20.82.169.132
		20.82.170.255
		20.50.64.32

SuccessFactors HR

West US	East US	North Europe

Possible Outbound IP Addresses	Possible Outbound IP Addresses	Possible Outbound IP Addresses
40.112.243.33	40.71.11.161	20.50.64.32
104.40.57.101	191.238.32.104	20.105.97.248
104.40.82.23	191.238.32.154	20.105.98.61
104.40.81.188	191.238.34.67	20.105.98.138
104.40.85.254	191.238.35.12	20.105.99.3
40.78.71.184	52.154.76.248	20.105.99.41
40.83.166.253	52.154.76.250	20.105.99.224
40.83.173.206	13.72.72.29	20.93.14.38
40.83.166.164	52.154.76.249	20.93.15.169
40.83.165.34	52.154.76.251	20.93.15.194
104.42.58.78	20.237.8.177	20.93.15.234
20.237.156.124	20.237.8.218	20.105.96.9
20.245.240.122	20.237.9.91	20.105.96.75
104.42.63.76	20.237.9.253	20.105.96.97
20.245.240.75	20.237.10.71	20.105.96.116
104.42.62.182	20.237.10.171	20.105.96.131
20.66.122.126	20.242.160.128	20.105.96.157
20.66.120.186	20.242.160.131	20.105.96.169
20.66.124.17	20.242.160.212	20.105.96.229
20.66.125.145	20.242.160.229	20.105.96.234
20.66.122.132	20.242.161.84	20.105.96.235
20.66.125.135	20.242.161.144	20.105.96.251
104.40.63.98	191.238.33.50	20.105.97.16
		20.67.164.71
		20.105.96.130
		20.105.97.17
		20.105.96.154
		20.67.209.167
		20.67.212.199
		20.82.169.132
		20.82.170.255
		20.50.64.32

NutShell

West US

Possible Outbound IP Addresses
40.112.243.33
104.40.57.101
104.40.82.23
104.40.81.188
104.40.85.254
40.78.71.184
40.83.166.253
40.83.173.206
40.83.166.164
40.83.165.34
104.42.58.78
20.237.156.124
20.245.240.122
104.42.63.76
20.245.240.75
104.42.62.182
20.66.122.126
20.66.120.186
20.66.124.17
20.66.125.145
20.66.122.132
20.66.125.135
104.40.63.98

East US

Possible Outbound IP Addresses
40.71.11.161
191.238.32.104
191.238.32.154
191.238.34.67
191.238.35.12
52.154.76.248
52.154.76.250
13.72.72.29
52.154.76.249
52.154.76.251
20.237.8.177
20.237.8.218
20.237.9.91
20.237.9.253
20.237.10.71
20.237.10.171
20.242.160.128
20.242.160.131
20.242.160.212
20.242.160.229
20.242.161.84
20.242.161.144
191.238.33.50

North Europe

Possible Outbound IP Addresses
20.50.64.32
20.105.97.248
20.105.98.61
20.105.98.138
20.105.99.3
20.105.99.41
20.105.99.224
20.93.14.38
20.93.15.169
20.93.15.194
20.93.15.234
20.105.96.9
20.105.96.75
20.105.96.97
20.105.96.116
20.105.96.131
20.105.96.157
20.105.96.169
20.105.96.229
20.105.96.234
20.105.96.235
20.105.96.251
20.105.97.16
20.67.164.71
20.105.96.130
20.105.97.17

Possible Outbound IP Addresses
20.105.96.154
20.67.209.167
20.67.212.199
20.82.169.132
20.82.170.255
20.50.64.32

Insightly

West US

Possible Outbound IP Addresses
40.112.243.33
104.40.57.101
104.40.82.23
104.40.81.188
104.40.85.254
40.78.71.184
40.83.166.253
40.83.173.206
40.83.166.164
40.83.165.34
104.42.58.78
20.237.156.124
20.245.240.122
104.42.63.76
20.245.240.75
104.42.62.182

East US

Possible Outbound IP Addresses
40.71.11.161
191.238.32.104
191.238.32.154
191.238.34.67
191.238.35.12
52.154.76.248
52.154.76.250
13.72.72.29
52.154.76.249
52.154.76.251
20.237.8.177
20.237.8.218
20.237.9.91
20.237.9.253
20.237.10.71
20.237.10.171

North Europe

Possible Outbound IP Addresses
20.50.64.32
20.105.97.248
20.105.98.61
20.105.98.138
20.105.99.3
20.105.99.41
20.105.99.224
20.93.14.38
20.93.15.169
20.93.15.194
20.93.15.234
20.105.96.9
20.105.96.75
20.105.96.97
20.105.96.116
20.105.96.131

Possible Outbound IP Addresses	Possible Outbound IP Addresses	Possible Outbound IP Addresses
20.66.122.126	20.242.160.128	20.105.96.157
20.66.120.186	20.242.160.131	20.105.96.169
20.66.124.17	20.242.160.212	20.105.96.229
20.66.125.145	20.242.160.229	20.105.96.234
20.66.122.132	20.242.161.84	20.105.96.235
20.66.125.135	20.242.161.144	20.105.96.251
104.40.63.98	191.238.33.50	20.105.97.16
		20.67.164.71
		20.105.96.130
		20.105.97.17
		20.105.96.154
		20.67.209.167
		20.67.212.199
		20.82.169.132
		20.82.170.255
		20.50.64.32

Egnyte

West US

Possible Outbound IP Addresses
40.112.243.33
104.40.57.101
104.40.82.23
104.40.81.188
104.40.85.254
40.78.71.184

East US

Possible Outbound IP Addresses
40.71.11.161
191.238.32.104
191.238.32.154
191.238.34.67
191.238.35.12
52.154.76.248

North Europe

Possible Outbound IP Addresses
20.50.64.32
20.105.97.248
20.105.98.61
20.105.98.138
20.105.99.3
20.105.99.41

Possible Outbound IP Addresses	Possible Outbound IP Addresses	Possible Outbound IP Addresses
40.83.166.253	52.154.76.250	20.105.99.224
40.83.173.206	13.72.72.29	20.93.14.38
40.83.166.164	52.154.76.249	20.93.15.169
40.83.165.34	52.154.76.251	20.93.15.194
104.42.58.78	20.237.8.177	20.93.15.234
20.237.156.124	20.237.8.218	20.105.96.9
20.245.240.122	20.237.9.91	20.105.96.75
104.42.63.76	20.237.9.253	20.105.96.97
20.245.240.75	20.237.10.71	20.105.96.116
104.42.62.182	20.237.10.171	20.105.96.131
20.66.122.126	20.242.160.128	20.105.96.157
20.66.120.186	20.242.160.131	20.105.96.169
20.66.124.17	20.242.160.212	20.105.96.229
20.66.125.145	20.242.160.229	20.105.96.234
20.66.122.132	20.242.161.84	20.105.96.235
20.66.125.135	20.242.161.144	20.105.96.251
104.40.63.98	191.238.33.50	20.105.97.16
		20.67.164.71
		20.105.96.130
		20.105.97.17
		20.105.96.154
		20.67.209.167
		20.67.212.199
		20.82.169.132
		20.82.170.255
		20.50.64.32

SugarCRM

West US	East US	North Europe

Possible Outbound IP Addresses	Possible Outbound IP Addresses	Possible Outbound IP Addresses
40.112.243.33	40.71.11.161	20.50.64.32
104.40.57.101	191.238.32.104	20.105.97.248
104.40.82.23	191.238.32.154	20.105.98.61
104.40.81.188	191.238.34.67	20.105.98.138
104.40.85.254	191.238.35.12	20.105.99.3
40.78.71.184	52.154.76.248	20.105.99.41
40.83.166.253	52.154.76.250	20.105.99.224
40.83.173.206	13.72.72.29	20.93.14.38
40.83.166.164	52.154.76.249	20.93.15.169
40.83.165.34	52.154.76.251	20.93.15.194
104.42.58.78	20.237.8.177	20.93.15.234
20.237.156.124	20.237.8.218	20.105.96.9
20.245.240.122	20.237.9.91	20.105.96.75
104.42.63.76	20.237.9.253	20.105.96.97
20.245.240.75	20.237.10.71	20.105.96.116
104.42.62.182	20.237.10.171	20.105.96.131
20.66.122.126	20.242.160.128	20.105.96.157
20.66.120.186	20.242.160.131	20.105.96.169
20.66.124.17	20.242.160.212	20.105.96.229
20.66.125.145	20.242.160.229	20.105.96.234
20.66.122.132	20.242.161.84	20.105.96.235
20.66.125.135	20.242.161.144	20.105.96.251
104.40.63.98	191.238.33.50	20.105.97.16
		20.67.164.71
		20.105.96.130
		20.105.97.17
		20.105.96.154
		20.67.209.167
		20.67.212.199
		20.82.169.132
		20.82.170.255
		20.50.64.32

Oracle IDCS

West US

Possible Outbound IP Addresses
40.112.243.33
104.40.57.101
104.40.82.23
104.40.81.188
104.40.85.254
40.78.71.184
40.83.166.253
40.83.173.206
40.83.166.164
40.83.165.34
104.42.58.78
20.237.156.124
20.245.240.122
104.42.63.76
20.245.240.75
104.42.62.182
20.66.122.126
20.66.120.186
20.66.124.17
20.66.125.145
20.66.122.132
20.66.125.135
104.40.63.98

East US

Possible Outbound IP Addresses
40.71.11.161
191.238.32.104
191.238.32.154
191.238.34.67
191.238.35.12
52.154.76.248
52.154.76.250
13.72.72.29
52.154.76.249
52.154.76.251
20.237.8.177
20.237.8.218
20.237.9.91
20.237.9.253
20.237.10.71
20.237.10.171
20.242.160.128
20.242.160.131
20.242.160.212
20.242.160.229
20.242.161.84
20.242.161.144
191.238.33.50

North Europe

Possible Outbound IP Addresses
20.50.64.32
20.105.97.248
20.105.98.61
20.105.98.138
20.105.99.3
20.105.99.41
20.105.99.224
20.93.14.38
20.93.15.169
20.93.15.194
20.93.15.234
20.105.96.9
20.105.96.75
20.105.96.97
20.105.96.116
20.105.96.131
20.105.96.157
20.105.96.169
20.105.96.229
20.105.96.234
20.105.96.235
20.105.96.251
20.105.97.16
20.67.164.71
20.105.96.130
20.105.97.17

Possible Outbound IP Addresses
20.105.96.154
20.67.209.167
20.67.212.199
20.82.169.132
20.82.170.255
20.50.64.32

Statuspage

West US

Possible Outbound IP Addresses
40.112.243.33
104.40.57.101
104.40.82.23
104.40.81.188
104.40.85.254
40.78.71.184
40.83.166.253
40.83.173.206
40.83.166.164
40.83.165.34
104.42.58.78
20.237.156.124
20.245.240.122
104.42.63.76
20.245.240.75
104.42.62.182

East US

Possible Outbound IP Addresses
40.71.11.161
191.238.32.104
191.238.32.154
191.238.34.67
191.238.35.12
52.154.76.248
52.154.76.250
13.72.72.29
52.154.76.249
52.154.76.251
20.237.8.177
20.237.8.218
20.237.9.91
20.237.9.253
20.237.10.71
20.237.10.171

North Europe

Possible Outbound IP Addresses
20.50.64.32
20.105.97.248
20.105.98.61
20.105.98.138
20.105.99.3
20.105.99.41
20.105.99.224
20.93.14.38
20.93.15.169
20.93.15.194
20.93.15.234
20.105.96.9
20.105.96.75
20.105.96.97
20.105.96.116
20.105.96.131

Possible Outbound IP Addresses	Possible Outbound IP Addresses	Possible Outbound IP Addresses
20.66.122.126	20.242.160.128	20.105.96.157
20.66.120.186	20.242.160.131	20.105.96.169
20.66.124.17	20.242.160.212	20.105.96.229
20.66.125.145	20.242.160.229	20.105.96.234
20.66.122.132	20.242.161.84	20.105.96.235
20.66.125.135	20.242.161.144	20.105.96.251
104.40.63.98	191.238.33.50	20.105.97.16
		20.67.164.71
		20.105.96.130
		20.105.97.17
		20.105.96.154
		20.67.209.167
		20.67.212.199
		20.82.169.132
		20.82.170.255
		20.50.64.32

Zendesk Sell

West US

Possible Outbound IP Addresses
40.112.243.33
104.40.57.101
104.40.82.23
104.40.81.188
104.40.85.254
40.78.71.184

East US

Possible Outbound IP Addresses
40.71.11.161
191.238.32.104
191.238.32.154
191.238.34.67
191.238.35.12
52.154.76.248

North Europe

Possible Outbound IP Addresses
20.50.64.32
20.105.97.248
20.105.98.61
20.105.98.138
20.105.99.3
20.105.99.41

Possible Outbound IP Addresses	Possible Outbound IP Addresses	Possible Outbound IP Addresses
40.83.166.253	52.154.76.250	20.105.99.224
40.83.173.206	13.72.72.29	20.93.14.38
40.83.166.164	52.154.76.249	20.93.15.169
40.83.165.34	52.154.76.251	20.93.15.194
104.42.58.78	20.237.8.177	20.93.15.234
20.237.156.124	20.237.8.218	20.105.96.9
20.245.240.122	20.237.9.91	20.105.96.75
104.42.63.76	20.237.9.253	20.105.96.97
20.245.240.75	20.237.10.71	20.105.96.116
104.42.62.182	20.237.10.171	20.105.96.131
20.66.122.126	20.242.160.128	20.105.96.157
20.66.120.186	20.242.160.131	20.105.96.169
20.66.124.17	20.242.160.212	20.105.96.229
20.66.125.145	20.242.160.229	20.105.96.234
20.66.122.132	20.242.161.84	20.105.96.235
20.66.125.135	20.242.161.144	20.105.96.251
104.40.63.98	191.238.33.50	20.105.97.16
		20.67.164.71
		20.105.96.130
		20.105.97.17
		20.105.96.154
		20.67.209.167
		20.67.212.199
		20.82.169.132
		20.82.170.255
		20.50.64.32

Workbooks

West US	East US	North Europe

Possible Outbound IP Addresses	Possible Outbound IP Addresses	Possible Outbound IP Addresses
40.112.243.33	40.71.11.161	20.50.64.32
104.40.57.101	191.238.32.104	20.105.97.248
104.40.82.23	191.238.32.154	20.105.98.61
104.40.81.188	191.238.34.67	20.105.98.138
104.40.85.254	191.238.35.12	20.105.99.3
40.78.71.184	52.154.76.248	20.105.99.41
40.83.166.253	52.154.76.250	20.105.99.224
40.83.173.206	13.72.72.29	20.93.14.38
40.83.166.164	52.154.76.249	20.93.15.169
40.83.165.34	52.154.76.251	20.93.15.194
104.42.58.78	20.237.8.177	20.93.15.234
20.237.156.124	20.237.8.218	20.105.96.9
20.245.240.122	20.237.9.91	20.105.96.75
104.42.63.76	20.237.9.253	20.105.96.97
20.245.240.75	20.237.10.71	20.105.96.116
104.42.62.182	20.237.10.171	20.105.96.131
20.66.122.126	20.242.160.128	20.105.96.157
20.66.120.186	20.242.160.131	20.105.96.169
20.66.124.17	20.242.160.212	20.105.96.229
20.66.125.145	20.242.160.229	20.105.96.234
20.66.122.132	20.242.161.84	20.105.96.235
20.66.125.135	20.242.161.144	20.105.96.251
104.40.63.98	191.238.33.50	20.105.97.16
		20.67.164.71
		20.105.96.130
		20.105.97.17
		20.105.96.154
		20.67.209.167
		20.67.212.199
		20.82.169.132
		20.82.170.255
		20.50.64.32

DocuSign

West US

Possible Outbound IP Addresses
40.112.243.33
104.40.57.101
104.40.82.23
104.40.81.188
104.40.85.254
40.78.71.184
40.83.166.253
40.83.173.206
40.83.166.164
40.83.165.34
104.42.58.78
20.237.156.124
20.245.240.122
104.42.63.76
20.245.240.75
104.42.62.182
20.66.122.126
20.66.120.186
20.66.124.17
20.66.125.145
20.66.122.132
20.66.125.135
104.40.63.98

East US

Possible Outbound IP Addresses
40.71.11.161
191.238.32.104
191.238.32.154
191.238.34.67
191.238.35.12
52.154.76.248
52.154.76.250
13.72.72.29
52.154.76.249
52.154.76.251
20.237.8.177
20.237.8.218
20.237.9.91
20.237.9.253
20.237.10.71
20.237.10.171
20.242.160.128
20.242.160.131
20.242.160.212
20.242.160.229
20.242.161.84
20.242.161.144
191.238.33.50

North Europe

Possible Outbound IP Addresses
20.50.64.32
20.105.97.248
20.105.98.61
20.105.98.138
20.105.99.3
20.105.99.41
20.105.99.224
20.93.14.38
20.93.15.169
20.93.15.194
20.93.15.234
20.105.96.9
20.105.96.75
20.105.96.97
20.105.96.116
20.105.96.131
20.105.96.157
20.105.96.169
20.105.96.229
20.105.96.234
20.105.96.235
20.105.96.251
20.105.97.16
20.67.164.71
20.105.96.130
20.105.97.17

Possible Outbound IP Addresses
20.105.96.154
20.67.209.167
20.67.212.199
20.82.169.132
20.82.170.255
20.50.64.32

Citrix ShareFile

West US

Possible Outbound IP Addresses
40.112.243.33
104.40.57.101
104.40.82.23
104.40.81.188
104.40.85.254
40.78.71.184
40.83.166.253
40.83.173.206
40.83.166.164
40.83.165.34
104.42.58.78
20.237.156.124
20.245.240.122
104.42.63.76
20.245.240.75
104.42.62.182

East US

Possible Outbound IP Addresses
40.71.11.161
191.238.32.104
191.238.32.154
191.238.34.67
191.238.35.12
52.154.76.248
52.154.76.250
13.72.72.29
52.154.76.249
52.154.76.251
20.237.8.177
20.237.8.218
20.237.9.91
20.237.9.253
20.237.10.71
20.237.10.171

North Europe

Possible Outbound IP Addresses
20.50.64.32
20.105.97.248
20.105.98.61
20.105.98.138
20.105.99.3
20.105.99.41
20.105.99.224
20.93.14.38
20.93.15.169
20.93.15.194
20.93.15.234
20.105.96.9
20.105.96.75
20.105.96.97
20.105.96.116
20.105.96.131

Possible Outbound IP Addresses	Possible Outbound IP Addresses	Possible Outbound IP Addresses
20.66.122.126	20.242.160.128	20.105.96.157
20.66.120.186	20.242.160.131	20.105.96.169
20.66.124.17	20.242.160.212	20.105.96.229
20.66.125.145	20.242.160.229	20.105.96.234
20.66.122.132	20.242.161.84	20.105.96.235
20.66.125.135	20.242.161.144	20.105.96.251
104.40.63.98	191.238.33.50	20.105.97.16
		20.67.164.71
		20.105.96.130
		20.105.97.17
		20.105.96.154
		20.67.209.167
		20.67.212.199
		20.82.169.132
		20.82.170.255
		20.50.64.32

Zendesk

West US

Possible Outbound IP Addresses
40.112.243.33
104.40.57.101
104.40.82.23
104.40.81.188
104.40.85.254
40.78.71.184

East US

Possible Outbound IP Addresses
40.71.11.161
191.238.32.104
191.238.32.154
191.238.34.67
191.238.35.12
52.154.76.248

North Europe

Possible Outbound IP Addresses
20.50.64.32
20.105.97.248
20.105.98.61
20.105.98.138
20.105.99.3
20.105.99.41

Possible Outbound IP Addresses	Possible Outbound IP Addresses	Possible Outbound IP Addresses
40.83.166.253	52.154.76.250	20.105.99.224
40.83.173.206	13.72.72.29	20.93.14.38
40.83.166.164	52.154.76.249	20.93.15.169
40.83.165.34	52.154.76.251	20.93.15.194
104.42.58.78	20.237.8.177	20.93.15.234
20.237.156.124	20.237.8.218	20.105.96.9
20.245.240.122	20.237.9.91	20.105.96.75
104.42.63.76	20.237.9.253	20.105.96.97
20.245.240.75	20.237.10.71	20.105.96.116
104.42.62.182	20.237.10.171	20.105.96.131
20.66.122.126	20.242.160.128	20.105.96.157
20.66.120.186	20.242.160.131	20.105.96.169
20.66.124.17	20.242.160.212	20.105.96.229
20.66.125.145	20.242.160.229	20.105.96.234
20.66.122.132	20.242.161.84	20.105.96.235
20.66.125.135	20.242.161.144	20.105.96.251
104.40.63.98	191.238.33.50	20.105.97.16
		20.67.164.71
		20.105.96.130
		20.105.97.17
		20.105.96.154
		20.67.209.167
		20.67.212.199
		20.82.169.132
		20.82.170.255
		20.50.64.32

Azure AD

West US	East US	North Europe

Possible Outbound IP Addresses	Possible Outbound IP Addresses	Possible Outbound IP Addresses
40.112.243.33	40.71.11.161	20.50.64.32
104.40.57.101	191.238.32.104	20.105.97.248
104.40.82.23	191.238.32.154	20.105.98.61
104.40.81.188	191.238.34.67	20.105.98.138
104.40.85.254	191.238.35.12	20.105.99.3
40.78.71.184	52.154.76.248	20.105.99.41
40.83.166.253	52.154.76.250	20.105.99.224
40.83.173.206	13.72.72.29	20.93.14.38
40.83.166.164	52.154.76.249	20.93.15.169
40.83.165.34	52.154.76.251	20.93.15.194
104.42.58.78	20.237.8.177	20.93.15.234
20.237.156.124	20.237.8.218	20.105.96.9
20.245.240.122	20.237.9.91	20.105.96.75
104.42.63.76	20.237.9.253	20.105.96.97
20.245.240.75	20.237.10.71	20.105.96.116
104.42.62.182	20.237.10.171	20.105.96.131
20.66.122.126	20.242.160.128	20.105.96.157
20.66.120.186	20.242.160.131	20.105.96.169
20.66.124.17	20.242.160.212	20.105.96.229
20.66.125.145	20.242.160.229	20.105.96.234
20.66.122.132	20.242.161.84	20.105.96.235
20.66.125.135	20.242.161.144	20.105.96.251
104.40.63.98	191.238.33.50	20.105.97.16
		20.67.164.71
		20.105.96.130
		20.105.97.17
		20.105.96.154
		20.67.209.167
		20.67.212.199
		20.82.169.132
		20.82.170.255
		20.50.64.32

Google Workspace

West US

Possible Outbound IP Addresses
40.112.243.33
104.40.57.101
104.40.82.23
104.40.81.188
104.40.85.254
40.78.71.184
40.83.166.253
40.83.173.206
40.83.166.164
40.83.165.34
104.42.58.78
20.237.156.124
20.245.240.122
104.42.63.76
20.245.240.75
104.42.62.182
20.66.122.126
20.66.120.186
20.66.124.17
20.66.125.145
20.66.122.132
20.66.125.135
104.40.63.98

East US

Possible Outbound IP Addresses
40.71.11.161
191.238.32.104
191.238.32.154
191.238.34.67
191.238.35.12
52.154.76.248
52.154.76.250
13.72.72.29
52.154.76.249
52.154.76.251
20.237.8.177
20.237.8.218
20.237.9.91
20.237.9.253
20.237.10.71
20.237.10.171
20.242.160.128
20.242.160.131
20.242.160.212
20.242.160.229
20.242.161.84
20.242.161.144
191.238.33.50

North Europe

Possible Outbound IP Addresses
20.50.64.32
20.105.97.248
20.105.98.61
20.105.98.138
20.105.99.3
20.105.99.41
20.105.99.224
20.93.14.38
20.93.15.169
20.93.15.194
20.93.15.234
20.105.96.9
20.105.96.75
20.105.96.97
20.105.96.116
20.105.96.131
20.105.96.157
20.105.96.169
20.105.96.229
20.105.96.234
20.105.96.235
20.105.96.251
20.105.97.16
20.67.164.71
20.105.96.130
20.105.97.17

Possible Outbound IP Addresses
20.105.96.154
20.67.209.167
20.67.212.199
20.82.169.132
20.82.170.255
20.50.64.32

Concur

West US

Possible Outbound IP Addresses
40.112.243.33
104.40.57.101
104.40.82.23
104.40.81.188
104.40.85.254
40.78.71.184
40.83.166.253
40.83.173.206
40.83.166.164
40.83.165.34
104.42.58.78
20.237.156.124
20.245.240.122
104.42.63.76
20.245.240.75
104.42.62.182

East US

Possible Outbound IP Addresses
40.71.11.161
191.238.32.104
191.238.32.154
191.238.34.67
191.238.35.12
52.154.76.248
52.154.76.250
13.72.72.29
52.154.76.249
52.154.76.251
20.237.8.177
20.237.8.218
20.237.9.91
20.237.9.253
20.237.10.71
20.237.10.171

North Europe

Possible Outbound IP Addresses
20.50.64.32
20.105.97.248
20.105.98.61
20.105.98.138
20.105.99.3
20.105.99.41
20.105.99.224
20.93.14.38
20.93.15.169
20.93.15.194
20.93.15.234
20.105.96.9
20.105.96.75
20.105.96.97
20.105.96.116
20.105.96.131

Possible Outbound IP Addresses	Possible Outbound IP Addresses	Possible Outbound IP Addresses
20.66.122.126	20.242.160.128	20.105.96.157
20.66.120.186	20.242.160.131	20.105.96.169
20.66.124.17	20.242.160.212	20.105.96.229
20.66.125.145	20.242.160.229	20.105.96.234
20.66.122.132	20.242.161.84	20.105.96.235
20.66.125.135	20.242.161.144	20.105.96.251
104.40.63.98	191.238.33.50	20.105.97.16
		20.67.164.71
		20.105.96.130
		20.105.97.17
		20.105.96.154
		20.67.209.167
		20.67.212.199
		20.82.169.132
		20.82.170.255
		20.50.64.32

Tableau

West US

Possible Outbound IP Addresses
40.112.243.33
104.40.57.101
104.40.82.23
104.40.81.188
104.40.85.254
40.78.71.184

East US

Possible Outbound IP Addresses
40.71.11.161
191.238.32.104
191.238.32.154
191.238.34.67
191.238.35.12
52.154.76.248

North Europe

Possible Outbound IP Addresses
20.50.64.32
20.105.97.248
20.105.98.61
20.105.98.138
20.105.99.3
20.105.99.41

Possible Outbound IP Addresses	Possible Outbound IP Addresses	Possible Outbound IP Addresses
40.83.166.253	52.154.76.250	20.105.99.224
40.83.173.206	13.72.72.29	20.93.14.38
40.83.166.164	52.154.76.249	20.93.15.169
40.83.165.34	52.154.76.251	20.93.15.194
104.42.58.78	20.237.8.177	20.93.15.234
20.237.156.124	20.237.8.218	20.105.96.9
20.245.240.122	20.237.9.91	20.105.96.75
104.42.63.76	20.237.9.253	20.105.96.97
20.245.240.75	20.237.10.71	20.105.96.116
104.42.62.182	20.237.10.171	20.105.96.131
20.66.122.126	20.242.160.128	20.105.96.157
20.66.120.186	20.242.160.131	20.105.96.169
20.66.124.17	20.242.160.212	20.105.96.229
20.66.125.145	20.242.160.229	20.105.96.234
20.66.122.132	20.242.161.84	20.105.96.235
20.66.125.135	20.242.161.144	20.105.96.251
104.40.63.98	191.238.33.50	20.105.97.16
		20.67.164.71
		20.105.96.130
		20.105.97.17
		20.105.96.154
		20.67.209.167
		20.67.212.199
		20.82.169.132
		20.82.170.255
		20.50.64.32

GoToMeeting

West US	East US	North Europe

Possible Outbound IP Addresses	Possible Outbound IP Addresses	Possible Outbound IP Addresses
40.112.243.33	40.71.11.161	20.50.64.32
104.40.57.101	191.238.32.104	20.105.97.248
104.40.82.23	191.238.32.154	20.105.98.61
104.40.81.188	191.238.34.67	20.105.98.138
104.40.85.254	191.238.35.12	20.105.99.3
40.78.71.184	52.154.76.248	20.105.99.41
40.83.166.253	52.154.76.250	20.105.99.224
40.83.173.206	13.72.72.29	20.93.14.38
40.83.166.164	52.154.76.249	20.93.15.169
40.83.165.34	52.154.76.251	20.93.15.194
104.42.58.78	20.237.8.177	20.93.15.234
20.237.156.124	20.237.8.218	20.105.96.9
20.245.240.122	20.237.9.91	20.105.96.75
104.42.63.76	20.237.9.253	20.105.96.97
20.245.240.75	20.237.10.71	20.105.96.116
104.42.62.182	20.237.10.171	20.105.96.131
20.66.122.126	20.242.160.128	20.105.96.157
20.66.120.186	20.242.160.131	20.105.96.169
20.66.124.17	20.242.160.212	20.105.96.229
20.66.125.145	20.242.160.229	20.105.96.234
20.66.122.132	20.242.161.84	20.105.96.235
20.66.125.135	20.242.161.144	20.105.96.251
104.40.63.98	191.238.33.50	20.105.97.16
		20.67.164.71
		20.105.96.130
		20.105.97.17
		20.105.96.154
		20.67.209.167
		20.67.212.199
		20.82.169.132
		20.82.170.255
		20.50.64.32

Coupa

West US

Possible Outbound IP Addresses
40.112.243.33
104.40.57.101
104.40.82.23
104.40.81.188
104.40.85.254
40.78.71.184
40.83.166.253
40.83.173.206
40.83.166.164
40.83.165.34
104.42.58.78
20.237.156.124
20.245.240.122
104.42.63.76
20.245.240.75
104.42.62.182
20.66.122.126
20.66.120.186
20.66.124.17
20.66.125.145
20.66.122.132
20.66.125.135
104.40.63.98

East US

Possible Outbound IP Addresses
40.71.11.161
191.238.32.104
191.238.32.154
191.238.34.67
191.238.35.12
52.154.76.248
52.154.76.250
13.72.72.29
52.154.76.249
52.154.76.251
20.237.8.177
20.237.8.218
20.237.9.91
20.237.9.253
20.237.10.71
20.237.10.171
20.242.160.128
20.242.160.131
20.242.160.212
20.242.160.229
20.242.161.84
20.242.161.144
191.238.33.50

North Europe

Possible Outbound IP Addresses
20.50.64.32
20.105.97.248
20.105.98.61
20.105.98.138
20.105.99.3
20.105.99.41
20.105.99.224
20.93.14.38
20.93.15.169
20.93.15.194
20.93.15.234
20.105.96.9
20.105.96.75
20.105.96.97
20.105.96.116
20.105.96.131
20.105.96.157
20.105.96.169
20.105.96.229
20.105.96.234
20.105.96.235
20.105.96.251
20.105.97.16
20.67.164.71
20.105.96.130
20.105.97.17

Possible Outbound IP Addresses
20.105.96.154
20.67.209.167
20.67.212.199
20.82.169.132
20.82.170.255
20.50.64.32

AWS Cognito

West US

Possible Outbound IP Addresses
40.112.243.33
104.40.57.101
104.40.82.23
104.40.81.188
104.40.85.254
40.78.71.184
40.83.166.253
40.83.173.206
40.83.166.164
40.83.165.34
104.42.58.78
20.237.156.124
20.245.240.122
104.42.63.76
20.245.240.75
104.42.62.182

East US

Possible Outbound IP Addresses
40.71.11.161
191.238.32.104
191.238.32.154
191.238.34.67
191.238.35.12
52.154.76.248
52.154.76.250
13.72.72.29
52.154.76.249
52.154.76.251
20.237.8.177
20.237.8.218
20.237.9.91
20.237.9.253
20.237.10.71
20.237.10.171

North Europe

Possible Outbound IP Addresses
20.50.64.32
20.105.97.248
20.105.98.61
20.105.98.138
20.105.99.3
20.105.99.41
20.105.99.224
20.93.14.38
20.93.15.169
20.93.15.194
20.93.15.234
20.105.96.9
20.105.96.75
20.105.96.97
20.105.96.116
20.105.96.131

Possible Outbound IP Addresses	Possible Outbound IP Addresses	Possible Outbound IP Addresses
20.66.122.126	20.242.160.128	20.105.96.157
20.66.120.186	20.242.160.131	20.105.96.169
20.66.124.17	20.242.160.212	20.105.96.229
20.66.125.145	20.242.160.229	20.105.96.234
20.66.122.132	20.242.161.84	20.105.96.235
20.66.125.135	20.242.161.144	20.105.96.251
104.40.63.98	191.238.33.50	20.105.97.16
		20.67.164.71
		20.105.96.130
		20.105.97.17
		20.105.96.154
		20.67.209.167
		20.67.212.199
		20.82.169.132
		20.82.170.255
		20.50.64.32

Okta

West US

Possible Outbound IP Addresses
40.112.243.33
104.40.57.101
104.40.82.23
104.40.81.188
104.40.85.254
40.78.71.184

East US

Possible Outbound IP Addresses
40.71.11.161
191.238.32.104
191.238.32.154
191.238.34.67
191.238.35.12
52.154.76.248

North Europe

Possible Outbound IP Addresses
20.50.64.32
20.105.97.248
20.105.98.61
20.105.98.138
20.105.99.3
20.105.99.41

Possible Outbound IP Addresses	Possible Outbound IP Addresses	Possible Outbound IP Addresses
40.83.166.253	52.154.76.250	20.105.99.224
40.83.173.206	13.72.72.29	20.93.14.38
40.83.166.164	52.154.76.249	20.93.15.169
40.83.165.34	52.154.76.251	20.93.15.194
104.42.58.78	20.237.8.177	20.93.15.234
20.237.156.124	20.237.8.218	20.105.96.9
20.245.240.122	20.237.9.91	20.105.96.75
104.42.63.76	20.237.9.253	20.105.96.97
20.245.240.75	20.237.10.71	20.105.96.116
104.42.62.182	20.237.10.171	20.105.96.131
20.66.122.126	20.242.160.128	20.105.96.157
20.66.120.186	20.242.160.131	20.105.96.169
20.66.124.17	20.242.160.212	20.105.96.229
20.66.125.145	20.242.160.229	20.105.96.234
20.66.122.132	20.242.161.84	20.105.96.235
20.66.125.135	20.242.161.144	20.105.96.251
104.40.63.98	191.238.33.50	20.105.97.16
		20.67.164.71
		20.105.96.130
		20.105.97.17
		20.105.96.154
		20.67.209.167
		20.67.212.199
		20.82.169.132
		20.82.170.255
		20.50.64.32

Apigee

West US	East US	North Europe

Possible Outbound IP Addresses	Possible Outbound IP Addresses	Possible Outbound IP Addresses
40.112.243.33	40.71.11.161	20.50.64.32
104.40.57.101	191.238.32.104	20.105.97.248
104.40.82.23	191.238.32.154	20.105.98.61
104.40.81.188	191.238.34.67	20.105.98.138
104.40.85.254	191.238.35.12	20.105.99.3
40.78.71.184	52.154.76.248	20.105.99.41
40.83.166.253	52.154.76.250	20.105.99.224
40.83.173.206	13.72.72.29	20.93.14.38
40.83.166.164	52.154.76.249	20.93.15.169
40.83.165.34	52.154.76.251	20.93.15.194
104.42.58.78	20.237.8.177	20.93.15.234
20.237.156.124	20.237.8.218	20.105.96.9
20.245.240.122	20.237.9.91	20.105.96.75
104.42.63.76	20.237.9.253	20.105.96.97
20.245.240.75	20.237.10.71	20.105.96.116
104.42.62.182	20.237.10.171	20.105.96.131
20.66.122.126	20.242.160.128	20.105.96.157
20.66.120.186	20.242.160.131	20.105.96.169
20.66.124.17	20.242.160.212	20.105.96.229
20.66.125.145	20.242.160.229	20.105.96.234
20.66.122.132	20.242.161.84	20.105.96.235
20.66.125.135	20.242.161.144	20.105.96.251
104.40.63.98	191.238.33.50	20.105.97.16
		20.67.164.71
		20.105.96.130
		20.105.97.17
		20.105.96.154
		20.67.209.167
		20.67.212.199
		20.82.169.132
		20.82.170.255
		20.50.64.32

DataDog

West US

Possible Outbound IP Addresses
40.112.243.33
104.40.57.101
104.40.82.23
104.40.81.188
104.40.85.254
40.78.71.184
40.83.166.253
40.83.173.206
40.83.166.164
40.83.165.34
104.42.58.78
20.237.156.124
20.245.240.122
104.42.63.76
20.245.240.75
104.42.62.182
20.66.122.126
20.66.120.186
20.66.124.17
20.66.125.145
20.66.122.132
20.66.125.135
104.40.63.98

East US

Possible Outbound IP Addresses
40.71.11.161
191.238.32.104
191.238.32.154
191.238.34.67
191.238.35.12
52.154.76.248
52.154.76.250
13.72.72.29
52.154.76.249
52.154.76.251
20.237.8.177
20.237.8.218
20.237.9.91
20.237.9.253
20.237.10.71
20.237.10.171
20.242.160.128
20.242.160.131
20.242.160.212
20.242.160.229
20.242.161.84
20.242.161.144
191.238.33.50

North Europe

Possible Outbound IP Addresses
20.50.64.32
20.105.97.248
20.105.98.61
20.105.98.138
20.105.99.3
20.105.99.41
20.105.99.224
20.93.14.38
20.93.15.169
20.93.15.194
20.93.15.234
20.105.96.9
20.105.96.75
20.105.96.97
20.105.96.116
20.105.96.131
20.105.96.157
20.105.96.169
20.105.96.229
20.105.96.234
20.105.96.235
20.105.96.251
20.105.97.16
20.67.164.71
20.105.96.130
20.105.97.17

Possible Outbound IP Addresses
20.105.96.154
20.67.209.167
20.67.212.199
20.82.169.132
20.82.170.255
20.50.64.32

Hideez

West US

Possible Outbound IP Addresses
40.112.243.33
104.40.57.101
104.40.82.23
104.40.81.188
104.40.85.254
40.78.71.184
40.83.166.253
40.83.173.206
40.83.166.164
40.83.165.34
104.42.58.78
20.237.156.124
20.245.240.122
104.42.63.76
20.245.240.75
104.42.62.182

East US

Possible Outbound IP Addresses
40.71.11.161
191.238.32.104
191.238.32.154
191.238.34.67
191.238.35.12
52.154.76.248
52.154.76.250
13.72.72.29
52.154.76.249
52.154.76.251
20.237.8.177
20.237.8.218
20.237.9.91
20.237.9.253
20.237.10.71
20.237.10.171

North Europe

Possible Outbound IP Addresses
20.50.64.32
20.105.97.248
20.105.98.61
20.105.98.138
20.105.99.3
20.105.99.41
20.105.99.224
20.93.14.38
20.93.15.169
20.93.15.194
20.93.15.234
20.105.96.9
20.105.96.75
20.105.96.97
20.105.96.116
20.105.96.131

Possible Outbound IP Addresses	Possible Outbound IP Addresses	Possible Outbound IP Addresses
20.66.122.126	20.242.160.128	20.105.96.157
20.66.120.186	20.242.160.131	20.105.96.169
20.66.124.17	20.242.160.212	20.105.96.229
20.66.125.145	20.242.160.229	20.105.96.234
20.66.122.132	20.242.161.84	20.105.96.235
20.66.125.135	20.242.161.144	20.105.96.251
104.40.63.98	191.238.33.50	20.105.97.16
		20.67.164.71
		20.105.96.130
		20.105.97.17
		20.105.96.154
		20.67.209.167
		20.67.212.199
		20.82.169.132
		20.82.170.255
		20.50.64.32

OpsGenie

West US

Possible Outbound IP Addresses
40.112.243.33
104.40.57.101
104.40.82.23
104.40.81.188
104.40.85.254
40.78.71.184

East US

Possible Outbound IP Addresses
40.71.11.161
191.238.32.104
191.238.32.154
191.238.34.67
191.238.35.12
52.154.76.248

North Europe

Possible Outbound IP Addresses
20.50.64.32
20.105.97.248
20.105.98.61
20.105.98.138
20.105.99.3
20.105.99.41

Possible Outbound IP Addresses	Possible Outbound IP Addresses	Possible Outbound IP Addresses
40.83.166.253	52.154.76.250	20.105.99.224
40.83.173.206	13.72.72.29	20.93.14.38
40.83.166.164	52.154.76.249	20.93.15.169
40.83.165.34	52.154.76.251	20.93.15.194
104.42.58.78	20.237.8.177	20.93.15.234
20.237.156.124	20.237.8.218	20.105.96.9
20.245.240.122	20.237.9.91	20.105.96.75
104.42.63.76	20.237.9.253	20.105.96.97
20.245.240.75	20.237.10.71	20.105.96.116
104.42.62.182	20.237.10.171	20.105.96.131
20.66.122.126	20.242.160.128	20.105.96.157
20.66.120.186	20.242.160.131	20.105.96.169
20.66.124.17	20.242.160.212	20.105.96.229
20.66.125.145	20.242.160.229	20.105.96.234
20.66.122.132	20.242.161.84	20.105.96.235
20.66.125.135	20.242.161.144	20.105.96.251
104.40.63.98	191.238.33.50	20.105.97.16
		20.67.164.71
		20.105.96.130
		20.105.97.17
		20.105.96.154
		20.67.209.167
		20.67.212.199
		20.82.169.132
		20.82.170.255
		20.50.64.32

Informatica Cloud Services

West US	East US	North Europe

Possible Outbound IP Addresses	Possible Outbound IP Addresses	Possible Outbound IP Addresses
40.112.243.33	40.71.11.161	20.50.64.32
104.40.57.101	191.238.32.104	20.105.97.248
104.40.82.23	191.238.32.154	20.105.98.61
104.40.81.188	191.238.34.67	20.105.98.138
104.40.85.254	191.238.35.12	20.105.99.3
40.78.71.184	52.154.76.248	20.105.99.41
40.83.166.253	52.154.76.250	20.105.99.224
40.83.173.206	13.72.72.29	20.93.14.38
40.83.166.164	52.154.76.249	20.93.15.169
40.83.165.34	52.154.76.251	20.93.15.194
104.42.58.78	20.237.8.177	20.93.15.234
20.237.156.124	20.237.8.218	20.105.96.9
20.245.240.122	20.237.9.91	20.105.96.75
104.42.63.76	20.237.9.253	20.105.96.97
20.245.240.75	20.237.10.71	20.105.96.116
104.42.62.182	20.237.10.171	20.105.96.131
20.66.122.126	20.242.160.128	20.105.96.157
20.66.120.186	20.242.160.131	20.105.96.169
20.66.124.17	20.242.160.212	20.105.96.229
20.66.125.145	20.242.160.229	20.105.96.234
20.66.122.132	20.242.161.84	20.105.96.235
20.66.125.135	20.242.161.144	20.105.96.251
104.40.63.98	191.238.33.50	20.105.97.16
		20.67.164.71
		20.105.96.130
		20.105.97.17
		20.105.96.154
		20.67.209.167
		20.67.212.199
		20.82.169.132
		20.82.170.255
		20.50.64.32

AppDynamics

West US

Possible Outbound IP Addresses
40.112.243.33
104.40.57.101
104.40.82.23
104.40.81.188
104.40.85.254
40.78.71.184
40.83.166.253
40.83.173.206
40.83.166.164
40.83.165.34
104.42.58.78
20.237.156.124
20.245.240.122
104.42.63.76
20.245.240.75
104.42.62.182
20.66.122.126
20.66.120.186
20.66.124.17
20.66.125.145
20.66.122.132
20.66.125.135
104.40.63.98

East US

Possible Outbound IP Addresses
40.71.11.161
191.238.32.104
191.238.32.154
191.238.34.67
191.238.35.12
52.154.76.248
52.154.76.250
13.72.72.29
52.154.76.249
52.154.76.251
20.237.8.177
20.237.8.218
20.237.9.91
20.237.9.253
20.237.10.71
20.237.10.171
20.242.160.128
20.242.160.131
20.242.160.212
20.242.160.229
20.242.161.84
20.242.161.144
191.238.33.50

North Europe

Possible Outbound IP Addresses
20.50.64.32
20.105.97.248
20.105.98.61
20.105.98.138
20.105.99.3
20.105.99.41
20.105.99.224
20.93.14.38
20.93.15.169
20.93.15.194
20.93.15.234
20.105.96.9
20.105.96.75
20.105.96.97
20.105.96.116
20.105.96.131
20.105.96.157
20.105.96.169
20.105.96.229
20.105.96.234
20.105.96.235
20.105.96.251
20.105.97.16
20.67.164.71
20.105.96.130
20.105.97.17

Possible Outbound IP Addresses
20.105.96.154
20.67.209.167
20.67.212.199
20.82.169.132
20.82.170.255
20.50.64.32

OneLogin

West US

Possible Outbound IP Addresses
40.112.243.33
104.40.57.101
104.40.82.23
104.40.81.188
104.40.85.254
40.78.71.184
40.83.166.253
40.83.173.206
40.83.166.164
40.83.165.34
104.42.58.78
20.237.156.124
20.245.240.122
104.42.63.76
20.245.240.75
104.42.62.182

East US

Possible Outbound IP Addresses
40.71.11.161
191.238.32.104
191.238.32.154
191.238.34.67
191.238.35.12
52.154.76.248
52.154.76.250
13.72.72.29
52.154.76.249
52.154.76.251
20.237.8.177
20.237.8.218
20.237.9.91
20.237.9.253
20.237.10.71
20.237.10.171

North Europe

Possible Outbound IP Addresses
20.50.64.32
20.105.97.248
20.105.98.61
20.105.98.138
20.105.99.3
20.105.99.41
20.105.99.224
20.93.14.38
20.93.15.169
20.93.15.194
20.93.15.234
20.105.96.9
20.105.96.75
20.105.96.97
20.105.96.116
20.105.96.131

Possible Outbound IP Addresses	Possible Outbound IP Addresses	Possible Outbound IP Addresses
20.66.122.126	20.242.160.128	20.105.96.157
20.66.120.186	20.242.160.131	20.105.96.169
20.66.124.17	20.242.160.212	20.105.96.229
20.66.125.145	20.242.160.229	20.105.96.234
20.66.122.132	20.242.161.84	20.105.96.235
20.66.125.135	20.242.161.144	20.105.96.251
104.40.63.98	191.238.33.50	20.105.97.16
		20.67.164.71
		20.105.96.130
		20.105.97.17
		20.105.96.154
		20.67.209.167
		20.67.212.199
		20.82.169.132
		20.82.170.255
		20.50.64.32

Marketo

West US

Possible Outbound IP Addresses
40.112.243.33
104.40.57.101
104.40.82.23
104.40.81.188
104.40.85.254
40.78.71.184

East US

Possible Outbound IP Addresses
40.71.11.161
191.238.32.104
191.238.32.154
191.238.34.67
191.238.35.12
52.154.76.248

North Europe

Possible Outbound IP Addresses
20.50.64.32
20.105.97.248
20.105.98.61
20.105.98.138
20.105.99.3
20.105.99.41

Possible Outbound IP Addresses	Possible Outbound IP Addresses	Possible Outbound IP Addresses
40.83.166.253	52.154.76.250	20.105.99.224
40.83.173.206	13.72.72.29	20.93.14.38
40.83.166.164	52.154.76.249	20.93.15.169
40.83.165.34	52.154.76.251	20.93.15.194
104.42.58.78	20.237.8.177	20.93.15.234
20.237.156.124	20.237.8.218	20.105.96.9
20.245.240.122	20.237.9.91	20.105.96.75
104.42.63.76	20.237.9.253	20.105.96.97
20.245.240.75	20.237.10.71	20.105.96.116
104.42.62.182	20.237.10.171	20.105.96.131
20.66.122.126	20.242.160.128	20.105.96.157
20.66.120.186	20.242.160.131	20.105.96.169
20.66.124.17	20.242.160.212	20.105.96.229
20.66.125.145	20.242.160.229	20.105.96.234
20.66.122.132	20.242.161.84	20.105.96.235
20.66.125.135	20.242.161.144	20.105.96.251
104.40.63.98	191.238.33.50	20.105.97.16
		20.67.164.71
		20.105.96.130
		20.105.97.17
		20.105.96.154
		20.67.209.167
		20.67.212.199
		20.82.169.132
		20.82.170.255
		20.50.64.32

Workday HR

West US	East US	North Europe

Possible Outbound IP Addresses	Possible Outbound IP Addresses	Possible Outbound IP Addresses
40.112.243.33	40.71.11.161	20.50.64.32
104.40.57.101	191.238.32.104	20.105.97.248
104.40.82.23	191.238.32.154	20.105.98.61
104.40.81.188	191.238.34.67	20.105.98.138
104.40.85.254	191.238.35.12	20.105.99.3
40.78.71.184	52.154.76.248	20.105.99.41
40.83.166.253	52.154.76.250	20.105.99.224
40.83.173.206	13.72.72.29	20.93.14.38
40.83.166.164	52.154.76.249	20.93.15.169
40.83.165.34	52.154.76.251	20.93.15.194
104.42.58.78	20.237.8.177	20.93.15.234
20.237.156.124	20.237.8.218	20.105.96.9
20.245.240.122	20.237.9.91	20.105.96.75
104.42.63.76	20.237.9.253	20.105.96.97
20.245.240.75	20.237.10.71	20.105.96.116
104.42.62.182	20.237.10.171	20.105.96.131
20.66.122.126	20.242.160.128	20.105.96.157
20.66.120.186	20.242.160.131	20.105.96.169
20.66.124.17	20.242.160.212	20.105.96.229
20.66.125.145	20.242.160.229	20.105.96.234
20.66.122.132	20.242.161.84	20.105.96.235
20.66.125.135	20.242.161.144	20.105.96.251
104.40.63.98	191.238.33.50	20.105.97.16
		20.67.164.71
		20.105.96.130
		20.105.97.17
		20.105.96.154
		20.67.209.167
		20.67.212.199
		20.82.169.132
		20.82.170.255
		20.50.64.32

PingOne

West US

Possible Outbound IP Addresses
40.112.243.33
104.40.57.101
104.40.82.23
104.40.81.188
104.40.85.254
40.78.71.184
40.83.166.253
40.83.173.206
40.83.166.164
40.83.165.34
104.42.58.78
20.237.156.124
20.245.240.122
104.42.63.76
20.245.240.75
104.42.62.182
20.66.122.126
20.66.120.186
20.66.124.17
20.66.125.145
20.66.122.132
20.66.125.135
104.40.63.98

East US

Possible Outbound IP Addresses
40.71.11.161
191.238.32.104
191.238.32.154
191.238.34.67
191.238.35.12
52.154.76.248
52.154.76.250
13.72.72.29
52.154.76.249
52.154.76.251
20.237.8.177
20.237.8.218
20.237.9.91
20.237.9.253
20.237.10.71
20.237.10.171
20.242.160.128
20.242.160.131
20.242.160.212
20.242.160.229
20.242.161.84
20.242.161.144
191.238.33.50

North Europe

Possible Outbound IP Addresses
20.50.64.32
20.105.97.248
20.105.98.61
20.105.98.138
20.105.99.3
20.105.99.41
20.105.99.224
20.93.14.38
20.93.15.169
20.93.15.194
20.93.15.234
20.105.96.9
20.105.96.75
20.105.96.97
20.105.96.116
20.105.96.131
20.105.96.157
20.105.96.169
20.105.96.229
20.105.96.234
20.105.96.235
20.105.96.251
20.105.97.16
20.67.164.71
20.105.96.130
20.105.97.17

Possible Outbound IP Addresses
20.105.96.154
20.67.209.167
20.67.212.199
20.82.169.132
20.82.170.255
20.50.64.32

Aha!

West US

Possible Outbound IP Addresses
40.112.243.33
104.40.57.101
104.40.82.23
104.40.81.188
104.40.85.254
40.78.71.184
40.83.166.253
40.83.173.206
40.83.166.164
40.83.165.34
104.42.58.78
20.237.156.124
20.245.240.122
104.42.63.76
20.245.240.75
104.42.62.182

East US

Possible Outbound IP Addresses
40.71.11.161
191.238.32.104
191.238.32.154
191.238.34.67
191.238.35.12
52.154.76.248
52.154.76.250
13.72.72.29
52.154.76.249
52.154.76.251
20.237.8.177
20.237.8.218
20.237.9.91
20.237.9.253
20.237.10.71
20.237.10.171

North Europe

Possible Outbound IP Addresses
20.50.64.32
20.105.97.248
20.105.98.61
20.105.98.138
20.105.99.3
20.105.99.41
20.105.99.224
20.93.14.38
20.93.15.169
20.93.15.194
20.93.15.234
20.105.96.9
20.105.96.75
20.105.96.97
20.105.96.116
20.105.96.131

Possible Outbound IP Addresses	Possible Outbound IP Addresses	Possible Outbound IP Addresses
20.66.122.126	20.242.160.128	20.105.96.157
20.66.120.186	20.242.160.131	20.105.96.169
20.66.124.17	20.242.160.212	20.105.96.229
20.66.125.145	20.242.160.229	20.105.96.234
20.66.122.132	20.242.161.84	20.105.96.235
20.66.125.135	20.242.161.144	20.105.96.251
104.40.63.98	191.238.33.50	20.105.97.16
		20.67.164.71
		20.105.96.130
		20.105.97.17
		20.105.96.154
		20.67.209.167
		20.67.212.199
		20.82.169.132
		20.82.170.255
		20.50.64.32

Hacker Rank

West US

Possible Outbound IP Addresses
40.112.243.33
104.40.57.101
104.40.82.23
104.40.81.188
104.40.85.254
40.78.71.184

East US

Possible Outbound IP Addresses
40.71.11.161
191.238.32.104
191.238.32.154
191.238.34.67
191.238.35.12
52.154.76.248

North Europe

Possible Outbound IP Addresses
20.50.64.32
20.105.97.248
20.105.98.61
20.105.98.138
20.105.99.3
20.105.99.41

Possible Outbound IP Addresses	Possible Outbound IP Addresses	Possible Outbound IP Addresses
40.83.166.253	52.154.76.250	20.105.99.224
40.83.173.206	13.72.72.29	20.93.14.38
40.83.166.164	52.154.76.249	20.93.15.169
40.83.165.34	52.154.76.251	20.93.15.194
104.42.58.78	20.237.8.177	20.93.15.234
20.237.156.124	20.237.8.218	20.105.96.9
20.245.240.122	20.237.9.91	20.105.96.75
104.42.63.76	20.237.9.253	20.105.96.97
20.245.240.75	20.237.10.71	20.105.96.116
104.42.62.182	20.237.10.171	20.105.96.131
20.66.122.126	20.242.160.128	20.105.96.157
20.66.120.186	20.242.160.131	20.105.96.169
20.66.124.17	20.242.160.212	20.105.96.229
20.66.125.145	20.242.160.229	20.105.96.234
20.66.122.132	20.242.161.84	20.105.96.235
20.66.125.135	20.242.161.144	20.105.96.251
104.40.63.98	191.238.33.50	20.105.97.16
		20.67.164.71
		20.105.96.130
		20.105.97.17
		20.105.96.154
		20.67.209.167
		20.67.212.199
		20.82.169.132
		20.82.170.255
		20.50.64.32

SAP Litmos

West US	East US	North Europe

Possible Outbound IP Addresses	Possible Outbound IP Addresses	Possible Outbound IP Addresses
40.112.243.33	40.71.11.161	20.50.64.32
104.40.57.101	191.238.32.104	20.105.97.248
104.40.82.23	191.238.32.154	20.105.98.61
104.40.81.188	191.238.34.67	20.105.98.138
104.40.85.254	191.238.35.12	20.105.99.3
40.78.71.184	52.154.76.248	20.105.99.41
40.83.166.253	52.154.76.250	20.105.99.224
40.83.173.206	13.72.72.29	20.93.14.38
40.83.166.164	52.154.76.249	20.93.15.169
40.83.165.34	52.154.76.251	20.93.15.194
104.42.58.78	20.237.8.177	20.93.15.234
20.237.156.124	20.237.8.218	20.105.96.9
20.245.240.122	20.237.9.91	20.105.96.75
104.42.63.76	20.237.9.253	20.105.96.97
20.245.240.75	20.237.10.71	20.105.96.116
104.42.62.182	20.237.10.171	20.105.96.131
20.66.122.126	20.242.160.128	20.105.96.157
20.66.120.186	20.242.160.131	20.105.96.169
20.66.124.17	20.242.160.212	20.105.96.229
20.66.125.145	20.242.160.229	20.105.96.234
20.66.122.132	20.242.161.84	20.105.96.235
20.66.125.135	20.242.161.144	20.105.96.251
104.40.63.98	191.238.33.50	20.105.97.16
		20.67.164.71
		20.105.96.130
		20.105.97.17
		20.105.96.154
		20.67.209.167
		20.67.212.199
		20.82.169.132
		20.82.170.255
		20.50.64.32

Slack

West US

Possible Outbound IP Addresses
40.112.243.33
104.40.57.101
104.40.82.23
104.40.81.188
104.40.85.254
40.78.71.184
40.83.166.253
40.83.173.206
40.83.166.164
40.83.165.34
104.42.58.78
20.237.156.124
20.245.240.122
104.42.63.76
20.245.240.75
104.42.62.182
20.66.122.126
20.66.120.186
20.66.124.17
20.66.125.145
20.66.122.132
20.66.125.135
104.40.63.98

East US

Possible Outbound IP Addresses
40.71.11.161
191.238.32.104
191.238.32.154
191.238.34.67
191.238.35.12
52.154.76.248
52.154.76.250
13.72.72.29
52.154.76.249
52.154.76.251
20.237.8.177
20.237.8.218
20.237.9.91
20.237.9.253
20.237.10.71
20.237.10.171
20.242.160.128
20.242.160.131
20.242.160.212
20.242.160.229
20.242.161.84
20.242.161.144
191.238.33.50

North Europe

Possible Outbound IP Addresses
20.50.64.32
20.105.97.248
20.105.98.61
20.105.98.138
20.105.99.3
20.105.99.41
20.105.99.224
20.93.14.38
20.93.15.169
20.93.15.194
20.93.15.234
20.105.96.9
20.105.96.75
20.105.96.97
20.105.96.116
20.105.96.131
20.105.96.157
20.105.96.169
20.105.96.229
20.105.96.234
20.105.96.235
20.105.96.251
20.105.97.16
20.67.164.71
20.105.96.130
20.105.97.17

Possible Outbound IP Addresses
20.105.96.154
20.67.209.167
20.67.212.199
20.82.169.132
20.82.170.255
20.50.64.32

ActiveCampaign

West US

Possible Outbound IP Addresses
40.112.243.33
104.40.57.101
104.40.82.23
104.40.81.188
104.40.85.254
40.78.71.184
40.83.166.253
40.83.173.206
40.83.166.164
40.83.165.34
104.42.58.78
20.237.156.124
20.245.240.122
104.42.63.76
20.245.240.75
104.42.62.182

East US

Possible Outbound IP Addresses
40.71.11.161
191.238.32.104
191.238.32.154
191.238.34.67
191.238.35.12
52.154.76.248
52.154.76.250
13.72.72.29
52.154.76.249
52.154.76.251
20.237.8.177
20.237.8.218
20.237.9.91
20.237.9.253
20.237.10.71
20.237.10.171

North Europe

Possible Outbound IP Addresses
20.50.64.32
20.105.97.248
20.105.98.61
20.105.98.138
20.105.99.3
20.105.99.41
20.105.99.224
20.93.14.38
20.93.15.169
20.93.15.194
20.93.15.234
20.105.96.9
20.105.96.75
20.105.96.97
20.105.96.116
20.105.96.131

Possible Outbound IP Addresses	Possible Outbound IP Addresses	Possible Outbound IP Addresses
20.66.122.126	20.242.160.128	20.105.96.157
20.66.120.186	20.242.160.131	20.105.96.169
20.66.124.17	20.242.160.212	20.105.96.229
20.66.125.145	20.242.160.229	20.105.96.234
20.66.122.132	20.242.161.84	20.105.96.235
20.66.125.135	20.242.161.144	20.105.96.251
104.40.63.98	191.238.33.50	20.105.97.16
		20.67.164.71
		20.105.96.130
		20.105.97.17
		20.105.96.154
		20.67.209.167
		20.67.212.199
		20.82.169.132
		20.82.170.255
		20.50.64.32

WebEx

West US

Possible Outbound IP Addresses
40.112.243.33
104.40.57.101
104.40.82.23
104.40.81.188
104.40.85.254
40.78.71.184

East US

Possible Outbound IP Addresses
40.71.11.161
191.238.32.104
191.238.32.154
191.238.34.67
191.238.35.12
52.154.76.248

North Europe

Possible Outbound IP Addresses
20.50.64.32
20.105.97.248
20.105.98.61
20.105.98.138
20.105.99.3
20.105.99.41

Possible Outbound IP Addresses	Possible Outbound IP Addresses	Possible Outbound IP Addresses
40.83.166.253	52.154.76.250	20.105.99.224
40.83.173.206	13.72.72.29	20.93.14.38
40.83.166.164	52.154.76.249	20.93.15.169
40.83.165.34	52.154.76.251	20.93.15.194
104.42.58.78	20.237.8.177	20.93.15.234
20.237.156.124	20.237.8.218	20.105.96.9
20.245.240.122	20.237.9.91	20.105.96.75
104.42.63.76	20.237.9.253	20.105.96.97
20.245.240.75	20.237.10.71	20.105.96.116
104.42.62.182	20.237.10.171	20.105.96.131
20.66.122.126	20.242.160.128	20.105.96.157
20.66.120.186	20.242.160.131	20.105.96.169
20.66.124.17	20.242.160.212	20.105.96.229
20.66.125.145	20.242.160.229	20.105.96.234
20.66.122.132	20.242.161.84	20.105.96.235
20.66.125.135	20.242.161.144	20.105.96.251
104.40.63.98	191.238.33.50	20.105.97.16
		20.67.164.71
		20.105.96.130
		20.105.97.17
		20.105.96.154
		20.67.209.167
		20.67.212.199
		20.82.169.132
		20.82.170.255
		20.50.64.32

Databricks

West US	East US	North Europe

Possible Outbound IP Addresses	Possible Outbound IP Addresses	Possible Outbound IP Addresses
40.112.243.33	40.71.11.161	20.50.64.32
104.40.57.101	191.238.32.104	20.105.97.248
104.40.82.23	191.238.32.154	20.105.98.61
104.40.81.188	191.238.34.67	20.105.98.138
104.40.85.254	191.238.35.12	20.105.99.3
40.78.71.184	52.154.76.248	20.105.99.41
40.83.166.253	52.154.76.250	20.105.99.224
40.83.173.206	13.72.72.29	20.93.14.38
40.83.166.164	52.154.76.249	20.93.15.169
40.83.165.34	52.154.76.251	20.93.15.194
104.42.58.78	20.237.8.177	20.93.15.234
20.237.156.124	20.237.8.218	20.105.96.9
20.245.240.122	20.237.9.91	20.105.96.75
104.42.63.76	20.237.9.253	20.105.96.97
20.245.240.75	20.237.10.71	20.105.96.116
104.42.62.182	20.237.10.171	20.105.96.131
20.66.122.126	20.242.160.128	20.105.96.157
20.66.120.186	20.242.160.131	20.105.96.169
20.66.124.17	20.242.160.212	20.105.96.229
20.66.125.145	20.242.160.229	20.105.96.234
20.66.122.132	20.242.161.84	20.105.96.235
20.66.125.135	20.242.161.144	20.105.96.251
104.40.63.98	191.238.33.50	20.105.97.16
		20.67.164.71
		20.105.96.130
		20.105.97.17
		20.105.96.154
		20.67.209.167
		20.67.212.199
		20.82.169.132
		20.82.170.255
		20.50.64.32

Hive

West US

Possible Outbound IP Addresses
40.112.243.33
104.40.57.101
104.40.82.23
104.40.81.188
104.40.85.254
40.78.71.184
40.83.166.253
40.83.173.206
40.83.166.164
40.83.165.34
104.42.58.78
20.237.156.124
20.245.240.122
104.42.63.76
20.245.240.75
104.42.62.182
20.66.122.126
20.66.120.186
20.66.124.17
20.66.125.145
20.66.122.132
20.66.125.135
104.40.63.98

East US

Possible Outbound IP Addresses
40.71.11.161
191.238.32.104
191.238.32.154
191.238.34.67
191.238.35.12
52.154.76.248
52.154.76.250
13.72.72.29
52.154.76.249
52.154.76.251
20.237.8.177
20.237.8.218
20.237.9.91
20.237.9.253
20.237.10.71
20.237.10.171
20.242.160.128
20.242.160.131
20.242.160.212
20.242.160.229
20.242.161.84
20.242.161.144
191.238.33.50

North Europe

Possible Outbound IP Addresses
20.50.64.32
20.105.97.248
20.105.98.61
20.105.98.138
20.105.99.3
20.105.99.41
20.105.99.224
20.93.14.38
20.93.15.169
20.93.15.194
20.93.15.234
20.105.96.9
20.105.96.75
20.105.96.97
20.105.96.116
20.105.96.131
20.105.96.157
20.105.96.169
20.105.96.229
20.105.96.234
20.105.96.235
20.105.96.251
20.105.97.16
20.67.164.71
20.105.96.130
20.105.97.17

Possible Outbound IP Addresses
20.105.96.154
20.67.209.167
20.67.212.199
20.82.169.132
20.82.170.255
20.50.64.32

PagerDuty

West US

Possible Outbound IP Addresses
40.112.243.33
104.40.57.101
104.40.82.23
104.40.81.188
104.40.85.254
40.78.71.184
40.83.166.253
40.83.173.206
40.83.166.164
40.83.165.34
104.42.58.78
20.237.156.124
20.245.240.122
104.42.63.76
20.245.240.75
104.42.62.182

East US

Possible Outbound IP Addresses
40.71.11.161
191.238.32.104
191.238.32.154
191.238.34.67
191.238.35.12
52.154.76.248
52.154.76.250
13.72.72.29
52.154.76.249
52.154.76.251
20.237.8.177
20.237.8.218
20.237.9.91
20.237.9.253
20.237.10.71
20.237.10.171

North Europe

Possible Outbound IP Addresses
20.50.64.32
20.105.97.248
20.105.98.61
20.105.98.138
20.105.99.3
20.105.99.41
20.105.99.224
20.93.14.38
20.93.15.169
20.93.15.194
20.93.15.234
20.105.96.9
20.105.96.75
20.105.96.97
20.105.96.116
20.105.96.131

Possible Outbound IP Addresses	Possible Outbound IP Addresses	Possible Outbound IP Addresses
20.66.122.126	20.242.160.128	20.105.96.157
20.66.120.186	20.242.160.131	20.105.96.169
20.66.124.17	20.242.160.212	20.105.96.229
20.66.125.145	20.242.160.229	20.105.96.234
20.66.122.132	20.242.161.84	20.105.96.235
20.66.125.135	20.242.161.144	20.105.96.251
104.40.63.98	191.238.33.50	20.105.97.16
		20.67.164.71
		20.105.96.130
		20.105.97.17
		20.105.96.154
		20.67.209.167
		20.67.212.199
		20.82.169.132
		20.82.170.255
		20.50.64.32

Dayforce

West US

Possible Outbound IP Addresses
40.112.243.33
104.40.57.101
104.40.82.23
104.40.81.188
104.40.85.254
40.78.71.184

East US

Possible Outbound IP Addresses
40.71.11.161
191.238.32.104
191.238.32.154
191.238.34.67
191.238.35.12
52.154.76.248

North Europe

Possible Outbound IP Addresses
20.50.64.32
20.105.97.248
20.105.98.61
20.105.98.138
20.105.99.3
20.105.99.41

Possible Outbound IP Addresses	Possible Outbound IP Addresses	Possible Outbound IP Addresses
40.83.166.253	52.154.76.250	20.105.99.224
40.83.173.206	13.72.72.29	20.93.14.38
40.83.166.164	52.154.76.249	20.93.15.169
40.83.165.34	52.154.76.251	20.93.15.194
104.42.58.78	20.237.8.177	20.93.15.234
20.237.156.124	20.237.8.218	20.105.96.9
20.245.240.122	20.237.9.91	20.105.96.75
104.42.63.76	20.237.9.253	20.105.96.97
20.245.240.75	20.237.10.71	20.105.96.116
104.42.62.182	20.237.10.171	20.105.96.131
20.66.122.126	20.242.160.128	20.105.96.157
20.66.120.186	20.242.160.131	20.105.96.169
20.66.124.17	20.242.160.212	20.105.96.229
20.66.125.145	20.242.160.229	20.105.96.234
20.66.122.132	20.242.161.84	20.105.96.235
20.66.125.135	20.242.161.144	20.105.96.251
104.40.63.98	191.238.33.50	20.105.97.16
		20.67.164.71
		20.105.96.130
		20.105.97.17
		20.105.96.154
		20.67.209.167
		20.67.212.199
		20.82.169.132
		20.82.170.255
		20.50.64.32

Smartsheet

West US	East US	North Europe

Possible Outbound IP Addresses	Possible Outbound IP Addresses	Possible Outbound IP Addresses
40.112.243.33	40.71.11.161	20.50.64.32
104.40.57.101	191.238.32.104	20.105.97.248
104.40.82.23	191.238.32.154	20.105.98.61
104.40.81.188	191.238.34.67	20.105.98.138
104.40.85.254	191.238.35.12	20.105.99.3
40.78.71.184	52.154.76.248	20.105.99.41
40.83.166.253	52.154.76.250	20.105.99.224
40.83.173.206	13.72.72.29	20.93.14.38
40.83.166.164	52.154.76.249	20.93.15.169
40.83.165.34	52.154.76.251	20.93.15.194
104.42.58.78	20.237.8.177	20.93.15.234
20.237.156.124	20.237.8.218	20.105.96.9
20.245.240.122	20.237.9.91	20.105.96.75
104.42.63.76	20.237.9.253	20.105.96.97
20.245.240.75	20.237.10.71	20.105.96.116
104.42.62.182	20.237.10.171	20.105.96.131
20.66.122.126	20.242.160.128	20.105.96.157
20.66.120.186	20.242.160.131	20.105.96.169
20.66.124.17	20.242.160.212	20.105.96.229
20.66.125.145	20.242.160.229	20.105.96.234
20.66.122.132	20.242.161.84	20.105.96.235
20.66.125.135	20.242.161.144	20.105.96.251
104.40.63.98	191.238.33.50	20.105.97.16
		20.67.164.71
		20.105.96.130
		20.105.97.17
		20.105.96.154
		20.67.209.167
		20.67.212.199
		20.82.169.132
		20.82.170.255
		20.50.64.32

Pingboard

West US

Possible Outbound IP Addresses
40.112.243.33
104.40.57.101
104.40.82.23
104.40.81.188
104.40.85.254
40.78.71.184
40.83.166.253
40.83.173.206
40.83.166.164
40.83.165.34
104.42.58.78
20.237.156.124
20.245.240.122
104.42.63.76
20.245.240.75
104.42.62.182
20.66.122.126
20.66.120.186
20.66.124.17
20.66.125.145
20.66.122.132
20.66.125.135
104.40.63.98

East US

Possible Outbound IP Addresses
40.71.11.161
191.238.32.104
191.238.32.154
191.238.34.67
191.238.35.12
52.154.76.248
52.154.76.250
13.72.72.29
52.154.76.249
52.154.76.251
20.237.8.177
20.237.8.218
20.237.9.91
20.237.9.253
20.237.10.71
20.237.10.171
20.242.160.128
20.242.160.131
20.242.160.212
20.242.160.229
20.242.161.84
20.242.161.144
191.238.33.50

North Europe

Possible Outbound IP Addresses
20.50.64.32
20.105.97.248
20.105.98.61
20.105.98.138
20.105.99.3
20.105.99.41
20.105.99.224
20.93.14.38
20.93.15.169
20.93.15.194
20.93.15.234
20.105.96.9
20.105.96.75
20.105.96.97
20.105.96.116
20.105.96.131
20.105.96.157
20.105.96.169
20.105.96.229
20.105.96.234
20.105.96.235
20.105.96.251
20.105.97.16
20.67.164.71
20.105.96.130
20.105.97.17

	Possible Outbound IP Addresses
	20.105.96.154
	20.67.209.167
	20.67.212.199
	20.82.169.132
	20.82.170.255
	20.50.64.32

Appendix X

Values for customer-specific configuration parameters in Workday HR connector

For many of the customer-specific configuration parameters default values are provided while configuring a connector in Starling Connect portal. Below are the details with which the customer can identify and provide the values to the configuration parameters if customer needs to override the default values. The values can be identified from the XML response from the Workday target system for the resources.

The values for the configuration are customer specific, for example 'OrganizationSubTypeID for CostCenter' for a cutomer could be either 'Cost_Center' / 'Cost Center' depending on their WorkdayHR instance configuration.

NOTE:

- The default value for custom attributes, which is customer specific, has been set to 'N/A', however the customer can set the appropriate value if in use.

Configuration Parameters	Default Value	XML data to be analyzed	Method to identify the value for configuration parameter
Additional Names Types	N/A	Employee	wd:Worker/wd:Worker_ Data/wd:Personal_ Data/wd:Name_ Data/wd:Additional_Name_ Data/wd:Name_Type_ Reference/wd:ID [@type='Additional_Name_Type_ ID']/text()
Business Process Types	Hire Employee;Contract Contingent Worker	Employee	wd:Worker/wd:Worker_ Data/wd:Transaction_Log_Entry_ Data/wd:Transaction_Log_ Entry/wd:Transaction_Log_ Data/wd:Transaction_Log_Type_

Configuration Parameters	Default Value	XML data to be analyzed	Method to identify the value for configuration parameter
			Reference[string(wd:Transaction_Log_Type_Reference/wd:ID/@type\)='Business_Process_Type' /text()='{value_for_the_UI_config_field_Business_Process_Type}']/Transaction_Log_Type_Reference/wd:ID[@type='Business_Process_Type']/text()
Certification Names	N/A	Employee	wd:Worker/wd:Worker_Data/wd:Qualification_Data/wd:Certification/wd:Certification_Data/wd:Certification_Name/text()
CustomIDTypeID for Code Of Conduct	Code_of_Conduct	Employee	wd:Worker/wd:Worker_Data/wd:Personal_Data/wd:Identification_Data/wd:Custom_ID/wd:Custom_ID_Data[string(wd:ID_Type_Reference/wd:ID/@type\)='Custom_ID_Type_ID' and string(wd:ID_Type_Reference/wd:ID[@type='Custom_ID_Type_ID'])/text()='{value_for_the_UI_config_field_CustomIDTypeID for Code Of Conduct}']/wd:ID/text()
CustomIDTypeID for Date Joined Industry	Date_Joined_Industry	Employee	wd:Worker/wd:Worker_Data/wd:Personal_Data/wd:Identification_Data/wd:Custom_ID/wd:Custom_ID_Data[string(wd:ID_Type_Reference/wd:ID/@type\)='Custom_ID_Type_ID' and string(wd:ID_Type_Reference/wd:ID[@type='Custom_ID_Type_ID'])/text()='{value_for_the_UI_config_field_CustomIDTypeID for Date Joined Industry}']/wd:ID/text()
CustomIDTypeID for External ID	N/A	Employee	wd:Worker/wd:Worker_Data/wd:Personal_

Configuration Parameters	Default Value	XML data to be analyzed	Method to identify the value for configuration parameter
			Data/wd:Identification_ Data/wd:Custom_ID/wd:Custom_ ID_Data[string(wd:ID_Type_ Reference/wd:ID/@type\)='Custo m_ID_Type_ID' and contains(' {value_for_the_UI_config_field_ CustomIDTypeID for Code Of Conduct}', string(wd:ID_Type_ Reference/wd:ID [@type='Custom_ID_Type_ ID'])/text())]/wd:ID/text()
Future Hire Interval	3	Employee	N/A
OrganizationRoleID for Department Head	N/A	Employee	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_ Data/wd:Position_Organizations_ Data/wd:Position_Organization_ Data/wd:Organization_Data/ [string(wd:Organization_Type_ Reference/wd:ID/@type\)='Organi zation_Type_ID' and string (wd:Organization_Support_Role_ Data/wd:Organization_Support_ Role/wd:Organization_Role_ Reference/wd:ID/@type\)='Organi zation_Role_ID' and string (wd:Organization_Type_ Reference/wd:ID [@type='Organization_Type_ ID'])/text()='{value_for_the_UI_ config_field_OrganizationTypeID for DepartmentHead}' and string (wd:Organization_Support_Role_ Data/wd:Organization_Support_ Role/wd:Organization_Role_ Data/wd:Assignment_From)/text ()='Assigned']/wd:Organization_ Support_Role_ Data/wd:Organization_Support_ Role/wd:Organization_Role_ Reference/wd:ID [@type='Organization_Role_ ID']/text()

Configuration Parameters	Default Value	XML data to be analyzed	Method to identify the value for configuration parameter
OrganizationSubTypeID for Asset Class	ORGANIZATION_SUBTYPE_DEPARTMENT_GROUP	Employee	wd:Worker/wd:Worker_Data/wd:Employment_Data/wd:Worker_Job_Data/wd:Position_Organizations_Data/wd:Position_Organization_Data/wd:Organization_Data[string(wd:Organization_Type_Reference/wd:ID/@type\)='Organization_Type_ID' and string(wd:Organization_Subtype_Reference/wd:ID/@type\)='Organization_Subtype_ID' and string(wd:Organization_Type_Reference/wd:ID[@type='Organization_Type_ID'])/text()='{value_for_the_UI_config_field_OrganizationTypeID for Asset Class}']/Organization_Subtype_Reference/wd:ID[@type='Organization_Subtype_ID']/text()
OrganizationSubTypeID for Company	Company	Employee	wd:Worker/wd:Worker_Data/wd:Employment_Data/wd:Worker_Job_Data/wd:Position_Organizations_Data/wd:Position_Organization_Data/wd:Organization_Data[string(wd:Organization_Type_Reference/wd:ID/@type\)='Organization_Type_ID' and string(wd:Organization_Subtype_Reference/wd:ID/@type\)='Organization_Subtype_ID' and string(wd:Organization_Type_Reference/wd:ID[@type='Organization_Type_ID'])/text()='{value_for_the_UI_config_field_OrganizationTypeID for Company}']/Organization_Subtype_Reference/wd:ID[@type='Organization_Subtype_ID']/text()

Configuration Parameters	Default Value	XML data to be analyzed	Method to identify the value for configuration parameter
OrganizationSubTypeID for CostCenter	Cost_Center	Employee	wd:Worker/wd:Worker_Data/wd:Employment_Data/wd:Worker_Job_Data/wd:Position_Organizations_Data/wd:Position_Organization_Data/wd:Organization_Data[string(wd:Organization_Type_Reference/wd:ID/@type\)='Organization_Type_ID' and string(wd:Organization_Subtype_Reference/wd:ID/@type\)='Organization_Subtype_ID' and string(wd:Organization_Type_Reference/wd:ID[@type='Organization_Type_ID'])/text()='{value_for_the_UI_config_field_OrganizationTypeID for CostCenter}']/Organization_Subtype_Reference/wd:ID[@type='Organization_Subtype_ID']/text()
OrganizationSubTypeID for Department	Department	Employee	wd:Worker/wd:Worker_Data/wd:Employment_Data/wd:Worker_Job_Data/wd:Position_Organizations_Data/wd:Position_Organization_Data/wd:Organization_Data[string(wd:Organization_Type_Reference/wd:ID/@type\)='Organization_Type_ID' and string(wd:Organization_Subtype_Reference/wd:ID/@type\)='Organization_Subtype_ID' and string(wd:Organization_Type_Reference/wd:ID[@type='Organization_Type_ID'])/text()='{value_for_the_UI_config_field_OrganizationTypeID for Department}']/Organization_Subtype_Reference/wd:ID[@type='Organization_Subtype_ID']/text()

Configuration Parameters	Default Value	XML data to be analyzed	Method to identify the value for configuration parameter
OrganizationSubTypeID for Desk	ORGANIZATION_SUBTYPE_DESK	Employee	wd:Worker/wd:Worker_Data/wd:Employment_Data/wd:Worker_Job_Data/wd:Position_Organizations_Data/wd:Position_Organization_Data/wd:Organization_Data[string(wd:Organization_Type_Reference/wd:ID/@type\)='Organization_Type_ID' and string(wd:Organization_Subtype_Reference/wd:ID/@type\)='Organization_Subtype_ID' and string(wd:Organization_Type_Reference/wd:ID [@type='Organization_Type_ID'])/text()='{value_for_the_UI_config_field_OrganizationTypeID for Desk}']/Organization_Subtype_Reference/wd:ID [@type='Organization_Subtype_ID']/text()
OrganizationSubTypeID for Division	Division	Employee	wd:Worker/wd:Worker_Data/wd:Employment_Data/wd:Worker_Job_Data/wd:Position_Organizations_Data/wd:Position_Organization_Data/wd:Organization_Data[string(wd:Organization_Type_Reference/wd:ID/@type\)='Organization_Type_ID' and string(wd:Organization_Subtype_Reference/wd:ID/@type\)='Organization_Subtype_ID' and string(wd:Organization_Type_Reference/wd:ID [@type='Organization_Type_ID'])/text()='{value_for_the_UI_config_field_OrganizationTypeID for Division}']/Organization_Subtype_Reference/wd:ID [@type='Organization_Subtype_ID']/text()

Configuration Parameters	Default Value	XML data to be analyzed	Method to identify the value for configuration parameter
OrganizationSubTypeID for Personal Assistant	N/A	Employee	wd:Worker/wd:Worker_Data/wd:Employment_Data/wd:Worker_Job_Data/wd:Position_Organizations_Data/wd:Position_Organization_Data/wd:Organization_Data[string(wd:Organization_Type_Reference/wd:ID/@type\)='Organization_Type_ID' and string(wd:Organization_Subtype_Reference/wd:ID/@type\)='Organization_Subtype_ID' and string(wd:Organization_Type_Reference/wd:ID[@type='Organization_Type_ID'])/text()='{value_for_the_UI_config_field_OrganizationTypeID for Personal Assistant}']/Organization_Subtype_Reference/wd:ID[@type='Organization_Subtype_ID']/text()
OrganizationSubTypeID for Region	Region	Employee	wd:Worker/wd:Worker_Data/wd:Employment_Data/wd:Worker_Job_Data/wd:Position_Organizations_Data/wd:Position_Organization_Data/wd:Organization_Data[string(wd:Organization_Type_Reference/wd:ID/@type\)='Organization_Type_ID' and string(wd:Organization_Subtype_Reference/wd:ID/@type\)='Organization_Subtype_ID' and string(wd:Organization_Type_Reference/wd:ID[@type='Organization_Type_ID'])/text()='{value_for_the_UI_config_field_OrganizationTypeID for Region}']/Organization_Subtype_Reference/wd:ID[@type='Organization_Subtype_ID']/text()

Configuration Parameters	Default Value	XML data to be analyzed	Method to identify the value for configuration parameter
OrganizationType reference ID for Location Hierarchy	LOCATION_ HIERARCHY	Organizati on	wd:Organization/wd:Organization_ Data/wd:Organization_Type_ Reference/wd:ID [@type='Organization_Type_ ID']/text()
OrganizationTypeID for Asset Class	AssetClass	Employee	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_ Data/wd:Position_Organizations_ Data/wd:Position_Organization_ Data/wd:Organization_Data[string (wd:Organization_Type_ Reference/wd:ID/@type\)='Organi zation_Type_ID' and string (wd:Organization_Subtype_ Reference/wd:ID/@type\)='Organi zation_Subtype_ID' and string (wd:Organization_Subtype_ Reference/wd:ID [@type='Organization_Subtype_ ID'])/text()='{value_for_the_UI_ config_field_ OrganizationSubTypeID for Asset Class}']/Organization_Type_ Reference/wd:ID [@type='Organization_Type_ ID']/text()
OrganizationTypeID for Company	COMPANY	Employee	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_ Data/wd:Position_Organizations_ Data/wd:Position_Organization_ Data/wd:Organization_Data[string (wd:Organization_Type_ Reference/wd:ID/@type\)='Organi zation_Type_ID' and string (wd:Organization_Subtype_ Reference/wd:ID/@type\)='Organi zation_Subtype_ID' and string (wd:Organization_Subtype_ Reference/wd:ID [@type='Organization_Subtype_

Configuration Parameters	Default Value	XML data to be analyzed	Method to identify the value for configuration parameter
			ID'])/text()='{value_for_the_UI_ config_field_ OrganizationSubTypeID for Company}']/Organization_Type_ Reference/wd:ID [@type='Organization_Type_ ID']/text()
OrganizationTypeID for CostCenter	COST_CENTER	Employee	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_ Data/wd:Position_Organizations_ Data/wd:Position_Organization_ Data/wd:Organization_Data[string (wd:Organization_Type_ Reference/wd:ID/@type\)='Organi zation_Type_ID' and string (wd:Organization_Subtype_ Reference/wd:ID/@type\)='Organi zation_Subtype_ID' and string (wd:Organization_Subtype_ Reference/wd:ID [@type='Organization_Subtype_ ID'])/text()='{value_for_the_UI_ config_field_ OrganizationSubTypeID for CostCenter}']/Organization_Type_ Reference/wd:ID [@type='Organization_Type_ ID']/text()
OrganizationTypeID for Department	SUPERVISORY	Employee	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_ Data/wd:Position_Organizations_ Data/wd:Position_Organization_ Data/wd:Organization_Data[string (wd:Organization_Type_ Reference/wd:ID/@type\)='Organi zation_Type_ID' and string (wd:Organization_Subtype_ Reference/wd:ID/@type\)='Organi zation_Subtype_ID' and string (wd:Organization_Subtype_

Configuration Parameters	Default Value	XML data to be analyzed	Method to identify the value for configuration parameter
			Reference/wd:ID [@type='Organization_Subtype_ ID'])/text()='{value_for_the_UI_ config_field_ OrganizationSubTypeID for Department}']/Organization_ Type_Reference/wd:ID [@type='Organization_Type_ ID']/text()
OrganizationTypeID for DepartmentHead	SUPERVISORY	Employee	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_ Data/wd:Position_Organizations_ Data/wd:Position_Organization_ Data/wd:Organization_Data/ [string(wd:Organization_Support_ Role_Data/wd:Organization_ Support_Role/wd:Organization_ Role_ Reference/wd:ID/@type\)='Organi zation_Role_ID' and string (wd:Organization_Support_Role_ Data/wd:Organization_Support_ Role/wd:Organization_Role_ Reference/wd:ID [@type='Organization_Role_ ID'])/text()= '{value_for_the_UI_ config_field_OrganizationRoleID for Department Head}' and string (wd:Organization_Support_Role_ Data/wd:Organization_Support_ Role/wd:Organization_Role_ Data/wd:Assignment_From)/text ()='Assigned']/wd:Organization_ Type_Reference/wd:ID [@type='Organization_Type_ ID']/text()
OrganizationTypeID for Desk	ORGANIZATIO N_TYPE_DESK	Employee	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_ Data/wd:Position_Organizations_ Data/wd:Position_Organization_

Configuration Parameters	Default Value	XML data to be analyzed	Method to identify the value for configuration parameter
			Data/wd:Organization_Data[string (wd:Organization_Type_ Reference/wd:ID/@type\)='Organization_Type_ID' and string (wd:Organization_Subtype_ Reference/wd:ID/@type\)='Organization_Subtype_ID' and string (wd:Organization_Subtype_ Reference/wd:ID [@type='Organization_Subtype_ ID'])/text()='{value_for_the_UI_ config_field_ OrganizationSubTypeID for Desk}']/Organization_Type_ Reference/wd:ID [@type='Organization_Type_ ID']/text()
OrganizationTypeID for Division	SUPERVISORY	Employee	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_ Data/wd:Position_Organizations_ Data/wd:Position_Organization_ Data/wd:Organization_Data[string (wd:Organization_Type_ Reference/wd:ID/@type\)='Organization_Type_ID' and string (wd:Organization_Subtype_ Reference/wd:ID/@type\)='Organization_Subtype_ID' and string (wd:Organization_Subtype_ Reference/wd:ID [@type='Organization_Subtype_ ID'])/text()='{value_for_the_UI_ config_field_ OrganizationSubTypeID for Division}']/Organization_Type_ Reference/wd:ID [@type='Organization_Type_ ID']/text()
OrganizationTypeID for Personal Assistant	N/A	Employee	wd:Worker/wd:Worker_ Data/wd:Employment_

Configuration Parameters	Default Value	XML data to be analyzed	Method to identify the value for configuration parameter
			Data/wd:Worker_Job_ Data/wd:Position_Organizations_ Data/wd:Position_Organization_ Data/wd:Organization_Data[string (wd:Organization_Type_ Reference/wd:ID/@type\)='Organization_Type_ID' and string (wd:Organization_Subtype_ Reference/wd:ID/@type\)='Organization_Subtype_ID' and string (wd:Organization_Subtype_ Reference/wd:ID [@type='Organization_Subtype_ ID'])/text()='{value_for_the_UI_ config_field_ OrganizationSubTypeID for Personal Assistant}']/Organization_Type_ Reference/wd:ID [@type='Organization_Type_ ID']/text()
OrganizationTypeID for Region	REGION	Employee	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_ Data/wd:Position_Organizations_ Data/wd:Position_Organization_ Data/wd:Organization_Data[string (wd:Organization_Type_ Reference/wd:ID/@type\)='Organization_Type_ID' and string (wd:Organization_Subtype_ Reference/wd:ID/@type\)='Organization_Subtype_ID' and string (wd:Organization_Subtype_ Reference/wd:ID [@type='Organization_Subtype_ ID'])/text()='{value_for_the_UI_ config_field_ OrganizationSubTypeID for Region}']/Organization_Type_ Reference/wd:ID [@type='Organization_Type_ ID']/text()

Configuration Parameters	Default Value	XML data to be analyzed	Method to identify the value for configuration parameter
SAM Account ID Type	N/A	Employee	wd:Worker/wd:Worker_ Data/wd:Personal_ Data/wd:Identification_ Data/wd:Custom_ID/wd:Custom_ ID_Data[string(wd:ID_Type_ Reference/wd:ID/@type\)='Custo m_ID_Type_ID' and string(wd:ID_ Type_Reference/wd:ID [@type='Custom_ID_Type_ ID'])/text()='{value_for_the_UI_ config_field_CustomIDTypeID for SAM Account ID Type}']/wd:ID/text()
Mobile Device Type ID	Mobile	Employee	wd:Worker/wd:Worker_ Data/wd:Personal_ Data/wd:Contact_Data/wd:Phone_ Data/wd:Phone_Device_Type_ Reference/wd:ID [@wd:type="Phone_Device_Type_ ID"]/text()='value for Mobile Device Type ID'
Landline Device Type ID	Landline	Employee	wd:Worker/wd:Worker_ Data/wd:Personal_ Data/wd:Contact_Data/wd:Phone_ Data/wd:Phone_Device_Type_ Reference/wd:ID [@wd:type="Phone_Device_Type_ ID"]/text()='value for Landline Device Type ID'
OrgTypeID for Custom Organizations	Supervisory	Employee	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_ Data/wd:Position_Organizations_ Data/wd:Position_Organization_ Data/wd:Organization_Data[string (wd:Organization_Type_ Reference/wd:ID/@type\)='Organi zation_Type_ID' and string (wd:Organization_Subtype_ Reference/wd:ID/@type\)='Organi zation_Subtype_ID' and string

Configuration Parameters	Default Value	XML data to be analyzed	Method to identify the value for configuration parameter
			(wd:Organization_Type_ Reference/wd:ID [@type='Organization_Type_ ID']/text()='{value_for_the_UI_ config_field_OrgTypeID for Custom Organizations}']/Organization_ Subtype_Reference/wd:ID [@type='Organization_Subtype_ ID']/text()
OrgSubTypeID for Custom Organizations	N/A	Employee	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_ Data/wd:Position_Organizations_ Data/wd:Position_Organization_ Data/wd:Organization_Data[string (wd:Organization_Type_ Reference/wd:ID/@type\)='Organi zation_Type_ID' and string (wd:Organization_Subtype_ Reference/wd:ID/@type\)='Organi zation_Subtype_ID' and string (wd:Organization_Subtype_ Reference/wd:ID [@type='Organization_Subtype_ ID']/text()='{value_for_the_UI_ config_field_OrgSubTypeID for Custom Organizations}']/Organization_ Type_Reference/wd:ID [@type='Organization_Type_ ID']/text()
OrganizationTypeID for Matrix	Matrix	Employee	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_ Data/wd:Position_Organizations_ Data/wd:Position_Organization_ Data/wd:Organization_Data[string (wd:Organization_Type_ Reference/wd:ID/@type\)='Organi zation_Type_ID' and string (wd:Organization_Subtype_ Reference/wd:ID/@type\)='Organi

Configuration Parameters	Default Value	XML data to be analyzed	Method to identify the value for configuration parameter
			zation_Subtype_ID' and string (wd:Organization_Subtype_ Reference/wd:ID [@type='Organization_Subtype_ ID'])/text()='{value_for_the_UI_ config_field_ OrganizationSubTypeID for Matrix}']/Organization_Type_ Reference/wd:ID [@type='Organization_Type_ ID']/text()
OrganizationSubTypeID for Matrix	Matrix	Employee	wd:Worker/wd:Worker_ Data/wd:Employment_ Data/wd:Worker_Job_ Data/wd:Position_Organizations_ Data/wd:Position_Organization_ Data/wd:Organization_Data[string (wd:Organization_Type_ Reference/wd:ID/@type\)='Organization_Type_ID' and string (wd:Organization_Subtype_ Reference/wd:ID/@type\)='Organization_Subtype_ID' and string (wd:Organization_Type_ Reference/wd:ID [@type='Organization_Type_ ID'])/text()='{value_for_the_UI_ config_field_OrganizationTypeID for Matrix}']/Organization_ Subtype_Reference/wd:ID [@type='Organization_Subtype_ ID']/text()

Additional configuration for update

This section is applicable only when “Use Change Contact Information API for Update” is enabled on the Starling portal.

This configuration uses individual update API of WorkdayHR, **Change_Home_ Contact_Information** for home and **Change_Work_Contact_Information** for work. This configuration will not resolve any existing business process dependency configured on WorkdayHR.

During provisioning of the contact details for an employee, the country information is mandatory since it will be used in extraction of ISO and International phone Code. The country information will be available in the Employees Endpoint in the attribute "addresses~country".

When the **Use Change Contact Information API for Update** configuration is enabled the following One Identity Manager synchronization editor mappings is required to provision the contact details(cell phone, business phone).

Please follow the below steps for provisioning of contact information

1. New mapping set must be created between One Identity Manager **DialogCountry** table and **Employee endpoint** on the target system. This mapping set is only meant for loading the **DialogCountry** table for ISO and International phone code extraction.
2. In provisioning mapping set of **Employee** endpoint, create two new virtual attributes on One Identity Manager end.
   a. Create a virtual attribute **vrtISOCode** of type script and provide the below script in the read section.

vrtISOCode Script

```
Imports VI.Projector.Connection

Dim phoneCode As ISystemObject = SystemObject.Connection.QueryObject
(SystemQuery. _
From("DialogCountry"). _
Select("Iso3166_3","Telephone"). _
Filter(String.Format("UID_DialogCountry='{0}'", $UID_Dialo-
gCountry$.ToString) _
) _
).Result.FirstOrDefault

return phoneCode.GetValue("Iso3166_3").AsString
```

   b. Create a virtual attribute **vrtInternationalPhoneCode** of type script and provide the below script in the read section.

VIProjectConn

```
Imports VI.Projector.Connection

Dim phoneCode As ISystemObject = SystemObject.Connection.QueryObject
(SystemQuery. _
From("DialogCountry"). _
Select("Iso3166_3","Telephone"). _
Filter(String.Format("UID_DialogCountry='{0}'", $UID_Dialo-
gCountry$.ToString) _
) _
).Result.FirstOrDefault

return phoneCode.GetValue("Telephone").AsString
```

3. Map the **vrtISOCode** to target system employee attribute **phoneNumbers** ~ **countryPhoneISOCode** or **phoneNumbersWork** ~ **countryPhoneISOCode** for home and work respectively.
4. Map the **vrtInternationalPhoneCode** to target system employee attribute **phoneNumbers** ~ **internationalPhoneCode** or **phoneNumbersWork** ~ **internationalPhoneCode** for home and work respectively.

Configuration changes required for update operation in Employees V3

If the changes does not exist by default, please follow the below sample steps to configure the WorkdayHR sync project and Person Table in OneIM.

1. Extend the Person Table with 3 new additional columns - **WorkPhoneLandline**, **WorkPhoneMobile**, **Primary Device Type**
   - WorkPhoneLandline - It is to store multiple non primary work landline numbers
   - WorkPhoneMobile - It is to store multiple non primary work mobile numbers

- Primary Device Type - It is to indicate which one of the phone number (landline/mobile) is primary

2. In the column properties of **workPhoneLandline** and **WorkPhoneMobile** created above in Person table, naviagte to value settings tab and enable the Multi-value column check box from designer.
3. In the column properties of **PrimaryDeviceType** created above in **Person** table, navigate to value settings. Add two permitted values **Phone** and **PhoneMobile**. Also enable the defined list of values check box.
4. In synchronisation editor, select the **WorkDayhr** project and create two new variables - **MobileDevice** and **LandlineDevice**.
   - **MobileDevice** - This is the customer specific value "Phone_Device_Type_ID" for mobile phone number.
   - **LandlineDevice** - This the customer specific value "Phone_Device_Type_ID" for landline phone number.
5. In **Employees** mapping set, create a new variable **vrtPrimaryDeviceType** on OneIM side and add the following Read Script

   ```
   If($PrimaryDeviceType$.Contains("Mobile"))
   Return $dprMobileDevice$
   Else
   Return $dprLandlineDevice$
   End If
   ```

6. In **Employees** mapping set, create new mappings for non primary numbers
   - **WorkPhoneLandline** on the left to **workPhoneLandline** on the right, towards the target system direction
   - Newly created **workPhoneMobile** on the left to **workPhoneMobile** on the right, towards the target system direction
   - **vrtISOCode** on the left to **CountryIsoCode** on the right, towards the target system direction
   - **vrtInternationalCode** on the left to **CountryPhoneCode** on the right, towards the target system direction
7. Create mappings for Primary phone number:

   Mapping from left to right direction
   - Phone to **WorkPhonePrimary** with a condition "Left.PrimaryDeviceType = Phone"
   - Mobile Phone to **WorkPhonePrimary** with a condition "Left.PrimaryDeviceType = PhoneMobile"

   Mapping from right to left direction
   - **WorkPhonePrimary** to phone with a condition "right.primaryDeviceType = $dprLandlineDevice$"

- **WorkPhonePrimary** to Mobile Phonewith a condition "right.primaryDeviceType = $dprMobileDevice$"

NOTE: **ISOCode**, **InternationalCode** and **primaryDeviceType** is mandatory to update the values in the target system

Appendix Y

Initiate an OAuth connection to SuccessFactors

Detailed steps to configure an OAuth client are described in this SAP Blog.

The brief notes of the steps to be followed are:

1. Create an interface User ID
2. Grant the necessary permissions to the User ID
   a. Create Permission Role
   b. Create Permission Group
   - If necessary access rights are not available for steps 1 and / or 2, the alternative steps are:
     - Use the default admin account "sfadmin" to configure the OAuth authentication.
     - Find the permission role "sfapi". By default, "sfadmin" would have the needed permission mapped already to this role.
     - Add "sfadmin" under the permission group "sfapi" following the step 2 (refer SAP Blog).
     - Similarly provide the linkage between the permission role "sfapi" and permission group "sfapi" and vice versa following the detailed information provided under step 2 (refer SAP Blog).
3. Register the OAuth2 Client
   a. Go to "Admin Centre", under Company Settings, click the link – "Manage OAuth2 Client Applications".
   b. Click on "Register Client Application".
   c. Generate X.509 certificate and download a copy of the X.509 certificate on your machine.
   d. Open the certificate file using text editor. The X.509 certificate has 2 parts – the private key and the certificate. Get the characters between ——BEGIN ENCRYPTED PRIVATE KEY—– and ——END ENCRYPTED PRIVATE KEY—– in the step for Registering the OAuth client.

e. Go to the OAuth application and take the API key.

f. Use the API Key (for Client Id configuration parameter) and Private Key from the X.509 certificate (for Client Secret configuration parameter) while configuring the Starling Connector.

Appendix Z

Creating custom editable/upsertable attributes in Successfactors employee central

NOTE: As a prerequisite, the SuccessFactors Instance should be enabled for the Employee Central Module which is a part of the HCM suite for SAP SuccessFactors.

1. Go to Admin Center on SuccessFactors Portal, select Manage Business Configuration under tools as following:

   Portal | AdminCenter | Tools | Manage Business Configuration

2. Select any of the object table from left side and add new custom attribute to it.

   Make sure the visibility of the newly added custom attribute is set to "Edit", only then it will be upsertable.

   `"Visibility": "Edit"`

Making the custom attribute upsertable

1. To check the upsertable status of any attribute, follow below path:

   Portal | Admin Center | Tools | OData API Data Dictionary

2. Filter the entity by name

   The Name to be used for filtering some of the entity types are:

   - employmentInfo → EmpEmployment
   - jobInfo → EmpJob
   - personalInfo → PerPersonal
   - personRelationshipInfo → PerPersonRelationship

3. Find the custom attribute and set "sap:upsertable" to **True**.

Managing the custom attribute's visibility in the Employee Data

1. Go to **Admin Center** | **Manage Security** | **Manage Permission Roles**.
2. Select the role **Employee Self Service**, click on **Permission** under "Permission settings".
3. Scroll down to get **Employee Data**, find the newly added custom attributes and provide the needed access levels (View / Edit).
4. Save the changes.

Appendix AA

Custom Foundation Objects in Successfactors HR connector

With Employee Central, there are a pre-defined set of Foundation Objects that are delivered such as Legal Entity, Business Unit, Cost Center, etc. There may be a business requirement to use more Foundation Objects in the Organization, Pay or Jobs Structure in the system. Using the Metadata Framework, you can create Custom Foundation Objects, which can be used in Employee Central > Job Information, to accommodate specific requirements which the pre-delivered set of Foundation objects may not cover.

Example Custom FO Configuration

1. Log into the Test/Sandbox instance as a System Administrator - one that has access to Configure Object Definitions, Manage Business Configuration (BCUI), Manage Data and Test Users
2. Navigate to Admin Center | Configure Object Definitions | Create New | Object Definition.
3. Complete all the required fields.

   For example, you will need to provide a unique Code value which you will need later on. Also, provide a value if the Object should use Effective Dating or not, and what Status the object should have.

   a. **Code**: Typically the Code is entirely up to you, but you should try and use a Code that identifies the object easily (as the Code will be used in other area's of the EC configuration - which we will touch on later in this article).

   b. **Effective Dating**: It is a good idea to select **Basic** as Effective Dating (in line with the MDF Foundation Objects configuration). Please do not use the **Multiple Changes per Day** option.

   c. **Status**: This should always be set to Active (always)
4. Once these options have been set, click **Save** at the bottom of the page.

   The Security, Business Rules and adding new fields can be done later.
5. Click "Take Action" button in the top right can be used to edit the values if required.

Custom attributes with needed data types can be added.

If **Security** is set to **Yes**, then to access this object, it is needed to grant the necessary role-based permissions as this object is an role-based permission secured object.

Implementation in the Starling Connect Connector

New version

Successfactors HR connector has enhanced with a new version v9.0 to support the custom object types dynamically. Customer can input the names of the custom objects to be supported in the connector in the configuration parameter "Custom Object Types" separating each type name by semi colon (;).

NOTE: All schema attributes are considered to be read-only, non-mandatory, not case-exact and not unique.

Mapping

Table 463: Employee mapping

SCIM properties	Successfactors properties
id	Base 64 encoded Composite Key or Simple Key of the object
meta.created	createdDateTime
meta.lastModified	lastModifiedDateTime
All other navigational and non-navigational attribute will have same names at both sides	

Limitations

- The connector implementation supports navigation attributes for custom object types with limitations. If any of the related entity type has not provided the needed rights to be accessed via APIs, the GET operation would fail. If any of the related entity type is not accessible via the 'Entity' API of Successfactors, the schemas in the connector

will not have details regarding those types. This would lead to get a partial set of schemas for custom object types.

> NOTE:
>
> While parsing the schemas for a custom object entity, a new entity metadata to be requested to get the custom object's navigation attribute's schemas.
>
> For example: "cust_ObjectA" has a navigational attribute which is mentioned under "navigationProperties" in the metadata. Under "toRole" of the navigational attribute information there would be a property called "EntitySet" which gives the information to which entity it navigates. However, there would be some entities of which the schemas / metadata could not be retrieved. For example, if the custom object has an association to "Employee Profile User Info", then the entity set as per the "navigationProperties/toRole/EntitySet" value is "EPUserInfoConfig". An error "Entity Entity with the given key is not found." would be returned if the Entity API is triggered to get the schemas of this object type. Even though it is possible to expand the navigation attributes under custom object types using OData API, it is not possible to expand the metadata or schemas for all the navigation attributes using Entity API as well.
>
> Hence the connector would result in partial schemas and responses for custom object types with respect to the navigational attributes.

- Even though the Starling Connector for Successfactors HR supports disabling attributes and adding custom attributes across all resource types, these features are not supported in custom object types as the schemas and mappings are always constructed dynamically.
- The connector currently supports only READ operations on the custom objects.
- The names of the custom object types to be configured in the Starling Connector are case-specific.
- Navigation attributes under a navigation object of a custom object is not supported. For example cust_ObjectA has a navigation attribute of type Business Unit. Any complex or navigation attributes under this Business Unit type attribute will not be processed in the connector.
- Due to multiple requests are being triggered to the target API to read the schemas and data dynamically, the connector functionalities involving custom object types are relatively slow to respond.
- System generated attributes like "mdfSystemXxx", navigation attributes for created by user, last modified by user and so on are not handled in the connector.

Appendix AB

Configuring additional datetime offset in connectors

- Customer can configure additional datetime offset values for the connectors in order to help in synchronizing the objects in the Identity Manager where the objects found missing due to time zone differences between the target and the Identity Manager.
- If the target returned data has offset included with datetime values and if a customer configures any valid offset value in the connector, then the target returned offset value will be replaced with the configured offset value.
- The connector returns the datetimes in UTC format (yyyy-MM-ddTHH:mm:ssZ).
- The datetime offset takes the format +/- HH:mm and the range offset values are -14:00 to +14:00, both inclusive.
- The default value for the offset is 'Z' which is the UTC offset of 00:00.

Appendix AC

How to Create custom attribute for Users in SuccessFactors portal

To create a custom attribute (Users)

1. Under Admin center, go to **Manage Business Configuration** | **Employee Profile** | **User Info** | **Create New**.
2. Create new attributes and click on **Save**.
3. Under **Employee Profile** | **View Template** | **sysUserDirectorySetting**, click **Details**.
4. Find *Userinfo Element*, and add the new field.

   Add the attributes you created.
5. Go to **Configure People Profile** under **Admin Center** and add the new field in *Personal Information* block of **Talent Profile**.
6. Add the newly created attribute in **Add** field and click **Save**.
7. In the **Manage Permission Roles** under **Admin center**, select the permission role **System Admin** | **permission**...| **Employee Data** | grant edit permission to newly created attribute under **User Information** and save.

   The newly created attribute is visible in the response.

To add value to the custom attributes

1. Under **Admin center**, search for *employee* and select any employee whom you want to add the values for custom attributes.
2. Click on **Talent Profile**.
3. Go to **Talent Profile** | **Personal information** | click **Show More** and then click **Edit**.
4. Provide the value to the custom attribute field you created and click Save.

   The newly created value for the attribute is visible in the response.

Appendix AD

SAP Cloud for Customer - Steps to add custom fields at One Identity Manager attributes

Steps to add custom fields at One Identity Manager for TimeZone attribute for Users

Synchronization of TimeZone attribute of User object at SAP Cloud for Customer Connector requires additional configuration at One Identity Manager. This will not be included in the default mapped attributes at One Identity Manager as part of the synchronization project creation. In order to attain this requires a custom mapping with a custom string field. TimeZone attribute often holds longer values than the default custom fields which are 64 char in length. Also these are readOnly fields and can not be modified. Hence the option to overcome this situation is creating a custom string field with 256 char in length.

Steps to create a custom field with 256 char length using Schema Extension

1. Open **Schema Extension** tool.
2. Login using database credentials.
3. In the **Select Method** select the option **Extend Table**.
4. In the **Extend table** window, select **CSMUser** table and click **Next**.
5. In the **Configure columns** window, click **Create New column (+)**.
6. In the **Create new column** window, enter a name for the column.
7. In the **Configure columns** window, select the data type as **string** from the **Data type** list, **256** as **length** and click **Next**.
8. In the **Access permissions** window, add appropriate permissions and click **Next**.
9. Click **Finish** after the compilation is done.
10. Repeat the steps from **4** to **9** for **UCIUser** table.

Steps to configure the mapping in Synchronization Editor

1. Open the **Synchronization Editor** tool.
2. Open the specific synchronization project.
3. Navigate to **Configuration | One Identity Manager Connection |Update Schema**.
4. Go to **Mapping**.
5. Select **Users** mapping.
6. Map the attribute with the newly created custom field.
7. Commit the database.
8. Activate the project.
9. Run full synchronization.
10. Open Manager tool and verify the values appeared in newly added custom field.

Steps to add custom fields at One Identity Manager for Role attribute for Users

Synchronization of **Roles** attribute of User object at **SAP Cloud for Customer** Connector requires additional configuration at One Identity Manager. This will not be included in the default mapped attributes at One Identity Manager as part of the synchronization project creation. In order to attain this requires a custom mapping with a custom multi value field. Roles attribute often holds multi values . Hence the option to overcome this situation is creating a custom field for multi value attribute.

Steps to create a custom field using Schema Extension

1. Open **Schema Extension** tool.
2. Login using database credentials.
3. In the **Select Method** select the option **Extend Table**.
4. In the **Extend table** window, select **CSMUser** table and click **Next**.
5. In the **Configure columns** window, click **Create New column (+)**.
6. In the **Create new column** window, enter a name for the column.
7. In the **Configure columns** window, select the data type as **string** from the **Data type** list, and click **Next**.
8. In the **Access permissions** window, add appropriate permissions and click **Next**.
9. Click **Finish** after the compilation is done.
10. Repeat the steps from **4** to **9** for **UCIUser** table.

Steps to making changes in Designer Tool for newly created custom field

1. Open **Designer** tool.
2. Login using database credentials.
3. Go to **One Identity Manger Schema**.
4. Select **CSMUser** from **Table**.
5. In the **Task** pane select **Show Table Definition** under **Schema Editor**.
6. In the **List** select newly created field.
7. Go to **More** tab under **Column Properties**.
8. Select **Multi-value column** checkbox.
9. Commit the database.
10. Repeat the steps from 3 to 9 for **UCIUser** table.
11. Go to **Database** menu and select **Compile Database**.
12. Go to **Process Orchestration** present in left bottom pane.
13. Select **UCI_UCIUser_Update** from **Processes Table**.
14. In the **Task** pane select **Edit Process 'UCI_UCIUser_Update' under Process Editor**.
15. Select **'PUT/PATCH' user**' and navigate to bottom section '**Parameters**'.
16. Double click on **ForceSyncOf** to edit Parameter.
17. Provide value template as Value = "Custom Field" (Example: **Value = "CCC_ Roles"**).
18. Commit the database.
19. Go to **Database** Menu and select **Compile Database**.

Steps to configuring the mapping in Synchronization Editor

1. Open the **Synchronization Editor** tool.
2. Open the specific synchronization project.
3. Navigate to **Configuration | One Identity Manager Connection |Update Schema**.
4. Go to **Mapping**.
5. Select **Users** mapping.
6. Map the attribute with the newly created custom field.
7. Commit the database.
8. Activate the project.
9. Run full synchronization.
10. Open Manager tool and verify the values appeared in newly added custom field.

Appendix AE

Creating a Service Principal for the Azure Infrastructure Connector

Use Azure CLI by accessing https://shell.azure.com , select "Bash" console.

Use the command

```
az ad sp create-for-rbac -n "{sp_name}" --role Reader --scopes /
```

to create a Service Principal with reader role for Root Scope.

Collect the values for "appId", "password" and "tenant" from the Azure CLI command response for "Client Id", "Client Secret" and "Tenant Id" respectively.

NOTE: To support Write operations, the service principal needs to have 'owner' role.

Appendix AF

Workday permissions needed to integrate via the Starling Connector

If the admin account credentials cannot be used in the SCIM integration setup through Starling Connector, the alternative approach is using the credentials of integration system user configured in the Workday tenant. This section describes how to create an integration system user in Workday and to provide the necessary permissions based on the business use-cases.

Creating an integration system user

To create an integration user:

1. Sign in to your Workday tenant using an administrator account. In the **Workday Application**, enter create user in the search box, and then click **Create Integration System User**.
2. Complete the **Create Integration System User** task by supplying a user name and password for a new Integration System User.
    - Leave the **Require New Password at Next Sign In** option unchecked, because this user will be log on through programmed steps.
    - Leave the **Session Timeout Minutes** with its default value of 0, which will prevent the user's sessions from timing out prematurely.
    - Select the option **Do Not Allow UI Sessions** as it provides an added layer of security that prevents a user with the password of the integration system from logging into Workday.

Creating an integration security group

In this step, you will create an unconstrained or constrained integration system security group in Workday and assign the integration system user created in the previous step to this group.

To create a security group:

1. Enter create security group in the search box, and then click Create Security Group.
2. Complete the **Create Security Group** task
    - There are two types of security groups in Workday:
        - **Unconstrained**: All members of the security group can access all data instances secured by the security group.
        - **Constrained**: All security group members have contextual access to a subset of data instances (rows) that the security group can access.
    - Please check with your Workday integration partner to select the appropriate security group type for the integration.
    - Once you know the group type, select **Integration System Security Group (Unconstrained)** or **Integration System Security Group (Constrained)** from the **Type of Tenanted Security Group** dropdown.
    - After the Security Group creation is successful, you will see a page where you can assign members to the Security Group.
    - Add the new integration system user created in the previous step to this security group. If you are using constrained security group, you will also need to select the appropriate organization scope.

Configuring domain security policy permissions

In this step, you'll grant "domain security" policy permissions for the worker data to the security group.

To configure domain security policy permissions:

1. Enter **Security Group Membership and Access** (or **Who are the Members of a Security Group**) in the search box and click on the report link.
2. Search and select the security group created in the previous step.
3. Click on the ellipsis (...) next to the group name and from the menu, select **Security Group > Maintain Domain Permissions for Security Group**.
4. Under **Integration Permissions**, add the following domains to the list **Domain Security Policies permitting Put access**:
    - *External Account Provisioning*
    - *Worker Data: Public Worker Reports*
    - *Person Data: Work Contact Information*
    - *Workday Accounts*

5. Under **Integration Permissions**, add the following domains to the list **Domain Security Policies permitting Get access**:
    - *Worker Data: Workers*
    - *Worker Data: All Positions*
    - *Worker Data: Current Staffing Information*
    - *Worker Data: Business Title on Worker Profile*
    - *Worker Data: Qualified Workers (Optional - add this to retrieve worker qualification data for provisioning)*
    - *Worker Data: Skills and Experience (Optional - add this to retrieve worker skills data for provisioning)*
    - *Job Information*
    - *Manage: Location*
    - *Manage: Location Hierarchy*
    - *Manage: Organization Integration*
    - *Manage: Supervisory Organization*
    - *Person Data: Date of Birth*
    - *Person Data: Gender*
    - *Person Data: ID Information*
6. After completing above steps, the permissions screen will appear summarizing the selected PUT and GET access permissions.
7. Click **OK** and **Done** on the next screen to complete the configuration.

Edit business process security policies

To edit the Business Process Security Policies for Functional Area report:

1. Access the **Business Process Security Policies for Functional Area** report.
2. Provide the needed "Functional Area" and the "Business Process", **click Edit Permissions** in the bottom of the screen.
3. Scroll and find the "Initiating Action" which has "(Web Service)" in it.
4. Add the Security Group created above.
5. Click **OK** and **Done** on the next screen to complete the configuration.
6. Following are the use-cases where permissions are needed when using with Starling Connect for Workday:

Table 464: Use cases for permissions

Use case in the connector	Functional Area	Business Process	Initiating Action
Edit Other / Custom IDs for Worker	Personal Data	Edit Other IDs	Change Other IDs (Web Service)
Modify home contact information	Contact Information	Home Contact Change	Change Home Contact Information (Web Service)
Modify work contact information	Contact Information	Work Contact Change	Change Work Contact Information (Web Service)
Modify contact information using maintain contact information API	Contact Information	Contact Change	Maintain Contact Information (Web Service)

Activating security policy changes

To activate security policy changes:

1. Enter activate in the search box, and then click on the link **Activate Pending Security Policy Changes**.
2. Begin the Activate Pending Security Policy Changes task by entering a comment for auditing purposes, and then click **OK**.
3. Complete the task on the next screen by checking the checkbox **Confirm**, and then click **OK**.

Appendix AG

Configuring integration application in DocuSign

Follow the below steps in order to configure an integration application and gather the required information for authentication.

1. Log in to the DocuSign eSignature Admin Dashboard. If demo instance is used, the admin dashboard can be accessed at eSignature Admin | DocuSign
2. From main menu "Settings", under side menu "Integrations", access "Apps and Keys".
3. Under "My Account Information", collect "User ID", "API Account ID" and "Account Base URI".
4. Click on "Add App and Integration Key" button to create an integration application, provide the App name.
5. Under "Authentication" section
   a. Select "Yes" for "User Application"
   b. Click "Add Secret Key" under "Authentication Method for your App" → "Authorization Code Grant" to add a secret key
6. Under "Service Integration" section
   a. Click "Generate RSA" to generate a RSA keypair
   b. Copy and save the "Private Key"
7. Under "Additional settings" section
   a. Click "Add URI" under "Redirect URIs" to add a redirect URI. For example: http://localhost/
8. "Save" the integration application and collect the "Integration Key" for thus created application under the "Apps and Integration Keys" list. The integration key acts as the Client Id in the authentication workflow.
9. Complete the admin (integration account) consent flow:
   a. Construct an URI in the format `https://<authentication_server>/oauth/auth?response_type=code&scope=impersonation%20signature&client_id=<integration_app's_`

integration_key>&redirect_uri=<integration_app's_configured_redirect_uri> and access the URI in the browser by authenticating using the admin credentials. Example value for the consent URL would be https://account-d.docusign.com/oauth/auth?response_type=code&scope=impersonation signature&client_id=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx&redirect_uri=http://localhost/

b. The authentication server would follow the values:
   i. *account-d.docusign.com* for developer environments
   ii. *account.docusign.com* for production environments
c. Provide the consent by clicking the "Allow Access" button in the browser page
d. Based on the redirect URI provided, the browser will redirect to the page with access code. This code can be ignored.

Appendix AH

Creating integration Connect Client in Coupa

Follow the below steps in order to configure an integration application and gather the required information for authentication.

1. Login to Coupa as an integrations enabled administrator to create an OAuth2/OIDC Client with a grant type Client Credentials. After configuration, the values of Client ID and Client Secret are used to gain access to the Coupa API.
2. To set up your Coupa test instance with a new connection, go to Setup > Oauth2/OpenID Connect Clients.

   NOTE: Type "OAuth" in search box to find the client name quickly.
3. Click Create.
4. For Grant Type select: Client credentials.
5. Specify a name for the Client, Login, Contact info, and Contact Email.
6. Select the scopes from:
   - *core.user_group.read*
   - *core.user_group.write*
   - *core.user.read*
   - *core.user.write*
   - *core.accounting.read*
   - *core.common.read*
7. Click **Save**.

   Saving the client gives you values of the client Identifier and Secret that reqired to gain access to the API scopes you have defined for it.

   NOTE: Coupa instance addresses take the form of

   https://{organization_name}.coupahost.com (for customer instances) or

   https://{organization_name}.coupacloud.com (for partner and demo instances)

Appendix AI

Retrieving Azure DevOps Personal Access Token (PAT)

Follow the below steps to generate/retrieve a PAT.

1. Login to the Azure DevOps portal of your orgainization.
2. From your home page, open user settings and select Personal access tokens.
3. Select + New Token.
4. Name your token, select the organization where you want to use the token, and then set your token to automatically expire after a set number of days.
5. Select scopes as full access and click on create.
6. Copy the token and store it in a secure location. For your security, it doesn't display again.

Appendix AJ

Setup integration system and field override service in Workday

Field Overrides are an alternate way to pull custom attribute information from Workday that replaces the existing custom report facility.

Configuration

To use Field Overrides, Workday administrators must create a new Field Override Integration System within Workday, add the desired custom attributes to it, and configure Okta to use this Integration System when fetching worker data.

To create a Field Override Integration

1. Log in to your Workday account as an administrator, search for Integration System in the search bar, and then click Create Integration System.
2. Enter the following:
   - **System Name**: Enter a name for your System Integration.
   - **Comment**: Optionally add a comment.
   - **Template**: Select **worker** from the **New using template** drop-down menu.
3. Press **Enter**.
4. From the list of results, select **Core Connector: Worker**, then click **OK**:
5. You're redirected to a page for your freshly created Integration System.
6. Scroll down to the **Custom Integration Services** section and click the + (plus) sign.
7. Click **Create**.
8. Select **Create Integration Field Override Service** from the list of services.
9. Enter a Name for the Field Override Service, and select **Worker** as the Business Object.

10. Add more fields to your Field Override Service by clicking the + (plus) sign. Property types are based on the property name, so if you want to have properties of different types, refer to Field Override Property Types for more information about the property types and naming conventions. Click **OK**.
11. Now you need to configure the field mappings after creating Integration Service. Go to **Actions** > **Integration System** > **Configure Integration Field Overrides**.
12. Select your Integration Service from the list on the left and configure the mappings for your fields. Type and search for a desired field. Make sure that property types are matching.
13. After you have mapped all the properties, click **OK**>**Done**.
14. Search for your Integration System in Workday, then go to **Actions** > **Integration IDs** > **View IDs**.
15. Copy and save the value of Integration_System_ID. You need this value to set up and update your provisioning settings.

Appendix AK

Retrieving Atlassian Cloud API Key and Directory ID

To generate API key and Directory ID:

1. Go to admin.atlassian.com and select your organization.
2. From the top menu, navigate to Security, and then click on Identity providers from the left-hand panel.
3. Choose the relevant Identity Provider.
4. Add the directory name and set up user provisioning.
5. Click on the Set up user provisioning and then click next.
6. Save SCIM base URL (https://api.atlassian.com/{directoryId}) and API key and click on save and continue.
7. Copy the value of base URL, directory Id and the API key and keep them in a safe place. We won't show them to you again.
8. Click on Stop and save SCIM configuration.
9. Use this SCIM base URL and API key to connect to the identity provider and sync the users and groups from identity provider to Atlassian.

About us

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