



Cisco CloudCenter Action Orchestrator 5.2 Documentation

First Published: May 29, 2019

Last Modified: July 20, 2021

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

1. Action Orchestrator 5.2 Home	5
1.1 Release Notes	6
1.1.1 Action Orchestrator 5.2.3	7
1.1.2 Action Orchestrator 5.2.2	8
1.1.3 Action Orchestrator 5.2.1	9
1.1.4 Action Orchestrator 5.2.0	10
1.2 Getting Started	12
1.2.1 About Action Orchestrator	13
1.2.2 Default Home Page	14
1.2.3 System Elements	17
1.2.4 Upgrading to Action Orchestrator 5.2.1	21
1.2.5 Extending Validity of Service Certificates	23
1.2.6 Migrating Database to Install Action Orchestrator 5.2.1	31
1.2.7 Migrating Database to Install Action Orchestrator 5.2.0	35
1.2.8 Cleaning Keys from REDIS	39
1.3 Configuring Workflows	40
1.3.1 Workflows Overview	41
1.3.2 Creating a Basic Workflow	43
1.3.3 Import Workflows	44
1.3.4 Export Workflows	45
1.3.5 Adding Workflow Properties	46
1.3.6 Adding Triggers	48
1.3.7 Activities	49
1.3.7.1 Activities Overview	50
1.3.7.2 Core Activities	51
1.3.7.2.1 Calculate Date	52
1.3.7.2.2 Calculate Date Time Difference	53
1.3.7.2.3 Convert JSON to XML	54
1.3.7.2.4 Convert XML to JSON	55
1.3.7.2.5 Escape Regex Metacharacters	56
1.3.7.2.6 Find String	57
1.3.7.2.7 Format Date	58
1.3.7.2.8 JSONPath Query	59
1.3.7.2.9 Match Regular Expression	60
1.3.7.2.10 Parse Date	61
1.3.7.2.11 Replace String	62
1.3.7.2.12 Set Variables	63
1.3.7.2.13 Sleep	64
1.3.7.2.14 Split String	65
1.3.7.2.15 Substring	66
1.3.7.2.16 To Lower	67
1.3.7.2.17 To Upper	68
1.3.7.2.18 Trim String	69
1.3.7.2.19 XPath Query	70
1.3.7.2.20 XSL Transform	74
1.3.7.3 AMQP	75
1.3.7.3.1 Bind AMQP Queue	76
1.3.7.3.2 Declare AMQP Exchange	77
1.3.7.3.3 Declare AMQP Queue	78
1.3.7.3.4 Get AMQP Message	79
1.3.7.3.5 Publish AMQP Message	80
1.3.7.4 AWS Service	81
1.3.7.4.1 Associate Subnet	82
1.3.7.4.2 Attach Internet Gateway	83
1.3.7.4.3 Create Account	84
1.3.7.4.4 Create Account Statuses	85
1.3.7.4.5 Create EC2 Instances	86
1.3.7.4.6 Create Internet Gateway	87
1.3.7.4.7 Create Keypair	88
1.3.7.4.8 Create Route	89
1.3.7.4.9 Create Route Table	90
1.3.7.4.10 Create Security Group	91
1.3.7.4.11 Create Security Group Rule	92
1.3.7.4.12 Create Subnet in a VPC	93
1.3.7.4.13 Create VPC	94
1.3.7.4.14 Delete Keypair	95
1.3.7.4.15 Delete Security Group	96
1.3.7.4.16 Delete Security Group Rules	97
1.3.7.4.17 Describe Route Tables	98
1.3.7.4.18 Describe Security Group	99
1.3.7.4.19 Describe Subnets	100
1.3.7.4.20 Describe VPCs	101
1.3.7.4.21 Disassociate Subnet	102
1.3.7.4.22 Generic AWS API Request	103
1.3.7.4.23 IAM Attach User Policy	104
1.3.7.4.24 IAM Create Access Key	105
1.3.7.4.25 IAM Create User	106
1.3.7.4.26 IAM List Policies	107
1.3.7.4.27 IAM List Users	108

1.3.7.4.28 Import Keypair	109
1.3.7.4.29 Reboot EC2 Instances	110
1.3.7.4.30 Start EC2 Instances	111
1.3.7.4.31 Stop EC2 Instances	112
1.3.7.4.32 Terminate EC2 Instances	113
1.3.7.5 Ansible Tower	114
1.3.7.5.1 Ansible Tower Get Job Info	115
1.3.7.5.2 Ansible Tower Launch Job Template	116
1.3.7.6 CloudCenter Suite	117
1.3.7.6.1 Add Billing Unit to Cost Group	118
1.3.7.6.2 Add Cloud Account	119
1.3.7.6.3 Associate Billing Unit to Cost Group	121
1.3.7.6.4 Create Cost Group	122
1.3.7.6.5 Find Billing Unit	123
1.3.7.6.6 Find Cost Group	124
1.3.7.6.7 Find Cost Group Type	125
1.3.7.6.8 Generic CCS API Request	126
1.3.7.6.9 Get Workload Manager Context	127
1.3.7.6.10 Manage Deployment Environment	130
1.3.7.6.11 Update Cost Group	131
1.3.7.6.12 Execute Action on Virtual Machine	132
1.3.7.7 Database Activities	133
1.3.7.7.1 Call Procedure Via JDBC	134
1.3.7.7.2 Delete from Table Via JDBC	135
1.3.7.7.3 Insert Bulk into Table Via JDBC	136
1.3.7.7.4 Insert into Table Via JDBC	137
1.3.7.7.5 Select from Table Via JDBC	138
1.3.7.7.6 Update Table Via JDBC	139
1.3.7.8 Email	140
1.3.7.8.1 Send Email	141
1.3.7.9 Google Cloud Platform	142
1.3.7.9.1 Configure IAM Permissions	143
1.3.7.9.2 Create Firewall Rule	144
1.3.7.9.3 Create Instance	145
1.3.7.9.4 Create Project	146
1.3.7.9.5 Create Service Account	147
1.3.7.9.6 Create VPC Network	148
1.3.7.9.7 Delete Firewall Rule	149
1.3.7.9.8 Delete Instance	150
1.3.7.9.9 Delete VPC Network	151
1.3.7.9.10 Generic GCP API Request	152
1.3.7.9.11 Get Firewall Rule	153
1.3.7.9.12 Get Instances Details	154
1.3.7.9.13 Get Project Details	155
1.3.7.9.14 Get VPC Network	156
1.3.7.9.15 List Firewall Rules	157
1.3.7.9.16 List Instances Templates	158
1.3.7.9.17 List Instances	159
1.3.7.9.18 List Machine Types	160
1.3.7.9.19 List VPC Networks	161
1.3.7.9.20 List Zones	162
1.3.7.9.21 Update Firewall Rule	163
1.3.7.9.22 Update VPC Network	164
1.3.7.10 KAFKA	165
1.3.7.10.1 Submit Kafka Message	166
1.3.7.11 Meraki	167
1.3.7.11.1 Bind Network to a Template	168
1.3.7.11.2 Claim Device into a Network	169
1.3.7.11.3 Create Network	170
1.3.7.11.4 Delete Network	171
1.3.7.11.5 Get Organizations	172
1.3.7.11.6 List Configuration Templates	173
1.3.7.11.7 List Networks	174
1.3.7.11.8 List VLANS of a Network	175
1.3.7.11.9 Update Network	176
1.3.7.12 Microsoft Windows	177
1.3.7.12.1 Control Windows Service	178
1.3.7.12.2 Copy Folder	179
1.3.7.12.3 Correlate Windows Events	180
1.3.7.12.4 Create Folder	181
1.3.7.12.5 Execute Command	182
1.3.7.12.6 Execute Powershell Script	183
1.3.7.12.7 Execute Windows Script	184
1.3.7.12.8 Get Folder Properties	185
1.3.7.12.9 Query Windows Events	186
1.3.7.12.10 Query Windows Performance Counter	187
1.3.7.12.11 Query Windows Registry	188
1.3.7.12.12 Query Windows Service	189
1.3.7.12.13 Read File	190

1.3.7.12.14 Restart Server	191
1.3.7.12.15 Stop Process	192
1.3.7.12.16 Uninstall Application	193
1.3.7.12.17 Microsoft Write File	194
1.3.7.13 Prime Service Catalog	195
1.3.7.13.1 Cancel Service Request	196
1.3.7.13.2 Create Service Items	197
1.3.7.13.3 Delete Service Items	198
1.3.7.13.4 Find Service Items	199
1.3.7.13.5 Get Service Item	200
1.3.7.13.6 Mark Task Complete	201
1.3.7.13.7 Submit Service Request	202
1.3.7.13.8 Update Service Items	204
1.3.7.14 Python	205
1.3.7.14.1 Execute Python Script	206
1.3.7.14.2 Execute Python Script Activity For Python 2.7 (Obsolete)	207
1.3.7.15 Table Activities	208
1.3.7.15.1 Add Row to Table	209
1.3.7.15.2 Delete From Table	210
1.3.7.15.3 Read Table from JSON	211
1.3.7.15.4 Read Table from Text	213
1.3.7.15.5 Read Table from XML	214
1.3.7.15.6 Select From Table	215
1.3.7.15.7 Update Row in Table	216
1.3.7.16 Task	217
1.3.7.16.1 Create Approval Request	218
1.3.7.16.2 Query Object	219
1.3.7.16.3 Wait For Event	220
1.3.7.17 Terminal	221
1.3.7.17.1 Execute Terminal Command(s)	222
1.3.7.18 Unix/Linux System	223
1.3.7.18.1 Execute Linux/Unix SSH Command	224
1.3.7.18.2 Execute Linux/Unix SSH Script	226
1.3.7.18.3 Write File	227
1.3.7.19 Web Service	228
1.3.7.19.1 HTTP Request	229
1.3.7.19.2 Swagger HTTP Request	230
1.3.7.20 Creating an Atomic Workflow	231
1.3.8 Adding Logic Components to a Workflow	232
1.3.9 Variable Reference	233
1.3.10 Share Workflow	234
1.4 Runs	235
1.5 Configuring Targets	236
1.5.1 Overview Targets	237
1.5.2 Targets	238
1.5.2.1 Targets Overview	239
1.5.2.2 AMQP Endpoint	240
1.5.2.3 AWS Endpoint	241
1.5.2.4 Amazon Device Endpoint	242
1.5.2.5 Ansible Tower Endpoint	243
1.5.2.6 CloudCenter Endpoint	244
1.5.2.7 Google Cloud Platform Endpoint	245
1.5.2.8 HTTP Endpoint	246
1.5.2.9 IMAP Endpoint	247
1.5.2.10 JDBC Database Server	248
1.5.2.11 KAFKA Endpoint	249
1.5.2.12 Meraki Endpoint	250
1.5.2.13 Microsoft Windows Endpoint	251
1.5.2.14 POP3 Endpoint	252
1.5.2.15 Prime Service Catalog Endpoint	253
1.5.2.16 SMTP Endpoint	254
1.5.2.17 Terminal Endpoint	255
1.5.2.18 Unix/Linux Endpoint	256
1.5.3 Target Groups	257
1.5.4 Add Target Type	258
1.6 Configuring Account Keys	259
1.6.1 Account Keys Overview	260
1.6.2 Amazon Alexa Device Credentials	261
1.6.3 AMQP Certificate-Based Credentials	262
1.6.4 AMQP Password-Based Credentials	263
1.6.5 AMQP Password-Less Certificate-Based Credentials	264
1.6.6 Ansible Tower Credentials	265
1.6.7 Cisco Prime Service Catalog Credentials	266
1.6.8 CloudCenter Suite Explicit User	267
1.6.9 AWS Credentials	268
1.6.10 Email Credentials	269
1.6.11 Git Password-Based Credentials	270
1.6.12 Google Cloud Platform Authentication	271
1.6.13 HTTP Basic Authentication	272

1.6.14 HTTP Client Certificate Authentication	273
1.6.15 JDBC Login Credentials	274
1.6.16 Kafka Authentication	275
1.6.17 Kafka Certificate Authentication	276
1.6.18 Meraki Credentials	277
1.6.19 Microsoft Windows Credentials	278
1.6.20 Terminal Key-Based Credentials	279
1.6.21 Terminal Password-Based Credentials	280
1.7 Configuring Variables	281
1.7.1 Adding Variables	282
1.7.2 Creating Global Variables	284
1.7.3 Creating Variable Type	285
1.8 Configuring Calendars	286
1.9 Configuring Tasks	287
1.10 Configuring Schedules	288
1.11 Configuring Events	289
1.11.1 Events Overview	290
1.11.2 AMQP Event	291
1.11.3 Approval Task Event	292
1.11.4 Email Event	293
1.11.5 KAFKA Event	294
1.12 Admin	295
1.12.1 Admin Overview	296
1.12.2 Action Orchestrator Roles	297
1.12.3 Integrations	301
1.12.3.1 Integrations Overview	302
1.12.3.2 Git Repositories	303
1.12.3.3 Add Git Repository	304
1.12.4 Schemas	305
1.12.4.1 Schemas Overview	306
1.12.4.2 Manage Schemas	307
1.12.4.3 Creating Schema	308
1.12.4.3.1 Activity	309
1.12.4.3.2 Adapter	312
1.12.4.3.3 Event	313
1.12.4.3.4 Account Key	314
1.12.4.3.5 Target	315
1.12.5 Categories	316
1.12.5.1 Categories Overview	317
1.12.5.2 Adding Category	318
1.13 File Operations Overview	319
1.14 Creating Custom Adapters	320
1.14.1 Creating Custom Adapters Overview	321
1.14.2 Python Adapter	322
1.14.2.1 Create Custom Adapter in Python	323
1.14.2.1.1 Python Adapter Template	324
1.14.3 Golang Adapter	326
1.14.3.1 Create Custom Adapter in Golang	327
1.14.3.1.1 Schema Generation Utility	328
1.14.3.1.2 GoLang Adapter Template	329
1.14.4 Java Adapter	330
1.14.4.1 Create Custom Adapter in Java	331
1.14.4.1.1 Java Adapter Template	332
1.15 Action Orchestrator Schemas	333
1.15.1 Overview	334
1.15.2 Data Schema	335
1.15.3 View Schema	337
1.15.4 Sample Schema	368
1.15.5 JSON Standard Keywords	372
1.16 Action Orchestrator API	373
1.16.1 API Overview	374
1.16.2 API Authentication	381
1.16.3 API Key	382
1.16.4 Base URI Format	384
1.16.5 HTTP Status Codes	386
1.16.6 CSRF Token Protection	387
1.16.7 API Permissions	389
1.16.8 Synchronous and Asynchronous Calls	391
1.16.9 Action Orchestrator Calls 5.2.0	393
1.16.10 Import/Export API Calls 5.2.0	394

Action Orchestrator 5.2 Home

CloudCenter Action Orchestrator 5.2 Documentation

System Announcements

Cisco released the following Action Orchestrator releases:

- [Action Orchestrator 5.2.0](#) released on May 29, 2020
- [Action Orchestrator 5.2.1](#) released on February 3, 2021
- [Action Orchestrator 5.2.2](#) released on April 8, 2021
- [Action Orchestrator 5.2.3](#) released on April 9, 2021

Search Action Orchestrator Documentation

Recent Updates

[Import/Export API Calls 5.1.0](#)

updated 44 minutes ago

[view change](#)

[Action Orchestrator Calls 5.1.0](#)

updated 44 minutes ago

[view change](#)

[Action Orchestrator 5.1.4](#)

updated yesterday at 2:14 PM

[view change](#)

Back to: [CloudCenter Suite Home](#)

Release Notes

Action Orchestrator Release Notes

- [Action Orchestrator 5.2.3](#)
- [Action Orchestrator 5.2.2](#)
- [Action Orchestrator 5.2.1](#)
- [Action Orchestrator 5.2.0](#)

Action Orchestrator 5.2.3

Action Orchestrator 5.2.3 Release Notes

- [Release Date](#)
- [Installation and Upgrade](#)
- [Deprecation Notice](#)
- [Documentation](#)
- [Known Issues](#)
- [Resolved Issues](#)

Release Date

First Published: April 9, 2021

Updated:

- July 20, 2021: Added the *Documentation* section in include a list of changed pages.

Installation and Upgrade

- Before upgrading from any version of Action Orchestrator to Action Orchestrator 5.2.1, you have to back up and migrate database of your existing Action Orchestrator version and then uninstall and delete any instances of existing Action Orchestrator from your system. For more details, see [Migrating Database to Install Action Orchestrator 5.2.1](#).
- Before accessing and working on Action Orchestrator 5.2.1, you have to clean up the keys from REDIS that were accumulated during backup of Action Orchestrator 5.2.0. For more details, see [Cleaning Keys from REDIS](#).
- See the [Suite Admin 5.2.4](#) release notes for additional context.
- To upgrade from Action Orchestrator 5.1.4 to Action Orchestrator 5.2.1, see [Upgrading to Action Orchestrator 5.2.1](#).
- Until Action Orchestrator 5.2.0, the service certificates are valid only for one year whereas Action Orchestrator 5.2.1 comes with the service certificates that are valid for three years. To extend the validity of service certificates and update to Action Orchestrator 5.2.1, see [Extending Validity of Service Certificates](#).

Deprecation Notice

According to the [Action Orchestrator 5.1.4](#) Release Notes, the Ansible Tower and Python 2.7 adapters have been officially deprecated in this release.

Documentation

The following documentation changes were implemented in Action Orchestrator 5.2.3:

- [Action Orchestrator Calls 5.2.0](#) (added API download link)
- [Import/Export API Calls 5.2.0](#) (added API download link)

Known Issues

- No updates.

Resolved Issues

- This release includes fixes for internally found issues that do not change the product behavior in any way.

Action Orchestrator 5.2.2

Action Orchestrator 5.2.2 Release Notes

- [Release Date](#)
- [Installation and Upgrade](#)
- [Deprecation Notice](#)
- [Known Issues](#)
- [Resolved Issues](#)

Release Date

First Published: April 8, 2021

Installation and Upgrade

- Before upgrading from any version of Action Orchestrator to Action Orchestrator 5.2.1, you have to back up and migrate database of your existing Action Orchestrator version and then uninstall and delete any instances of existing Action Orchestrator from your system. For more details, see [Migrating Database to Install Action Orchestrator 5.2.1](#).
- Before accessing and working on Action Orchestrator 5.2.1, you have to clean up the keys from REDIS that were accumulated during backup of Action Orchestrator 5.2.0. For more details, see [Cleaning Keys from REDIS](#).
- See the [Suite Admin 5.2.4](#) release notes for additional context.
- To upgrade from Action Orchestrator 5.1.4 to Action Orchestrator 5.2.1, see [Upgrading to Action Orchestrator 5.2.1](#).
- Until Action Orchestrator 5.2.0, the service certificates are valid only for one year whereas Action Orchestrator 5.2.1 comes with the service certificates that are valid for three years. To extend the validity of service certificates and update to Action Orchestrator 5.2.1, see [Extending Validity of Service Certificates](#).

Deprecation Notice

According to the [Action Orchestrator 5.1.4](#) Release Notes, the Ansible Tower and Python 2.7 adapters have been officially deprecated in this release.

Known Issues

- No updates.

Resolved Issues

- This release includes fixes for internally found issues that do not change the product behavior in any way.

Action Orchestrator 5.2.1

Action Orchestrator 5.2.1 Release Notes

- [Release Date](#)
- [Installation and Upgrade](#)
- [Deprecation Notice](#)
- [Known Issues](#)
- [Resolved Issues](#)

Release Date

First Published: February 3, 2021

Installation and Upgrade

- Before upgrading from any version of Action Orchestrator to Action Orchestrator 5.2.1, you have to back up and migrate database of your existing Action Orchestrator version and then uninstall and delete any instances of existing Action Orchestrator from your system. For more details, see [Migrating Database to Install Action Orchestrator 5.2.1](#).
- Before accessing and working on Action Orchestrator 5.2.1, you have to clean up the keys from REDIS that were accumulated during backup of Action Orchestrator 5.2.0. For more details, see [Cleaning Keys from REDIS](#).
- See the [Suite Admin 5.2.4](#) release notes for additional context.
- To upgrade from Action Orchestrator 5.1.4 to Action Orchestrator 5.2.1, see [Upgrading to Action Orchestrator 5.2.1](#).
- Until Action Orchestrator 5.2.0, the service certificates are valid only for one year whereas Action Orchestrator 5.2.1 comes with the service certificates that are valid for three years. To extend the validity of service certificates and update to Action Orchestrator 5.2.1, see [Extending Validity of Service Certificates](#).

Deprecation Notice

According to the [Action Orchestrator 5.1.4](#) Release Notes, the Ansible Tower and Python 2.7 adapters have been officially deprecated in this release.

Known Issues

- No updates.

Resolved Issues

- Upgraded ArangoDB Database from v3.6.1 to v3.7.6 to address several security and performance-related issues.
- Extended Action Orchestrator TLS certificate expiration dates.

Action Orchestrator 5.2.0

Action Orchestrator 5.2.0 Release Notes

- [Release Date](#)
- [Installation and Upgrade](#)
- [Features](#)
- [Action Orchestrator UI](#)
- [Security](#)
- [API](#)
 - [New APIs](#)
 - [Updated APIs](#)
- [Integrations](#)
- [Documentation](#)
- [Known Issues](#)
- [Resolved Issues](#)

Release Date

First Published: May 29, 2020

Updated:

- February 3, 2021: Updated the *Documentation* section to include updated pages

Installation and Upgrade

- Before upgrading from Action Orchestrator 5.0 or Action Orchestrator 5.1 to Action Orchestrator 5.2.0, you have to back up and migrate database of your existing Action Orchestrator version and then uninstall and delete any instances of existing Action Orchestrator from your system. For more details, see [Migrating Database to Install Action Orchestrator 5.2.0](#).
- See the [Suite Admin 5.2.0](#) release notes for additional context.

Features

- **Webhook:** This feature is included in Action Orchestrator 5.2.0 under [Adding Triggers](#).
- **File Operations:** See [File Operations Overview](#) for additional details.

Action Orchestrator UI

- **Browser Compatibility:** See [Browser Compatibility](#) for a list of compatible browsers.
- **Localization:** See [UI Language Availability](#).
- Refer to the Suite Admin for additional context on [Suite Architecture](#) and [Administration and Governance](#).

Security

See [Security Considerations](#) for details.

API

Action Orchestrator 5.2.0 includes the following new and updated APIs:

New APIs

- [Action Orchestrator Calls 5.2.0](#) > Webhooks:
 - Handler to get all webhooks information: `Get/v1/webhooks`
 - Handler to create a webhook: `Post/v1/webhooks`
 - Handler to return Webhook information: `Get/v1/webhooks/{webhook_id} readWebhookByID`
 - Handler to update webhook: `Put/v1/webhooks/{webhook_id}`
 - Handler to delete webhook: `Delete/v1/webhooks/{webhook_id}`
 - Handler to refresh api_key for webhook: `Post/v1/webhooks/{webhook_id}/refresh_api_key`

Updated APIs

- [Action Orchestrator Calls 5.2.0](#) > WorkflowInstances
 - Handler to get a summary of workflows instances: `Get/v1/instances/summary`

- [Action Orchestrator Calls 5.2.0](#) > Workflows
 - Handler to start workflow execution: Post/v1.1/workflows/start
 - Handler to get a summary of workflows: Get/v1/workflows/summary
- [Action Orchestrator Calls 5.2.0](#) > Targets > ValidateTargets
 - Handler to perform target validations: Post/v1/targets/validate
- See [Action Orchestrator API](#) for additional details.

Integrations

You have read only access to the [Cisco Action Orchestrator Public Repository](#). You will be able to import workflow examples and atomic actions from this repository. For more information, see [Add Git Repository](#).

Documentation

The following documentation change was implemented in Action Orchestrator 5.2.0:

- [Migrating Database to Install Action Orchestrator 5.2.0](#) (added a fourth bullet regarding installation of arangodb to the *Prerequisites* section and added a note to the code block in Step 9 of the *Procedure* section)
- [Migrating Database to Install Action Orchestrator 5.2.0](#) (changed the page name from *Migrating Database*)

Known Issues

Action Orchestrator 5.2.0 has the following known issues:

- If a workflow has more than one parallel branch within a parallel block and if both the parallel branches are trying to update same table variable, the workflow run fails intermittently with a conflict error.
- If a target group exists in the system and if the user is trying to create more than one target in parallel which matches the criteria defined in target group, the target creation may fail intermittently with a conflict error.
- If the triggers are not triggering the workflows even after the Action Orchestrator 5.2 is up and the database migration is completed, disable the trigger and then enable the trigger.

Resolved Issues

No updates

- Changed the heading from *Migrating Database* to [Migrating Database to Install Action Orchestrator 5.2.0](#).

Getting Started

Getting Started with Action Orchestrator

- [About Action Orchestrator](#)
- [Default Home Page](#)
- [System Elements](#)
- [Upgrading to Action Orchestrator 5.2.1](#)
- [Extending Validity of Service Certificates](#)
- [Migrating Database to Install Action Orchestrator 5.2.1](#)
- [Migrating Database to Install Action Orchestrator 5.2.0](#)
- [Cleaning Keys from REDIS](#)

About Action Orchestrator

About Action Orchestrator

Action Orchestrator is a powerful workflow automation, technology-agnostic, and cross-domain orchestration product. This orchestration platform easily binds Cisco products together and connects smoothly to third-party products and open-source solutions, providing a unified solution. The following designs are applicable to provide advanced automation:

- Cloud native application with microservices running in containers help maintain a relatively lesser cloud footprint.
- Available as a Service and can support multi-tenant and multi-instance options.
- For information on infrastructure requirements see [Prepare Infrastructure](#).
- For information on installation see [Suite Installer 5.1 Home](#).
- Can be embedded into other products and solutions. Here are two scenarios:
 - Action Orchestrator shall be embedded in one or more base or host Cisco applications (CloudCenter Suite) that provide GTM vehicles for the underlying platform and frameworks.
 - Other Cisco platforms and applications (NSO, MSX, DNAC, Webex Teams, and so forth.) may choose to use Action Orchestrator capabilities by embedding a Action Orchestrator automation framework; or by a loose or tight coupling with the Action Orchestrator.

Service-oriented Orchestration provides the agility to model and act on IT services. These features make creating orchestration active and dynamic, and allow for:

- Defining new, higher-level services in the system, and to deploy new services quickly.
- In real time, after these new types of services have been defined, creating real-time instances of those new services.
- Using events to watch for patterns in these services, enabling policy-driven automation.

Service-oriented Orchestration combines several industry trends to synthesize a fresh approach to orchestration:

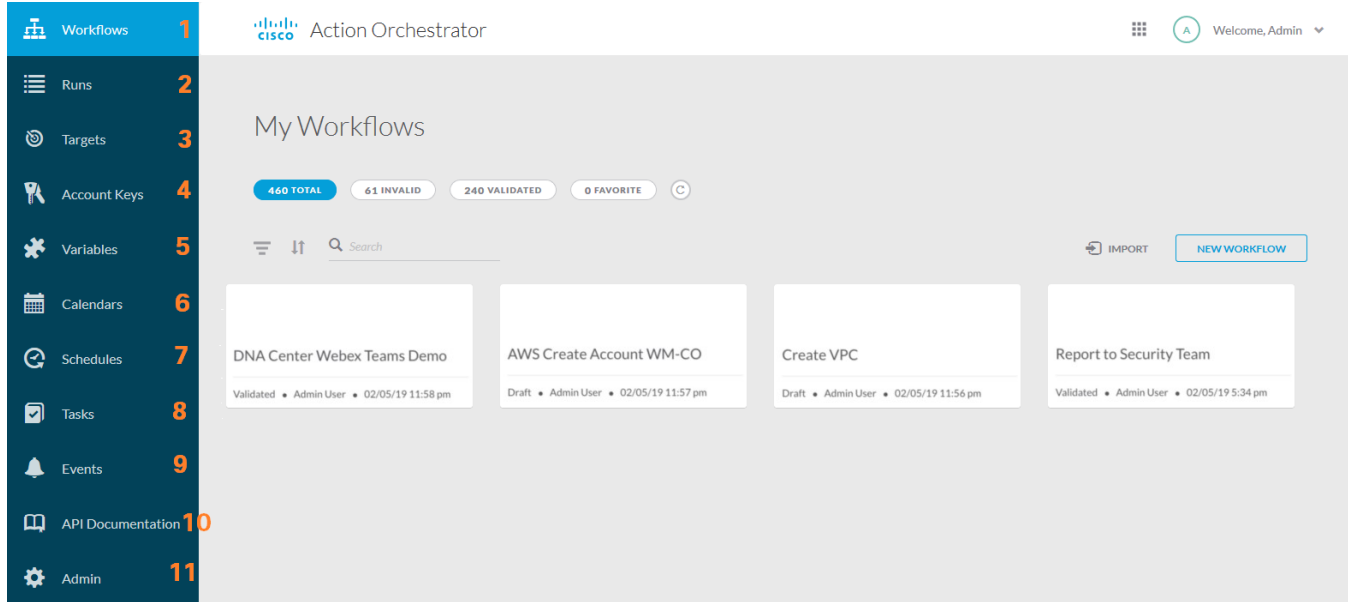
- Action Orchestrator provides fluid mechanisms to exchange service information with the CloudCenter Suite, advancing the integration of these systems.
- The feature delivers many of the capabilities of object-oriented design and programming into the Run-Book-Automation (RBA) / IT Process Automation (ITPA) world. The shift from traditional orchestration to service-oriented orchestration is similar to the shift from procedural to object-oriented programming. Today, virtually all programming is done with object-oriented languages, and object-oriented design has transformed the industry to higher levels of productivity and quality. Service-oriented orchestration holds the same promise.
- The feature aligns to industry standards like the DMTF Common Information Model (CIM) and the Topology and Orchestration Specification for Cloud Applications (TOSCA).
- Model-based automation is becoming popular via script-based tools, especially in the configuration management space. Action Orchestrator combines the capability to model services with the openness to integrate with these tools to leverage their strengths. Moreover, the feature allows model-driven orchestration atop legacy tools to bring the full power of model-driven approaches to integrate with other IT tools.

Default Home Page

Default Home Page

After you log in to Action Orchestrator, you are taken to the Action Orchestrator home page, which displays My Workflows page as a default page. You will be able to traverse to the following pages using the side navigation bar.

Action Orchestrator Home Page





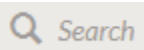





For more information on header and footer, see [Suite Admin Dashboard](#).



When you are logged into Action Orchestrator, you can only view and access the objects for which you have permissions. For more information on roles and permissions, see [Action Orchestrator Roles](#).

1. Workflows: You will be able to switch between **My Workflows** and **Atomic Workflows** pages. Both the pages displays the existing workflows. To create a new workflow click on **NEW WORKFLOW** tab. This page displays the list of created workflows along with their ready state. You can click on the icons of the workflow home page to perform the following tasks:

<p>Module Navigation</p> 	Switch back and forth between the Action Orchestrator module and/or the Suite Admin dashboard.
<p>Bell icon</p> 	When any important Action Orchestrator generated messages are produced, they are listed here. See Suite Admin Dashboard > The Header > Notifications for more details.
<p>Filter icon</p> 	Allows you to filter the workflows based on the Ready State , Category Tags , and Owner .
<p>Order icon</p> 	Sorts the listed workflows based on the Recently modified or Date Created .
<p>Search icon</p> 	Allows you to search the workflows based on the names.

<p>Import icon</p> 	<p>Allows you to import workflows from Git repository. For more information, see Git Repositories.</p>
<p>Dropdown list</p> 	<p>Allows you to select either Run, Delete, Share, View Runs, Change Owner or view Used By details, hover your mouse pointer over the created workflow card and click the dropdown list.</p>
<p>Favorite icon</p> 	<p>Allows you to add workflows to your favorites, hover your mouse pointer over the created workflow card and click the favorite icon.</p>

The workflow defines the automation steps (activities), the logic or flow between these steps, and how to flow data from one step to the next. The atomic workflows allow you to group the workflows in a group name under the activities. This helps you to drag and drop the workflows as activities from the customized group name. For more information, see section [Configuring Workflows](#).

You can view the number of total, draft, validated, published, and favorite workflows on the top of My Workflow page.

2. Runs: The **Runs** page is used to monitor the workflows that are created, paused, cancelled, currently running, and to verify workflows that are successfully completed, and verify workflows that have failed. For more information, see [Runs](#).
3. Targets: You will be able to switch between **Targets** and **Target Groups** page.
 - a. The **Targets** page displays the list of targets added to the Action Orchestrator with their **Display Name** (along with the target type), **Created ON** and **Owner** information. You can see the target **Used by** details, delete the added target by performing the **Delete** action, and **Change Owner** using the dropdown from the **Actions** column. To add a new target, click on **NEW TARGET**.
 - b. The **Target Group** page displays the list of target groups added to the Action Orchestrator with their **Display Name** (along with the target type), **Created ON** and **Owner** information. You can see the target **Used by** details, delete the added target by performing the **Delete** action, and **Change Owner** using the drop down from the **Actions** column. To add a new target group, click on **NEW TARGET GROUP**.

A workflow executes an action within some environment. The specifics of the definition of the connection to the environment are encompassed in the target. The target identifies the host/endpoint that an action or workflow will use while executing. For more information, see section [Configuring Targets](#).

4. Account Keys: The **Account Keys** page displays the **Display Name** (along with the account key type), **Owner**, and **Last Modified** details. You can see the account key **Used by** details, delete the added account key by performing the **Delete** action, and **Change Owner** using the dropdown from the **Actions** column. To add a new account key, click on **ADD ACCOUNT KEY**.

An Account Keys record stores information about the user security context and passes this information to the adapters for activity execution, event monitoring, and some target operations (such as availability monitoring and discovery). Account Keys instances can be shared across targets and workflows. For more information, see section [Configuring Account Keys](#).

5. Variables: You will be able to switch between **Global Variables** and **Variable Types** page.
 - a. The **Global Variables** page displays the **Display Name** (along with the data type), **Scope**, **Value**, **Owner**, and **Last Modified** details. You can see the variable **Used by** details, delete the added variable by performing the **Delete** action, and **Change Owner** using the dropdown from the **Actions** column. To add a new variable, click on **New Variable**.
 - b. The **Variables Types** page displays the **Display Name** (along with the variable type), **Defined By**, **Last Modified By** details, **Owner**, and **Last Modified** details. You can delete the added variable type by performing the **Delete** action and **Change Owner** using the dropdown from the **Actions** column. To add a new variable type, click on **New Variable Type**.

The variables feature provides a storage area for information that is used on a regular basis to avoid having to specify the same information in several places. Data stored in a variable can be altered to affect process execution behavior. For more information, see section [Configuring Variables](#).

6. Calendars: The **Calendars** page displays the **Display Name** (along with the type), **Owner**, and **Last Modified** details. You can delete the Calendars by performing the **Delete** action and **Change Owner** using the dropdown from the **Actions** column. Calendars are reusable for schedules within many workflows. For more information, see section [Configuring Calendars](#).
7. Tasks: The **Tasks** page displays the **Display Name**, **Status**, **Priority**, **Due date**, **Task Requestor**, **Task Owner**, **Task Assignees**, **Last Modified** details. You can **Approve** or **Reject** the task by using the dropdown from the **Actions** column. For more information, see section [Configuring Tasks](#).
8. Schedules: The **Schedules** page displays the **Display Name** (along with the type), **Owner**, and **Last Modified** details. You can see the schedules **Used by** details, delete the added schedule by performing the **Delete** action, and **Change Owner** using the dropdown from the **Actions** column. To add a new schedule, click on **New Schedule**.

When defining a process, you can specify when the process will execute. You can execute a process based on a schedule. A schedule specifies one or more times of day, and is combined with a calendar that specifies on which days the schedule should initiate the process. For more information, see section [Configuring Schedules](#).

9. Events: The **Events** page displays the **Display Name** (along with the type), **Target**, **Owner**, and **Last Modified** details. You can see the event **Used by** details, delete the added event by performing the **Delete** action, and **Change Owner** using the dropdown from the **Actions** column. To add a new event, click on **New Event**.

The Action Orchestrator can monitor events from the environment, and you can specify triggers that initiate workflows when the subscribed event occurs. For more information, see section [Configuring Events](#).

10. API Documentation: This **API Documentation** page displays information on the REST APIs used in Action Orchestrator. For more information, see [Action Orchestrator API](#).
11. Admin: The admin page has the following tabs:
 - a. Main Menu: This brings you back to the page from which you accessed the admin page.

- b. Roles: The **Roles** page displays **Name**, **Description**, **Role Type**, and **OWNER**. You can **Edit** and **Change Owner** using the dropdown from the **Actions** column. Roles are a collection of permissions. Each permission pairs a set of operations that can be performed over some set of objects. A user assignment gives end users the ability to perform the role. Access rights include Create, View, Update, Delete, Run, and so forth. Objects are Action Orchestrator workflows, targets, account keys, variables, and so forth. For more information, see section [Action Orchestrator Roles](#).
- c. Integrations: The Action Orchestrator provides integrations with various technologies and can integrate with repositories such as Git Repositories, see section [Integrations](#).
- d. Schemas: The Action Orchestrator User Interface is completely driven by schema definitions of object types. Each object type has its own schema definition. Each object types schema includes both data schema and view schema, see section [Schemas](#).
- e. Categories: The Categories feature in Action Orchestrator provides a way to organize your workflows based on your organizational or functional requirements. The categories are tags for grouping workflows within the UI, see section [Categories](#).

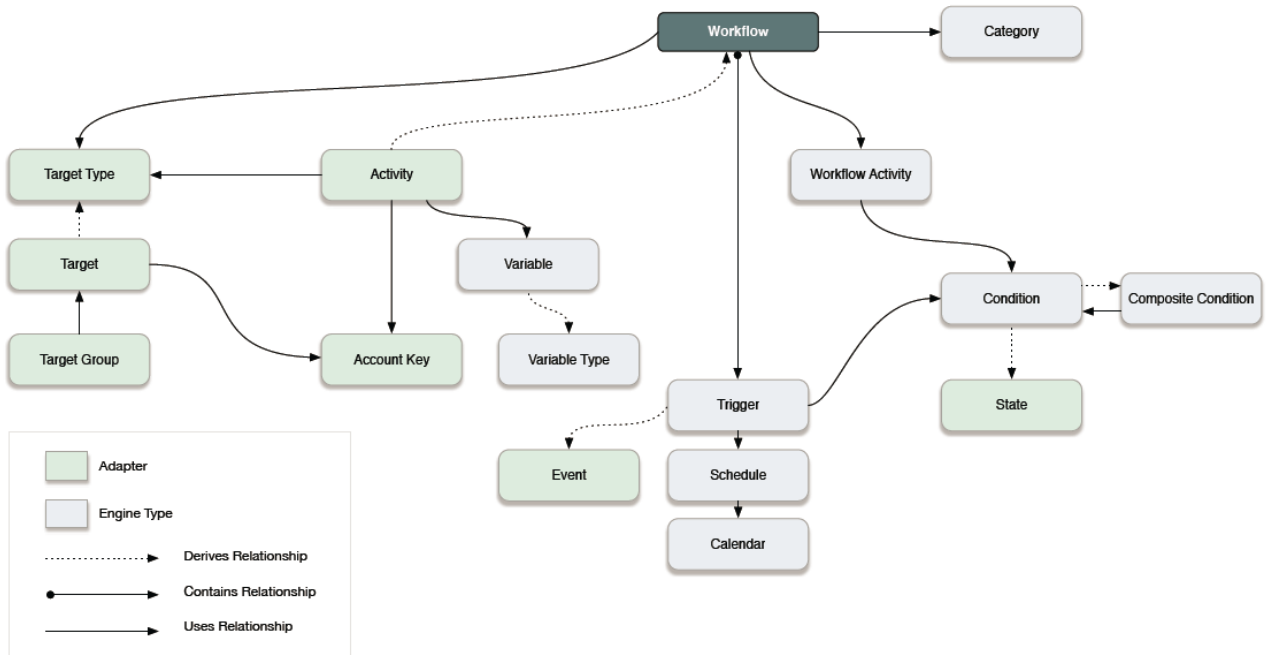
System Elements

Action Orchestrator System Elements

The following diagram shows the major functional elements of the Action Orchestrator system. These elements are discussed in the sections that follow:

- [Workflow](#)
- [Category](#)
- [Activities](#)
- [Conditions](#)
- [Account Keys](#)
- [Targets](#)
- [Target Groups](#)
- [Target Types](#)
- [Triggers](#)
- [Events](#)
- [Schedules](#)
- [Calendars](#)
- [Variables](#)

Action Orchestrator Functional Model



Workflow

Use Action Orchestrator to automate an ITES by defining a workflow, then running instances of the defined workflow. The workflow defines the automation steps (activities), the logic or flow between these steps, and how to flow data from one step to the next. The engine manages the state and lifecycle of a workflow, bringing it into existence, running its steps, and finally terminating it. During and (by default) after workflow execution, the engine retains information so that operators can view the status of their running workflows.

Related Topics

[Creating a Basic Workflow](#)

Category

Action Orchestrator workflows, tasks and several other elements of the functional model can be placed into categories. Categories in Action Orchestrator work just like Microsoft Outlook categories with respect to tagging objects for grouping in the UI. Objects such as workflows can be in multiple categories. For example, a workflow can be both a network best practice and a security best practice. The Categories feature provides a way to organize your workflows based on your organizational or functional requirements. Action Orchestrator ships with predefined categories but provides the functionality for you to create your own business-specific categories. When creating a workflow, you can assign the workflow to a category. You can also add other categories to a category to create a hierarchy.

Activities

Activities are the steps in a workflow. They are customized to perform integration with some environment. Activities can be provided by adapters (binary components in Action Orchestrator) or by automation packs. Therefore both adapters and automation packs can contribute to a particular integration. Workflow activities provide the logic or flow aspects of the workflow. Workflow activities are exposed in the Logic tab of the workflow Editor.

Related Topic

[Adding Logic Components to a Workflow](#)

Conditions

Many workflow logic elements perform tests to control execution. Conditions implement these tests. For example, a Condition Branch can split execution to take one path if a condition exists, and another if it does not. A While Block can iterate execution while a condition exists.

Conditions can also be placed on a workflow trigger, allowing control of situations in which the workflow can run. For example, a scenario might require the workflow to run during two different time ranges, which would require two triggers: one trigger with an 8am-5pm condition and a totally different trigger with a 5pm-8am condition.

There are two basic types of conditions:

Composite conditions

A composite condition builds a compound condition from individual conditions. It allows combining conditions with AND logic, where all of the conditions must be TRUE for the composite condition to be TRUE, or OR logic, where any of the conditions can be TRUE for the composite condition to return TRUE. Compound conditions can be used in other compound conditions to produce complex logic, such as ((X AND Y) OR (A AND B)).

Account Keys

An account key record stores information about the user security context and passes this information to the adapters for activity execution, event monitoring, and some target operations (such as availability monitoring and discovery). Account Key instances can be shared across targets and workflows. For example, if a single set of credentials can be used to access a set of network devices, only one account key instance must be created. When it is time to change the credentials, users can go to the account keys list and edit the single instance to change the credentials. This greatly reduces the configuration load when credentials tend to change often in some environments.

Account Key credentials can be used in a workflow, but no workflow can retrieve credentials. If your workflow must access credentials, use hidden string variables.

The account key user concept allows the product to implement delegation. For example:

1. An IT help desk operator comes to Action Orchestrator to run a workflow.
2. This operator is presented with a list of workflows that Action Orchestrator role-based access control allows them to run. These workflows might include activities that require a level of security permission that the operator does not natively have.
3. The operator can perform actions as a part of the established workflow that are not possible for them to perform manually.

This concept can also be leveraged to reveal where operators make changes outside of a workflow. By examining auditing logs such as Windows logs for things being done under the operator's credentials rather than the Action Orchestrator account key user credentials, it is possible to determine how the operator is doing things outside of workflow and determine how to close things down. So a side effect of Action Orchestrator automation is that customers might be able to tighten security in their environment.

Targets

Targets are instances created from a target type. For example:

- A terminal target allows SSH or telnet to some specific network device.
- A database target allows connection to specific supported databases.

A workflow or activity executes an action within some environment. The specifics of the definition of the connection to the environment are encompassed in the target. For example, a target for:

- An SSH command might be a specific UNIX system or network device.
- A database query might be a specific database.

Workflows can restrict the type of target which they can accept. For example, it is not appropriate to run a workflow to change a network device's configuration against a Windows computer.

A workflow acts on a target. This allows the workflow to perform actions against an external tool or environment. Although a default target instance can be specified directly by a workflow, more commonly it is associated to the workflow at run time.

Activities, which are the steps in a workflow (see [Activities](#)), can also specify a target. Typically, activities default to use the workflow target, but a step in a workflow might need to happen against a different system than the workflow target. For example, a workflow overall might deal with a network device, but a step in the workflow might need to update a database. Often workflows can determine the target on which an activity may act by using a relationship to the target for the workflow, or doing a query on some data such as a name to find a matching target instance.

Related Topics

- [Configuring Targets](#)
- [Adding Triggers](#)

Target Groups

Target groups are collections of targets. Often automation might need to run against all machines in a collection, or against one of the machines in a collection. Target groups provide this functionality.

Adapters can provide target groups to leverage grouping definitions where they exist. For example:

- Active Directory OU: Customers are frustrated when they must recode their grouping information into yet another product. The Active Directory adapter seeks grouping information where it is defined. For example, an Active Directory target group looks up computers in some organizational unit (OU) in the directory.
- Target Type group: Using queries of their attributes, the Action Orchestrator provides type-based groupings of targets. For example, use a target group to group all targets of a given type, or to perform additional filtering to pattern match against a field in the target definition.
- Virtual group: A target group can be a virtual group. Use a virtual group to specify an explicit list of targets, providing the capability to manually select targets and establish group membership. A virtual group can also allow the inclusion of other target groups so that group membership can be defined hierarchically. For example, a virtual group called "Production switches" might include all members of the "Houston data center switches" group as well as all members of the "London data center switches" group, but not members of the "Engineering lab switches."

A default target for a workflow can specify a target group along with a target selection algorithm:

- Typically, a target selection algorithm chooses one or more members of a target group to specify the target instances on which the workflow will act.
- At execution time the target selection algorithm resolves the then-present members of the target group and selects a target.
- When a user or API call interactively runs a workflow ad-hoc (on demand), the user can accept the default target specified in the workflow or override it with a specific target.
- Where a target selection algorithm resolves to multiple target instances, the engine spins up separate workflow instances for each target. Thus at execution time, a workflow instance has a specific target on which it will act, against which the workflow encodes actions.

Related Topics

- [Configuring Targets](#)

Target Types

Target types provide a way to define a service or other IT element that is not represented by any target type provided by an adapter. A target type can:

- Extend an existing adapter-provided target type
- Extend another target type
- Define a completely new target type

All new targets are created based upon a target type. Some target types are 'abstract', meaning they cannot be directly instantiated into targets but are only available for inheritance by other target types. In Action Orchestrator, these target types are marked as either 'creatable' or 'not creatable'.

A target type:

- Exposes (and inherits from its ancestor target types) properties and inter-target named relationships that can be read and set either manually or by an Update Target activity.
- Defines property default values.

Triggers

Workflow instances can come into existence in the following ways:

- A workflow can be invoked manually.
- A workflow can be invoked by another workflow.
- A trigger can fire, which initiates the workflow.
- A workflow can be invoked using the API call.

Triggers are events and conditions in the system that determine how or when the workflow will be executed. Multiple triggers can be added that can be initiated when certain conditions are met.

Action Orchestrator supports two types of rule-based triggers: events and schedules.

Events

The Action Orchestrator can monitor for events from the environment, and you can specify triggers that initiate workflows when the subscribed event occurs. For example, an event might be an incoming stop trap or a fault on a UCS system.

Workflow Events

Workflow events allow one workflow to pass an event to other workflows. For example:

- A Raise workflow Event activity can post a workflow event, and a trigger can monitor for a specific event.
- A Correlate workflow events activity allows monitoring for an event within a workflow.

Workflow events include elements of the Action Orchestrator functional model so that they are aware of internal schema elements. For example, you can include a target type in your subscription criteria.

Workflow events are exposed in the web service, so an external system can programmatically submit an event to Action Orchestrator. However, the use cases for workflow events generally center more around Action Orchestrator-internal use cases; Advanced Message Queuing Protocol (AMQP) is preferred for external message passing.

For internal use cases, Workflow events have the advantage because they are native and lightweight within Action Orchestrator. It is easy to create message driven architectures within Action Orchestrator using workflow events. Since these events are not persisted to the database, they are very lightweight. Workflow events have the advantage that they do not require external setup and installation, as would be the case with AMQP.

Schedules

Schedules allow triggering workflows at some time by leveraging another object called a calendar. Calendars define which days something can occur. Calendars can be selected days or sequences of dates such as weekly or monthly, they can represent dates like fiscal quarter end, or they can be combined hierarchically. Schedules then associate a time with a calendar. When the day is in the calendar, the time is evaluated. Times can be explicit or repeating (for example, hourly).

Calendars

Calendars are reusable for schedules within many workflows. For example, you can define a calendar for Saturdays. When defining a workflow that you want to run on Saturdays, you reference the Saturday calendar. Other examples include a calendar that includes weekends and company holidays when IT might perform scheduled maintenance, or the last week of a fiscal quarter when IT might exclude non-essential automation or deny change requests. The calendars feature defines the calendar to be associated with a schedule, time, or condition. This feature simplifies:

- Reusing calendar definitions across workflows.
- Building complex calendars from other calendars.
- Viewing the workflows that run based on a specific calendar.

Variables

The variables feature provides a storage area for information that is used on a regular basis to avoid having to specify the same information in several places. Data stored in a variable can be altered to affect workflow execution behavior.

Activity Configuration

One of the most common uses of variables is to define activity configuration. Any field in an activity can refer to a variable value rather than an explicit value. For example, you can use a variable to:

- Specify the target as the machine where an event occurred.
- Specify the start date of the workflow' operations window as a parameter to an operating system command.
- Specify a condition, such as a file that should not exist after a job is initially triggered by the arrival of that file where a prior activity should have deleted the file.

Workflow Control Components

Workflows can use variables to define the control components. For example, you can use a variable to define:

- A Conditional activity to look at the exit code of a prior activity.
- A While Loop activity to loop until a query fails or loop for a number of times corresponding to a number of objects pulled from a query.

Workflow Parameters

Variables can be parameterized so that a workflow definition can be vague enough to be reused in multiple places and the specifics can remain undefined so that they can be defined by the person or workflow that invokes the workflow or activity.

For example, a workflow called notify server owner might use a variable server for the name of the server that has a problem. The workflow retrieves the email address of the owner of the server and sends an email.

This workflow might be called from multiple places; a step in a server maintenance job fails, so the maintenance job populates the Server variable and invokes the notify server owner workflow. Another workflow might notify the server owner when a backup completes.

Formulas as Variable Values

You can specify a formula anywhere a variable value is used. For example, an operating system command's parameter might be formed from concatenating two variables' values or from parsing the output of a prior command.

Variable Types

Variable type provide a way to define a new user defined variable type that is not represented by any default variable type. All new variable types are created based on system builtin type variable such as boolean, secure string, and so forth., but creating from these system builtin types are not supported. You can add properties to the new variable type such as Boolean, Encrypted string, Identity, Number, String, and Table or you can add reference to either target or another variable.

Upgrading to Action Orchestrator 5.2.1

Upgrading to Action Orchestrator 5.2.1

- [Prerequisites to Upgrade to Action Orchestrator 5.2.1](#)
- [To Upgrade Action Orchestrator 5.1.4 to Action Orchestrator 5.2.1:](#)
 - [Upgrade from Action Orchestrator 5.1.4 to Action Orchestrator 5.2.0:](#)
 - [Upgrade from Action Orchestrator 5.2.0 to Action Orchestrator 5.2.1:](#)
- [After Upgrading to Action Orchestrator 5.2.1:](#)

Prerequisites to Upgrade to Action Orchestrator 5.2.1

Current Version	Upgrade Version	Comments
Action Orchestrator 5.2.0	Action Orchestrator 5.2.1	You must migrate the database before upgrading from Action Orchestrator 5.2.0 to Action Orchestrator 5.2.1. For more information, see Migrating Database to Install Action Orchestrator 5.2.1 .
Action Orchestrator 5.1.4	<ol style="list-style-type: none">1. Upgrade to Action Orchestrator 5.2.02. Upgrade to Action Orchestrator 5.2.1	You must migrate the database before upgrading from Action Orchestrator 5.1.4 to Action Orchestrator 5.2.0. For more information, see Migrating Database to Install Action Orchestrator 5.2.0 .
Action Orchestrator 5.1.x	<ol style="list-style-type: none">1. Upgrade to Action Orchestrator 5.1.42. Upgrade to Action Orchestrator 5.2.03. Upgrade to Action Orchestrator 5.2.1	You must migrate the database before upgrading from Action Orchestrator 5.1.4 to Action Orchestrator 5.2.0. For more information, see Migrating Database to Install Action Orchestrator 5.2.0 .



You cannot directly upgrade from Action Orchestrator 5.1.4 to Action Orchestrator 5.2.1 without upgrading to Action Orchestrator 5.2.0.

To Upgrade Action Orchestrator 5.1.4 to Action Orchestrator 5.2.1:

First, you must upgrade from Action Orchestrator 5.1.4 to Action Orchestrator 5.2.0. Then, you must upgrade from Action Orchestrator 5.2.0 to Action Orchestrator 5.2.1.

Upgrade from Action Orchestrator 5.1.4 to Action Orchestrator 5.2.0:

1. You have to back up and migrate the database from Action Orchestrator 5.1.4 to Action Orchestrator 5.2.0. For more information, see [Migrating Database to Install Action Orchestrator 5.2.0](#).
2. Uninstall Action Orchestrator 5.1.4. For more information, see [Migrating Database to Install Action Orchestrator 5.2.0](#).
3. Delete the secrets of Action Orchestrator using the command.

```
kubectl
delete secret $(kubectl get secrets -n cisco | grep action | awk '{print $1}')
-n cisco
```

4. Install Action Orchestrator 5.2.0. For more information, see [Migrating Database to Install Action Orchestrator 5.2.0](#).
5. Restore Action Orchestrator database on Action Orchestrator 5.2.0. For more information, see [Migrating Database to Install Action Orchestrator 5.2.0](#).

Upgrade from Action Orchestrator 5.2.0 to Action Orchestrator 5.2.1:

1. You have to back up and migrate the database from Action Orchestrator 5.2.0 to Action Orchestrator 5.2.1. For more information, see [Migrating Database to Install Action Orchestrator 5.2.1](#).

2. Until Action Orchestrator 5.2.0, the service certificates are valid only for one year whereas Action Orchestrator 5.2.1 comes with the service certificates that are valid for three years. To extend the validity of service certificates and update to Action Orchestrator 5.2.1, see [Extending Validity of Service Certificates](#).

After Upgrading to Action Orchestrator 5.2.1:

1. Run below commands to verify if the *action-orchestrator-pers-redis* deployment is cleaned up.

```
kubect1 get pods -n <namespace> | grep -iE "redis-master|redis-slave"  
kubect1 get sts -n <namespace> action-orchestrator-pers-redis-master  
kubect1 get service -n <namespace> action-orchestrator-pers-redis-master
```

2. Run below commands to delete the old *redis* deployment's volume and secret.

```
kubect1 delete secret -n <namespace> action-orchestrator-redis-secret  
kubect1 delete pvc -n <namespace> redis-data-action-orchestrator-pers-redis-master-0
```

3. For more information, see [Cleaning Keys from REDIS](#).

Extending Validity of Service Certificates

Extending Validity of Service Certificates

- [Overview](#)
- [Extend the Service Certificates to Three Years](#)
- [Steps to Back Up and Restore postgresql](#)
 - [Back Up postgresql](#)
 - [Restore postgresql](#)
- [Steps for Action Orchestratorarangodb Backup and Restore](#)
 - [Back Up Action Orchestrator arangodb](#)
 - [Restore Action Orchestrator arangodb](#)

Overview

Until Action Orchestrator5.2.0, Action Orchestrator service certificates are valid only for one year.

Extend the Service Certificates to Three Years

1. You must back up [ArangoDB](#) and [postgres SQL](#) from Action Orchestrator5.2.0.Action Orchestrator5.2.1. (This will have certificates with 3 years validity).
2. Uninstall Action Orchestrator5.2.0.
3. Delete the secrets of Action Orchestrator using the command:

```
kubectl delete secret $(kubectl get secrets -n cisco | grep action | awk '{print $1}') -n cisco
```

4. Click install Action Orchestrator 5.2.1 from [CloudCenter Suite 5.2](#) dashboard.



Keep *kubectl* with configuration files ready. As soon as the installation starts, scale down LDS and other core-backend services to 0 using the given commands.

```
"kubectl get pods -n cisco -w | grep be-lds"
```

In 10ish seconds the lds will start. As soon as it starts coming up, execute the given commands to bring down core-backend services.

```
kubectl scale deploy -n cisco action-orchestrator-be-lds --replicas=0
kubectl scale deploy -n cisco action-orchestrator-be-console --replicas=0
kubectl scale deploy -n cisco action-orchestrator-be-bootstrap --replicas=0
kubectl scale deploy -n cisco action-orchestrator-be-orchestrator --replicas=0
kubectl scale deploy -n cisco action-orchestrator-be-rbac --replicas=0
kubectl scale deploy -n cisco action-orchestrator-be-event --replicas=0
kubectl scale deploy -n cisco action-orchestrator-be-schedule --replicas=0
kubectl scale deploy -n cisco action-orchestrator-be-importexport --replicas=0
```



Wait for adapter services and *arangodb* services to come up completely, then resume to restore data.

5. Restore [Arango DB](#) and [postgres SQL](#) databases.

Now, you can work on Action Orchestrator5.2.1.

Steps to Back Up and Restore *postgresql*



Note:The applications *pg_dumpall* and *psql* must be installed to back up and restore *postgresql*.

Back Up *postgresql*

1. Find the suite-random-password used by the *postgresql* user

```
kubectl -n cisco get secret suite-random-password -o jsonpath="{.data.password}" | base64 -d
```

2. Set the variable PGPASSWORD to the suite-random-password

```
export PGPASSWORD=<suite-random-password>
```

3. Find the port for *suite-postgresql* (usually, it is 5432).

```
kubectl -n cisco get svc suite-postgresql
```

4. Port forward the *suite-postgresql* port locally. So, you can reach it.

```
kubectl -n cisco port-forward svc/suite-postgresql 31003:5432
```

5. Back up *postgresql* DB. Because of port forwarding, the host is a localhost. The port is the local port that you port forwarded to 5432 and the user is *quicksilver*.

```
pg_dumpall -h localhost -p 31003 -U quicksilver -w > backupfilename.txt
```

Restore postgresql

1. Edit the backup file that you just created and comment two lines. The first line is '*CREATE ROLE quicksilver*;' and the second line (usually the next line) starts with '*ALTER ROLE quicksilver*'.



The reason to comment these two lines is that while you restore to a new environment, the user quicksilver will already exist, and its password will be set to the suite-random-password and the '*ALTER ROLE quicksilver*' line will mess that password.

2. Find the suite-random-password used by the *postgresql* user.

```
kubectl -n cisco get secret suite-random-password -o jsonpath="{.data.password}" | base64 -d
```

3. Set the variable PGPASSWORD to the suite-random-password.

```
export PGPASSWORD=<suite-random-password>
```

4. Find the port for *suite-postgresql* (usually, it is 5432).

```
kubectl -n cisco get svc suite-postgresql
```

5. Port forward the *suite-postgresql* port locally. So, you can reach it.

```
kubectl -n cisco port-forward svc/suite-postgresql 31003:5432
```



You must scale down some pods, stateful sets, and daemon sets in the next few steps. You must make sure to make a note of the scale settings before you scale them down to 0 because you must scale them back to its original scale settings at the end.

6. Scale down all the common framework pods. These use the *postgresql* DB and you cannot restore if the DB is in use.

```
kubectl get deploy -n cisco | awk '/common-framework/ {print $1}' | xargs -n1 -I{} kubectl -n cisco scale --replicas=0 deployment/{}
```

7. Scale down the stateful sets.

```
kubectl -n cisco scale --replicas=0
statefulset/common-framework-elasticsearch-data

kubectl -n cisco scale --replicas=0
statefulset/common-framework-elasticsearch-master

kubectl -n cisco scale --replicas=0
statefulset/common-framework-grafana

kubectl -n cisco scale --replicas=0
statefulset/common-framework-prometheus-server

kubectl -n cisco scale --replicas=0
statefulset/common-framework-suite-license

kubectl -n cisco scale --replicas=0
statefulset/common-framework-suite-nats
```

8. Delete the daemon sets. The command will save the daemon set information to a file. So, they can be restored at the end.

```
kubectl get daemonsets -n cisco -o yaml > daemonsets.yaml $ kubectl get daemonsets -n cisco | awk
'{print $1}' | xargs kubectl -n cisco delete daemonset
```

9. Scale down all the Action Orchestrator pods

```
kubectl get deploy -n cisco | awk '/^action-orchestrator/ {print $1}' | xargs -n1 -I{} kubectl -n cisco
scale --replicas=0 deployment/{}
```

10. Delete the *postgresql* databases as the restore step creates them.

```

psql
-h localhost -p 31003 -U quicksilver -c 'DROP
DATABASE IF EXISTS "suite-auth";'

psql
-h localhost -p 31003 -U quicksilver -c 'DROP
DATABASE IF EXISTS "suite-cryptoservice";'

psql
-h localhost -p 31003 -U quicksilver -c 'DROP
DATABASE IF EXISTS "suite-email";'

psql
-h localhost -p 31003 -U quicksilver -c 'DROP
DATABASE IF EXISTS "suite-idm";'

psql
-h localhost -p 31003 -U quicksilver -c 'DROP
DATABASE IF EXISTS "suite-jwt-keys";'

psql
-h localhost -p 31003 -U quicksilver -c 'DROP
DATABASE IF EXISTS "suite-license";'

psql
-h localhost -p 31003 -U quicksilver -c 'DROP
DATABASE IF EXISTS "suite-monitor";'

psql
-h localhost -p 31003 -U quicksilver -c 'DROP
DATABASE IF EXISTS "suite-notification";'

psql
-h localhost -p 31003 -U quicksilver -c 'DROP
DATABASE IF EXISTS "suite-password";'

psql -h localhost -p 31003 -U quicksilver -c 'DROP
DATABASE IF EXISTS "suite-res-mgmt";'

```

11. Restore the *postgresql* DB.

```

psql
-h localhost -p 31003 -U quicksilver -f ./backupfilename.txt postgres

```

12. Scale up the common framework pods to its original scale. (This command is assuming the scale is 1 for all the commonframework pods).

```

kubectl
get deploy -n cisco | awk '/common-framework/ {print $1}' | xargs -n1 -I{}
kubectl -n cisco scale --replicas=1 deployment/{}

```

13. Scale up the stateful sets to its original scale. (This command is assuming for most of them the scale is 1, except *elasticsearch-data* is 2 and *elasticsearch-master* is 3).

```

kubect1 -n cisco scale --replicas=1
statefulset/common-framework-elasticsearch-data

kubect1 -n cisco scale --replicas=1 statefulset/common-framework-elasticsearch-master

kubect1 -n cisco scale --replicas=1
statefulset/common-framework-grafana

kubect1 -n cisco scale --replicas=1
statefulset/common-framework-prometheus-server

kubect1 -n cisco scale --replicas=1 statefulset/common-framework-suite-license

kubect1 -n cisco scale --replicas=1
statefulset/common-framework-suite-nats

kubect1 -n cisco scale --replicas=2
statefulset/common-framework-elasticsearch-data

kubect1 -n cisco scale --replicas=3
statefulset/common-framework-elasticsearch-master

```

14. Restore the daemon sets.

```

kubect1
apply -f daemonsets.yaml

```

15. Scale up the Action Orchestratorpods to its original scale. (This command is assuming the scale is 1 for all Action Orchestratorpods).

```

kubect1
get deploy -n cisco | awk '/^action-orchestrator/ {print $1}' | xargs -n1 -I{}
kubect1 -n cisco scale --replicas=1 deployment/{}

```

Steps for Action Orchestratorarangodb Backup and Restore



The applications arangodump and arangorestore must be installed to back up and restore arangodb databases.

Back Up Action Orchestrator arangodb

1. Find the arangodb root password.

```

kubect1
get secret action-orchestrator-pers-arangodb-root-password -n cisco -o yaml |
grep password: | awk '
{print $2}' | base64 --decode

```

2. Find the port for *pers-arangodb* (usually it is 8529).

```

kubect1
get service -n cisco action-orchestrator-pers-arangodb

```

3. Port forward the *pers-arangodb* port locally. So, you can reach it.

```
kubectl
-n cisco port-forward svc/action-orchestrator-pers-arangodb 31003:8529
```

4. Back up arangodb. Because of port forwarding, the host is a localhost. The port is the local port that you port forwarded to 8529 and the user is root.

```
arangodump
--server.endpoint ssl://localhost:31003 --server.username root
--server.password **** --all-databases true --threads 4 --output-directory dump
```

Restore Action Orchestrator arangodb

1. Find the arangodb root password.

```
kubectl
get secret action-orchestrator-pers-arangodb-root-password -n cisco -o yaml |
grep password: | awk '{print $2}'
| base64 --decode
```

2. Find the port for *pers-arangodb* (usually it is 8529).

```
kubectl
get service -n cisco action-orchestrator-pers-arangodb
```

3. Port forward the *pers-arangodb* port locally. So, you can reach it.

```
kubectl
-n cisco port-forward svc/action-orchestrator-pers-arangodb 31003:8529
```

4. Scale down all the Action Orchestrator backend services.

```
kubectl scale deploy -n cisco action-orchestrator-be-lds
--replicas=0

kubectl scale deploy -n cisco action-orchestrator-be-console
--replicas=0

kubectl scale deploy -n cisco
action-orchestrator-be-bootstrap --replicas=0

kubectl scale deploy -n cisco
action-orchestrator-be-orchestrator --replicas=0

kubectl scale deploy -n cisco action-orchestrator-be-rbac
--replicas=0

kubectl scale deploy -n cisco action-orchestrator-be-event
--replicas=0

kubectl scale deploy -n cisco
action-orchestrator-be-schedule --replicas=0

kubectl scale deploy -n cisco
action-orchestrator-be-importexport --replicas=0
```

5. Restore *arangodb*. Because of port forwarding, the host is a localhost. The port is the local port that you port forwarded to 8529 and the user is root.

```
arangorestore
--server.endpoint ssl://localhost:31003 --server.username root
--server.password ***** --all-databases true --overwrite true --create-database
true --replication-factor 3 --threads 4 --input-directory dump
```

6. After the restore is completed, scale up the AO backend services. Note that bootstrap is scaled to 1. Do not go above 1 for bootstrap.

```
kubectl scale deploy -n cisco action-orchestrator-be-lds  
--replicas=2
```

```
kubectl scale deploy -n cisco action-orchestrator-be-console  
--replicas=2
```

```
kubectl scale deploy -n cisco  
action-orchestrator-be-bootstrap --replicas=1
```

```
kubectl scale deploy -n cisco action-orchestrator-be-orchestrator  
--replicas=2
```

```
kubectl scale deploy -n cisco action-orchestrator-be-rbac  
--replicas=2
```

```
kubectl scale deploy -n cisco action-orchestrator-be-event  
--replicas=2
```

```
kubectl scale deploy -n cisco  
action-orchestrator-be-schedule --replicas=2
```

```
kubectl scale deploy -n cisco  
action-orchestrator-be-importexport --replicas=2
```


Migrating Database to Install Action Orchestrator 5.2.1

Migrating Database to Install Action Orchestrator 5.2.1.

- [Overview](#)
- [Prerequisites to Upgrade from Action Orchestrator 5.2.0 to Action Orchestrator 5.2.1](#)
- [Procedure](#)

Overview

Before upgrading to Action Orchestrator 5.2.1, you have to back up and migrate the database from the existing version of Action Orchestrator.

Backing up and migrating the database from the existing version of Action Orchestrator to Action Orchestrator 5.2.1 is essential to retain all your existing data including the workflows created, triggers, activities, logical components, and variables added to the workflows, the targets and the target groups.

You have to back up your database from existing version of Action Orchestrator before upgrading to Action Orchestrator 5.2.1 to prevent any data loss.



- You must follow this procedure if you are migrating from Action Orchestrator 5.0 or Action Orchestrator 5.1 to Action Orchestrator 5.2.
- You must first upgrade to Action Orchestrator 5.2.0 before upgrading to Action Orchestrator 5.2.1 as direct upgradation from any other version of Action Orchestrator to Action Orchestrator 5.2.1 is not possible.

Prerequisites to Upgrade from Action Orchestrator 5.2.0 to Action Orchestrator 5.2.1

- You have to upgrade to [Suite Admin 5.2.4](#) before proceeding with database backup.
- You must not use port forward to back up database instead enable LB for ArangoDB Service and use the external IP.
- You must have a fast internet connection that is good enough to have the machine in same network of cluster or same region to back up and restore database.
- You must install arangodb on the machine before you take the backup.

Execute below commands to install arangodb tools

Ubuntu Machine:

```
curl -OL https://download.arangodb.com/arangodb36/DEBIAN/Release.key
sudo apt-key add - < Release.key
echo 'deb https://download.arangodb.com/arangodb36/DEBIAN/ /' | sudo tee /etc/apt/sources.list.d
/arangodb.list
sudo apt-get install apt-transport-https
sudo apt-get update
sudo apt-get install arangodb3=3.6.3.1-1
```

Centos:

```
cd /etc/yum.repos.d/
curl -OL https://download.arangodb.com/arangodb36/RPM/arangodb.repo
yum -y install arangodb3-3.6.3-1
```

- You can execute these steps only if you are a System/Lab admin with access to Installation Configuration.

Procedure

1. Edit *pers-arangodb* service and save.

```
kubectl get svc -n cisco | grep arango
kubectl edit svc -n cisco pers-arangodb
```

```
Update:
  type: ClusterIP
to
  type: LoadBalancer (or) NodePort
```

Run below command to get the loadbalancerIp or Nodeport
kubectl get service -n cisco pers-arangodb

2. Start the *ArangoDB* backup after the service is updated.

Get DB Credentials: (Only Lab/System admin can do this)

If you have 5.1.4 or less version, do below steps, to change database credentials.

```
kubectl -n cisco get secret action-orchestrator-jwt-secret -o jsonpath="{.data.jwtSecret}"
echo ***** | base64 --decode
```

Note: If npm is not installed on your machine, install it by executing below commands.

For Ubuntu:

1. curl -sL https://deb.nodesource.com/setup_12.x | sudo -E bash -
2. sudo apt-get install nodejs
3. npm -v

```
sudo npm install -g jwtgen
jwtgen -a HS256 -s $decodedvalue -c server_id=setup -c iss=arangodb
curl -X PUT http://<host>:<port>/_api/user/root -H 'Authorization: Bearer <token>' -d '{ "passwd" :
"admin" }'
```

Back up Pre-requisite:

Backup:

```
arangodump --server.endpoint ssl://x.x.x.x:<port> --server.username root --server.password ***** --all-
databases true --threads 4 --output-directory dump
```

3. After the backup is completed, uninstall existing Action Orchestrator 5.0 or Action Orchestrator 5.1 from [CloudCenter Suite 5.2](#) dashboard.
4. Make sure all Action Orchestrator related objects are deleted. Check using *k8s* commands and make sure all Action Orchestrator objects are deleted properly. Wait for five minutes before you install Action Orchestrator 5.2.

```
kubectl get pods -n cisco | grep action-orchestrator
kubectl get secrets -n cisco
kubectl get services -n cisco
kubectl get pvc -n cisco
kubectl get pv -n cisco
```

5. Click install Action Orchestrator 5.2.1 from [CloudCenter Suite 5.2](#) dashboard.



Keep access to kubectl with config file ready, execute below command to watch when *be-lds* pod starts creating.

```
kubectl get pods -n cisco -w | grep be-lds
```

6. Monitor *kubectl* and wait for a few seconds for *be-lds* to start creating. As soon as it starts creating, break the command, execute the following commands to scale down all backend services.

```
kubectl scale deploy -n cisco action-orchestrator-be-lds --replicas=0
kubectl scale deploy -n cisco action-orchestrator-be-console --replicas=0
kubectl scale deploy -n cisco action-orchestrator-be-bootstrap --replicas=0
kubectl scale deploy -n cisco action-orchestrator-be-orchestrator --replicas=0
kubectl scale deploy -n cisco action-orchestrator-be-rbac --replicas=0
kubectl scale deploy -n cisco action-orchestrator-be-event --replicas=0
kubectl scale deploy -n cisco action-orchestrator-be-schedule --replicas=0
kubectl scale deploy -n cisco action-orchestrator-be-importexport --replicas=0
```



Wait for arangodb and adapter services to come up.

7. Repeat step 1.

```
kubectl edit svc -n cisco action-orchestrator-pers-arangodb
Update:
  type: ClusterIP
  to
  type: LoadBalancer (or) NodePort

Run below command to get the loadbalancerIp or Nodeport
kubectl get service -n cisco action-orchestrator-pers-arangodb
```

8. Restore the database backup performed in step 2.

```
Get DB Password:
-----
      kubectl -n cisco get secret action-orchestrator-pers-arangodb-root-password -o jsonpath="{.data.password}" | base64 --decode

Restore
-----

arangorestore --server.endpoint ssl://x.x.x.x:<port> --server.username root --server.password ***** --
all-databases true --overwrite true --create-database true --replication-factor 3 --threads 4 --input-
directory dump
```

9. After the database restore is successful, scale up the replicas of *be-lds* to 1. This will start the migration of data to Action Orchestrator 5.2.1 compatible.

```
List LDS backend deployment service:
      kubectl get deploy -n cisco | grep action-orchestrator-be-lds

Scale Up only LDS core Service to 1
      kubectl scale deploy -n cisco action-orchestrator-be-lds --replicas=1

Note: Only scale LDS at this moment, not other backed services.
```

10. Log into ArangoDB (system).

```
URL: https://x.x.x.x:<port>
enter credentials on UI
username: root
password: <get from step-8>

Select "_system" DB once login is successful
e.g. https://<IP of CCS:NodePort or Load Balancer Port of db>
```

11. Check if there are any tenants with *migration-failed* state.

```
FOR i in lhtenants
FILTER i.enabled==true AND i.deleted==false AND i.status.state == "migration-failed"
return i
```

12. Check the status of all the tenants in database by executing this query on system database.

```
FOR i in lhtenants
FILTER i.enabled==true AND i.deleted==false AND i.status.state == "bootstrap-successful"
return i
```

13. If all the enabled tenants' status is *migration-successful* then scale up *be-lds* to 2 and scale the following core back-end services.

```
List all core backed pods:
kubect1 get deploy -n cisco | grep action-orchestrator-be

Scale Up all core Services
kubect1 scale deploy -n cisco action-orchestrator-be-console --replicas=2
kubect1 scale deploy -n cisco action-orchestrator-be-orchestrator --replicas=2
kubect1 scale deploy -n cisco action-orchestrator-be-rbac --replicas=2
kubect1 scale deploy -n cisco action-orchestrator-be-event --replicas=2
kubect1 scale deploy -n cisco action-orchestrator-be-schedule --replicas=2
kubect1 scale deploy -n cisco action-orchestrator-be-importexport --replicas=2
```

14. If restore of Action Orchestrator 5.2.1 is not along with [Suite Admin 5.2.4](#), then after restore is completed, log into Action Orchestrator with your tenant, create user from this tenant, give the user all roles, log out/log in with this user, add all Action Orchestrator roles to this tenant user. Now, this tenant can access the Action Orchestrator, repeat same process for all the tenants.



If restore of Action Orchestrator 5.2.1 is along with [Suite Admin 5.2.4](#), then above step is not required as [Suite Admin 5.2.4](#) restore will restore the *postgres* that will cover above steps.

15. Before scaling bootstrap deployment, wait for all the services status to change to *running*.

```
kubect1 scale deploy -n cisco action-orchestrator-be-bootstrap --replicas=1 (bootstrap service always
needs to have '1' replicas. Do not scale this to >1)
```

16. After all the pods are up, try to access Action Orchestrator UI and try to run existing workflows. All Action Orchestrator features will work as expected.

17. Repeat step 1. Change *Arangodb* service back to *ClusterIP*.

```
kubect1 get svc -n cisco | grep arango
kubect1 edit svc -n cisco action-orchestrator-pers-arangodb

Update:
type: LoadBalancer (or) NodePort
to
type: ClusterIP
```



If you have any issues, please contact Action Orchestrator support team.

18. Clear the *redis* cache. For more information, see [Cleaning Keys from REDIS](#).



If you have not taken backup/restore of *postgresql*, then you have to manually add roles for tenants. If you have taken backup/restore of *postgresql*, then this is not needed.

19. Launch Action Orchestrator 5.2.1 and access your previous data.

Migrating Database to Install Action Orchestrator 5.2.0

Migrating Database to Install Action Orchestrator 5.2.0

- [Overview](#)
- [Prerequisites](#)
- [Procedure](#)

Overview

Before upgrading to Action Orchestrator 5.2, you have to back up and migrate the database from the existing version of Action Orchestrator.

Backing up and migrating the database from the existing version of Action Orchestrator to Action Orchestrator 5.2 is essential to retain all your existing data including the workflows created, triggers, activities, logical components, and variables added to the workflows, the targets and the target groups.

You have to back up your database from Action Orchestrator 5.0 or Action Orchestrator 5.1 before upgrading to Action Orchestrator 5.2 to prevent any data loss.



- You must skip this procedure if you are installing Action Orchestrator 5.2 for the first time.
- You must follow this procedure if you are migrating from Action Orchestrator 5.0 or Action Orchestrator 5.1 to Action Orchestrator 5.2.

Prerequisites

- You have to upgrade to [Suite Admin 5.2.0](#) before proceeding with database backup.
- You must not use port forward to back up database instead enable LB for ArangoDB Service and use the external IP.
- You must have a fast internet connection that is good enough to have the machine in same network of cluster or same region to back up and restore database.
- You must install arangodb on the machine before you take the backup.

```
Execute below commands to install arangodb tools
```

```
Ubuntu Machine:
```

```
-----
```

```
curl -OL https://download.arangodb.com/arangodb36/DEBIAN/Release.key
sudo apt-key add - < Release.key
echo 'deb https://download.arangodb.com/arangodb36/DEBIAN/ /' | sudo tee /etc/apt/sources.list.d
/arangodb.list
sudo apt-get install apt-transport-https
sudo apt-get update
sudo apt-get install arangodb3=3.6.3.1-1
```

```
Centos:
```

```
-----
```

```
cd /etc/yum.repos.d/
curl -OL https://download.arangodb.com/arangodb36/RPM/arangodb.repo
yum -y install arangodb3-3.6.3-1
```

- You can execute these steps only if you are a System/Lab admin with access to Installation Configuration.

Procedure

1. Edit `pers-arangodb` service and save.

```
kubectl get svc -n cisco | grep arango
kubectl edit svc -n cisco pers-arangodb
```

```
Update:
  type: ClusterIP
to
  type: LoadBalancer (or) NodePort
```

Run below command to get the loadbalancerIp or Nodeport
kubectl get service -n cisco pers-arangodb

2. Start the *ArangoDB* backup after the service is updated.

```
Get DB Credentials: (Only Lab/System admin can do this)
```

```
-----
If you have 5.1.4 or less version, do below steps, to change database credentials.
  kubectl -n cisco get secret action-orchestrator-jwt-secret -o jsonpath="{.data.jwtSecret}"
  echo ***** | base64 --decode
```

Note: If npm is not installed on your machine, install it by executing below commands.

For Ubuntu:

1. curl -sL https://deb.nodesource.com/setup_12.x | sudo -E bash -
2. sudo apt-get install nodejs
3. npm -v

```
sudo npm install -g jwtgen
jwtgen -a HS256 -s $decodedvalue -c server_id=setup -c iss=arangodb
curl -X PUT http://<host>:<port>/_api/user/root -H 'Authorization: Bearer <token>' -d '{ "passwd" :
"admin" }'
```

```
Back up Pre-requisite:
```

```
-----
```

```
Backup:
```

```
-----
```

```
arangodump --server.endpoint tcp://x.x.x.x:<port> --server.username root --server.password ***** --all-
databases true --threads 4 --output-directory dump
```

3. After the backup is completed, uninstall existing Action Orchestrator 5.0 or Action Orchestrator 5.1 from [CloudCenter Suite 5.2](#) dashboard.
4. Make sure all Action Orchestrator related objects are deleted. Check using *k8s* commands and make sure all Action Orchestrator objects are deleted properly. Wait for five minutes before you install Action Orchestrator 5.2.

```
kubectl get pods -n cisco | grep action-orchestrator
kubectl get secrets -n cisco
kubectl get services -n cisco
kubectl get pvc -n cisco
kubectl get pv -n cisco
```

5. Install Action Orchestrator 5.2 from [CloudCenter Suite 5.2](#) dashboard.
6. After the installation is successful, scale down Action Orchestrator core backed services to 0.

```

List backend deployments:
  kubectl get deploy -n cisco | grep action-orchestrator-be

Scale Down Core Services
  kubectl scale deploy -n cisco action-orchestrator-be-lds --replicas=0
  kubectl scale deploy -n cisco action-orchestrator-be-console --replicas=0
  kubectl scale deploy -n cisco action-orchestrator-be-bootstrap --replicas=0
  kubectl scale deploy -n cisco action-orchestrator-be-orchestrator --replicas=0
  kubectl scale deploy -n cisco action-orchestrator-be-rbac --replicas=0
  kubectl scale deploy -n cisco action-orchestrator-be-event --replicas=0
  kubectl scale deploy -n cisco action-orchestrator-be-schedule --replicas=0
  kubectl scale deploy -n cisco action-orchestrator-be-importexport --replicas=0

```

7. Repeat step 1.

```

kubectl edit svc -n cisco action-orchestrator-pers-arangodb
Update:
  type: ClusterIP
  to
  type: LoadBalancer (or) NodePort

Run below command to get the loadbalancerIp or Nodeport
kubectl get service -n cisco action-orchestrator-pers-arangodb

```

8. Restore the database backup performed in step 2.

```

Get DB Password:
-----
  kubectl -n cisco get secret action-orchestrator-pers-arangodb-root-password -o jsonpath="{.data.password}" | base64 --decode

Restore
-----

arangorestore --server.endpoint ssl://x.x.x.x:<port> --server.username root --server.password ***** --
all-databases true --overwrite true --create-database true --replication-factor 3 --threads 4 --input-
directory dump

```

9. After the database restore is successful, scale up the replicas of *be-lds* to 2. This will start the migration of data to Action Orchestrator 5.2 compatible.

```

List LDS backend deployment service:
  kubectl get deploy -n cisco | grep action-orchestrator-be-lds

Scale Up only LDS core Service to 2
  kubectl scale deploy -n cisco action-orchestrator-be-lds --replicas=2

Note: Only scale LDS at this moment, not other backed services.

```

10. Log into *ArangoDB* (system).

```
URL: https://x.x.x.x:<port>
enter credentials on UI
username: root
password: <get from step-8>

Select "_system" DB once login is successful
e.g. https://<IP of CCS:NodePort or Load Balancer Port of db>
```

11. Check if there are any tenants with *migration-failed* state.

```
FOR i in lhtenants
FILTER i.enabled==true AND i.deleted==false AND i.status.state == "migration-failed"
return i
```

12. Check the status of all the tenants in database by executing this query on system database.

```
FOR i in lhtenants
FILTER i.enabled==true AND i.deleted==false AND i.status.state == "migration-successful"
return i
```

13. If all the enabled tenants' status is *migration-successful* then scale all the core back-end services.

```
List all core backed pods:
  kubectl get deploy -n cisco | grep action-orchestrator-be

Scale Up all core Services
  kubectl scale deploy -n cisco action-orchestrator-be-console --replicas=2
  kubectl scale deploy -n cisco action-orchestrator-be-orchestrator --replicas=2
  kubectl scale deploy -n cisco action-orchestrator-be-rbac --replicas=2
  kubectl scale deploy -n cisco action-orchestrator-be-event --replicas=2
  kubectl scale deploy -n cisco action-orchestrator-be-schedule --replicas=2
  kubectl scale deploy -n cisco action-orchestrator-be-importexport --replicas=2
```

14. Before scaling bootstrap deployment, wait for all the services status to change to *running*.

```
kubectl scale deploy -n cisco action-orchestrator-be-bootstrap --replicas=1 (bootstrap service always
needs to have '1' replicas. Do not scale this to >1)
```

15. After all the pods are up, try to access Action Orchestrator UI and try to run existing workflows. All Action Orchestrator features will work as expected.
16. Repeat step 1. Change *Arangodb* service back to *ClusterIP*.

```
kubectl get svc -n cisco | grep arango
kubectl edit svc -n cisco action-orchestrator-pers-arangodb

Update:
  type: LoadBalancer (or) NodePort
  to
  type: ClusterIP
```



If you have any issues, please contact Action Orchestrator support team.

Cleaning Keys from REDIS

Cleaning Keys from REDIS

When you back up data from Action Orchestrator 5.2.0 and restore it in Action Orchestrator 5.2.1, the REDIS contains keys of previous data. You must clean them from the REDIS.

To clean up keys of previous data from REDIS

1. You need to ssh into each REDIS pod, `rfr-action-orchestrator-pers-redis-ha-0`, `rfr-action-orchestrator-pers-redis-ha-1`, and `rfr-action-orchestrator-pers-redis-ha-2`, to identify value of the role.
2. Execute below commands in each of them to identify value of the role.

```
redis-cli -a $REDIS_PASSWORD
Next, execute
Info
```



The POD having role master is the correct master POD on which you have to execute from step 3 to 5. Generally, `ha-0` happens to be the master POD.

3. Access CloudCenter Suite cluster from the terminal. Locate and ssh into the REDIS HA master POD using the command.

```
kubectl exec -it rfr-action-orchestrator-pers-redis-ha-0 -n cisco sh
```



First, you must ssh into each REDIS POD namely `rfr-action-orchestrator-pers-redis-ha-0`, `rfr-action-orchestrator-pers-redis-ha-1`, and `rfr-action-orchestrator-pers-redis-ha-2`.

Then, you must execute the below commands in each one of them, identify value of the role. The POD having role master is the correct master POD. The rest of the steps mentioned in the document must be executed on this Master POD. Generally, `ha-0` happens to be the master POD.

```
redis-cli -a $REDIS_PASSWORD
Next, execute
info
```

4. Execute the command

```
redis-cli -a $REDIS_PASSWORD
next, execute;
KEYS *lds-microservice.metadata_metadata_cryptokey_longhorn
```

5. Delete the listed keys using the command

```
DEL <key from above result>
```

For more details, refer the example

```
[/data $ redis-cli -a $REDIS_PASSWORD
Warning: Using a password with '-a' or '-u' option on the command line interface may not be safe.
127.0.0.1:6379> KEYS *lds-microservice.metadata_metadata_cryptokey_longhorn
1) "1.lds-microservice.metadata_metadata_cryptokey_longhorn"
127.0.0.1:6379>
127.0.0.1:6379>
127.0.0.1:6379> DEL 1.lds-microservice.metadata_metadata_cryptokey_longhorn
(integer) 1
127.0.0.1:6379>
```

Now, you can access and proceed to work on Action Orchestrator 5.2.1.

Configuring Workflows

Configuring Workflows

- [Workflows Overview](#)
- [Creating a Basic Workflow](#)
- [Import Workflows](#)
- [Export Workflows](#)
- [Adding Workflow Properties](#)
- [Adding Triggers](#)
- [Activities](#)
- [Adding Logic Components to a Workflow](#)
- [Variable Reference](#)
- [Share Workflow](#)

Workflows Overview

Creating Workflows Overview

- [Activities Panel](#)
- [Workflow Panel](#)
- [Properties Panel](#)
- [Header](#)
- [Toggling the Workflow Editor View](#)
- [Expanding the Workflow View](#)
- [Collapsing the Workflow View](#)

A workflow is basically a constructed workflow that consists of activities, invocations of child workflows, and logic components that can be included to complete the workflow. Action Orchestrator allows you to automate IT processes based on your organizational requirements using a workflow format. The Action Orchestrator also includes many predefined workflows in its packaged automation packs.

The following sections provide information about creating and managing workflows:

Action Orchestrator simplifies workflow creation using a drag and drop workflow designer. The Workflow Editor allows you to drag activities, workflow activities (logic), or workflows you want to invoke into a workflow definition where you want it to occur. The Workflow Editor dynamically accepts the new addition and shows the resulting logic.

Unlike drag-and-wire approaches common to other Process Orchestrators, the logic of the workflow is always clear, without having to constantly modify the layout as the workflow definition evolves. This makes it easier for other operators to view or edit workflows that have previously been created. You can also collapse sections of the workflow that are not currently of interest.

Use the Workflow Editor to:

- View and modify the properties of an existing workflow
- Define properties
- Construct a new workflow
- Construct a new workflow as a atomic workflow



The procedure to access the editor depends on the task to be performed.

To access the Workflow Editor:

- If you are creating a new workflow, choose **My Workflows > NEW WORKFLOW** from the default home page or from the side task bar choose **Workflows > My Workflows > NEW WORKFLOW**. For more information, see [Creating a Basic Workflow](#).
- If you are creating a new workflow as an atomic workflow, choose **Atomic Workflows > NEW WORKFLOW** from the default home page or from the side task bar choose **Workflows > Atomic Workflows > NEW WORKFLOW**. The atomic workflows allow you to group the workflows in a group name under the activities. This helps you to drag and drop the workflows as activities from the customized group name. For more information, see [Creating an Atomic Workflow](#).




Conditions for Atomic Workflow



- The users with *Adapter Author* role only would be able to view, create, and modify atomic workflows. This options would not be enabled for other roles. For more information on Roles and Permissions, see [Action Orchestrator Roles](#).
- A workflow with trigger can't be marked as atomic workflow.
- The atomic workflow can't run individually as a workflow, it can only be a part of a workflow.
- An atomic workflow can have another atomic workflow as a child. But it can't have any other workflow as a child.

- If you are modifying an existing workflow, choose the respective workflow from the My Workflows page and you will be able edit it in the workflow pane.

Activities Panel

The left pane of the editor includes these views. The navigation items displayed in the pane depend on the view that is selected.

	<p>The Activities view displays the list of activities that are used to construct the workflow. The activities that display depend on the adapters that are installed.</p> <p>For more information, see Activities.</p>
---	---

<p>Logic</p> 	<p>The Logic view displays the list of workflow components that support or define the workflow logic and provide control over the execution of the workflow logic. For information about configuring the logic components, see Adding Logic Components to a Workflow.</p>
<p>Workflows</p> 	<p>The workflows view displays the list of defined workflows that can be included in other workflows. To add an existing workflow to a new workflow, drag and drop the appropriate workflow onto the workflow pane and define the criteria for execution of the workflow.</p>

Workflow Panel

The Workflow pane is a canvas located in the center portion of the Workflow Editor. Use this area to create workflows by dragging and dropping activities, other workflows, and components from the toolbox onto the canvas.

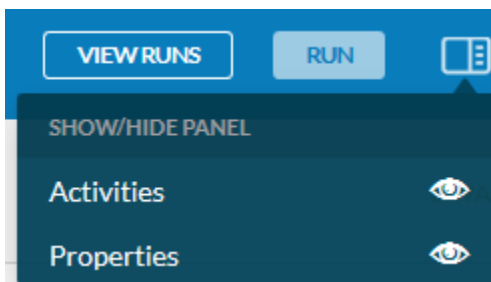
Properties Panel

The workflow pane is located on the right side of the editor and displays the properties for the selected workflow, as well as selected activity, child workflow, or workflow logic element properties.

Header

The header displays the actions that can be performed on the workflow such as **Validate**, **Commit**, **View Runs**, **Run**, and **Close**. For more information on View Runs, see [Runs](#).

And it also allows you to show or hide Activities and Properties panel by using the following icon:



- Click on the icon to hide or show both Activities and Properties panel.
- Hover over the icon and click on the Show/Hide icon on the SHOW/HIDE panel to display or hide either Activities or Properties panels based on your requirements.

Toggling the Workflow Editor View

In the Workflow Editor view, you can toggle the view between the workflow property pages and the activity view pages. To switch to the workflow properties in the Workflow pane, click anywhere outside of the activities in the workflow.

Expanding the Workflow View

To expand the workflow, click the +Expand tool.


Collapsing the Workflow View

To collapse the activities in the Workflow pane, click the -Collapse tool.

Creating a Basic Workflow

Creating a Basic Workflow

The following procedure provides information on creating a basic workflow in Action Orchestrator:

 Identify any drag-and-drop objects in the toolbox that will be required by your new workflow.

1. Choose **Workflows > My Workflows > NEW WORKFLOW**.
2. On the Workflow Properties panel, define the workflow properties (see [Adding Workflow Properties](#)).
3. From the Activities pane, drag and drop the appropriate items onto the workflow pane (see [Activities Panel](#)).
4. On the Properties panel, define the properties for each object selected on the workflow pane. The available property pages are determined by the selected objects (see [Activities](#)).
5. When all of the property pages are complete, click **VALIDATE** on the header to validate the workflow.



If the workflow is not valid, click on activities that are orange and determine warnings in the upper right corner of the Properties pane. Enter the required information and validate again.

6. Once the workflow is successfully validated, click **Commit** on the header to export the workflow to your repository.
 - On the **Commit** panel, enter the **File Name** and **Commit Message**.
 - Click **Commit**, to export the workflow.



This is an optional step.

For more information on workflow export, see [Export Workflows](#).

For more information on repository, see [Git Repositories](#).

7. Once the workflow is successfully validated, click **RUN** on the header to execute the workflow.
8. Once the workflow execution starts, you will be taken to the **Runs** page, where you can observe the workflow:
 - a. Status: Such as Running, Success, and Failed in the top left next to the workflow name.
 - b. Auto-Refresh: You can switch **ON** or **OFF** the auto refresh using the **Switch** icon on the top right.
 - c. Cancel Run: Click **Cancel Run** on the top right to cancel the running workflow.
 - d. Run time: Displays the time taken for the completion of the workflow on the top right.



For more information, see [Runs](#).

9. Click **Edit Workflow** on the top right of the Runs page to edit the workflow. This option will be enabled only after workflow completion.

Import Workflows

Import Workflows

Use the Import icon to import workflows from your git repository. Perform the following procedure to import a workflow:

1. Choose **Workflows > My Workflows > IMPORT** or Choose **Workflows > Atomic Workflows > Import**.



The users with *Adapter Author* role only would be able to import atomic workflows. For more information on Roles and Permissions, see [Action Orchestrator Roles](#).

2. On the **Import Workflow** panel, choose either **Git** or **Browse** option and perform the following procedure:

- a. **Git**

- i. Under **Git Repository**, select the repository from the dropdown list. For more information on adding a repository, see [Git Repositories](#).
- ii. Under **File Name**, select the file name from the dropdown list.
- iii. Under **Git Version**, select the version from the dropdown list.
- iv. Check the **Import As A New Workflow (Clone)** check box to import the workflow as a clone.

- b. **Browse**

- i. You can either paste the workflow definition JSON file directly in the text box or
- ii. Click **Browse** to choose the appropriate workflow definition JSON file from your local machine.



If you have any credentials or secret values, update the JSON file before pasting or browsing into the text box.

- iii. Check the **Import As A New Workflow (Clone)** check box to import the workflow as a clone.




If the *Import As A New Workflow (Clone)* check box remains unchecked. The workflow from the selected new Git version will override the workflow if the workflow is already existing.

3. Click **IMPORT**, to import the workflow.

Export Workflows

Export Workflows

Use export workflows to export the workflow to your repository. Perform the following procedure on the workflow properties pane to export a workflow:


 For more information on Workflow properties pane, see [Adding Workflow Properties](#).

Under **Version**, enter the following information:


1. Under **Git Repository**, select the appropriate repository from the dropdown list or Click **+ADD NEW** from the dropdown list to create a repository. For more information, see [Git Repositories](#).
2. Click **Validate** on the header to validate the workflow.

 You would be able to continue the export if the workflow is valid. If not, please fix the problem and try after re-validation.

3. Click **Commit** on the header to export the workflow to your repository.
4. On the **Commit** panel, enter the **File Name** and **Commit Message**.

 The file name is used as folder name along with the unique workflow name in the git repo. The file name also helps you to easily identify the workflow during import.

5. Click **Commit**, to export the workflow.

 If you have already exported a workflow and if you would like to override the existing version with an older version. Under **Git Version**, click **Load New Version**, in the Load New version dialog box select the version from the dropdown list and click **Import**.

Adding Workflow Properties

Adding Workflow Properties

The following procedure provides information on details to be filled in the workflow properties pane:

1. Under **Version**, enter the following information:
 - a. Under **Git Repository**, select the appropriate repository from the dropdown list or click **Add New** to add a new git repository. For more information, see [Add Git Repository](#).
 - b. Under **Git Version**, click **Load New Version**.
 - c. On the **Load New Version** panel, select the **Git version** from the dropdown list.



The selected new version will override the existing git version.

- d. Click **IMPORT**, to import the required git version.



The Step 1.a is required for exporting a workflow using commit. For more information, see [Export Workflows](#).

The Step 1.a, 1.b, 1.c, and 1.d provides information on importing a workflow. And if you have already exported a workflow and if you would like to override the existing version with an older version you can use the following steps.

2. Enter the unique **DISPLAY NAME** for the new workflow.
3. Enter the **OWNER** name of the workflow.
4. Enter a brief **DESCRIPTION** about the workflow.
5. Check the **Delete Workflow Instance After Execution** check box to delete the executed workflow instance.
6. Check the **Is Atomic Workflow** check box to list the workflow as an activity under [Activities](#). Once this check box is enabled it enables the **Group Name**, specify the appropriate information in group name:
 - Select the appropriate existing group name from the dropdown list or
 - Enter the new group name and choose **Create** from the dropdown list to create a group name.



Conditions for Atomic Workflow

- The users with *Adapter Author* role only would be able to create or modify atomic workflows. These options would not be enabled for other roles. For more information on Roles and Permissions, see [Action Orchestrator Roles](#).
- A workflow with trigger can't be marked as atomic workflow.
- The atomic workflow can't run individually as a workflow, it can only be a part of a workflow.
- An atomic workflow can have another atomic workflow as a child. But it can't have any other workflow as a child.

7. Select the **CATEGORY** from the dropdown list. For example, you will be able to see categories such as Cisco, Monitoring, Networking, Windows, and so forth.
8. Select an already created **Variable** or create a new variable by clicking on **ADD VARIABLE** under Variables. For more information, see [Configuring Variables](#).
9. Select an already created **Trigger** or create a new trigger by clicking on **ADD TRIGGER** under Triggers. For more information, see [Adding Triggers](#).
10. You can select either of the following details under Target:
 - a. No Target: Select this radio button to ignore target for the workflow.
 - b. Execute on this Target: Select this radio button to add the **Target Type** and **Target** from respective dropdown lists.

To add new target choose **+ADD NEW** from the dropdown list. For more information, see [Configuring Targets](#).
 - c. Specify Target On Workflow Start: Select this radio button to enter the target during the start of the workflow and select the **Target Type** from the dropdown list.



Target types provide a way to define a service or other IT element that is not represented by any target type provided by an adapter. All new targets are created based upon an existing target type.

- d. Execute on this Target Group: Select this radio button to choose the target group from the dropdown list for your workflow and specify the following information:

To add new target group choose **+ADD NEW** from the dropdown list. For more information, see [Configuring Targets](#).

- i. Select Target Types: Choose the appropriate target type from the dropdown list. The target type list depends on the target group selected.
- ii. Check the **All Targets in this Group** check box to execute the workflow on all targets in this group.
- iii. Conditions: Click **+ADD** to specify the condition, enter the following information in the **Add Conditions** dialog box:

1. Left Operand: Enter the value for the left operand.

2. Operator: From the dropdown list, choose the operator to use for comparing the value:
 - a. Does not match wildcard: Determines if the item does not match all items in the wildcard example
 - b. Equal: Determines if the left side equals the right side.
 - c. Equal (case-insensitive): Determines if the left side equals the right side (if this is a string comparison, this is case-insensitive)
 - d. Greater Than: Determines if a value is greater than another value.
 - e. Greater Than or Equal to: Determines if a value is greater than or equal to another value.
 - f. Less Than: Determines if a value is less than another value.
 - g. Less Than or Equal to: Determines if a value is less than or equal to another value.
 - h. Match regular expression: Determines if the left side matches the regular expression specified on the right side.
 - i. Matches wildcard: Determines if the left side matches the wildcard specified on the right side.
 - j. Not equals: Determines if the left side does not equal the right side.
3. Right Operand: Enter the value for the right operand.
4. Click **Save**, to save the conditions.
- iv. Select Target Group Criteria: Choose the target group criteria from the dropdown list:
 1. Choose all with matching criteria: Executes the workflow on all targets defined by the criteria specified in the target group.
 2. Choose first with matching criteria: Executes the workflow on the first matching target defined by the criteria specified in the target group.

Adding Triggers

Adding Triggers

- [Adding Triggers](#)
 - [Schedules](#)
 - [Events](#)
 - [Webhooks](#)
- [Creating Triggers](#)

Triggers are events and conditions in the system that can fire off workflows. The attributes of the trigger are referenced in the workflow. Workflows often use this data to control execution. If a workflow contains a trigger, you can view its properties in the workflow Editor. The workflow properties pane displays all triggers associated with the workflow, and allows you to create new triggers, modify the properties of a trigger, and delete triggers.

Workflow instances can come into existence in the following ways:

- A workflow can be invoked manually.
- A workflow can be invoked by another workflow.
- A trigger can fire, which initiates the workflow.
- A workflow can be invoked using the northbound web service.

Triggers are events and conditions in the system that determine how or when the workflow will be executed. Multiple triggers can be added that can be initiated when certain conditions are met.

Action Orchestrator supports two types of rule-based triggers: Schedules and Events.

Schedules

Schedules allow triggering workflows at some time by leveraging another object called a calendar. Calendars define which days something can occur. Calendars can be selected days or sequences of dates such as weekly or monthly, they can represent dates like fiscal quarter end, or they can be combined hierarchically. Schedules then associate a time with a calendar. When the day is in the calendar, the time is evaluated. Times can be explicit or repeating (for example, hourly).

Events

The Action Orchestrator platform can monitor for events from the environment, and you can specify triggers that initiate workflows when the subscribed event occurs. For example, an event might be an incoming stop trap or a fault on a UCS system.

Webhooks

Action Orchestrator provides the ability to configure a webhook as an event to trigger a workflow or wait for an event activity. This is very useful for third party software integration.

Creating Triggers

To create a new trigger for a workflow:

1. On the Workflow Properties pane, click **+ADD TRIGGER**.
2. Under **General**, select **Disabled** as **True** or **False** from the dropdown list.
3. Under **Triggers**, enter the name, description, and specify the following information:
 - a. Under **Type**, select either **Schedule** or **Event** type from the dropdown list.

The display of Schedule or Event option depends on the trigger type selected under Type.
 - b. Under **Schedule**, select the appropriate schedule from the dropdown list or
 - c. Under **Event**, select the appropriate event from the dropdown list. For more information, see [Configuring Schedules](#) or [Configuring Events](#).
4. Click **SAVE**, to apply the changes.

Activities

Activities

- [Activities Overview](#)
- [Core Activities](#)
- [AMQP](#)
- [AWS Service](#)
- [Ansible Tower](#)
- [CloudCenter Suite](#)
- [Database Activities](#)
- [Email](#)
- [Google Cloud Platform](#)
- [KAFKA](#)
- [Meraki](#)
- [Microsoft Windows](#)
- [Prime Service Catalog](#)
- [Python](#)
- [Table Activities](#)
- [Task](#)
- [Terminal](#)
- [Unix/Linux System](#)
- [Web Service](#)
- [Creating an Atomic Workflow](#)

Activities Overview

Overview

Activities are the steps in a workflow. They are customized to perform integration with some environment. Activities can be provided by adapters (binary components in Action Orchestrator) or by automation packs. Therefore both adapters and automation packs can contribute to a particular integration. Workflow activities provide the logic or flow aspects of the workflow. Workflow activities are exposed in the Logic tab of the workflow Editor.

Related Topic

[Adding Logic Components to a Workflow](#)

Core Activities

Core Activities

These are the activities that are provided by the CoreActivitiesadapter:

- Calculate Date
- Calculate Date Time Difference
- Convert JSON to XML
- Convert XML to JSON
- Escape Regex Metacharacters
- Find String
- Format Date
- JSONPath Query
- Match Regular Expression
- Parse Date
- Replace String
- Set Variables
- Sleep
- Split String
- Substring
- To Lower
- To Upper
- Trim String
- XPath Query
- XSL Transform

Calculate Date

Calculate Date

Use the Calculate Date activity to calculate a new date/time value based on a specified base date/time and adjustments.

1. In the Workflow Editor Toolbox, choose **Core Activities > Calculate Date**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Calculate Date**, enter the following information or click [Variable Reference](#) icon to choose any variable.
 - i. Original date/time: Select a date/time of the variable to calculate.
 - ii. Adjustment: Enter the number of seconds to increase or decrease the time frame. Enter minus (-) prior to the value to decrease or enter plus (+) prior to the value to increase. (ex. -5)

Back to: [Core Activities](#)

Calculate Date Time Difference

Calculate Date Time Difference

Use the Calculate Date Time Difference activity to calculate a new date/time difference value based on a specified base date/time and subtract date.

1. In the Workflow Editor Toolbox, choose **Core Activities > Calculate Date Time Difference**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Calculate Date Time Difference**, enter the following information or click [Variable Reference](#) icon to choose any variable.
 - i. Original date/time: Select a date/time of the variable to calculate.
 - ii. Subtract date/time: Enter the date/time of the variable to be subtracted.

Back to: [Core Activities](#)

Convert JSON to XML

Convert JSON to XML

The Convert JSON to XML activity makes it easier for users to parse and manipulate XML configuration.

1. In the Workflow Editor Toolbox, choose **Core Activities**>**Convert JSON to XML**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **JSON Source**>**Input JSON**, enter the JSON text to be converted to XML or click [Variable Reference](#) icon to choose any variable. For example:

```
Sample JSON Source

{
  "items": {
    "item": [
      {
        "title": "Empire Burlesque",
        "note": "Special Edition",
        "quantity": "1",
        "price": "10.90"
      },
      {
        "title": "Hide your heart",
        "quantity": "1",
        "price": "9.90"
      }
    ]
  }
}
```

- c. Under **Replace List**, click **+ADD** and enter the following information:
 - i. Replaced String: Enter the specific string to be replaced.
 - ii. Replacement String: Enter the string for replacement.

Back to: [Core Activities](#)

Convert XML to JSON

Convert XML to JSON

Use the Convert XML to JSON activity to convert XML to JSON text which makes it easier for users to parse and manipulate JSON configuration.

1. In the Workflow Editor Toolbox, choose **Core Activities > Convert XML to JSON**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **XML Source > Input XML**, enter the XML text to be converted to JSON or click [Variable Reference](#) icon to choose any variable. For example:

Sample Source XML

```
<items>
<item>
<title>Empire Burlesque</title>
<note>Special Edition</note>
<quantity>1</quantity>
<price>10.90</price>
</item>
<item>
<title>Hide your heart</title>
<quantity>1</quantity>
<price>9.90</price>
</item>
</items>
```

Back to: [Core Activities](#)

Escape Regex Metacharacters

Escape Regex Metacharacters

You can use Escape Regex activity to escape the mentioned regular expression in the workflow.

1. In the Workflow Editor Toolbox, choose **Core Activities > Escape Regex Metacharacters**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Text Conversion**, enter the source string to be escaped or click [Variable Reference](#) icon to choose any variable.

Back to: [Core Activities](#)

Find String

Find String

You can use String activities to search, replace, and modify string content in the objects within Action Orchestrator. Search for specific content in a string.

1. In the Workflow Editor Toolbox, choose **Core Activities > Find String**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Find String**, enter the following information:
 - i. Source String: Enter the source string or click [Variable Reference](#) icon to choose any variable..
 - ii. Searched String: Enter the specific string to be searched or click [Variable Reference](#) icon to choose any variable.

Back to: [Core Activities](#)

Format Date

Format Date

Use the Format Date activity to convert date and time into a string text format.

1. In the Workflow Editor Toolbox, choose **Core Activities > Format Date**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Format Date**, enter the following information or click [Variable Reference](#) icon to choose any variable.
 - i. Output date/time string format: Select the output date/time string format from the drop-down list.
 - ii. Use custom date/time format: Check this check box to define your own date/time format.
 - iii. Original date/time: Select a date/time of the variable to calculate.

Back to: [Core Activities](#)

JSONPath Query

JSONPath Query

Use the JSON Path Query activity to query information based on JSON path expressions and nodes. If the query matches more than one node in the JSON document, an error will be generated.

1. In the Workflow Editor Toolbox, choose **Core Activities > JSON Path Query**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **JSON Query**, enter the following information:
 - i. Under **Source JSON To Query**, enter the source JSON text to be queried or click [Variable Reference](#) icon to choose any variable. For example:

Sample Source JSON

```
{
  "store": {
    "book": [
      { "category": "reference",
        "author": "Nigel Rees",
        "title": "Sayings of the Century",
        "price": 8.95
      },
      { "category": "fiction",
        "author": "Evelyn Waugh",
        "title": "Sword of Honour",
        "price": 12.99
      }
    ],
  }
}
```

- c. Under **JSONPath Queries**, click **+ADD** to add new JSON Path Query:
 - i. JSON Path Query: Enter the path expression to query. For example: `$.store.book[0].author`
 - ii. Property Name: Enter the property name to display on the Results page after the activity has run. For example: Author
 - iii. Property Type: Select the property type associated with the path expression to query such as Boolean, Date, Time, String, and so forth. For example, you select: String
3. The workflow run page displays the result of the JSON Path Query. For this example the result is: Author:Nigel Rees.

Back to: [Core Activities](#)

Match Regular Expression

Match Regular Expression

Use the Match Regular Expression activity to match specified string text against a specified regular expression.

1. In the Workflow Editor Toolbox, choose **Core Activities > Match Regular Expression**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Regular Expression**, enter the properties specific to the activity:
 - i. Regular Expression: Specify a fixed string to represent the regular expression to be used in matching or click [Variable Reference](#) icon to choose any variable.
 - ii. Match case: Check the check box to specify whether regular expression matching should be case-sensitive.
 - iii. Input string: Enter the input string for text to be parsed and matched against the specified regular expression or click [Variable Reference](#) icon to choose any variable.



For more information, see <https://golang.org/pkg/regexp/syntax/>.

Back to: [Core Activities](#)

Parse Date

Parse Date

Use the Parse Date activity to convert string text into a date/time format.

1. In the Workflow Editor Toolbox, choose **Core Activities > Parse Date**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. **Display Name**: Enter the unique display name for the activity.
 - ii. **Description**: Enter the brief description about the activity.
 - iii. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Parse Date**, enter the following information or click [Variable Reference](#) icon to choose any variable.
 - i. **Input date/time format**: Select the output date/time string format from the dropdown list. For example:

```
Format string - yyyyMMdd hh:mm:ss tt
yyyy - Denotes Year
MM - Denotes Month
dd - Denotes Day
hh - Denotes Hours
mm - Denotes Minutes
ss - Denotes Seconds
tt - Denotes AM/PM
```

- ii. **Use custom date/time format**: Check this check box to define your own date/time format.
- iii. **Input string**: Enter the date or time string to be parsed. For example:

```
Input string - "20171101 12:52:35 AM"
```

Back to: [Core Activities](#)

Replace String

Replace String

You can use String activities to search, replace, and modify string content in the objects within Action Orchestrator. Replace specific content substrings in a string.

1. In the Workflow Editor Toolbox, choose **Core Activities > Replace String**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. **Display Name**: Enter the unique display name for the activity.
 - ii. **Description**: Enter the brief description about the activity.
 - iii. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Replace String**, enter the following information:
 - i. Under **Input String**, enter the input string or click **Variable Reference** icon to choose any variable.
 - ii. Under **Replace List**, click **+ADD** to enter the following information:
 1. **Replaced String**: Enter the specific string to be replaced.
 2. **Replacement String**: Enter the string for replacement.

Back to: [Core Activities](#)

Set Variables

Set Variables

Use the Set Variables activity to update variable in a single activity. This activity will update each defined variable in the activity, one by one, as well as perform the necessary auditing for each updated variable.

1. In the Workflow Editor Toolbox, choose **Core Activities > Set Variables**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Variable**, click **+ADD** to enter the following information:
 - i. Variable to update: Enter the appropriate variable to be modified or click [Variable Reference](#) icon to choose any variable.
 - ii. New value: Enter a new value of the variable or click [Variable Reference](#) icon to choose any variable.
 1. For a Boolean variable, the text entered in this field (true or false) is case-sensitive and must be entered all lowercase.
 2. Formulas can also be included to modify variable values. For example:
 - 5+10
 - [Activity.Reference1] / [Activity.Reference2] * 100) + [Activity.Reference3]
 - [Activity.PropertyName1] [Activity.PropertyName2]

Back to: [Core Activities](#)

Sleep

Sleep

Use the Sleep activity to specify the time period to pause between activities in the workflow.

1. In the Workflow Editor Toolbox, choose **Core Activities > Sleep**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Sleep**, enter the **Sleep Interval** in seconds or click [Variable Reference](#) icon to choose any variable.

Back to: [Core Activities](#)

Split String

Split String

You can use String activities to search, replace, and modify string content in the objects within Action Orchestrator. Split a string into multiple parts around matches of the given delimiter or delimiters.

1. In the Workflow Editor Toolbox, choose **Core Activities > SplitString**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Split String**, enter the following information:
 - i. Input String: Enter the input string or click [Variable Reference](#) icon to choose any variable.
 - ii. Remove empty string from result set: Check this check box to remove the empty spaces in the result.
 - iii. Use regexp in Delimiters: Check this check box to split the regular expressions in the string.
 - iv. Under **Split Options**, enter the appropriate **Delimiter Text**. Click **+ADD**, to add new delimiter text.

Back to: [Core Activities](#)

Substring

Substring

You can use String activities to search, replace, and modify string content in the objects within Action Orchestrator. It allows you to return part of a string starting with the characters in the start position and ending with the character in the specified end position.

1. In the Workflow Editor Toolbox, choose **Core Activities > Substring**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Substring**, enter the following information:
 - i. Source String: Enter the source string or click [Variable Reference](#) icon to choose any variable.
 - ii. Beginning Index: Enter the begin index of the string to be returned.
 - iii. End Index: Enter the End index of the string to be returned.

For example:

```
Input string = dictionary
```

```
Start position = 4
```

```
End position = 6
```

```
Dictionary
```

```
0123456 <- using 0 as the starting point
```

```
Positions 4 through 6 yield ion
```

Back to: [Core Activities](#)

To Lower

To Lower

You can use String activities to search, replace, and modify string content in the objects within Action Orchestrator. Lower the text case in a string.

1. In the Workflow Editor Toolbox, choose **Core Activities > To Lower**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. **Display Name**: Enter the unique display name for the activity.
 - ii. **Description**: Enter the brief description about the activity.
 - iii. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Text Conversion**, enter the source string to lower the text case in a string or click [Variable Reference](#) icon to choose any variable.

Back to: [Core Activities](#)

To Upper

To Upper

You can use String activities to search, replace, and modify string content in the objects within Action Orchestrator. Capitalize the text case in a string.

1. In the Workflow Editor Toolbox, choose **Core Activities > To Upper**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Text Conversion**, enter the source string to upper the text case in a string or click [Variable Reference](#) icon to choose any variable.

Back to: [Core Activities](#)

Trim String

Trim String

You can use String activities to search, replace, and modify string content in the objects within Action Orchestrator. It allows you to trim characters from the content in a string. When no character is specified, the activity will trim all leading and trailing blank space characters, including empty lines at the beginning and at the end.

1. In the Workflow Editor Toolbox, choose **Core Activities > Trim String**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **String Trimming**, enter the following information:
 - i. Source String: Enter the source string or click [Variable Reference](#) icon to choose any variable.
 - ii. Characters to Trim: Enter characters to be trimmed or click [Variable Reference](#) icon to choose any variable.
 - iii. Trim Leading Characters: Enter true, false, or Boolean variable by clicking.
 - iv. Trim Trailing Characters: Enter true, false, or Boolean variable by clicking.

Back to: [Core Activities](#)

XPath Query

XPath Query

Use the XPath Query activity to query information based on XML path expressions, nodes, as well as namespace definitions. If the query matches more than one node in the XML document, an error will be generated.

1. In the Workflow Editor Toolbox, choose **Core Activities > XPath Query**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **XML Query**, enter the following information:
 - i. Source XML To Query: Enter the source XML text to be queried or click [Variable Reference](#) icon to choose any variable.
 - ii. Namespaces: Click **+ADD** to add new namespace and enter the **Prefix** and **URI** for the new namespace.



An XML namespace provides a way to avoid element and attribute name conflicts within an XML document. An XML namespace is uniquely identified by a Uniform Resource Identifier (URI) and is assigned a prefix (unique to the XML document) used for its element and attribute names.

- iii. Under **Xpath Queries**, click **+ADD** to add new XPath Queries and enter the following information:
 - XPath Query: Enter the path expression to query.
 - Property Name: Enter the property name to display on the Results after the activity has run.
 - Property Type: Select the data type associated with the path expression to query (String, Numeric, or and so forth).

Related Topic

- [XPath Example Syntax](#)
- [XPath Query Example](#)
- [XPath Query Example 2](#)

Back to: [Core Activities](#)

XPath Example Syntax

XPath Example Syntax

The following expressions can be used when selecting nodes in a path expression.

Path Expression	Description
nodename	Selects all child nodes of the named node
/	Selects from the root node
//	Selects nodes in the document from the current node that match the selection no matter where they are
.	Selects the current node
..	Selects the parent of the current node
@	Selects attribute

Back to: [XPath Query](#)

Back to: [Core Activities](#)

XPath Query Example

XPath Query Example

The following is an example of source XML.

Example

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<bookstore>
<book>
<title lang="eng">Harry Potter</title>
<price>29.99</price>
</book>
<book>
<title lang="eng">Learning XML</title>
<price>39.95</price>
</book>
</bookstore>
```

The following example path expressions and related results are based on the preceding source XML.

Path Expression	Description
bookstore	Selects all child nodes of the bookstore element
/bookstore	Selects the root element bookstore. If the path starts with a slash (/) it always represents an absolute path to an element.
bookstore/book	Selects all book elements that are children of bookstore
//book	Selects all book elements no matter where they are in the document
bookstore//book	Selects all book elements that are descendant of the bookstore element, no matter where they are under the bookstore element
//@lang	Selects all attributes that are named lang



For additional examples, see https://www.w3schools.com/xml/xpath_syntax.asp.

Back to: [XPath Query](#)

Back to: [Core Activities](#)

XPath Query Example 2

XPath Query Example 2

In the following example, the elements prefixed with xdc are associated with a namespace whose name is <http://www.xml.com>, while those prefixed with h are associated with a namespace whose name is <http://msdn.microsoft.com/en-us/library/ms950779.aspx>.

Example XML

```
<h:html xmlns:xdc="http://www.xml.com/books"
xmlns:h="http://www.w3.org/HTML/1998/html4">
<h:head><h:title>Book Review</h:title></h:head>
<h:body>
<xdc:bookreview>
<xdc:title>XML: A Primer</xdc:title>
<h:table>
<h:tr align="center">
<h:td>Author</h:td><h:td>Price</h:td>
<h:td>Pages</h:td><h:td>Date</h:td></h:tr>
<h:tr alignment">
<h:td><xdc:author>Simon St. Laurent</xdc:author></h:td>
<h:td><xdc:price>31.98</xdc:price></h:td>
<h:td><xdc:pages>352</xdc:pages></h:td>
<h:td><xdc:date>1998/01</xdc:date></h:td>
</h:tr>
</h:table>
</xdc:bookreview>
</h:body>
</h:html>
```



For additional examples, see <http://msdn.microsoft.com/en-us/library/ms950779.aspx>.

Back to: [XPath Query](#)

Back to: [Core Activities](#)

XSL Transform

XSL Transform

Use the XSL Transform activity to apply XSLT transformation to specific XML text. XSLT transformation can transform XML into plain text, HTML, or other XML.

1. In the Workflow Editor Toolbox, choose **Core Activities > XSL Transform**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **XSLT**, enter the following information:
 - i. Style Sheet: Enter the XSLT style sheet for the XSL document or click [Variable Reference](#) icon to choose any variable.
 - ii. Document: Enter the XSLT document or click [Variable Reference](#) icon to choose any variable.

Back to: [Core Activities](#)

AMQP

AMQP

The Advanced Message Queuing Protocol (AMQP) is an open standard application layer protocol for message-oriented middleware. It delivers message orientation, queuing, routing (including point-to-point and publish-and-subscribe), reliability and security. AMQP came out of the financial industry, and is proven highly scalable in demanding environments (refer <http://www.amqp.org/>).

AMQP is the emerging standard for messaging and events in the cloud. For example:

- vCloud Director can publish vCloud Messages, also known as blocking tasks, notifications, or call-outs, related to different provisioning. An orchestrator can not only receive these events, but can also respond to them to delay execution.
- AMQP is supported with vCloud Orchestrator.
- OpenStack selected AMQP as the messaging technology for OpenStack.

AMQP is integrated with more than 70 developer platforms, providing a nice framework for event-oriented integrations.

AMQP enables event-driven capabilities of Enterprise Service Bus-style designs. It enables queuing, so automation can fetch messages when there is capacity. You can use asynchronous methods servicing requests as capacity allows when possible, and reserve real-time, synchronous methods only when absolutely needed. AMQP's open platform is a natural choice for event and message design patterns.

Action Orchestrator can trigger processes in response to messages placed on AMQP queues/exchanges. Processes can also read messages from queues/exchanges one at a time if they want to respond to messages one at a time rather than in parallel, to operate more as a queue. Processes can submit messages to queues/exchanges.

JMS is another possible integration enabled through AMQP. AMQP has providers to place JMS messages on queues/exchanges.

The Cisco Advanced Message Queuing Protocol (AMQP) software adapter allows you to automate messaging activities on Cisco AMQP instances.

The following sections display AMQP activities:

- [Bind AMQP Queue](#)
- [Declare AMQP Exchange](#)
- [Declare AMQP Queue](#)
- [Get AMQP Message](#)
- [Publish AMQP Message](#)

Bind AMQP Queue

Bind AMQP Queue

Use the Bind AMQP Queue activity to bind a queue to an AMQP broker exchange.

1. In the Workflow Editor Toolbox, choose **Activities > AMQP > Bind AMQP Queue**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Bind AMQP Queue activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [AMQP Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate account key or **+ADD NEW** from the dropdown list. For more information, see [AMQP Certificate-Based Credentials](#) or [AMQP Password-Based Credentials](#) or [AMQP Password-Less Certificate-Based Credentials](#).
 - d. Under **AMQP**, specify the following information or Click [Variable Reference](#) icon to choose any variable:
 - i. Queue Name: Name of the queue you want to bind to an exchange.
 - ii. Exchange Name: Name of the exchange you want to bind to a queue.
 - iii. Routing Key: The key to be sent with the message.
 - iv. Arguments: Click **+ADD** to enter the **Key** and **Value** pair arguments for the queue.

Back to: [AMQP](#)

Declare AMQP Exchange

Declare AMQP Exchange

Use the Declare Exchange activity to create or check an AMQP broker exchange.

1. In the Workflow Editor Toolbox, choose **Activities > AMQP > Declare AMQP Exchange**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the AMQP activity.
 - ii. Description: Enter the brief description about the AMQP activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Declare AMQP Exchange activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [AMQP Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate account key or **+ADD NEW** from the dropdown list. For more information, see [AMQP Certificate-Based Credentials](#) or [AMQP Password-Based Credentials](#) or [AMQP Password-Less Certificate-Based Credentials](#).
 - d. Under **AMQP**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Exchange Name: Name of the exchange you want to declare.
 - ii. Type: Select the appropriate type of exchange you want to declare from the dropdown list:
 1. **Direct**: The Direct exchange type routes messages with a routing key equal to the routing key declared by the binding queue.
 2. **Topic**: The Topic exchange type routes messages to queues whose routing key matches all, or a portion of a routing key.
 3. **Fanout**: The Fanout exchange type routes messages to all bound queues indiscriminately.
 4. **Headers**: The Headers exchange type routes messages based upon a matching of message headers to the expected headers specified by the binding queue.
 - iii. Durable: Check the check box if the queue is durable. Durable queues survive broker restart whereas transient queues do not (they must be redeclared when the broker comes back online). Not all scenarios and use cases require durable queues.
 - iv. Auto delete: Check this check box to delete the queue when it is empty.
 - v. Arguments: Click **+ADD** to enter the **Key** and **Value** pair arguments for the queue.

Back to: [AMQP](#)

Declare AMQP Queue

Declare AMQP Queue

Use the Declare Queue activity to create or check a queue on the AMQP broker. This activity will create a queue if the queue does not already exist.

When you declare a new queue, you can specify various properties that control the durability of the queue and its contents and the level of sharing for the queue.

1. In the Workflow Editor Toolbox, choose **Activities > AMQP > Declare AMQP Queue**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. **Display Name**: Enter the unique display name for the AMQP activity.
 - ii. **Description**: Enter the brief description about the AMQP activity.
 - iii. **Activity Timeout (Seconds)**: Enter the number of seconds to wait for Declare AMQP Queue activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. **Use Workflow Target**: Check this radio button to use the workflow target.
 - ii. **Override Workflow Target**: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [AMQP Endpoint](#).
 - iii. **Use Workflow Target Group**: Check this radio button to use the workflow target group.
 - iv. **Override Workflow Target Group Criteria**: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. **Use Target's Default Account Key**: Check this radio button to use the target's default account key.
 - ii. **Override Account Key**: Check this radio button to override the workflow account key. You can select the appropriate Account Key User ID or **+ADD NEW** from the dropdown list. For more information, see [AMQP Certificate-Based Credentials](#) or [AMQP Password-Based Credentials](#) or [AMQP Password-Less Certificate-Based Credentials](#).
 - d. Under **AMQP**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. **Queue Name**: Enter the unique queue name.
 - ii. **Durable**: Check this check box if the queue is durable. Durable queues survive broker restart whereas transient queues do not (they must be redeclared when the broker comes back online). Not all scenarios and use cases require durable queues.
 - iii. **Auto delete**: Check this check box to delete the queue when it is empty.
 - iv. **Arguments**: Click **+ADD** to enter the key and value pair arguments for the queue.

Back to: [AMQP](#)

Get AMQP Message

Get AMQP Message

Use the Get Message activity to retrieve the next available message from a given queue on the AMQP broker.



This activity will open and close the channel to get one message; it is not designed to put it into a tight loop. This activity is considered to be a destructive way to get a message from an AMQP queue. The typical way is to subscribe to an AMQP queue.

1. In the Workflow Editor Toolbox, choose **Activities > AMQP > Get AMQP Message**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the AMQP activity.
 - ii. Description: Enter the brief description about the AMQP activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Get AMQP Message activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [AMQP Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key User: Check this radio button to use the target's default account key user.
 - ii. Override Account Key User: Check this radio button to override the workflow account key user. You can select the appropriate account key User ID or **+ADD NEW** from the dropdown list. For more information, see [AMQP Certificate-Based Credentials](#) or [AMQP Password-Based Credentials](#) or [AMQP Password-Less Certificate-Based Credentials](#).
 - d. Under **AMQP**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Queue Name: Name of the queue from which you want to receive message.
 - ii. No Acknowledgment Mode: If this option is checked, no acknowledgment is sent after retrieving the message. The server will auto-acknowledge the message.

Back to: [AMQP](#)

Publish AMQP Message

Publish AMQP Message

Use the Publish Message activity to publish a text message to an existing exchange on the AMQP broker. The message will be routed to queues as defined by the exchange configuration and distributed when the transaction, if any, is committed.

For example, VMWare vCloud Director can publish vCloud AMQP Messages (also known as blocking tasks, notifications, or call-outs) related to different provisioning tasks. Action Orchestrator can not only receive these events, but can respond to them to delay execution.

1. In the Workflow Editor Toolbox, choose **Activities > AMQP > Publish AMQP Message**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the AMQP activity.
 - ii. Description: Enter the brief description about the AMQP activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Publish AMQP Message activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [AMQP Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate account key or **+ADD NEW** from the dropdown list. For more information, see [AMQP Certificate-Based Credentials](#) or [AMQP Password-Based Credentials](#) or [AMQP Password-Less Certificate-Based Credentials](#).
 - d. Under **AMQP**, specify the following information or [Variable Reference](#) icon to choose any variable:

Field	Description
Exchange Name	Name of the exchange you want to publish.
Routing Key	The key to be sent with the message.
Message Body	Enter the appropriate message to be transferred.
Message Headers	Enter the header and value for the message.
APP ID	Enter the application ID of the publishing application.
Content Encoding	Enter the content to be encoded.
Content Type	Enter the required content type such as Json, XMI, and so forth.
Correlation ID	Enter the correlation ID of the AMQP header.
Delivery Mode	Enter the delivery mode as either persistent or non persistent.
Expiration (Milliseconds)	Enter the time to live period for a basic publish.
Message ID	Enter the unique message ID.
Priority	Select the priority for the transfer of message from the dropdown list.
Reply To	Enter the reply to attribute for the AMQP message.
Time Stamp	Enter the time stamp for the AMQP event.
Type	Enter the AMQP type.
User ID	Enter the unique user ID.

Back to: [AMQP](#)

AWS Service

AWS Service

Amazon Elastic Compute Cloud (Amazon EC2) provides scalable computing capacity in the Amazon Web Services (AWS) cloud. Using Amazon EC2 eliminates your need to invest in hardware up front, so you can develop and deploy applications faster. You can use Amazon EC2 to launch as many or as few virtual servers as you need, configure security and networking, and manage storage. Amazon EC2 enables you to scale up or down to handle changes in requirements or spikes in popularity, reducing your need to forecast traffic.

The following sections display activities that are provided by the AWS Service adapter:

- [Associate Subnet](#)
- [Attach Internet Gateway](#)
- [Create Account](#)
- [Create Account Statuses](#)
- [Create EC2 Instances](#)
- [Create Internet Gateway](#)
- [Create Keypair](#)
- [Create Route](#)
- [Create Route Table](#)
- [Create Security Group](#)
- [Create Security Group Rule](#)
- [Create Subnet in a VPC](#)
- [Create VPC](#)
- [Delete Keypair](#)
- [Delete Security Group](#)
- [Delete Security Group Rules](#)
- [Describe Route Tables](#)
- [Describe Security Group](#)
- [Describe Subnets](#)
- [Describe VPCs](#)
- [Disassociate Subnet](#)
- [Generic AWS API Request](#)
- [IAM Attach User Policy](#)
- [IAM Create Access Key](#)
- [IAM Create User](#)
- [IAM List Policies](#)
- [IAM List Users](#)
- [Import Keypair](#)
- [Reboot EC2 Instances](#)
- [Start EC2 Instances](#)
- [Stop EC2 Instances](#)
- [Terminate EC2 Instances](#)

Associate Subnet

Associate Subnet

To define the Associate Subnet with Route Table activity:

1. In the Workflow Editor Toolbox, choose **Activities > AWS Service > Associate Subnet**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - b. Route Table ID: Enter the Route Table ID to be associated with the Subnet.
 - i. Description: Enter the brief description about the activity.
 - ii. Activity Timeout (Seconds): Enter the number of seconds to wait for Associate Subnet activity to fail because it timed out.
 - iii. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - c. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [AWS Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - d. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account Key or **+ADD NEW** from the dropdown list. For more information, see [AWS Credentials](#).
 - e. Under **Associate**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Route Table ID: Enter the Route Table ID to be associated.
 - ii. Subnet ID: Enter the subnet ID to be associated with the route table.

Back to: [AWS Service](#)

Attach Internet Gateway

Attach Internet Gateway

To define the Attach Internet Gateway activity:

1. In the Workflow Editor Toolbox, choose **Activities > AWS Service > Attach Internet Gateway**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Attach Internet Gateway activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [AWS Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account Key or **+ADD NEW** from the dropdown list. For more information, see [AWS Credentials](#).
 - d. Under **Attach Gateway**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. VPC ID: Enter the Virtual Private Cloud (VPC) ID to set up a connection.
 - ii. Internet Gateway ID: Enter the Internet Gateway ID to set up connection to the public internet.

Back to: [AWS Service](#)

Create Account

Create Account

Use the Create Account activity to create an AWS account.

1. In the Workflow Editor Toolbox, choose **AWS Service > Create Account** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Create Account activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [AWS Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the dropdown list. For more information, see [AWS Credentials](#).
 - d. Under **Create Account**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Enter Account Name: Enter the name for your AWS account.
 - ii. Enter Email: Enter the email address.

Back to: [AWS Service](#)

Create Account Statuses

Create Account Statuses

Use the Create Account Statuses activity to retrieve the current status of a request to create an account.

1. In the Workflow Editor Toolbox, choose **AWS Service > Create Account Statuses** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Create Account Statuses activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [AWS Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the dropdown list. For more information, see [AWS Credentials](#).
 - d. Under **Account States**, specify the following information :
 - i. Enter States: Enter the status of the request.

Back to: [AWS Service](#)

Create EC2 Instances

Create EC2 Instances

To define the Create EC2 Instances activity:

1. In the Workflow Editor Toolbox, choose **Activities > AWS Service > Create EC2 Instances**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:

- a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Create EC2 Instances activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
- b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [AWS Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
- c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account Key or **+ADD NEW** from the dropdown list. For more information, see [AWS Credentials](#).
- d. Under **EC2 Request**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. AMI Image ID: Enter the Amazon Machine Image (AMI) ID to launch an EC2 instance.
 - ii. Security Group IDs: Click **+ADD** to enter the security group ID.
 - iii. KeyPair Name: Enter the Keypair name to secure information for your instance.
 - iv. Maximum Instances Count: Enter the maximum number of instance counts.
 - v. Minimum Instances Count: Enter the minimum number of instance counts.
 - vi. Private IP Address: Enter the private IP address.
 - vii. Instance Type: Enter the instance type to determine the hardware of the host computer to be used for the instance.
 - viii. Subnet ID: Enter the subnet ID to be associated.
 - ix. Auto-Assign Public IP: Select **Enable** or **Disable** from the dropdown list.

Back to: [AWS Service](#)

Create Internet Gateway

Create Internet Gateway

To define the Create Internet Gateway activity:

1. In the Workflow Editor Toolbox, choose **Activities > AWS Service > Create Internet Gateway**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. **Display Name**: Enter the unique display name for the activity.
 - ii. **Description**: Enter the brief description about the activity.
 - iii. **Activity Timeout (Seconds)**: Enter the number of seconds to wait for Create Internet Gateway activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. **Use Workflow Target**: Check this radio button to use the workflow target.
 - ii. **Override Workflow Target**: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [AWS Endpoint](#).
 - iii. **Use Workflow Target Group**: Check this radio button to use the workflow target group.
 - iv. **Override Workflow Target Group Criteria**: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. **Use Target's Default Account Key**: Check this radio button to use the target's default account key.
 - ii. **Override Account Key**: Check this radio button to override the workflow account key. You can select the appropriate Account Key or **+ADD NEW** from the dropdown list. For more information, see [AWS Credentials](#).
 - d. Under **Create Gateway**, specify the following information:

Name Tag: Enter the name tag for the internet gateway.

Back to: [AWS Service](#)

Create Keypair

Create Keypair

To define the Create Keypair activity:

1. In the Workflow Editor Toolbox, choose **Activities > AWS Service > Create Keypair**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Create Keypair activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [AWS Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account Key or **+ADD NEW** from the dropdown list. For more information, see [AWS Credentials](#).
 - d. Under **EC2 Request**, specify the following information or click [Variable Reference](#) icon to choose any variable:

Keypair Name: Enter the keypair name to secure login information for your instance.

Back to: [AWS Service](#)

Create Route

Create Route

To define the Create Route activity:

1. In the Workflow Editor Toolbox, choose **Activities > AWS Service > Create Route**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. **Display Name**: Enter the unique display name for the activity.
 - ii. **Description**: Enter the brief description about the activity.
 - iii. **Activity Timeout (Seconds)**: Enter the number of seconds to wait for Create Route activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. **Use Workflow Target**: Check this radio button to use the workflow target.
 - ii. **Override Workflow Target**: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [AWS Endpoint](#).
 - iii. **Use Workflow Target Group**: Check this radio button to use the workflow target group.
 - iv. **Override Workflow Target Group Criteria**: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. **Use Target's Default Account Key**: Check this radio button to use the target's default account key.
 - ii. **Override Account Key**: Check this radio button to override the workflow account key. You can select the appropriate Account Key or **+ADD NEW** from the dropdown list. For more information, see [AWS Credentials](#).
 - d. Under **Create Route**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. **Destination CIDR Block**: Enter the destination CIDR block to associate with your VPC.
 - ii. **Gateway ID**: Enter the gateway ID to enable communication.
 - iii. **Route Table ID**: Enter the route table ID to enable routing within the VPC.

Back to: [AWS Service](#)

Create Route Table

Create Route Table

To define the Create Route Table activity:

1. In the Workflow Editor Toolbox, choose **Activities > AWS Service > Create Route Table**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Create Route Table activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [AWS Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account Key or **+ADD NEW** from the dropdown list. For more information, see [AWS Credentials](#).
 - d. Under **Create Route Table**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Name Tag: Enter the name tag for the route table.
 - ii. VPC ID: Enter the Virtual Private Cloud (VPC) ID to associate VPC with the route table.

Back to: [AWS Service](#)

Create Security Group

Create Security Group

To define the Create Security Group Table activity:

1. In the Workflow Editor Toolbox, choose **Activities > AWS Service > Create Security Group**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Create Security Group activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [AWS Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account Key or **+ADD NEW** from the dropdown list. For more information, see [AWS Credentials](#).
 - d. Under **Security Group**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Name: Enter the name for security group to associate with VPC.
 - ii. Description: Enter the brief description about the security group.
 - iii. VPC ID: Enter the Virtual Private Cloud (VPC) ID to associate VPC with the security group.

Back to: [AWS Service](#)

Create Security Group Rule

Create Security Group Rule

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. When you launch an instance in a VPC, you can assign up to five security groups to the instance. Security groups act at the instance level, not the subnet level. Therefore, each instance in a subnet in your VPC could be assigned to a different set of security groups. If you don't specify a particular group at launch time, the instance is automatically assigned to the default security group for the VPC.

To define the Create Security Group Rule activity:

1. In the Workflow Editor Toolbox, choose **Activities > AWS Service > Create Security Group Rule**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. **Display Name**: Enter the unique display name for the activity.
 - ii. **Description**: Enter the brief description about the activity.
 - iii. **Activity Timeout (Seconds)**: Enter the number of seconds to wait for Create Security Group Rule activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. **Use Workflow Target**: Check this radio button to use the workflow target.
 - ii. **Override Workflow Target**: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [AWS Endpoint](#).
 - iii. **Use Workflow Target Group**: Check this radio button to use the workflow target group.
 - iv. **Override Workflow Target Group Criteria**: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. **Use Target's Default Account Key**: Check this radio button to use the target's default account key.
 - ii. **Override Account Key**: Check this radio button to override the workflow account key. You can select the appropriate Account Key or **+ADD NEW** from the dropdown list. For more information, see [AWS Credentials](#).
 - d. Under **Security Group**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. **Group ID**: Enter the security group ID.
 - ii. **InBound Rules**: Click **+ADD** to specify the following information:
 1. **IP Protocol**: Select the IP protocol from the dropdown list such as Custom TCP, Custom UDP, and Custom Custom ICMP.
 2. **From Port**: Enter the From Port number for the port range.
 3. **To Port**: Enter the To Port number for the port range.
 4. **CIDR Block IP4**: Specify the IPv4 CIDR block as the source.
 - iii. **OutBound Rules**: Click **+ADD** to specify the following information:
 1. **IP Protocol**: Select the IP protocol from the dropdown list such as Custom TCP, Custom UDP, and Custom Custom ICMP.
 2. **From Port**: Enter the From Port number for the port range.
 3. **To Port**: Enter the To port number for the port range.
 4. **CIDR Block IP4**: Specify the IPv4 CIDR block as the destination.

Back to: [AWS Service](#)

Create Subnet in a VPC

Create Subnet in a VPC

To define the Create Subnet in a VPC activity:

1. In the Workflow Editor Toolbox, choose **Activities > AWS Service > Create Subnet in a VPC**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. **Display Name**: Enter the unique display name for the activity.
 - ii. **Description**: Enter the brief description about the activity.
 - iii. **Activity Timeout (Seconds)**: Enter the number of seconds to wait for Create Subnet in a VPC activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. **Use Workflow Target**: Check this radio button to use the workflow target.
 - ii. **Override Workflow Target**: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [AWS Endpoint](#).
 - iii. **Use Workflow Target Group**: Check this radio button to use the workflow target group.
 - iv. **Override Workflow Target Group Criteria**: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. **Use Target's Default Account Key**: Check this radio button to use the target's default account key.
 - ii. **Override Account Key**: Check this radio button to override the workflow account key. You can select the appropriate Account Key or **+ADD NEW** from the dropdown list. For more information, see [AWS Credentials](#).
 - d. Under **Create Subnet**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. **Name Tag**: Enter the name tag for the subnet.
 - ii. **VPC ID**: Enter the Virtual Private Cloud (VPC) ID to associate with the subnet.
 - iii. **IPv4 CIDR Block**: Enter the IPv4 CIDR block for the subnet, which is a subset of the VPC CIDR block.
 - iv. **Availability Zone**: Enter the availability zone in which the subnet has to be created.

Back to: [AWS Service](#)

Create VPC

Create VPC

To define the Create VPC activity:

1. In the Workflow Editor Toolbox, choose **Activities > AWS Service > Create VPC**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. **Display Name**: Enter the unique display name for the activity.
 - ii. **Description**: Enter the brief description about the activity.
 - iii. **Activity Timeout (Seconds)**: Enter the number of seconds to wait for Create VPC activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. **Use Workflow Target**: Check this radio button to use the workflow target.
 - ii. **Override Workflow Target**: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [AWS Endpoint](#).
 - iii. **Use Workflow Target Group**: Check this radio button to use the workflow target group.
 - iv. **Override Workflow Target Group Criteria**: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. **Use Target's Default Account Key**: Check this radio button to use the target's default account key.
 - ii. **Override Account Key**: Check this radio button to override the workflow account key. You can select the appropriate Account Key or **+ADD NEW** from the dropdown list. For more information, see [AWS Credentials](#).
 - d. Under **Create VPC**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. **Name Tag**: Enter the name tag for the Virtual Private Cloud (VPC).
 - ii. **IPv4 CIDR Block**: Enter the IPv4 Classless Inter-Domain Routing (CIDR) block for VPC.
 - iii. **IPv6 CIDR Block**: Enter the IPv6 Classless Inter-Domain Routing (CIDR) block for VPC.
 1. **No IPv6 CIDR Block**: Click on this radio button, if you have no IPv6 CIDR block.
 2. **Amazon Provided IPv6 CIDR Block**: Click on this radio button if you have Amazon provided IPv6 CIDR block.
 - iv. **Instance Tenancy**: Select either **Default** or **Dedicated** tenancy value from the dropdown list.
 1. **Default**: An instance launched into the VPC runs on shared hardware by default, unless you explicitly specify a different tenancy during instance launch.
 2. **Dedicated**: An instance launched into the VPC is a Dedicated Instance by default, unless you explicitly specify a tenancy of host during instance launch. You cannot specify a tenancy of default during instance launch.

Back to: [AWS Service](#)

Delete Keypair

Delete Keypair

To define the Delete Keypair activity:

1. In the Workflow Editor Toolbox, choose **Activities > AWS Service > Delete Keypair**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Keypair Name: Enter the name of the keypair to be deleted.
 - iii. Description: Enter the brief description about the activity.
 - iv. Activity Timeout (Seconds): Enter the number of seconds to wait for Delete Keypair activity to fail because it timed out.
 - v. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target group.
 - ii. Override Workflow Target: Check this radio button to override the workflow target group criteria. You can select the appropriate target group or **+ADD NEW** from the dropdown list. For more information, see [AWS Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account Key or **+ADD NEW** from the dropdown list. For more information, see [AWS Credentials](#).
 - d. Under **EC2 Request**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Keypair Name: Enter the keypair name to be associated with the public key.

Back to: [AWS Service](#)

Delete Security Group

Delete Security Group

To define the Delete Security Group activity:

1. In the Workflow Editor Toolbox, choose **Activities > AWS Service > Delete Security Group**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:

a. Under **General**, specify the following information:

- i. **Display Name:** Enter the unique display name for the activity.
- ii. **Description:** Enter the brief description about the activity.
- iii. **Activity Timeout (Seconds):** Enter the number of seconds to wait for Delete Security Group activity to fail because it timed out.
- iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.

b. Under **Target**, specify the following information:

- i. **Use Workflow Target:** Check this radio button to use the workflow target.
- ii. **Override Workflow Target:** Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the drop-down list. For more information, see [AWS Endpoint](#).
- iii. **Use Workflow Target Group:** Check this radio button to use the workflow target group.
- iv. **Override Workflow Target Group Criteria:** Check this radio button to override the workflow target group criteria.

c. Under **Credentials**, specify the following information:

- i. **Use Target's Default Account Key:** Check this radio button to use the target's default account key.
- ii. **Override Account Key:** Check this radio button to override the workflow account key. You can select the appropriate Account Key or **+ADD NEW** from the drop-down list. For more information, see [AWS Credentials](#).

d. Under **Security Group**, specify the following information or click [Variable Reference](#) icon to choose any variable:

Group ID: Enter the security group ID to be deleted.

Back to: [AWS Service](#)

Delete Security Group Rules

Delete Security Group Rules

To define the Delete Security Group Rules activity:

1. In the Workflow Editor Toolbox, choose **Activities > AWS Service > Delete Security Group Rules**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Delete Security Group Rules activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [AWS Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account Key or **+ADD NEW** from the dropdown list. For more information, see [AWS Credentials](#).
 - d. Under **Security Group**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Group ID: Enter the security group ID.
 - ii. InBound Rules: Click **+ADD** to specify the following information:
 1. IP Protocol: Select the IP protocol from the dropdown list such as Custom ICMP, Custom TCP, and Custom UDP.
 2. From Port: Enter the Fromport number for the port range.
 3. To Port: Enter the To port number for the port range.
 4. CIDR Block IP4: Specify the IPv4 CIDR block as the source.
 - iii. OutBound Rules: Click **+ADD** to specify the following information:
 1. IP Protocol: Select the IP protocol from the dropdown list such as Custom ICMP, Custom TCP, and Custom UDP.
 2. From Port: Enter the Fromport number for the port range.
 3. To Port: Enter the To port number for the port range.
 4. CIDR Block IP4: Specify the IPv4 CIDR block as the destination.

Back to: [AWS Service](#)

Describe Route Tables

Describe Route Tables

To define the Describe Route Tables activity:

1. In the Workflow Editor Toolbox, choose **Activities > AWS Service > Describe Route Tables**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Describe Route Tables activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [AWS Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account Key or **+ADD NEW** from the dropdown list. For more information, see [AWS Credentials](#).
 - d. Under **Describe Tables**, click **+ADD** to specify the following information or click [Variable Reference](#) icon to choose any variable:
Route Table IDS: Enter the ID of the route table involved in the association.
 - e. Under **Filters**, click **+ADD** to specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Name: Enter the name to be filtered.
 - ii. Value: Enter the associated value.

Back to: [AWS Service](#)

Describe Security Group

Describe Security Group

To define the Describe Security Group activity:

1. In the Workflow Editor Toolbox, choose **Activities > AWS Service > Describe Security Group**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name - Enter the unique display name for the activity.
 - ii. Description - Enter the brief description about the activity.
 - iii. Timeout in Seconds - Enter the number of seconds to wait for Describe Security Group activity to fail because it timed out.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target - Check this radio button to use the workflow target.
 - ii. Override Workflow Target - Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the drop-down list. For more information, see [AWS Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key - Check this radio button to use the target's default account key.
 - ii. Override Account Key - Check this radio button to override the workflow account key. You can select the appropriate Account Key or **+ADD NEW** from the drop-down list. For more information, see [AWS Credentials](#).
 - d. Under **Security Group**, specify the following information or click [Variable Reference](#) icon to choose any variable:
Group ID - Enter the security group ID to be described.

Back to: [AWS Service](#)

Describe Subnets

Describe Subnets

To define the Describe Subnets activity:

1. In the Workflow Editor Toolbox, choose **Activities > AWS Service > Describe Subnets**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Describe Subnets activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the drop-down list. For more information, see [AWS Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account Key or **+ADD NEW** from the drop-down list. For more information, see [AWS Credentials](#).
 - d. Under **Describe Subnets**, specify the following information or click [Variable Reference](#) icon to choose any variable:
Subnet IDS: Enter the Subnet ID to be described.
 - e. Under **Filters**, click **+ADD** to specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Name: Enter the name to be filtered.
 - ii. Value: Enter the associated value.

Back to: [AWS Service](#)

Describe VPCs

Describe VPCs

To define the Describe VPCs activity:

1. In the Workflow Editor Toolbox, choose **Activities > AWS Service > Describe VPCs**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Describe VPCs activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the drop-down list. For more information, see [AWS Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account Key or **+ADD NEW** from the drop-down list. For more information, see [AWS Credentials](#).
 - d. Under **Describe VPCs**, click **+ADD** to specify the following information or click [Variable Reference](#) icon to choose any variable:

VPC IDS: Enter the Virtual Private Cloud (VPC) ID to be described.
 - e. Under **Filters**, click **+ADD** to specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Name: Enter the name to be filtered.
 - ii. Value: Enter the associated value.

Back to: [AWS Service](#)

Disassociate Subnet

Disassociate Subnet

To define the Disassociate Subnet from Route Table activity:

1. In the Workflow Editor Toolbox, choose **Activities > AWS Service > Disassociate Subnet**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:

- a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Disassociate Subnet activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
- b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the drop-down list. For more information, see [AWS Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
- c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account Key or **+ADD NEW** from the drop-down list. For more information, see [AWS Credentials](#)
- d. Under **Disassociate**, specify the following information or click [Variable Reference](#) icon to choose any variable:

Association ID: Enter the association ID to disassociate subnet from route table.

Back to: [AWS Service](#)

Generic AWS API Request

Generic AWS API Request

To define the Generic AWS API Request activity:

1. In the Workflow Editor Toolbox, choose **Activities > AWS Service > Generic AWS API Request**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. **Display Name**: Enter the unique display name for the activity.
 - ii. **Description**: Enter the brief description about the activity.
 - iii. **Activity Timeout (Seconds)**: Enter the number of seconds to wait for Generic AWS API Request activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. **Use Workflow Target**: Check this radio button to use the workflow target.
 - ii. **Override Workflow Target**: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the drop-down list. For more information, see [AWS Endpoint](#).
 - iii. **Use Workflow Target Group**: Check this radio button to use the workflow target group.
 - iv. **Override Workflow Target Group Criteria**: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. **Use Target's Default Account Key**: Check this radio button to use the target's default account key.
 - ii. **Override Account Key**: Check this radio button to override the workflow account key. You can select the appropriate Account Key or **+ADD NEW** from the drop-down list. For more information, see [AWS Credentials](#).
 - d. Under **AWS API Request**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. **URL**: Enter the relative URL for the API request from AWS.
 - ii. **API Method**: Enter the request method such as Get, Post, Put, etc.
 - iii. **Request Body**: Enter the request body that has to be received or sent.

Back to: [AWS Service](#)

IAM Attach User Policy

IAM Attach User Policy

Use the IAM Attach User Policy activity to attach the specified managed policy to the specified user.

1. In the Workflow Editor Toolbox, choose **AWS Service > IAM Attach User Policy** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for IAM Attach User Policy activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the drop-down list. For more information, see [AWS Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the drop-down list. For more information, see [AWS Credentials](#).
 - d. Under **IAM User**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Enter Username: Enter the IAM user name to attach the specified managed policy.
 - ii. Enter Policyarn: Enter the Amazon resources name (ARN) to identify resources in AWS.

Back to: [AWS Service](#)

IAM Create Access Key

IAM Create Access Key

Use the IAM Create Access Key activity to create access keys that are used as long time credentials for an IAM user.

1. In the Workflow Editor Toolbox, choose **AWS Service > IAM Create Access Key** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for IAM Create Access Key activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the drop-down list. For more information, see [AWS Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the drop-down list. For more information, see [AWS Credentials](#).
 - d. Under **IAM User**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Enter Username: Enter the IAM user name that the new key will belong to.

Back to: [AWS Service](#)

IAM Create User

IAM Create User

Use the IAM Create User activity to create a new IAM user for your AWS account.

1. In the Workflow Editor Toolbox, choose **AWS Service > IAM Create User** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for IAM Create User activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the drop-down list. For more information, see [AWS Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the drop-down list. For more information, see [AWS Credentials](#).
 - d. Under **IAM User**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Enter Username: Enter the user name that you like to create as an entity to represent a person or application that uses it to interact with AWS.

Back to: [AWS Service](#)

IAM List Policies

IAM List Policies

Use the IAM List Policies activity to lists all the managed policies that are available in your AWS account.

1. In the Workflow Editor Toolbox, choose **AWS Service > IAM List Policies** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for IAM List Policies activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the drop-down list. For more information, see [AWS Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the drop-down list. For more information, see [AWS Credentials](#).

Back to: [AWS Service](#)

IAM List Users

IAM List Users

Use the IAM List Users activity to list all the AWS identity and management users.

1. In the Workflow Editor Toolbox, choose **AWS Service > IAM List Users** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for IAM List Users activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the drop-down list. For more information, see [AWS Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the drop-down list. For more information, see [AWS Credentials](#).

Back to: [AWS Service](#)

Import Keypair

Import Keypair

To define the Import Keypair activity:

1. In the Workflow Editor Toolbox, choose **Activities > AWS Service > Import Keypair**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Import Keypair activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the drop-down list. For more information, see [AWS Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account Key or **+ADD NEW** from the drop-down list. For more information, see [AWS Credentials](#).
 - d. Under **EC2 Request**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Keypair Name: Enter the keypair name to be associated with the public key.
 - ii. Public Key: Enter the public key to be imported.

Back to: [AWS Service](#)

Reboot EC2 Instances

Reboot EC2 Instances

To define the Reboot EC2 Instances activity:

1. In the Workflow Editor Toolbox, choose **Activities > AWS Service > Reboot EC2 Instances**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. **Display Name**: Enter the unique display name for the activity.
 - ii. **Description**: Enter the brief description about the activity.
 - iii. **Activity Timeout (Seconds)**: Enter the number of seconds to wait for Reboot EC2 Instances activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. **Use Workflow Target**: Check this radio button to use the workflow target.
 - ii. **Override Workflow Target**: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [AWS Endpoint](#).
 - iii. **Use Workflow Target Group**: Check this radio button to use the workflow target group.
 - iv. **Override Workflow Target Group Criteria**: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. **Use Target's Default Account Key**: Check this radio button to use the target's default account key.
 - ii. **Override Account Key**: Check this radio button to override the workflow account key. You can select the appropriate Account Key or **+ADD NEW** from the dropdown list. For more information, see [AWS Credentials](#).
 - d. Under **EC2 Request**, specify the following information or click [Variable Reference](#) icon to choose any variable:
InstanceIDs: Click **+ADD** to enter the EC2 Instance ID to be rebooted.

Back to: [AWS Service](#)

Start EC2 Instances

Start EC2 Instances

To define the Start EC2 Instances activity:

1. In the Workflow Editor Toolbox, choose **Activities > AWS Service > Start EC2 Instances**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Start EC2 Instances activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [AWS Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account Key or **+ADD NEW** from the dropdown list. For more information, see [AWS Credentials](#).
 - d. Under **EC2 Request**, specify the following information:

InstanceIDs: Click **+ADD** to enter the EC2 Instance ID to start the EC2 instance.

Back to: [AWS Service](#)

Stop EC2 Instances

Stop EC2 Instances

To define the Stop EC2 Instances activity:

1. In the Workflow Editor Toolbox, choose **Activities > AWS Service > Stop EC2 Instances**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Stop EC2 Instances activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [AWS Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account Key or **+ADD NEW** from the dropdown list. For more information, see [AWS Credentials](#).
 - d. Under **EC2 Request**, specify the following information:
 - i. InstanceIDs: Click **+ADD** to enter the EC2 Instance ID to stop the EC2 instance.
 - ii. Force Stop: Check this check box to force stop the EC2 instance, even though the instance is running.

Back to: [AWS Service](#)

Terminate EC2 Instances

Terminate EC2 Instances

To define the Terminate EC2 Instances activity:

1. In the Workflow Editor Toolbox, choose **Activities**>**AWS Service**>**Terminate EC2 Instances**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Terminate EC2 Instances activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [AWS Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account Key or **+ADD NEW** from the dropdown list. For more information, see [AWS Credentials](#).
 - d. Under **EC2 Request**, specify the following information:

InstanceIDs: Click **+ADD** to enter the EC2 Instance ID to delete the EC2 instance.

Back to: [AWS Service](#)

Ansible Tower

Ansible Tower

The following sections display Ansible Tower activities:

- [Ansible Tower Get Job Info](#)
- [Ansible Tower Launch Job Template](#)

Ansible Tower Get Job Info

Use the Ansible Tower Get Job Info activity to get information and status about the job.

To define the Ansible Tower Get Job Info activity:

1. In the Workflow Editor Toolbox, choose **Activities>Meraki>Ansible Tower Get Job Info**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. **Display Name:** Enter the unique display name for the activity.
 - ii. **Description:** Enter the brief description about the activity.
 - iii. **Activity Timeout (Seconds):** Enter the number of seconds to wait for Ansible Tower Get Job Info activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. **Use Workflow Target:** Click this radio button to use the workflow target.
 - ii. **Override Workflow Target:** Click this radio button to override the workflow target. You can select the appropriate target or **ADD NEW** from the dropdown list. For more information, see [Ansible Tower Endpoint](#).
 - iii. **Use Workflow Target Group:** Check this radio button to use the workflow target group.
 - iv. **Override Workflow Target Group Criteria:** Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. **Use Target's Default Account Key:** Click this radio button to use the target's default account key.
 - ii. **Override Account Key:** Click this radio button to override the workflow account key. You can select the appropriate account key or **ADD NEW** from the dropdown list. For more information, see [Ansible Tower Credentials](#).
 - d. Under **Ansible Tower**, specify the following information or click [Variable Reference](#) icon to choose any variable:

Job ID: Enter the job ID to identify the job.

Back to: [Ansible Tower](#)

Ansible Tower Get Job Info

Ansible Tower Get Job Info

Use the Ansible Tower Get Job Info activity to get information and status about the job.

To define the Ansible Tower Get Job Info activity:

1. In the Workflow Editor Toolbox, choose **Activities > Meraki > Ansible Tower Get Job Info**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. **Display Name**: Enter the unique display name for the activity.
 - ii. **Description**: Enter the brief description about the activity.
 - iii. **Activity Timeout (Seconds)**: Enter the number of seconds to wait for Ansible Tower Get Job Info activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. **Use Workflow Target**: Click this radio button to use the workflow target.
 - ii. **Override Workflow Target**: Click this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Ansible Tower Endpoint](#).
 - iii. **Use Workflow Target Group**: Check this radio button to use the workflow target group.
 - iv. **Override Workflow Target Group Criteria**: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. **Use Target's Default Account Key**: Click this radio button to use the target's default account key.
 - ii. **Override Account Key**: Click this radio button to override the workflow account key. You can select the appropriate account key or **+ADD NEW** from the dropdown list. For more information, see [Ansible Tower Credentials](#).
 - d. Under **Ansible Tower**, specify the following information or click [Variable Reference](#) icon to choose any variable:

Job ID: Enter the job ID to identify the job.

Back to: [Ansible Tower](#)

Ansible Tower Launch Job Template

Ansible Tower Launch Job Template

Use the Ansible Tower Launch Job Template activity to execute a job template. A job template is a definition and set of parameters for running an Ansible job. Job templates are useful to execute the same job many times. Job templates also encourage the reuse of Ansible playbook content and collaboration between teams.

To define the Ansible Tower Launch Job Template activity:

1. In the Workflow Editor Toolbox, choose **Activities > Meraki > Ansible Tower Launch Job Template**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Ansible Tower Launch Job Template activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Click this radio button to use the workflow target.
 - ii. Override Workflow Target: Click this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the drop-down list. For more information, see [Ansible Tower Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Click this radio button to use the target's default account key.
 - ii. Override Account Key: Click this radio button to override the workflow account key. You can select the appropriate account key or **+ADD NEW** from the drop-down list. For more information, see [Ansible Tower Credentials](#).
 - d. Under **Ansible Tower Job Template**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Ansible Tower Job Template ID (Target should be defined before browsing required launch_variables): Select the job template ID to launch the job template.
 - ii. Launch Job Template Parameters: Enter the set of parameters for running an Ansible job.

Back to: [Ansible Tower](#)

CloudCenter Suite

CloudCenter Suite

The CloudCenter Suite is Cisco's hybrid cloud deployment platform. This platform takes a unique approach to install, configure, and maintain hybrid cloud environments that are often encountered by Information Technology (IT) departments to adopt business agility and improve time-to-market solutions within an enterprise. The CloudCenter Suite provides a solution that is cloud agnostic, works with diverse workloads, and integrates easily in an agile world.

The following sections display activities that are provided by the CloudCenter Suite adapter:

- [Add Billing Unit to Cost Group](#)
- [Add Cloud Account](#)
- [Associate Billing Unit to Cost Group](#)
- [Create Cost Group](#)
- [Find Billing Unit](#)
- [Find Cost Group](#)
- [Find Cost Group Type](#)
- [Generic CCS API Request](#)
- [Get Workload Manager Context](#)
- [Manage Deployment Environment](#)
- [Update Cost Group](#)
- [Execute Action on Virtual Machine](#)

Add Billing Unit to Cost Group

Add Billing Unit to Cost Group

Use the Add Billing Unit to Cost Group activity to associate a billing unit from the list of available billing units to the selected cost group under a specific cost group type.

1. In the Workflow Editor Toolbox, choose **Activities > CloudCenter Suite > Add Billing Unit to Cost Group**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. **Display Name**: Enter the unique display name for the activity.
 - ii. **Description**: Enter the brief description about the activity.
 - iii. **Activity Timeout (Seconds)**: Enter the number of seconds to wait for add billing unit to cost group activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. **Use Workflow Target**: Check this radio button to use the workflow target.
 - ii. **Override Workflow Target**: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [CloudCenter Endpoint](#).
- iii. **Use Workflow Target Group**: Check this radio button to use the workflow target group.
- iv. **Override Workflow Target Group Criteria**: Check this radio button to override the workflow target group criteria.
- c. Under **Credentials**, specify the following information:
 - i. **Use Target's Default Account Key**: Check this radio button to use the target's default account key.
 - ii. **Override Account Key**: Check this radio button to override the workflow account key. You can select the appropriate account key or **+ADD NEW** from the dropdown list. For more information, see [CloudCenter Suite Explicit User](#).
- d. Under **CloudCenter Suite**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. **Cost Group Type ID**: Enter the ID of the cost group type defined in the Cost Optimizer of CloudCenter Suite.
 - ii. **Cost Group ID**: Enter the ID of the cost group defined under specific cost group type in the Cost Optimizer of CloudCenter Suite.
 - iii. **Billing Unit ID**: Enter the ID of the billing unit defined under cost group type in the Cost Optimizer of CloudCenter Suite.



By default the target is *Suite Internal Target*, you will be able to override this default target using the *+Add New* option from the dropdown list.

Back to: [CloudCenter Suite](#)

Add Cloud Account

Add Cloud Account

Use the Add Cloud Account activity to add a cloud account.

1. In the Workflow Editor Toolbox, choose **Activities** > **CloudCenter Suite** > **Add Cloud Account**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for add cloud account activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [CloudCenter Endpoint](#).



By default the target is *Suite Internal Target*, you will be able to override this default target using the *+Add New* option from the dropdown list.

- iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
- c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate account key or **+ADD NEW** from the dropdown list. For more information, see [CloudCenter Suite Explicit User](#).
 - d. Under **Cloud Details**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Cloud Family: Select the cloud family from the dropdown list such as [Amazon](#), [AzureRM](#), [Google](#), [Kubernetes](#), [Openstack](#), [Vmware](#), and so forth.
 - ii. Cloud Instance: Select the cloud instance from the dropdown list based on the cloud family selected.
 - e. Under **Cloud Account Properties**, specify the following information based on the Cloud Family you have selected or click [Variable Reference](#) icon to choose any variable:



The following information should be used based on the Cloud Family selected.

Amazon

- i. Name: Enter the unique name for the Amazon cloud account.
- ii. Account Description: Enter the brief description about the account.
- iii. Email Address: Enter the email address of the Amazon account.
- iv. AWS Account Number: Enter the AWS account number.
- v. Access Key ID: Enter the AWS access key ID.
- vi. Secret Key: Enter the AWS secret key.

AzureRM

- i. Name: Enter the unique name for the Azure cloud account.
- ii. Account Description: Enter the brief description about the account.
- iii. Azure Login ID: Enter the login ID for the Azure account.
- iv. Azure Subscription ID: Enter the subscription ID associated with your Azure account.
- v. Tenant ID: Enter the Azure tenant ID.
- vi. Client ID: Enter the Azure Client ID.
- vii. Secret Key: Enter the appropriate secret key for the client ID.

Google

- i. Name: Enter the unique name for the Google cloud account.
- ii. Account Description: Enter the brief description about the account.
- iii. GCP Email Address: Enter the email address of the Google Cloud Platform (GCP).
- iv. GCP Service Account Key: Enter the GCP service account key.

Kubernetes

- i. Name: Enter the unique name for the Kubernetes cloud account.
- ii. Account Description: Enter the brief description about the account.

- iii. Service Account Name: Enter the Kubernetes service account name.
- iv. Check the **Show Service Account Token** check box to display the service account token.
- v. Service Account Token: Enter the service account token for the kubernetes account.

Openstack

- i. Name: Enter the unique name for the Openstack cloud account.
- ii. Account Description: Enter the brief description about the account.
- iii. Openstack UserName: Enter the Openstack user name.
- iv. Openstack Account Password: Enter the appropriate account password.
- v. Default Domain Name (V3): Enter the default domain name of Openstack version 3.
- vi. Default Domain ID: Enter the default domain ID of Openstack.
- vii. Default Tenant Name (V3 Project Name): Enter the default Tenant name of Openstack version 3.
- viii. Default Tenant ID (V3 Project ID): Enter the default Tenant ID of Openstack version 3

Vmware

- i. Name: Enter the unique name for the Vmware cloud account.
- ii. Account Description: Enter the brief description about the account.
- iii. vCenter UserName: Enter the user name for the vCenter account.
- iv. vCenter Password: Enter the appropriate password for the vCenter account.

Back to: [CloudCenter Suite](#)

Associate Billing Unit to Cost Group

Associate Billing Unit to Cost Group

Use the Associate Billing Unit to Cost Group activity to associate a billing unit from the list of available billing units to the selected cost group under a specific cost group type.

1. In the Workflow Editor Toolbox, choose **Activities > CloudCenter Suite > Associate Billing Unit to Cost Group**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. **Display Name**: Enter the unique display name for the activity.
 - ii. **Description**: Enter the brief description about the activity.
 - iii. **Activity Timeout (Seconds)**: Enter the number of seconds to wait for associate billing unit to cost group activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. **Use Workflow Target**: Check this radio button to use the workflow target.
 - ii. **Override Workflow Target**: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [CloudCenter Endpoint](#).
- iii. **Use Workflow Target Group**: Check this radio button to use the workflow target group.
- iv. **Override Workflow Target Group Criteria**: Check this radio button to override the workflow target group criteria.
- c. Under **Credentials**, specify the following information:
 - i. **Use Target's Default Account Key**: Check this radio button to use the target's default account key.
 - ii. **Override Account Key**: Check this radio button to override the workflow account key. You can select the appropriate account key or **+ADD NEW** from the dropdown list. For more information, see [CloudCenter Suite Explicit User](#).
- d. Under **CloudCenter Suite**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. **Cost Group Type**: Select the Cost Group Type from the drop-down list, which lists the cost group type defined in the Cost Optimizer of CloudCenter Suite.
 - ii. **Cost Group**: Select the cost group from the dropdown list, which lists the cost group defined under specific cost group type in the Cost Optimizer of CloudCenter Suite.
 - iii. **Billing Unit**: Select the billing unit from the dropdown list, which lists the billing units defined under cost group type in the Cost Optimizer of CloudCenter Suite.



By default the target is *Suite Internal Target*, you will be able to override this default target using the *+Add New* option from the dropdown list.

Back to: [CloudCenter Suite](#)

Create Cost Group

Create Cost Group

Use the Create Cost Group activity to create a cost group in the Cost Optimizer of CloudCenter Suite.

1. In the Workflow Editor Toolbox, choose **Activities > CloudCenter Suite > Create Cost Group**, then drag and drop the activity onto the Workflow pane.

2. On the Workflow Properties pane, enter the following information:

a. Under **General**, specify the following information:

- i. Display Name: Enter the unique display name for the activity.
- ii. Description: Enter the brief description about the activity.
- iii. Activity Timeout (Seconds): Enter the number of seconds to wait for create cost group type activity to fail because it timed out.
- iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.

b. Under **Target**, specify the following information:

- i. Use Workflow Target: Check this radio button to use the workflow target.
- ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [CloudCenter Endpoint](#).



By default the target is *Suite Internal* Target, you will be able to override this default target using the *+Add New* option from the dropdown list.

- iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
- iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.

c. Under **Credentials**, specify the following information:

- i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
- ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate account key or **+ADD NEW** from the dropdown list. For more information, see [CloudCenter Suite Explicit User](#).

d. Under **CloudCenter Suite**, specify the following information or click [Variable Reference](#) icon to choose any variable.

- i. Cost Group Name: Enter the cost group name to be created.
- ii. Cost Group Description: Enter the brief description about the cost group.
- iii. Cost Group Type: Select the cost group type from the dropdown list, which is defined under specific cost group type in the Cost Optimizer of CloudCenter Suite.
- iv. Parent: Select the parent cost group from the dropdown list. This is optional.
- v. Billing Unit: Select the billing unit from the dropdown list.

Back to: [CloudCenter Suite](#)

Find Billing Unit

Find Billing Unit

Use the Find Billing Unit activity to find the billing units used in the Cost Optimizer of CloudCenter Suite.

1. In the Workflow Editor Toolbox, choose **Activities** > **CloudCenter Suite** > **Find Billing Unit**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for find billing unit activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [CloudCenter Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
- c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate account key or **+ADD NEW** from the dropdown list. For more information, see [CloudCenter Suite Explicit User](#).
- d. Under **CloudCenter Suite**, specify the following information or click [Variable Reference](#) icon to choose any variable.
 - i. Cost Group Type ID: Enter the ID of the cost group type defined in the Cost Optimizer of CloudCenter Suite.
 - ii. Billing Unit Name: Enter the name of the billing unit defined under cost group type in the Cost Optimizer of CloudCenter Suite.



By default the target is *Suite Internal* Target, you will be able to override this default target using the *+Add New* option from the dropdown list.

Back to: [CloudCenter Suite](#)

Find Cost Group

Find Cost Group

Use the Find Cost Group activity to find the cost group used in the Cost Optimizer of CloudCenter Suite.

1. In the Workflow Editor Toolbox, choose **Activities > CloudCenter Suite > Find Cost Group**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. **Display Name**: Enter the unique display name for the activity.
 - ii. **Description**: Enter the brief description about the activity.
 - iii. **Activity Timeout (Seconds)**: Enter the number of seconds to wait for find cost group type activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. **Use Workflow Target**: Check this radio button to use the workflow target.
 - ii. **Override Workflow Target**: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [CloudCenter Endpoint](#).
 - iii. **Use Workflow Target Group**: Check this radio button to use the workflow target group.
 - iv. **Override Workflow Target Group Criteria**: Check this radio button to override the workflow target group criteria.
- c. Under **Credentials**, specify the following information:
 - i. **Use Target's Default Account Key**: Check this radio button to use the target's default account key.
 - ii. **Override Account Key**: Check this radio button to override the workflow account key. You can select the appropriate account key or **+ADD NEW** from the dropdown list. For more information, see [CloudCenter Suite Explicit User](#).
- d. Under **CloudCenter Suite**, specify the following information or click [Variable Reference](#) icon to choose any variable.
 - i. **Cost Group Type ID**: Enter the ID of the cost group defined under specific cost group type in the Cost Optimizer of CloudCenter Suite to be queried.
 - ii. **Cost Group Name**: Enter the cost group name to be queried.



By default the target is *Suite Internal* Target, you will be able to override this default target using the *+Add New* option from the dropdown list.

Back to: [CloudCenter Suite](#)

Find Cost Group Type

Find Cost Group Type

Use the Find Cost Group Type activity to find the cost group type used in the Cost Optimizer of CloudCenter Suite.

1. In the Workflow Editor Toolbox, choose **Activities** > **CloudCenter Suite** > **Find Cost Group Type**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. **Display Name**: Enter the unique display name for the activity.
 - ii. **Description**: Enter the brief description about the activity.
 - iii. **Activity Timeout (Seconds)**: Enter the number of seconds to wait for find cost group type activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. **Use Workflow Target**: Check this radio button to use the workflow target.
 - ii. **Override Workflow Target**: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [CloudCenter Endpoint](#).
- iii. **Use Workflow Target Group**: Check this radio button to use the workflow target group.
- iv. **Override Workflow Target Group Criteria**: Check this radio button to override the workflow target group criteria.
- c. Under **Credentials**, specify the following information:
 - i. **Use Target's Default Account Key**: Check this radio button to use the target's default account key.
 - ii. **Override Account Key**: Check this radio button to override the workflow account key. You can select the appropriate account key or **+ADD NEW** from the dropdown list. For more information, see [CloudCenter Suite Explicit User](#).
- d. Under **CloudCenter Suite**, specify the **Cost Group Type** or click [Variable Reference](#) icon to choose any variable.



By default the target is *Suite Internal* Target, you will be able to override this default target using the *+Add New* option from the dropdown list.

Back to: [CloudCenter Suite](#)

Generic CCS API Request

Generic CCS API Request

Use the Generic CCS API Request activity to make API requests to and from CloudCenter Suite.

1. In the Workflow Editor Toolbox, choose **Activities > CloudCenter Suite > Generic CCS API Request**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. **Display Name**: Enter the unique display name for the activity.
 - ii. **Description**: Enter the brief description about the activity.
 - iii. **Activity Timeout (Seconds)**: Enter the number of seconds to wait for generic CCS API request activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. **Use Workflow Target**: Check this radio button to use the workflow target.
 - ii. **Override Workflow Target**: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [CloudCenter Endpoint](#).
 - iii. **Use Workflow Target Group**: Check this radio button to use the workflow target group.
 - iv. **Override Workflow Target Group Criteria**: Check this radio button to override the workflow target group criteria.
- c. Under **Credentials**, specify the following information:
 - i. **Use Target's Default Account Key**: Check this radio button to use the target's default account key.
 - ii. **Override Account Key**: Check this radio button to override the workflow account key. You can select the appropriate account key or **+ADD NEW** from the dropdown list. For more information, see [CloudCenter Suite Explicit User](#).
- d. Under **CCS API Request**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. **Relative URL**: Enter the relative URL for the API request from CloudCenter Suite.
 - ii. **Method**: Enter the request method such as Get, Post, Put, and so forth.
 - iii. **Request Body**: Enter the request body that has to be received or sent.



By default the target is *Suite Internal* Target, you will be able to override this default target using the *+Add New* option from the dropdown list.

Back to: [CloudCenter Suite](#)

Get Workload Manager Context

Get Workload Manager Context

Use the Get Workload Manager Context activity to read details of a specific deployment whether currently undergoing or completed.

1. In the Workflow Editor Toolbox, choose **Activities** > **CloudCenter Suite** > **Get Workload Manager Context**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for get Workload Manager context activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [CloudCenter Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate account key or **+ADD NEW** from the dropdown list. For more information, see [CloudCenter Suite Explicit User](#).
 - d. Under **Workload Manager Configuration**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Workload Manager Configuration: Click **+ADD** to [Add Workload Manager configuration](#).
 - ii. Job ID: Click [Variable Reference](#) icon and choose **Workflow > Input > CC_RUN_ID** variable (Default is CC_RUN_ID variable).



By default the target is *Suite Internal* Target, you will be able to override this default target using the **+Add New** option from the dropdown list.



To create CC_RUN_ID variable

Create a new input variable with the following properties:

- Data Type: String
- Display Name: CC_RUN_ID
- Scope: Input

You can create the variable either from the workflow properties pane or choose *Variable > Global Variable > New Variable*. For more information, see [Configuring Variables](#).

Add Workload Manager Configuration

This section provides information on configuring Workload Manager.

1. Under **General**, select the appropriate Workflow Availability:
 - a. Lifecycle: Using the Lifecycle option you can automatically execute these actions based on a resources lifecycle. You can execute the action on a span of resources which contains the lifecycle action with the possible resources in this type of action are Application Profile, Service, and Cloud Region.
 - b. On Demand: Using the On Demand option you have to explicitly execute these actions from an individual object.
2. Under **Execute Action**, select where to run this type of action:
 - a. On Virtual Machine OS: On a VM with an agent installed.
 - b. External: On a Docker container that runs on the CCO (not dependent on the worker image in any way). For example, if you need to configure external CLIs on a Docker container for a specific cloud, you can determine a Custom Field with the CLI items in a list format.
3. Check the **Reboot the VM after action execution** check box if you want to reboot the VM after the action execution.
4. Check the **Sync VM information after action execution** check box if you want to sync the VM information after the action execution.



Step 3 & Step 4 is applicable only when On Demand is selected in Step 1.

5. Under **Resource Mappings**, Click **+ADD** to display the **Add Resource Mappings** dialog box provides the option to add the resource type and allows you to specify where this action has to be applied. The options in the add resource dialog box differs based on the Workflow Availability and Execute Action you select:
 - a. [Lifecycle > On Virtual Machine OS](#)
 - b. [Lifecycle > External](#)
 - c. [On Demand > On Virtual Machine OS](#)
 - d. [On Demand > External](#)
6. Click **Save**, to add the Workload Manager Configuration.



The action library action is created on the Workload Manager.

Lifecycle > On Virtual Machine OS

1. Under **General**, select the appropriate resource type:
 - a. Application Profile: An *application* in CloudCenter parlance refers to an installed/deployed *application* either before modeling or after deployment.
 - b. Service: A *service* is a mid-tier building block for an application.
2. Under **Applied To**, specify the following information:
 - a. Application Profile: Select the appropriate application profile from the dropdown list.
 - b. Service: Select the appropriate service from the dropdown list.
3. Click **Save**, to add the resource mappings.

Lifecycle > External

1. Under **General**, select the appropriate resource type:
 - a. Application Profile: An *application* in CloudCenter parlance refers to an installed/deployed *application* either before modeling or after deployment.
 - b. Service: A *service* is a mid-tier building block for an application.
 - c. Cloud Region: Workload Manager manages clouds on a per region basis, and the main point of that control is the cloud region API endpoint.
2. Under **Applied To**, specify the following information:
 - a. Application Profile: Select the appropriate application profile from the dropdown list.
 - b. Service: Select the appropriate service from the dropdown list.
 - c. Cloud Region: Select the appropriate cloud region from the dropdown list.
3. Click **Save**, to add the resource mappings.

On Demand > On Virtual Machine OS

1. Under **General**, select the appropriate resource type:
 - a. CloudCenter Deployed VMs
 - b. Imported VMs With Agent Installed



You can use Step 2 or Step 3 based on the choice in Step 1.

2. Under **CloudCenter Deployed VMs**, specify the applied to information from the appropriate dropdown list:
 - a. Application Profile: Select the appropriate application profile from the dropdown list.
 - b. Cloud Region: Select the appropriate cloud region from the dropdown list.
 - c. Cloud Account: Select the appropriate cloud account from the dropdown list.
 - d. Service: Select the appropriate service from the dropdown list.
3. Under **Imported VMs with Agent Installed**, specify the applied to information from the appropriate dropdown list:
 - a. Cloud Region: Select the appropriate cloud region from the dropdown list.
 - b. Cloud Account: Select the appropriate cloud account from the dropdown list.
 - c. OS Types: Select the OS types from the dropdown list such as Linux or Windows.
4. Click **Save**, to add the resource mappings.

On Demand > External

1. Under **General**, select the appropriate resource type:
 - a. CloudCenter Deployed VMs
 - b. Imported VMs With Agent Installed



You can use Step 2 or Step 3 based on the choice in Step 1.

2. Under **CloudCenter Deployed VMs**, specify the applied to information from the appropriate dropdown list:
 - a. Application Profile: Select the appropriate application profile from the dropdown list.
 - b. Cloud Region: Select the appropriate cloud region from the dropdown list.
 - c. Cloud Account: Select the appropriate cloud account from the dropdown list.
 - d. Service: Select the appropriate service from the dropdown list.
3. Under **Imported VMs with Agent Installed**, specify the applied to information from the appropriate dropdown list:
 - a. Cloud Region: Select the appropriate cloud region from the dropdown list.
 - b. Cloud Account: Select the appropriate cloud account from the dropdown list.
 - c. OS Types: Select the OS types from the dropdown list such as Linux or Windows.
4. Click **Save**, to add the resource mappings.


Back to: [CloudCenter Suite](#)

Manage Deployment Environment

Manage Deployment Environment

Use the Manage Deployment Environment activity to manage the deployment environments and perform management actions.

1. In the Workflow Editor Toolbox, choose **Activities > CloudCenter Suite > Manage Deployment Environment**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. **Display Name**: Enter the unique display name for the activity.
 - ii. **Description**: Enter the brief description about the activity.
 - iii. **Activity Timeout (Seconds)**: Enter the number of seconds to wait for manage deployment environment activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. **Use Workflow Target**: Check this radio button to use the workflow target.
 - ii. **Override Workflow Target**: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [CloudCenter Endpoint](#).

 By default the target is *Suite Internal* Target, you will be able to override this default target using the *+Add New* option from the dropdown list.

 - iii. **Use Workflow Target Group**: Check this radio button to use the workflow target group.
 - iv. **Override Workflow Target Group Criteria**: Check this radio button to override the workflow target group criteria.


- c. Under **Credentials**, specify the following information:
 - i. **Use Target's Default Account Key**: Check this radio button to use the target's default account key.
 - ii. **Override Account Key**: Check this radio button to override the workflow account key. You can select the appropriate account key or **+ADD NEW** from the dropdown list. For more information, see [CloudCenter Suite Explicit User](#).
- d. Under **Environment**, specify the following information:
 - i. **Deployment Environment**: Select the deployment environments from the dropdown list that is currently defined in Workload Manager.
 - ii. **Region**: Select the region from the dropdown list that is currently defined in Workload Manager.
- e. Under **Management Actions**, select the **Manage Action** from the dropdown list such as Add Cloud Account.

Back to: [CloudCenter Suite](#)

Update Cost Group

Update Cost Group

Use the Update Cost Group activity to update or modify the cost group used in the Cost Optimizer of CloudCenter Suite.

1. In the Workflow Editor Toolbox, choose **Activities** > **CloudCenter Suite** > **Update Cost Group**, then drag and drop the activity onto the Workflow pane.
 2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for update cost group type activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [CloudCenter Endpoint](#).
-  By default the target is *Suite Internal* Target, you will be able to override this default target using the *+Add New* option from the dropdown list.
- iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
- c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate account key or **+ADD NEW** from the dropdown list. For more information, see [CloudCenter Suite Explicit User](#).
- d. Under **CloudCenter Suite**, specify the following information or click [Variable Reference](#) icon to choose any variable.
 - i. Cost Group Type: Select the cost group type from the drop-down list defined under specific cost group type in the Cost Optimizer of CloudCenter Suite.
 - ii. Cost Group: Select the cost group from the dropdown list, which lists the cost group defined under specific cost group type in the Cost Optimizer of CloudCenter Suite.
 - iii. Cost Group Name: Enter the cost group name to be created.
 - iv. Cost Group Description: Enter the brief description about the cost group.
 - v. Parent: Select the parent cost group from the dropdown list. This is optional.
 - vi. Billing Unit: Select the billing unit from the dropdown list.

Back to: [CloudCenter Suite](#)

Execute Action on Virtual Machine

Execute Action on Virtual Machine

Execute Action on Virtual Machine is an atomic workflow activity used to execute a command or script on a Virtual Machine as part of application deployment. The workflow with Execute Action on Virtual Machine must include [Get Workload Manager Context](#) activity as the first step to create integration with Workload Manager. Perform the following steps to execute an action on a Virtual Machine:

1. In the Workflow Editor Toolbox, choose **Activities > CloudCenter Suite > Execute Action on Virtual Machine**, then drag and drop the activity onto the Workflow pane.



You have to import this atomic workflow from the Cisco public repository to view Execute Action on Virtual Machine as an activity under CloudCenter Suite activity. For more information on adding a repository and importing workflow, see [Add Git Repository](#) and [Import Workflows](#).

2. On the Workflow Properties pane, enter the following information:
 - a. Get CloudCenter Context Response: Click [Variable Reference](#) icon and choose **Activities > Get Workload Manager Context > Response Body** and click **Save**.
 - b. Node ID: Click [Variable Reference](#) icon and choose **Workflow > Input > NODE_ID** and click **Save** for lifecycle workflow or enter **Null** for on demand workflow.



To create NODE_ID variable

Create a new input variable with the following properties:

- Data Type: String
- Display Name: NODE_ID
- Scope: Input

You can create the variable either from the workflow properties pane or choose *Variable > Global Variable > New Variable*. For more information, see [Configuring Variables](#).

- c. Action Type: Click [Variable Reference](#) icon and choose **Activities > Get Workload Manager Context > Action Type** and click **Save**.
- d. Script: Enter the script or command to be executed on the Virtual Machine. The script may be a shell script for Linux or a PowerShell script for Windows Virtual Machines.



All other properties in this activity are auto-populated, do not modify.

Back to: [CloudCenter Suite](#)

Database Activities

Database Activities

The following are database activities that are executed using Java Database Connectivity (JDBC):

- [Call Procedure Via JDBC](#)
- [Delete from Table Via JDBC](#)
- [Insert Bulk into Table Via JDBC](#)
- [Insert into Table Via JDBC](#)
- [Select from Table Via JDBC](#)
- [Update Table Via JDBC](#)

Call Procedure Via JDBC

Call Procedure Via JDBC

Use the call procedure via JDBC activity to call a database procedure using the specified JDBC connection.

1. In the Workflow Editor Toolbox, choose **Activities > Database Activities > Call Procedure Via JDBC**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [JDBC Database Server](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate account key or **+ADD NEW** from the dropdown list. For more information, see [JDBC Login Credentials](#).
 - d. Under **Call Procedure**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Procedure Name: Enter the name of the database procedure to call.
 - ii. Persist Table: Check this check box to perform query against data that has already been summarized, this helps reducing the query time and database load.
 - iii. Read all columns from the procedure: Check this check box to read all the columns from the call.
 - iv. Under **Stored procedure inputs**, enter the appropriate information:
 1. Parameter name: Enter the appropriate parameter name.
 2. Parameter type: Select the appropriate data type from the dropdown list such as IN, IN/OUT, and OUT.
 3. Parameter value type: Select the appropriate data type from the dropdown list such as Boolean, Decimal, Integer, and String.
 4. Parameter value: Enter the appropriate parameter value.
 - v. Columns to read: Click **+ADD** to enter the **Column Name** and select the **Column Type** from dropdown list such as Boolean, integer, number, and so forth.
 - vi. Number of rows to return: The maximum number of rows to display (default is 200).

Back to: [Database Activities](#)

Delete from Table Via JDBC

Delete from Table Via JDBC

Use the delete from table via JDBC activity to delete column from the table by executing SQL query.

1. In the Workflow Editor Toolbox, choose **Activities**>**Database Activities**>**Delete from Table Via JDBC**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [JDBC Database Server](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate account key or **+ADD NEW** from the dropdown list. For more information, see [JDBC Login Credentials](#).
 - d. Under **Read Table**, enter the **SQL query to be executed** or click [Variable Reference](#) icon to choose any variable. For example, sample query to delete a column:

```
Simple DELETE statement  
DELETE from mytable where mycolumn = 'zzz'
```

Back to: [Database Activities](#)

Insert Bulk into Table Via JDBC

Insert Bulk into Table Via JDBC

The insert bulk into table via JDBC activity provides source table for data inserted into a database.

1. In the Workflow Editor Toolbox, choose **Activities>Database Activities>Insert Bulk into Table Via JDBC**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [JDBC Database Server](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate account key or **+ADD NEW** from the dropdown list. For more information, see [JDBC Login Credentials](#).
 - d. Under **Insert Table**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Source data: Enter the source data to be inserted into the database.
 - ii. Name of the target table: Enter the name of the target table in which the data has to be inserted.
 - iii. Columns to write: Click **+ADD** to enter the appropriate information:
 1. Source column: Enter the source column name.
 2. Column type: Select the column type from dropdown list such as Boolean, Decimal, Integer, and String.
 3. Target Column: Enter the target column.

Back to: [Database Activities](#)

Insert into Table Via JDBC

Insert into Table Via JDBC

Use the insert into table via JDBC activity to insert values into the table by executing SQL query.

1. In the Workflow Editor Toolbox, choose **Activities>Database Activities>Insert into Table Via JDBC**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [JDBC Database Server](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate account key or **+ADD NEW** from the dropdown list. For more information, see [JDBC Login Credentials](#).
 - d. Under **Read Table**, enter the SQL query to be executed or click [Variable Reference](#) icon to choose any variable. For example, this query inserts values into a table:

```
into mytable (column1,column2) VALUES ('val1','val2')
```

Back to: [Database Activities](#)

Select from Table Via JDBC

Select from Table Via JDBC

Use the select from table via JDBC activity to read table by executing the SQL query.

1. In the Workflow Editor Toolbox, choose **Activities**>**Database Activities**>**Select from Table Via JDBC**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [JDBC Database Server](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate account key or **+ADD NEW** from the dropdown list. For more information, see [JDBC Login Credentials](#).
 - d. Under **Read Table**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. SQL query to execute: Enter the SQL query to be executed. The data in the database is case-sensitive. For example, this is a sample query that selects specific columns from a table:
 - `SELECT column1, column2 from mytable`
 - This is a sample query that selects the country code and the name of the country:
 - `SELECT code, name from country`
 - ii. Persist Table: Check this check box to perform query against data that has already been summarized, this helps reducing the query time and database load.
 - iii. Read all columns from SQL Query: Check this check box to read all the columns from the SQL query.
 - iv. Columns to read: Click **+ADD** to enter the column name and select the type from dropdown list such as Boolean, Date Time, Decimal, Integer, and String.
 - v. Number of rows to return: The maximum number of rows to display (default=200).

Back to: [Database Activities](#)

Update Table Via JDBC

Update Table Via JDBC

Use the update table via JDBC activity to update columns in table by executing SQL query.

1. In the Workflow Editor Toolbox, choose **Activities**>**Database Activities**>**Update Table Via JDBC**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [JDBC Database Server](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate account key or **+ADD NEW** from the dropdown list. For more information, see [JDBC Login Credentials](#).
 - d. Under **Read Table**, enter the **SQL query to be executed** or click [Variable Reference](#) icon to choose any variable. For example, this query updates columns in a table:

```
Update mytable set column1 = 'newvalue' where column2 = 'zzz'
```

Back to: [Database Activities](#)

Email

Email

Use the Email activity to specify the information required for sending an email as part of the process. The following section display Email activity:

- [Send Email](#)

Send Email

Send Email

The Send Email adapter provides the ability to send email messages to a specified user.

1. In the Workflow Editor Toolbox, choose **Activities>Email>Send Email**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the Send Email activity.
 - ii. Description: Enter the brief description about the Send Email activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Send Email activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [SMTP Endpoint](#) or [POP3 Endpoint](#) or [IMAP Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key User: Check this radio button to use the target's default account key user.
 - ii. Override Account Key User: Check this radio button to override the workflow account key user. You can select the appropriate Account Key User ID or **+ADD NEW** from the dropdown list. For more information, see [Email Credentials](#).
 - d. Under **Email**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. To: Enter the email address of the primary recipient(s) of the email.
 - ii. CC: Enter the email address of the recipient(s) who are to be carbon-copied on the email.
 - iii. BCC: Enter the email address of the recipient(s) who are to blind carbon-copied on the email.
 - iv. Subject: Enter the subject heading of the email.
 - v. Message: Enter the content of the message in the body of the email.
 - vi. Send as HTML: Check this check box to send Email as HTML.

Back to: [Email](#)

Google Cloud Platform

Google Cloud Platform

Google Cloud Platform (GCP) is a suite of cloud computing services. GCP allows you to compute, store, and develop application that run on Google Hardware.

The following sections display activities that are provided by the Google Cloud Platform adapter:

- [Configure IAM Permissions](#)
- [Create Firewall Rule](#)
- [Create Instance](#)
- [Create Project](#)
- [Create Service Account](#)
- [Create VPC Network](#)
- [Delete Firewall Rule](#)
- [Delete Instance](#)
- [Delete VPC Network](#)
- [Generic GCP API Request](#)
- [Get Firewall Rule](#)
- [Get Instances Details](#)
- [Get Project Details](#)
- [Get VPC Network](#)
- [List Firewall Rules](#)
- [List Instances Templates](#)
- [List Instances](#)
- [List Machine Types](#)
- [List VPC Networks](#)
- [List Zones](#)
- [Update Firewall Rule](#)
- [Update VPC Network](#)

Configure IAM Permissions

Configure IAM Permissions

Use the Configure IAM Permissions activity to configure identity and access management permissions. Which lets you manage access control by defining who has what access for which resource.

1. In the Workflow Editor Toolbox, choose **Google Cloud Platform >Configure IAM Permissions** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Configure IAM Permissions activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the drop-down list. For more information, see [Google Cloud Platform Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the drop-down list. For more information, see [Google Cloud Platform Authentication](#).
 - d. Under **GCP Configure IAM Permissions**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Project ID: Enter the unique identifier of the project.
 - ii. Service Account: Enter the GCP service account that has to be configured for IAM permissions.
 - iii. Role: Enter the specific roles to be given access to specific GCP resources.

Back to: [Google Cloud Platform](#)

Create Firewall Rule

Create Firewall Rule

Use the Create Firewall Rule activity to create Firewall Rule. The firewall rule provides provision to allow or deny traffic to and from your Virtual Machine (VM) based on the configurations you specify.

1. In the Workflow Editor Toolbox, choose **Google Cloud Platform >Create Firewall Rule** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Create Firewall Rule activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Google Cloud Platform Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the dropdown list. For more information, see [Google Cloud Platform Authentication](#).
 - d. Under **Google Cloud Platform**, specify the following information or click [Variable Reference](#) icon to choose any variable:

Field	Description
Project ID	Enter the unique identifier of the project.
Firewall Rule Name	Enter the name for the firewall rule.
Firewall Action	Select Allow or Deny action from the dropdown list.
Firewall Description	Enter the description about the firewall rule.
Network	Enter the network for which the firewall rule has to be applied.
Direction of Traffic	Choose EGRESS (outgoing traffic) or INGRESS (incoming traffic) direction from the dropdown list.
Priority for this Rule	Enter an integer from 0 to 65535, inclusive. Lower integer indicate higher priorities.
IP Protocol	Select the IP protocol from the dropdown list such as AH, ESP, ICMP, IPIP, SCTP, TCP, UDP, and so forth, to narrow the scope of the firewall rule.
Ports	Enter the port number or port range for the firewall rule.
Source Range	Specify the ranges of IP addresses as sources of packets. The source parameter is only applicable to ingress rules.
Destination Range	Specify the ranges of IP addresses. The destination parameter is only applicable to egress rules.
Source Tags	Enter the source tags to limit the source by network tag.
Target Tags	Enter the target tags, if you want to apply the rule to select instances by network (target) tags.
Source Service Accounts	Enter the service account name to limit the source by service account.
Target Service Accounts	Enter the service account name to apply the rule to select instances by associated service accounts.

[Back to: Google Cloud Platform](#)

Create Instance

Create Instance

Use the Create Instance activity to create a new instance in Google cloud Platform.

1. In the Workflow Editor Toolbox, choose **Google Cloud Platform > Create Instances** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Create Instances activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the drop-down list. For more information, see [Google Cloud Platform Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the drop-down list. For more information, see [Google Cloud Platform Authentication](#).
 - d. Under **Google Cloud Platform**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Project ID: Enter the unique identifier of the project.
 - ii. Zone Name: Enter the zone name to host your resources.
 - iii. Source Instance Template URL: Enter the source instance template URL.
 - iv. Type of Machine: Enter the machine type for your instance.
 - v. Name of Instance: Enter the name for your instance.

Back to: [Google Cloud Platform](#)

Create Project

Create Project

Use the Create Project activity to create a new project in Google Cloud Platform.

1. In the Workflow Editor Toolbox, choose **Google Cloud Platform >Create Project** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Create Project activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Google Cloud Platform Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the dropdown list. For more information, see [Google Cloud Platform Authentication](#).
 - d. Under **Google Cloud Platform**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Project ID: Enter the unique identifier for the project.
 - ii. Project Name: Enter the unique name for the project.

Back to: [Google Cloud Platform](#)

Create Service Account

Create Service Account

Use the Create Service Account activity to create a new service account.

1. In the Workflow Editor Toolbox, choose **Google Cloud Platform >Create Service Account** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Create Service Account activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the drop-down list. For more information, see [Google Cloud Platform Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the drop-down list. For more information, see [Google Cloud Platform Authentication](#).
 - d. Under **Google Cloud Platform**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Account ID: Enter the unique identifier for the service account.
 - ii. Project ID: Enter the unique identifier for the service account.
 - iii. Account Name: Enter a name for the service account.

Back to: [Google Cloud Platform](#)

Create VPC Network

Create VPC Network

Use the Create VPC Network activity to create a new VPC network in Google Cloud Platform .

1. In the Workflow Editor Toolbox, choose **Google Cloud Platform >Create VPC Network** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Create VPC Network activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Google Cloud Platform Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the dropdown list. For more information, see [Google Cloud Platform Authentication](#).
 - d. Under **Google Cloud Platform**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Project ID: Enter the unique identifier of the project.
 - ii. Network Name: Enter a name for the network.
 - iii. Auto Create Subnetworks: Select **True** or **False** from the dropdown list to either create or not to create subnetworks automatically.
 - iv. Routing Mode: Select **Global** or **Regional** from the dropdown list either to route to all the subnets in the VPC network regardless of the region or to route to the subnets in the same region as the Cloud Router.
 - v. IPV4 Range: Enter the broader CIDR block for IPV4 range.

Back to: [Google Cloud Platform](#)

Delete Firewall Rule

Delete Firewall Rule

Use the Delete Firewall Rule activity to delete the firewall rule.

1. In the Workflow Editor Toolbox, choose **Google Cloud Platform >Delete Firewall Rule** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Delete Firewall Rule activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Google Cloud Platform Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the dropdown list. For more information, see [Google Cloud Platform Authentication](#).
 - d. Under **Google Cloud Platform**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Project ID: Enter the unique identifier of the project.
 - ii. Firewall Rule Name: Enter the firewall rule name to be deleted.

Back to: [Google Cloud Platform](#)

Delete Instance

Delete Instance

Use the Delete Instance activity to delete the instance in Google Cloud Platform.

1. In the Workflow Editor Toolbox, choose **Google Cloud Platform>Delete Instance** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Delete Instance activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Google Cloud Platform Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the dropdown list. For more information, see [Google Cloud Platform Authentication](#).
 - d. Under **Google Cloud Platform**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Project ID: Enter the unique identifier of the project.
 - ii. Zone Name: Enter the zone name of the instance.
 - iii. Instance Name: Enter the instance name to be deleted.

Back to: [Google Cloud Platform](#)

Delete VPC Network

Delete VPC Network

Use the Delete VPC Network activity to delete the VPC network in Google Cloud Platform.

1. In the Workflow Editor Toolbox, choose **Google Cloud Platform >Delete VPC Network** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Delete VPC Network activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Google Cloud Platform Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the dropdown list. For more information, see [Google Cloud Platform Authentication](#).
 - d. Under **Google Cloud Platform**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Project Name: Enter the name of the project to be deleted.
 - ii. Network Name: Enter the name of the VPC network to be deleted.

Back to: [Google Cloud Platform](#)

Generic GCP API Request

Generic GCP API Request

Use the Generic GCP API Request activity to request API in Google Cloud Platform.

1. In the Workflow Editor Toolbox, choose **Google Cloud Platform >Generic GCP API Request** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Generic GCP API Request activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Google Cloud Platform Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the dropdown list. For more information, see [Google Cloud Platform Authentication](#).
 - d. Under **GCP API Request**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. URL: Enter the relative URL for the API request from Google Cloud Platform.
 - ii. API Method: Enter the request method such as Get, Post, Put, and so forth.
 - iii. Request Body: Enter the request body that has to be received or sent.

Back to: [Google Cloud Platform](#)

Get Firewall Rule

Get Firewall Rule

Use the Get Firewall Rule activity to view the firewall rules details to inspect a firewall rule to see it's name, applicable network, and components.

1. In the Workflow Editor Toolbox, choose **Google Cloud Platform** > **Get Firewall Rule** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Get Firewall Rule activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the drop-down list. For more information, see [Google Cloud Platform Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the drop-down list. For more information, see [Google Cloud Platform Authentication](#).
 - d. Under **Google Cloud Platform**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Project ID: Enter the unique identifier of the project to be viewed.
 - ii. Firewall Rule Name: Enter the firewall rule name to be viewed.

Back to: [Google Cloud Platform](#)

Get Instances Details

Get Instances Details

Use the Get Instances Details activity to view the details of instances in Google Cloud Platform.

1. In the Workflow Editor Toolbox, choose **Google Cloud Platform >Get Instances Details** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Get Instances Details activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the drop-down list. For more information, see [Google Cloud Platform Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the drop-down list. For more information, see [Google Cloud Platform Authentication](#).
 - d. Under **Google Cloud Platform**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Project ID: Enter the unique identifier of the project to be viewed.
 - ii. Zone Name: Enter the zone name of the instance.
 - iii. Instance Name: Enter the instance name to be viewed.

Back to: [Google Cloud Platform](#)

Get Project Details

Get Project Details

Use the Get Project Details activity to view the project details in Google Cloud Platform.

1. In the Workflow Editor Toolbox, choose **Google Cloud Platform >Get Project Details** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Get Project Details activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the drop-down list. For more information, see [Google Cloud Platform Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the drop-down list. For more information, see [Google Cloud Platform Authentication](#).
 - d. Under **Google Cloud Platform**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Project ID: Enter the unique identifier of the project to be queried.

Back to: [Google Cloud Platform](#)

Get VPC Network

Get VPC Network

Use the Get VPC Network activity to view the VPC network details in Google Cloud Platform.

1. In the Workflow Editor Toolbox, choose **Google Cloud Platform >Get VPC Network** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Get VPC Network activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the drop-down list. For more information, see [Google Cloud Platform Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the drop-down list. For more information, see [Google Cloud Platform Authentication](#).
 - d. Under **Google Cloud Platform**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Project ID: Enter the unique identifier of the project to be viewed.
 - ii. Network Name: Enter the VPC network name to be viewed.

Back to: [Google Cloud Platform](#)

List Firewall Rules

List Firewall Rules

Use the List Firewall Rules activity to list all firewall rules for all networks in your project in Google Cloud Platform.

1. In the Workflow Editor Toolbox, choose **Google Cloud Platform >List Firewall Rules** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for List Firewall Rules activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the drop-down list. For more information, see [Google Cloud Platform Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the drop-down list. For more information, see [Google Cloud Platform Authentication](#).
 - d. Under **Google Cloud Platform**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Project ID: Enter the unique identifier of the project to list the firewalls rules in GCP.

Back to: [Google Cloud Platform](#)

List Instances Templates

List Instances Templates

Use the `List Instances Templates` activity to list all the instance templates in your project in Google Cloud Platform.

1. In the Workflow Editor Toolbox, choose **Google Cloud Platform >List Instances Templates** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for `List Instances Templates` activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the drop-down list. For more information, see [Google Cloud Platform Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the drop-down list. For more information, see [Google Cloud Platform Authentication](#).
 - d. Under **Google Cloud Platform**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Project ID: Enter the unique identifier of the project to list the instances templates in GCP.

Back to: [Google Cloud Platform](#)

List Instances

List Instances

Use the List Instances activity to list all the instances in your project in Google Cloud Platform.

1. In the Workflow Editor Toolbox, choose **Google Cloud Platform >List Instances** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for List Instances activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the drop-down list. For more information, see [Google Cloud Platform Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the drop-down list. For more information, see [Google Cloud Platform Authentication](#).
 - d. Under **Google Cloud Platform**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Project ID: Enter the unique identifier of the project to list the instances.
 - ii. Zone Name: Enter the zone name of the instance.

Back to: [Google Cloud Platform](#)

List Machine Types

List Machine Types

Use the List Machine Types activity to list all the machine types in your project in Google Cloud Platform.

1. In the Workflow Editor Toolbox, choose **Google Cloud Platform >List Machine Types** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for List Machine Types activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the drop-down list. For more information, see [Google Cloud Platform Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the drop-down list. For more information, see [Google Cloud Platform Authentication](#).
 - d. Under **Google Cloud Platform**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Project ID: Enter the unique identifier of the project to list the machine types in GCP.
 - ii. Zone Name: Enter the zone name from which the machine types has to be listed.

Back to: [Google Cloud Platform](#)

List VPC Networks

List VPC Networks

Use the List VPC Networks activity to list all the VPC networks in your project in Google Cloud Platform.

1. In the Workflow Editor Toolbox, choose **Google Cloud Platform >List VPC Networks** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for List VPC Networks activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the drop-down list. For more information, see [Google Cloud Platform Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the drop-down list. For more information, see [Google Cloud Platform Authentication](#).
 - d. Under **Google Cloud Platform**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Project ID: Enter the unique identifier of the project to list the VPC networks in GCP.

Back to: [Google Cloud Platform](#)

List Zones

List Zones

Use the List Zones activity to list all the zones in your project in Google Cloud Platform.

1. In the Workflow Editor Toolbox, choose **Google Cloud Platform >List Zones** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for List Zones activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the drop-down list. For more information, see [Google Cloud Platform Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the drop-down list. For more information, see [Google Cloud Platform Authentication](#).
 - d. Under **Google Cloud Platform**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Project ID: Enter the unique identifier of the project to list the zones in GCP.

Back to: [Google Cloud Platform](#)

Update Firewall Rule

Update Firewall Rule

Use the Update Firewall Rule activity to modify any component of a firewall rule except for its name, its network, the action, and the direction of traffic. If you need change these parameters you have to delete the rule and create a new rule instead.

1. In the Workflow Editor Toolbox, choose **Google Cloud Platform > Update Firewall Rule** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for update firewall rule activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Google Cloud Platform Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the dropdown list. For more information, see [Google Cloud Platform Authentication](#).
 - d. Under **Google Cloud Platform**, specify the following information or click [Variable Reference](#) icon to choose any variable:

Field	Description
Project ID	Enter the unique identifier of the project to be updated.
Firewall Rule Name	Enter the name for the firewall rule to be updated.
IP Protocol	Select the IP protocol from the dropdown list such as AH, ESP, ICMP, IPIP, SCTP, TCP, UDP, and so forth, to narrow the scope of the firewall rule.
Ports	Enter the port number or port range for the firewall rule.
Firewall Description	Enter the description about the firewall rule.
Source Range	Specify the ranges of IP addresses as sources of packets. The source parameter is only applicable to ingress rules.
Source Tags	Enter the source tags to limit the source by network tag.
Target Tags	Enter the target tags, if you want to apply the rule to select instances by network (target) tags.

Back to: [Google Cloud Platform](#)

Update VPC Network

Update VPC Network

Use the Update VPC Network activity to modify the VPC networks.

1. In the Workflow Editor Toolbox, choose **Google Cloud Platform >Update VPC Network** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Update VPC Network activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Google Cloud Platform Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the dropdown list. For more information, see [Google Cloud Platform Authentication](#).
 - d. Under **Google Cloud Platform**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Project ID: Enter the unique identifier of the project to be updated.
 - ii. Network Name: Enter the name of the network.
 - iii. Routing Mode: Select **Global** or **Regional** from the dropdown list as routing mode.

Back to: [Google Cloud Platform](#)

KAFKA

KAFKA

Kafka is a distributed streaming platform. Kafka works well as a replacement for a more traditional message broker. Message brokers are used for a variety of reasons (to decouple processing from data producers, to buffer unprocessed messages, and so forth). In comparison to most messaging systems Kafka has better throughput, built-in partitioning, replication, and fault-tolerance, making it a good solution for large scale message processing applications.

A streaming platform has 3 key capabilities:

1. Publish and subscribe to streams of records, similar to a message queue or enterprise messaging system.
2. Store streams of records in a fault-tolerant durable way.
3. Process streams of records as they occur.

Kafka is generally used for 2 broad classes of applications:

1. Building real-time streaming data pipelines that reliably get data between systems or applications.
2. Building real-time streaming applications that transform or react to the streams of data.

The following section display Kafka activity:

- [Submit Kafka Message](#)

Submit Kafka Message

Submit Kafka Message

To define the Submit Kafka Message activity:

1. In the Workflow Editor Toolbox, choose **Activities > Kafka > Submit Kafka Message**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Submit Kafka Message activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [KAFKA Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account Key or **+ADD NEW** from the dropdown list. For more information, see [Kafka Certificate Authentication](#) or [Kafka Authentication](#).
 - d. Under **Message**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Topic Name: Enter the Topic name to be associated with the message.
 - ii. Message Headers: Click **+ADD**, to enter the **Header** and **Value** for the message.
 - iii. KafkaMessage Details: Enter the message to be published.

Back to: [KAFKA](#)

Meraki

Meraki

Meraki products are built from the ground up for cloud management, and come out of the box with centralized management, layer 7 device and application visibility, real time web-based diagnostics, monitoring, reporting, and much more. Meraki deploys quickly and easily, without training or proprietary command line interfaces.

The Meraki adapter integrates with Meraki through its Dashboard APIs. The adapter provides activities to provision networks, devices, and to manage networks in an organization. The following sections display Meraki activities:

- [Bind Network to a Template](#)
- [Claim Device into a Network](#)
- [Create Network](#)
- [Delete Network](#)
- [Get Organizations](#)
- [List Configuration Templates](#)
- [List Networks](#)
- [List VLANS of a Network](#)
- [Update Network](#)

Bind Network to a Template

Bind Network to a Template

Use the Bind Network to a Template activity to bind any network to template.

Networks within Organization can be bound to a template so that they can inherit the settings and only has to be configured once. If this configuration is no longer required they can be bound to a different template, or reverted to the configuration state they had before they were bound. This reduces monotonous administrative tasks and prevents human error.

To define the Bind Network to a Template activity:

1. In the Workflow Editor Toolbox, choose **Activities > Meraki > Bind Network to a Template**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Bind Network to a Template activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Click this radio button to use the workflow target.
 - ii. Override Workflow Target: Click this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Meraki Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Click this radio button to use the target's default account key.
 - ii. Override Account Key: Click this radio button to override the workflow account key. You can select the appropriate account key or **+ADD NEW** from the dropdown list. For more information, see [Meraki Credentials](#).
 - d. Under **Meraki**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Network ID: Enter the network ID of the device to bind to a template.
 - ii. Template ID: Enter the configuration template ID to which the network should be bound.
 - iii. Autobind: Select true or false from the drop-down list, to indicate whether the network's switches should automatically bind to profiles of the same model,



This option only affects switch networks and switch templates. Auto-bind is not valid unless the switch template has at least one profile and has at most one profile per switch model.

Back to: [Meraki](#)

Claim Device into a Network

Claim Device into a Network

Use the Claim Device into a Network activity to add the device to the network.

To define the Claim Device into a Network activity:

1. In the Workflow Editor Toolbox, choose **Activities > Meraki > Claim Device into a Network**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Claim Device into a Network activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Click this radio button to use the workflow target.
 - ii. Override Workflow Target: Click this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Meraki Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Click this radio button to use the target's default account key.
 - ii. Override Account Key: Click this radio button to override the workflow account key. You can select the appropriate account key or **+ADD NEW** from the dropdown list. For more information, see [Meraki Credentials](#).
 - d. Under **Meraki**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Network ID: Enter the network ID to claim device into a network. This will add the device to the network.
 - ii. Device Serial: Enter the device serial number to be claimed into the network.

Back to: [Meraki](#)

Create Network

Create Network

Use the Create Network activity to create a network that holds devices and information related to those devices. A network can contain any number of access points or switches, but only a single security appliance, VM concentrator, or instance of Systems Manager.

To define the Create Network activity:

1. In the Workflow Editor Toolbox, choose **Activities > Meraki > Create Network**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. **Display Name**: Enter the unique display name for the activity.
 - ii. **Description**: Enter the brief description about the activity.
 - iii. **Activity Timeout (Seconds)**: Enter the number of seconds to wait for Create Network activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. **Use Workflow Target**: Click this radio button to use the workflow target.
 - ii. **Override Workflow Target**: Click this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Meraki Endpoint](#).
 - iii. **Use Workflow Target Group**: Check this radio button to use the workflow target group.
 - iv. **Override Workflow Target Group Criteria**: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. **Use Target's Default Account Key**: Click this radio button to use the target's default account key.
 - ii. **Override Account Key**: Click this radio button to override the workflow account key. You can select the appropriate account key or **+ADD NEW** from the dropdown list. For more information, see [Meraki Credentials](#).
 - d. Under **Meraki**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. **Org ID**: Enter the organization ID to create network.
 - ii. **Network Name**: Enter the specific name for the network.
 - iii. **Type**: Enter the network type to be created such as wireless, switch, security appliance, and so forth.
 - iv. **Tags**: Specify the tags to be applied. Tags are used to differentiate the devices.

Back to: [Meraki](#)

Delete Network

Delete Network

Use the Delete Network activity to delete a network. Networks can be deleted when they are no longer needed. The devices from the network will remain in the inventory and can later be added to new networks.



It is not possible to delete a network if it has billing transactions associated with it.

To define the Delete Network activity:

1. In the Workflow Editor Toolbox, choose **Activities > Meraki > Delete Network**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Delete Network activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Click this radio button to use the workflow target.
 - ii. Override Workflow Target: Click this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Meraki Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Click this radio button to use the target's default account key.
 - ii. Override Account Key: Click this radio button to override the workflow account key. You can select the appropriate account key or **+ADD NEW** from the dropdown list. For more information, see [Meraki Credentials](#).
 - d. Under **Meraki**, specify the following information or click [Variable Reference](#) icon to choose any variable:

Network ID: Enter the network ID of the network to be deleted.

Back to: [Meraki](#)

Get Organizations

Get Organizations

To define the `Get Organizations` activity:

1. In the Workflow Editor Toolbox, choose **Activities > Meraki > Get Organizations**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. **Display Name**: Enter the unique display name for the activity.
 - ii. **Description**: Enter the brief description about the activity.
 - iii. **Activity Timeout (Seconds)**: Enter the number of seconds to wait for `Get Organizations` activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. **Use Workflow Target**: Click this radio button to use the workflow target.
 - ii. **Override Workflow Target**: Click this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Meraki Endpoint](#).
 - iii. **Use Workflow Target Group**: Check this radio button to use the workflow target group.
 - iv. **Override Workflow Target Group Criteria**: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. **Use Target's Default Account Key**: Click this radio button to use the target's default account key.
 - ii. **Override Account Key**: Click this radio button to override the workflow account key. You can select the appropriate account key or **+ADD NEW** from the dropdown list. For more information, see [Meraki Credentials](#).

Back to: [Meraki](#)

List Configuration Templates

List Configuration Templates

To define the List Configurations Templates activity:

1. In the Workflow Editor Toolbox, choose **Activities > Meraki > List Configurations Templates**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. **Display Name**: Enter the unique display name for the activity.
 - ii. **Description**: Enter the brief description about the activity.
 - iii. **Activity Timeout (Seconds)**: Enter the number of seconds to wait for List Configurations Templates activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. **Use Workflow Target**: Click this radio button to use the workflow target.
 - ii. **Override Workflow Target**: Click this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Meraki Endpoint](#).
 - iii. **Use Workflow Target Group**: Check this radio button to use the workflow target group.
 - iv. **Override Workflow Target Group Criteria**: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. **Use Target's Default Account Key**: Click this radio button to use the target's default account key.
 - ii. **Override Account Key**: Click this radio button to override the workflow account key. You can select the appropriate account key or **+ADD NEW** from the dropdown list. For more information, see [Meraki Credentials](#).
 - d. Under **Meraki**, specify the following information or click [Variable Reference](#) icon to choose any variable:

Org ID: Enter the organization ID to list the configuration templates.

Back to: [Meraki](#)

List Networks

List Networks

Use the List Networks activity to list the network of the organization.

To define the List Networks activity:

1. In the Workflow Editor Toolbox, choose **Activities > Meraki > List Networks**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for List Networks activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Click this radio button to use the workflow target.
 - ii. Override Workflow Target: Click this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Meraki Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Click this radio button to use the target's default account key.
 - ii. Override Account Key: Click this radio button to override the workflow account key. You can select the appropriate account key or **+ADD NEW** from the dropdown list. For more information, see [Meraki Credentials](#).
 - d. Under **Meraki**, specify the following information or click [Variable Reference](#) icon to choose any variable:

Org ID: Enter the organization ID to list the existing networks of the organization.

Back to: [Meraki](#)

List VLANs of a Network

List VLANs of a Network

Use the List VLANs of a Network activity to list the VLANs present in a network.

To define the List VLANs of a Network activity:

1. In the Workflow Editor Toolbox, choose **Activities > Meraki > List VLANs of a Network**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for List VLANs of a Network activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Click this radio button to use the workflow target.
 - ii. Override Workflow Target: Click this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Meraki Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Click this radio button to use the target's default account key.
 - ii. Override Account Key: Click this radio button to override the workflow account key. You can select the appropriate account key or **+ADD NEW** from the dropdown list. For more information, see [Meraki Credentials](#).
 - d. Under **Meraki**, specify the following information or click [Variable Reference](#) icon to choose any variable:

Network ID: Enter the network ID of the network to list VLANs.

Back to: [Meraki](#)

Update Network

Update Network

Use the Update Network activity to update the network information.

To define the Update Network activity:

1. In the Workflow Editor Toolbox, choose **Activities > Meraki > Update Network**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Update Network activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Click this radio button to use the workflow target.
 - ii. Override Workflow Target: Click this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Meraki Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Click this radio button to use the target's default account key.
 - ii. Override Account Key: Click this radio button to override the workflow account key. You can select the appropriate account key or **+ADD NEW** from the dropdown list. For more information, see [Meraki Credentials](#).
 - d. Under **Meraki**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Org ID: Enter the organization ID of the organization.
 - ii. Network ID: Enter the network ID of the network to be updated.
 - iii. Network Name: Enter the network name.
 - iv. Type: Enter the network type such as wireless, switch, security appliance, and so forth.
 - v. Updates Tags: Specify the tags to be updated in the network.
 - vi. Updates Timezone: Specify the timezone to be updated in the network.

Back to: [Meraki](#)

Microsoft Windows

Microsoft Windows

Action Orchestrator process automation engine provides the logical constructs necessary to support even the most complex requirements to automate Microsoft Windows server operating systems tasks. The Microsoft Windows Adapter provides the ability to easily query Windows performance data and execute Windows commands and scripts. The Windows Adapter provides the following activities for querying specific Windows performance information.

- [Control Windows Service](#)
- [Copy Folder](#)
- [Correlate Windows Events](#)
- [Create Folder](#)
- [Execute Command](#)
- [Execute Powershell Script](#)
- [Execute Windows Script](#)
- [Get Folder Properties](#)
- [Query Windows Events](#)
- [Query Windows Performance Counter](#)
- [Query Windows Registry](#)
- [Query Windows Service](#)
- [Read File](#)
- [Restart Server](#)
- [Stop Process](#)
- [Uninstall Application](#)
- [Microsoft Write File](#)

Control Windows Service

Control Windows Service

Use the Control Windows Service activity to specify the Windows service to which an action should be performed.



To ensure this Windows activity executes properly, verify that the Remote Registry service is enabled on your machine.

1. In the Workflow Editor Toolbox, choose **Microsoft Windows > Control Windows Service** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Control Windows Service activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - v. Check the **Skip Activity Execution** check box to skip the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Microsoft Windows Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the dropdown list. For more information, see [Microsoft Windows Credentials](#).
 - d. Under **Inputs**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Service Name: Enter the Windows service name.
 - ii. Action On Service: Select the action that should be performed against the service from the dropdown list such as Pause, Restart, Resume, and so forth.
 - iii. Seconds to Wait: Enter the amount of time to wait before completion.

Back to: [Microsoft Windows](#)

Copy Folder

Copy Folder

Use the Copy Folders activity to copy file folders from one location to another.

1. In the Workflow Editor Toolbox, choose **Microsoft Windows > Copy Folder** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Copy Folder activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - v. Check the **Skip Activity Execution** check box to skip the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Microsoft Windows Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the dropdown list. For more information, see [Microsoft Windows Credentials](#).
 - d. Under **Windows**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Source: Files or folders to be copied.
 - ii. Destination: Location to where the files or folders will be copied.

Back to: [Microsoft Windows](#)

Correlate Windows Events

Correlate Windows Events

Use the Correlate Windows Events activity to specify the event log information that is to be located on the target.



To ensure this Windows activity executes properly, verify that the Remote Registry service is enabled on your machine.

1. In the Workflow Editor Toolbox, choose **Microsoft Windows > Correlate Windows Events** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Correlate Windows Events activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - v. Check the **Skip Activity Execution** check box to skip the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Microsoft Windows Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the dropdown list. For more information, see [Microsoft Windows Credentials](#).
 - d. Under **Windows**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Entry Type: Check the check boxes for the types of events that must be matched from the dropdown list.
 - ii. Log Name: The name of the event log to be matched. Enter a name or expression in the text field.
 - iii. After Time: Correlate events that occurred after the specified time.
 - iv. Before Time: Correlate events that occurred before the specified time.
 - v. Event Source: Check the check box and then enter the source or click the Reference tool to select a variable to find event log entries by where they occurred.
 - vi. Event Number: Check the check box and then enter the event ID or click the Reference tool to select a variable to find an event log entry by the event ID.
 - vii. Event Description: Check the check box and then enter the description or click the Reference tool to select a variable to find an event log entry matching a description.
 - viii. Event Computer Name: Check this check box to find an event log entry by matching a specific computer. Enter the computer name in the text field that should be matched or click the Reference tool to select a variable for the field value.
 - ix. Check the **Persist Table** check box to persist the resulting table to the Action Orchestrator database so you can view the results when the workflow instance is viewed.

Back to: [Microsoft Windows](#)

Create Folder

Create Folder

Use the Create Folder activity to create a file path for the folder.

1. In the Workflow Editor Toolbox, choose **Microsoft Windows > Create Folder** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Create Folder activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - v. Check the **Skip Activity Execution** check box to skip the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Microsoft Windows Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the dropdown list. For more information, see [Microsoft Windows Credentials](#).
 - d. Under **Windows**, specify the **Directory Path** or click [Variable Reference](#) icon to choose the path.

Back to: [Microsoft Windows](#)

Execute Command

Execute Command

Use the Execute Command activity to specify a Windows command and the target directory on which to execute that command.



To ensure this Windows activity executes properly, verify that the Remote Registry service is enabled on your machine.

1. In the Workflow Editor Toolbox, choose **Microsoft Windows > Execute Command** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. **Display Name**: Enter the unique display name for the activity.
 - ii. **Description**: Enter the brief description about the activity.
 - iii. **Activity Timeout (Seconds)**: Enter the number of seconds to wait for Execute Command activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - v. Check the **Skip Activity Execution** check box to skip the activity.
 - b. Under **Target**, specify the following information:
 - i. **Use Workflow Target**: Check this radio button to use the workflow target.
 - ii. **Override Workflow Target**: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Microsoft Windows Endpoint](#).
 - iii. **Use Workflow Target Group**: Check this radio button to use the workflow target group.
 - iv. **Override Workflow Target Group Criteria**: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. **Use Target's Default Account Key**: Check this radio button to use the target's default account key.
 - ii. **Override Account Key**: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the dropdown list. For more information, see [Microsoft Windows Credentials](#).
 - d. Under **Windows**, specify the **Windows Command** or click [Variable Reference](#) icon to choose any variable:

Back to: [Microsoft Windows](#)

Execute Powershell Script

Execute Powershell Script

Use this activity to specify a Windows command and the target directory on which to execute.



To ensure this Windows activity executes properly, verify that the Remote Registry service is enabled on your machine.

1. In the Workflow Editor Toolbox, choose **Microsoft Windows > Execute Powershell Script** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. **Display Name**: Enter the unique display name for the activity.
 - ii. **Description**: Enter the brief description about the activity.
 - iii. **Activity Timeout (Seconds)**: Enter the number of seconds to wait for **Execute Powershell Script** activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - v. Check the **Skip Activity Execution** check box to skip the activity.
 - b. Under **Target**, specify the following information:
 - i. **Use Workflow Target**: Check this radio button to use the workflow target.
 - ii. **Override Workflow Target**: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Microsoft Windows Endpoint](#).
 - iii. **Use Workflow Target Group**: Check this radio button to use the workflow target group.
 - iv. **Override Workflow Target Group Criteria**: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. **Use Target's Default Account Key**: Check this radio button to use the target's default account key.
 - ii. **Override Account Key**: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the dropdown list. For more information, see [Microsoft Windows Credentials](#).
 - d. Under **Windows**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. **Powershell Script**: Enter the Powershell script to be executed on the specified target.
 - ii. **Script Arguments**: Enter the collection of argument values for the script. Multi-line script arguments are not supported.
 - iii. **Working Directory**: Enter the path to the local working directory on the Windows target where the script will be executed.
 - iv. Check the **Execute Remote File** check box to indicate that the script will access remote resources.
 - v. **Remote File**: Enter the remote file path.

Back to: [Microsoft Windows](#)

Execute Windows Script

Execute Windows Script

Use the Execute Windows Script activity to specify a Windows script and the target directory on which to execute.



To ensure this Windows activity executes properly, verify that the Remote Registry service is enabled on your machine.

1. In the Workflow Editor Toolbox, choose **Microsoft Windows > Execute Windows Script** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Execute Windows Script activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - v. Check the **Skip Activity Execution** check box to skip the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Microsoft Windows Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the dropdown list. For more information, see [Microsoft Windows Credentials](#).
 - d. Under **Windows**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Windows Script: Enter the Windows command script to be executed on the specified target.
 - ii. Script Arguments: Enter the collection of argument values for the script. Multi-line script arguments are not supported.
 - iii. Working Directory: Enter the actual script code to use to execute an activity on the specified local working directory on the Windows target computer.
 - iv. Check the **Execute Remote File** check box to indicate that the script will access remote resources.
 - v. Remote File: Enter the remote file path.

Back to: [Microsoft Windows](#)

Get Folder Properties

Get Folder Properties

Use the Get Folder Properties activity to retrieve folder properties.

1. In the Workflow Editor Toolbox, choose **Microsoft Windows > Get Folder Properties** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Get Folder Properties activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - v. Check the **Skip Activity Execution** check box to skip the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Microsoft Windows Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the dropdown list. For more information, see [Microsoft Windows Credentials](#).
 - d. Under **Windows**, specify the **Folder Path** (the file path for the appropriate folder) or click [Variable Reference](#) icon to choose any variable.

Back to: [Microsoft Windows](#)

Query Windows Events

Query Windows Events

Use the Query Windows Events activity to specify information about the event logs that you want to find on the target. The activity searches the event log on the specified target and returns all matching events in the activity instance.



To ensure this Windows activity executes properly, verify that the Remote Registry service is enabled on your machine.

1. In the Workflow Editor Toolbox, choose **Microsoft Windows > Query Windows Events** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Query Windows Events activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - v. Check the **Skip Activity Execution** check box to skip the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Microsoft Windows Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the dropdown list. For more information, see [Microsoft Windows Credentials](#).
 - d. Under **Windows**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Check the **Persist Table** check box to persist the resulting table to the Action Orchestrator database so you can view the results when the workflow instance is viewed.
 - ii. Event Type: Check the type of events check box that must be matched from the dropdown list (Information, Warning, Error, Success Audit, Failure Audit).
 - iii. Log Name: The name in the text field of the event log to be matched.
 - iv. Event Source: Check the check box and enter the source or click the Reference tool to select a variable to find event log entries by where they occurred.
 - v. Event Number: Check the check box and enter the event ID or click the Reference tool to select a variable to find an event log entry by the event ID.
 - vi. Event Description: Check this check box and enter the description in the field to find an event log entry to match the description.
 - vii. Check the **Get Latest Event** check box if you want only the most recent event to be returned.
 - viii. Events Generated within the Last: Specify a time period in which the event occurred.
 - ix. Events with Format: Select the time unit (minutes, hours, or days).

Back to: [Microsoft Windows](#)

Query Windows Performance Counter

Query Windows Performance Counter

Specifies the information used to collect performance data for your monitoring system components.



To ensure this Windows activity executes properly, verify that the Remote Registry service is enabled on your machine.

1. In the Workflow Editor Toolbox, choose **Microsoft Windows > Query Windows Performance Counter** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. **Display Name**: Enter the unique display name for the activity.
 - ii. **Description**: Enter the brief description about the activity.
 - iii. **Activity Timeout (Seconds)**: Enter the number of seconds to wait for Query Windows Performance Counter activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - v. Check the **Skip Activity Execution** check box to skip the activity.
 - b. Under **Target**, specify the following information:
 - i. **Use Workflow Target**: Check this radio button to use the workflow target.
 - ii. **Override Workflow Target**: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Microsoft Windows Endpoint](#).
 - iii. **Use Workflow Target Group**: Check this radio button to use the workflow target group.
 - iv. **Override Workflow Target Group Criteria**: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. **Use Target's Default Account Key**: Check this radio button to use the target's default account key.
 - ii. **Override Account Key**: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the dropdown list. For more information, see [Microsoft Windows Credentials](#).
 - d. Under **Windows**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. **Object Name**: A name of the category that contains the performance counter.
 - ii. **Counter Name**: The name of the performance counter.
 - iii. **Instance Name**: The name of the instance specific to the selected counter. For instance names containing common wildcard expressions, add an escape value \ to the expression. For example, the instance name `java#1`, should be `java\#1`.

Back to: [Microsoft Windows](#)

Query Windows Registry

Query Windows Registry

Specifies the information necessary to read information from the registry keys.



To ensure this Windows activity executes properly, verify that the Remote Registry service is enabled on your machine.

1. In the Workflow Editor Toolbox, choose **Microsoft Windows > Query Windows Registry** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Query Windows Registry activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - v. Check the **Skip Activity Execution** check box to skip the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Microsoft Windows Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the dropdown list. For more information, see [Microsoft Windows Credentials](#).
 - d. Under **Windows**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Registry Hive: The name of the registry hive where the registry key and value are located.
 - ii. Registry Key: Enter the registry key.
 - iii. Check for Key Existence Only: Query the registry to determine whether the key exists. Select the true or false from the dropdown list.
 - iv. Value Name: Read the value associated with the specified registry key.

Back to: [Microsoft Windows](#)

Query Windows Service

Query Windows Service

Use the Query Windows Service activity to produce the current state of the service, the startup type of the service, and specifies the Windows service to be queried.



To ensure this Windows activity executes properly, verify that the Remote Registry service is enabled on your machine.

1. In the Workflow Editor Toolbox, choose **Microsoft Windows > Query Windows Service** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. **Display Name**: Enter the unique display name for the activity.
 - ii. **Description**: Enter the brief description about the activity.
 - iii. **Activity Timeout (Seconds)**: Enter the number of seconds to wait for Query Windows Service activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - v. Check the **Skip Activity Execution** check box to skip the activity.
 - b. Under **Target**, specify the following information:
 - i. **Use Workflow Target**: Check this radio button to use the workflow target.
 - ii. **Override Workflow Target**: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Microsoft Windows Endpoint](#).
 - iii. **Use Workflow Target Group**: Check this radio button to use the workflow target group.
 - iv. **Override Workflow Target Group Criteria**: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. **Use Target's Default Account Key**: Check this radio button to use the target's default account key.
 - ii. **Override Account Key**: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the dropdown list. For more information, see [Microsoft Windows Credentials](#).
 - d. Under **Windows**, specify the **Service Name** (specify the name of the Windows service to be queried) or click [Variable Reference](#) icon to choose any variable.

Back to: [Microsoft Windows](#)

Read File

Read File

Use the Read File activity to read the content a file that resides on a remote machine.

1. In the Workflow Editor Toolbox, choose **Microsoft Windows > Read File** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Read File activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - v. Check the **Skip Activity Execution** check box to skip the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Microsoft Windows Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the dropdown list. For more information, see [Microsoft Windows Credentials](#).
 - d. Under **Windows**, specify the **Remote File Path** (Name of file as it was saved on the local computer) or click [Variable Reference](#) icon to choose any variable.

Back to: [Microsoft Windows](#)

Restart Server

Restart Server

Use the Restart Server activity to indicate the time to delay before restarting a server and the server restart notification message.

1. In the Workflow Editor Toolbox, choose **Microsoft Windows > Restart Server** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Restart Server activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - v. Check the **Skip Activity Execution** check box to skip the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Microsoft Windows Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the dropdown list. For more information, see [Microsoft Windows Credentials](#).
 - d. Under **Windows**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Delay (in Seconds) - Time to Wait before forcing the Restart.
 - ii. Note - Reason To Restart Server.

Back to: [Microsoft Windows](#)

Stop Process

Stop Process

Use the Stop a Windows Process activity to stop a running Windows process.



To launch this activity, the runtime user should have local administrative rights to the target.

1. In the Workflow Editor Toolbox, choose **Microsoft Windows > Stop Process** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. **Display Name**: Enter the unique display name for the activity.
 - ii. **Description**: Enter the brief description about the activity.
 - iii. **Activity Timeout (Seconds)**: Enter the number of seconds to wait for Stop Process activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - v. Check the **Skip Activity Execution** check box to skip the activity.
 - b. Under **Target**, specify the following information:
 - i. **Use Workflow Target**: Check this radio button to use the workflow target.
 - ii. **Override Workflow Target**: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Microsoft Windows Endpoint](#).
 - iii. **Use Workflow Target Group**: Check this radio button to use the workflow target group.
 - iv. **Override Workflow Target Group Criteria**: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. **Use Target's Default Account Key**: Check this radio button to use the target's default account key.
 - ii. **Override Account Key**: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the dropdown list. For more information, see [Microsoft Windows Credentials](#).
 - d. Under **Windows**, specify the **Process PID** or click [Variable Reference](#) icon to choose any variable.

Back to: [Microsoft Windows](#)

Uninstall Application

Uninstall Application

Use this activity to uninstall a specific application.

1. In the Workflow Editor Toolbox, choose **Microsoft Windows > Uninstall Application** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Uninstall Application activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - v. Check the **Skip Activity Execution** check box to skip the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Microsoft Windows Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the dropdown list. For more information, see [Microsoft Windows Credentials](#).
 - d. Under **Windows**, specify the **Application Name** or click [Variable Reference](#) icon to choose any variable.

Back to: [Microsoft Windows](#)

Microsoft Write File

Write File

Use the Write File activity to write content into a file that resides on a remote machine.



To ensure this Windows activity executes properly, verify that the Remote Registry service is enabled on your machine.

1. In the Workflow Editor Toolbox, choose **Microsoft Windows > Write File** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Write File activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - v. Check the **Skip Activity Execution** check box to skip the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Microsoft Windows Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the dropdown list. For more information, see [Microsoft Windows Credentials](#).
 - d. Under **Windows**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. File Name: File path including the name of the file in which the contents are written. For example: C:\Documents and Settings\user name\My Documents\file name
 - ii. File Content: Enter the appropriate contents to include in the file.
 - iii. Encoding: Select the appropriate encoding class for the file, as necessary:
 1. ASCII: An encoding for the ASCII (7-bit) character set
 2. UTF-16: An encoding for the UTF-16 format using the little endian byte order
 3. UTF-32: An encoding object for the UTF-32 format using the little endian byte order
 4. UTF-7: An encoding for the UTF-7 format and is less robust and secure than UTF-8, UTF-16, or UTF-32
 5. UTF-8: An encoding for the UTF-8 format
 - iv. Options: Select the appropriate action to take when saving the file.

Back to: [Microsoft Windows](#)

Prime Service Catalog

Prime Service Catalog

The Prime Service Catalog adapter establishes a relationship between Action Orchestrator and the Prime Service Catalog. In Action Orchestrator, you can:

- Manage services items and service requests in Prime Service Catalog.
- Create, delete, and update service items using attributes of the service item.
- Submit and update service requests by manually creating dictionaries or browsing for dictionaries in a Prime Service Catalog Server target.

The following displays activities that are provided by the Cisco Prime Service Catalog adapter:

- [Cancel Service Request](#)
- [Create Service Items](#)
- [Delete Service Items](#)
- [Find Service Items](#)
- [Get Service Item](#)
- [Mark Task Complete](#)
- [Submit Service Request](#)
- [Update Service Items](#)

Cancel Service Request

Cancel Service Request

Use the Cancel Service Request activity to cancel a request for a service order on the Cisco Prime Service Catalog.

1. In the Workflow Editor Toolbox, choose **Prime Service Catalog > Cancel Service Request** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Cancel Service Request activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - v. Check the **Skip Activity Execution** check box to skip the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Prime Service Catalog Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the dropdown list. For more information, see [Cisco Prime Service Catalog Credentials](#).
 - d. Under **PSC**, specify the **Requisition ID** of the service to be canceled or click [Variable Reference](#) icon to choose any variable.

Back to: [Prime Service Catalog](#)

Create Service Items

Create Service Items

Use the Create Service Item activity to create a service item to be delivered in response to a service request. A service item may be a virtual machine type or a user-defined type in the Cisco Prime Service Catalog.

1. In the Workflow Editor Toolbox, choose **Prime Service Catalog > Create Service Items** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Create Service Items activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - v. Check the **Skip Activity Execution** check box to skip the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Prime Service Catalog Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the dropdown list. For more information, see [Cisco Prime Service Catalog Credentials](#).
 - d. Under **PSC**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Service Item Type: Enter the type of physical or virtual asset for the service item. The service item can be a virtual machine or a user-defined item.
 - ii. Attributes: Enter the list of attributes to be used to create the service item. The attribute properties provide additional data used to create service item.

Back to: [Prime Service Catalog](#)

Delete Service Items

Delete Service Items

Use the Delete Service Items activity to delete an existing service item in the Cisco Prime Service Catalog.

1. In the Workflow Editor Toolbox, choose **Prime Service Catalog > Delete Service Items** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Delete Service Items activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - v. Check the **Skip Activity Execution** check box to skip the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Prime Service Catalog Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the dropdown list. For more information, see [Cisco Prime Service Catalog Credentials](#).
 - d. Under **PSC**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Service Item Type: Enter the type of physical or virtual asset for the service item. The service item can be a virtual machine or a user-defined item.
 - ii. Attributes: Enter the list of attributes to be deleted in the service item. The attribute properties provide additional data used to delete the service item.

Back to: [Prime Service Catalog](#)

Find Service Items

Find Service Items

Use the Find Service Item activity to search for attribute properties for the service item.

1. In the Workflow Editor Toolbox, choose **Prime Service Catalog > Find Service Items** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Find Service Items activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - v. Check the **Skip Activity Execution** check box to skip the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Prime Service Catalog Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the dropdown list. For more information, see [Cisco Prime Service Catalog Credentials](#).
 - d. Under **PSC**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Service Item Type: Enter the type of physical or virtual asset for the service item. The service item can be a virtual machine or a user-defined type.
 - ii. Populate Columns From JSON: Check this check box to use the data from the source text as table columns in the output result.
 - iii. Service Item Filters: Click **ADD** button to add a attribute properties pane to the find service item. Select one of the following options for adding a search criteria:
 1. Attribute Name: Enter the attribute name to be compared.
 2. Attribute Operator: From the drop-down list, choose the operator to use for comparing the value:
 - a. Contains: Iterates through the contents of the collection and determines if the specified item exists (if this is a string collection, this is case-insensitive)
 - b. Equal: Determines if the attribute name equals the attribute value.
 - c. Greater Than: Determines if a value is greater than another value.
 - d. Greater Than or Equal to: Determines if a value is greater than or equal to another value.
 - e. Less Than: Determines if a value is less than another value.
 - f. Less Than or Equal to: Determines if a value is less than or equal to another value.
 - g. Not equals: Determines if the attribute name does not equal the attribute value.
 - h. Starts With: Determines if the attribute name starts with the specified value.
 - i. is not null: Determines if there are items in the collection or not.
 - j. is null: Determines if there are items in the collection or not.
 3. Attribute Value: Enter the attribute value for the right operand.
 - iv. Columns to Read: Specify the columns **Name** in the JSON output to read.

Back to: [Prime Service Catalog](#)

Get Service Item

Get Service Item

Use the Get Service Item activity to get the service item in the Cisco Prime Service Catalog.

1. In the Workflow Editor Toolbox, choose **Prime Service Catalog > Get Service Item** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Get Service Item activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - v. Check the **Skip Activity Execution** check box to skip the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Prime Service Catalog Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the dropdown list. For more information, see [Cisco Prime Service Catalog Credentials](#).
 - d. Under **PSC**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Service Item Type: Enter the type of physical or virtual asset for the service item. The service item can be a virtual machine or a user-defined type.
 - ii. Service Item Name: Enter the name of the service to be ordered.

For example:

Order a Virtual Machine

-or-

Start User Provisioning Process
 - iii. Populate Columns from JSON: Check this check box to use the data from the source text as table columns in the output result.
 - iv. Columns to Read: Specify the columns **Name** in the JSON output to read.

Back to: [Prime Service Catalog](#)

Mark Task Complete

Mark Task Complete

Use the Mark Task Complete activity to mark the completed task in the Cisco Prime Service Catalog.

1. In the Workflow Editor Toolbox, choose **Prime Service Catalog > Mark Task Complete** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Mark Task Complete activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - v. Check the **Skip Activity Execution** check box to skip the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Prime Service Catalog Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the dropdown list. For more information, see [Cisco Prime Service Catalog Credentials](#).
 - d. Under **PSC**, specify the **Task ID** to be marked complete or click [Variable Reference](#) icon to choose any variable.

Back to: [Prime Service Catalog](#)

Submit Service Request

Submit Service Request

Use the Submit Service Request activity to submit a request for a service order on the Cisco Prime Service Catalog. In this activity, users can add multiple dictionaries to the service request manually or by browsing for an existing dictionary on a target.

1. In the Workflow Editor Toolbox, choose **Prime Service Catalog > Submit Service Request** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Submit Service Request activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - v. Check the **Skip Activity Execution** check box to skip the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Prime Service Catalog Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the dropdown list. For more information, see [Cisco Prime Service Catalog Credentials](#).
 - d. Under **PSC**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Customer Login Name: Enter the log in name for the customer of the service being requested.
 - ii. Services: Enter the list of services along with the body to submit.



You can enter one or more services at a time.

For example

```
{
  "requisition": {
    "customerLoginName": "admin",
    "services": [
      {
        "name": "SampleService",
        "quantity": "1",
        "version": "0",
        "dictionaries": [
          {
            "name": "LaptopComputerDict",
            "data": {
              "Name": "ThinkPad",
              "Vendor": "Lenovo",
              "Model": "5567",
              "Status": "Available",
              "Comments": "Lenovo ThinkPad",
              "Price": "1200"
            }
          }
        ]
      },
      {
        "name": "Test01",
        "quantity": "1",
        "version": "0",
        "dictionaries": [
          {
            "name": "LaptopComputerDict",
            "data": {
              "Name": "ThinkPad",
              "Vendor": "Lenovo",
              "Model": "W530",
              "Status": "Available",
              "Comments": "Pavan Lenovo ThinkPad",
              "Price": "1499"
            }
          }
        ]
      }
    ]
  }
}
```

[Back to: Prime Service Catalog](#)

Update Service Items

Update Service Items

Use the Update Service Item activity to update the attributes for an existing service item on the Cisco Prime Service Catalog.

1. In the Workflow Editor Toolbox, choose **Prime Service Catalog > Update Service Items** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Update Service Items activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - v. Check the **Skip Activity Execution** check box to skip the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Prime Service Catalog Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the dropdown list. For more information, see [Cisco Prime Service Catalog Credentials](#).
 - d. Under **PSC**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Service Item Type: Enter the type of physical or virtual asset for the service item. The service item can be a virtual machine or a user-defined item.
 - ii. Attributes: Enter the list of attributes to be used to update the service item. The attribute properties provide additional data used to update service item.

Back to: [Prime Service Catalog](#)

Python

Python

The Python adapter provides the functionality to execute Python scripts. The following section display Python activity:

- [Execute Python Script](#)
- [Execute Python Script Activity For Python 2.7 \(Obsolete\)](#)

Execute Python Script

Execute Python Script

Use the following procedure to execute python script.



This activity is applicable for Python 3.x versions.

1. In the Workflow Editor Toolbox, choose **Activities > Python > Execute Python Script**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. **Display Name**: Enter the unique display name for the activity.
 - ii. **Description**: Enter the brief description about the activity.
 - iii. **Activity Timeout (Seconds)**: Enter the number of seconds to wait for Execute Python Script activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Python Query**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. **Script Arguments**: Enter the collection of argument values for the script, users can pass to sys module in Python code.
 - ii. **Script to Execute on Target**: Enter the script code to be executed.
 - iii. **Script Output Variables**: Click **+ADD** to enter the following information:
 1. **Script Variable**: Enter the variable name as used in the script code to be queried.
 2. **Property Name**: Enter the property name, under which the value of Script Variable will be accessible in Action Orchestrator workflow.
 3. **Property Type**: Select the property type from the dropdown list such as Boolean, Date/Time, Decimal, and so forth.

Back to: [Python](#)

Execute Python Script Activity For Python 2.7 (Obsolete)

Execute Python Script Activity For Python 2.7 (Obsolete)

Use the following procedure to execute python script activity for Python 2.7.



This activity is obsolete, no longer produced or used or out of date.

1. In the Workflow Editor Toolbox, choose **Activities > Python > Execute Python Script Activity For Python 2.7 (Obsolete)**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. **Display Name**: Enter the unique display name for the activity.
 - ii. **Description**: Enter the brief description about the activity.
 - iii. **Activity Timeout (Seconds)**: Enter the number of seconds to wait for Execute Python Script Activity For Python 2.7 (Obsolete) activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Python Query**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. **Script Arguments**: Enter the collection of argument values for the script, users can pass to sys module in Python code.
 - ii. **Script to Execute on Target**: Enter the script code to be executed.
 - iii. **Script Output Variables**: Click **+ADD** to enter the following information:
 1. **Script Variable**: Enter the variable name as used in the script code to be queried.
 2. **Property Name**: Enter the property name, under which the value of Script Variable will be accessible in Action Orchestrator workflow.
 3. **Property Type**: Select the property type from the dropdown list such as Boolean, Date/Time, Decimal, etc.

Back to: [Python](#)

Table Activities

Table Activities

You can use Table activities to modify the format for existing defined table variables. The following sections display Table activities:

- [Add Row to Table](#)
- [Delete From Table](#)
- [Read Table from JSON](#)
- [Read Table from Text](#)
- [Read Table from XML](#)
- [Select From Table](#)
- [Update Row in Table](#)



Any Boolean and numeric values that are used by the Table activities in the product are not localized. Numbers use [.] for the decimal format regardless of the regional and language options. Boolean values for substitutable Boolean must be true or false regardless of the installed language.

Add Row to Table

Add Row to Table

Append new rows to a table variable. The row is added to the end of the table.



This activity will not work on tables that are outputs of other activities.

1. In the Workflow Editor Toolbox, choose **Activities > Table Activities > Add Row to Table**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. **Display Name**: Enter the unique display name for the activity.
 - ii. **Description**: Enter the brief description about the activity.
 - iii. **Activity Timeout (Seconds)**: Enter the number of seconds to wait for Add Row to Table activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Table**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. **Input Table**: Enter the name of table from which the new rows has to be added.

Back to: [Table Activities](#)

Delete From Table

Delete From Table

Delete one or more rows from a table variable based on specified criteria.



This activity will not work on tables that are outputs of other activities.

1. In the Workflow Editor Toolbox, choose **Activities > Table Activities > Delete from Table**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Delete from Table activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Select**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Input Table: Enter the name of table from which the specified information has to be deleted.
 - ii. Under **Rows**, specify the following information:
 1. All Rows: Click on this radio button to include all rows of the table.
 2. Rows Matching Specified Criteria: Click on this radio button to specify the criteria.

Where Clause: Enter the where clause to limit the number of rows to be deleted.

Back to: [Table Activities](#)

Read Table from JSON

Read Table from JSON

Read an JSON and convert it into a table with a specified set of columns.

1. In the Workflow Editor Toolbox, choose **Activities**>**Table Activities**>**Read Table from JSON**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Read Table from JSON activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Read Table**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. JSON Path: Enter the JSON path to be used as columns.
 - ii. Persist Table: Check this check box to make the table persistent.
 - iii. Populate columns from JSON: Check this check box to use JSON elements from the source JSON as table columns in the output result.

By enabling this check box, the Columns to read field is hidden. When you enable this check box for existing activities with data in Columns to read field. All existing data in columns in read is deleted.
 - iv. Columns to Read: Click **+ADD** to enter the Name of the column to be read and select the Type from the drop-down list such as string, number, and Boolean.
 - v. Source JSON: Enter the appropriate source JSON.

For Example:

JSON Path:

`$.store.book[*].author`

Source JSON

```
{
  "store":
  "book": [
    { "category": "reference",
      "author": "Nigel Rees",
      "title": "Sayings of the century",
      "price": 8.95
    },
    { "category": "fiction",
      "author": "Evelyn Waugh",
      "title": "Sword of Honour", "price": 12.99
    },
    { "category": "fiction",
      "author": "Herman Melville",
      "title": "Moby Dick",
      "isbn": "0-553-21311-3",
      "price": 8.99
    },
    { "category": "fiction",
      "author": "J.R.R. Tolkien",
      "title": "The Lord of the Rings",
      "isbn": "0-395-19395-8",
      "price": 22.99
    }
  ]
  "bicycle": {
    "color": "red",
    "price": 19.95
  },
}
```

This produces a table with author as column name, with four rows containing author names. For example:

author
NigelRees
Evelyn Waugh
Herman Melville
J.R.R. Tolkien

Back to: [Table Activities](#)

Read Table from Text

Read Table from Text

Read a string variable and convert the text into a table with a specified set of columns.

1. In the Workflow Editor Toolbox, choose **Activities**>**Table Activities**>**Read Table from Text**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Read Table from Text activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Read Table**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Populate columns from the first line in text: Check this check box to use text from first line in the source text as table columns in the output result.



By enabling this check box, the Columns to read field is hidden. When you enable this check box for existing activities with data in Columns to read field. All existing data in columns in read is deleted.

- ii. Columns to Read: Click **+ADD** to enter the Name of the column to be read and select the Type from the drop-down list such as string, number, and Boolean.
- iii. Source Text: Enter the appropriate source Text.
- iv. Split Options: Enter the **Delimiter** to split a string into multiple parts around matches of the given delimiter or delimiters.
- v. Persist Table: Check this check box to make the table persistent.

For Example,

If the Populate columns from first record in source text is checked & File type is delimited by Comma:

Source Text:

City,County,State

"Georgetown","Williamson","TX"

Georgetown,Williamson,TX

"Georgetown","\Williamson","\TX"

Georgetown,Taylor,LibertyHill,Williamson,TX

"Georgetown,Taylor,LibertyHill",Williamson,TX

City	County	State
Georgetown	Williamson	TX
Georgetown	Williamson	TX
Georgetown	Williamson	TX
Georgetown	Taylor	LibertyHill
Georgetown,Taylor,LibertyHill	Williamson	TX

The following example explains how you can include multiple strings in a single column using double quotes (Last row) and you can use slash (\) to include double quotes along with the string (Third row).

The fourth row displays only the first three strings being considered as City, County, and State as we have three columns only.

Back to: [Table Activities](#)

Read Table from XML

Read Table from XML

Read an XML snippet and convert it into a table with a specified set of columns.

1. In the Workflow Editor Toolbox, choose **Activities**>**Table Activities**>**Read Table from XML**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Read Table from XML activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Read Table**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. XML Path: Enter the XML path to be used as columns.
 - ii. Persist Table: Check this check box to make the table persistent.
 - iii. Populate columns from xml: Check this check box to use xml elements from the source xml as table columns in the output result.

By enabling this check box, the Columns to read field is hidden. When you enable this check box for existing activities with data in Columns to read field. All existing data in columns in read is deleted.
 - iv. Columns to Read: Click **+ADD** to enter the Name of the column to be read and select the Type from the drop-down list such as string, number, and Boolean.
 - v. Source XML: Enter the appropriate source XML.

For Example:

Row XML Element Name:

MyRow

Columns to read:

Name String
Age Integer

Source XML:

Source XML

```
<MyData>
<MyRow>
<Name>Jeff</Name>
<Age>32</Age>
</MyRow>
<MyRow>
<Name>Mark</Name>
<Age>31</Age>
</MyRow>
<MyRow>
<Name>Jay</Name>
<Age>30</Age>
</MyRow>
</MyData>
```

This produces a table with two columns (name, age), with three rows.

Back to: [Table Activities](#)

Select From Table

Select From Table

Query and select rows from a source table using specified criteria. The user can also determine the order of the rows selected as well as limit the number of rows displayed.

1. In the Workflow Editor Toolbox, choose **Activities > Table Activities > Select from Table**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Select from Table activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Select**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Input Table: Enter the table name to be used.
 - ii. Where Clause: Enter the where clause to limit the number of rows returned by the query.
 - iii. Results Column: Select the columns to be displayed in the results from the dropdown list such as All or the specific column name.
 - iv. Persist Table: Check this check box to make the table persistent.
 - v. Number of Rows: Select the appropriate radio button:
 1. All Rows: Click on this radio button to include all rows of the table.
 2. At Most: Click on this radio button to limit the number of rows in the result.
 - a. First N Rows: Specify the number of rows to be returned.
 - vi. Sorting: Select the appropriate radio button:
 1. No Sort: Click on this radio button to ignore sorting.
 2. Sort By: Click on this radio button to sort by using the following:
 - a. Column Name: Enter the appropriate column name that has to be sorted.
 - b. Order: Click on Ascending or Descending radio button to sort the result.

Back to: [Table Activities](#)

Update Row in Table

Update Row in Table

Update the selected rows of a table variable. The new rows become part of the variable being modified.

1. In the Workflow Editor Toolbox, choose **Activities > Table Activities > Update Row in Table**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name - Enter the unique display name for the activity.
 - ii. Description - Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds) - Enter the number of seconds to wait for Update Row in Table activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Table**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Input Table: Enter the name of table from which the rows has to be updated.
 - ii. Result Columns: Select the result columns to be updated.
 - iii. Under **Update Rows > Select > Rows**, specify the following information:
 1. All Rows - Click on this radio button to include all rows of the table.
 2. Rows Matching Specified Criteria - Click on this radio button to specify the criteria.

Where Clause - Enter the where clause to limit the number of rows to be updated.

Back to: [Table Activities](#)

Task

Task


- [Create Approval Request](#)
- [Query Object](#)
- [Wait For Event](#)


Create Approval Request

Create Approval Request


Use the Create Approval Request task to specify the user required to approve a task including the message associated for the approver.

1. In the Workflow Editor Toolbox, choose **Task > Create Approval Request** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - iv. Check the **Skip Activity Execution** check box to skip the activity.
 - b. Under **Approval Configuration**, specify the following information:
 - i. Task Requestor: Enter the Email ID of a task requestor from this tenant.
 - ii. Task Owner: Enter the Email ID of a task owner from this tenant.
 - iii. Add Task Assignee's: Enter the Email ID of a assignee from this tenant.
 - iv. Minimum No. of Approvals: Enter the minimum number of approvals required for this task request.
 - v. Priority: Select the priority from the dropdown list such as High, Low, or Normal.
 - vi. Subject Line: Enter the subject line for approval request.
 - vii. Approval Message: Message that informs the approver what is being requested.
 - viii. Approval Choices: The approval choices available (Approve, Reject).
 - c. Under **Set Task Due Date**, specify the following information:

 Due date should be less than expiration date.

 Use toggle button to disable or enable the task due date setting.


- i. Specified Date: Check this radio button to specify appropriate date the task should be completed.

 You can see the supported date formats by hovering over the *i* symbol.

- ii. Relative Time: Check this radio button to specify the following information:

1. Duration: Enter the appropriate time.
2. Time Units: Select the time unit from dropdown list such as Weeks, Days, Hours, etc.

- d. Under **Set Expiration Date**, specify the following information:

 Expiration date should be past the due date.

- i. Specified Date: Check this radio button to specify appropriate date the task should be expired.
- ii. Relative Time: Check this radio button to specify the following information:

1. Duration: Enter the appropriate time.
2. Time Units: Select the time unit from dropdown list such as Weeks, Days, Hours, etc.

- e. Under **Set Status On Expiration Date**, specify the **Expiration Status** (A flag indicating if the approval request had expired or not).

Back to: [Task](#)

Query Object

Query Object

Use the Query Object task to find task or event.

1. In the Workflow Editor Toolbox, choose **Task > Query Object** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Cancel Service Request activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - v. Check the **Skip Activity Execution** check box to skip the activity.
 - b. Under **Query Object**, specify the following information:
 - i. Query Task: Select the appropriate task to be queried such as Approval task, Generic task, etc.
 - ii. Query Event: Select the appropriate event to be queried such as AMQP Event, Approval Task Event, Email Event, etc.
 - c. Under **Criteria**, specify the **Condition** or click [Variable Reference](#) icon to choose any variable:
 - i. Left Operand: Enter the value for the left operand.
 - ii. Operator: From the dropdown list, choose the operator to use for comparing the value:
 1. Does not match wildcard: Determines if the item does not match all items in the wildcard example
 2. Equal: Determines if the left side equals the right side.
 3. Equal (case-insensitive): Determines if the left side equals the right side (if this is a string comparison, this is case-insensitive)
 4. Match regular expression: Determines if the left side matches the regular expression specified on the right side.
 5. Matches wildcard: Determines if the left side matches the wildcard specified on the right side.
 6. Not equals: Determines if the left side does not equal the right side.
 - iii. Right Operand: Enter the value for the right operand.


Back to: [Task](#)

Wait For Event

Wait For Event

The wait for event allows the Action Orchestrator workflow to wait for some action to be performed by some user such as approve, reject, and so forth or Wait for a task to match a specific state before the activity continues. You can define a workflow to wait for certain event and when the event occurs the workflow execution resumes. To create a wait for event perform the following procedure:

1. In the Workflow Editor Toolbox, choose **Task > Wait For Event** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Cancel Service Request activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - v. Check the **Skip Activity Execution** check box to skip the activity.
 - b. Under **Event Info**, specify the following information:
 - i. Event Type: Select the event type from the dropdown list such as **AMQP Event**, **Approval Task Event**, **Email Event**, or **Kafka Event**.
 - ii. Under **Event Info**, check the **Use Existing Event** to use the existing event or check the **Add Event** radio button to add a new event and specify the following information:
 1. Use Existing Event:
 - a. Event Identifier: Click the [Variable Reference](#) icon to choose the event ID.
 - b. Override Event Criteria: Choose **Yes** using the toggle button to override the conditions specified in the chosen event criteria and specify other additional conditions or click [Variable Reference](#) icon to choose any variable:

 The default option is *No*.
 - iii. Left Operand: Enter the value for the left operand.
 - ii. Operator: From the dropdown list, choose the operator to use for comparing the value:
 1. Does not match wildcard: Determines if the item does not match all items in the wildcard example
 2. Equal: Determines if the left side equals the right side.
 3. Equal (case Insensitive): Determines if the left side equals the right side (if this is a string comparison, this is case-insensitive)
 4. Match regular expression: Determines if the left side matches the regular expression specified on the right side.
 5. Matches wildcard: Determines if the left side matches the wildcard specified on the right side.
 6. Not equals: Determines if the left side does not equal the right side.
 - iii. Right Operand: Enter the value for the right operand.
2. Use Add Event:
 - a. Left Operand: Enter the value for the left operand.
 - b. Operator: From the dropdown list, choose the operator to use for comparing the value:
 - i. Does not match wildcard: Determines if the item does not match all items in the wildcard example
 - ii. Equal: Determines if the left side equals the right side.
 - iii. Equal (case Insensitive): Determines if the left side equals the right side (if this is a string comparison, this is case-insensitive)
 - iv. Match regular expression: Determines if the left side matches the regular expression specified on the right side.
 - v. Matches wildcard: Determines if the left side matches the wildcard specified on the right side.
 - vi. Not equals: Determines if the left side does not equal the right side.
 - c. Right Operand: Enter the value for the right operand.

Back to: [Task](#)

Terminal

Terminal

The Terminal adapter provides the functionality to execute commands, scripts and session-based activities against a system or network device using SSH or Telnet. While SSH is more secure than telnet, many environments use a telnet connection and using a SSH connection against such devices will not be possible. The Terminal adapter allows you the flexibility to execute against those devices.

The Terminal adapter allows Action Orchestrator to run commands and script activities on a system or network device that has Secure Shell (SSH) enabled. The Terminal adapter also contains three session-based activities that allow you to open new SSH/Telnet sessions and interact with the previously opened sessions.

SSH and Telnet leverage the same command execution activities differentiated by the target type they are deployed against. For example, an IOS target can have SSH or telnet optionally configured.

Action Orchestrator requires SFTP to be configured on the Unix/Linux system to execute SSH activities. SFTP is not needed for the SSH/Telnet Terminal Session activities.

The Terminal Adapter for Action Orchestrator:

Provides host-based and public key authentication and improves upon the existing expects functionality. The authentication enhancement allows users to apply host-based authentication from the adapter level. Users can also apply public key authentication on the device target level.

1. Allows you to create expect templates for their login expects. Expect templates allow you to leverage existing login expect sequences when applying expects to a device target or activity.
2. Is now FIPS-compliant and allows you to enable FIPS-compliant algorithms.

The following sections display Terminal activities:

- [Execute Terminal Command\(s\)](#)

Execute Terminal Command(s)

Execute Terminal Command(s)

Use the Execute Terminal Command(s) activity to send commands to a session started by a previous Open Terminal Session activity. To define the Execute Terminal Command(s) activity:

1. In the Workflow Editor Toolbox, choose **Activities > Terminal > Execute Terminal Command(s)**, then drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for execute terminal command(s) activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Terminal Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key User: Check this radio button to use the target's default account key user.
 - ii. Override Account Key User: Check this radio button to override the workflow account key user. You can select the appropriate Account key User ID or **+ADD NEW** from the dropdown list. For more information, see [Terminal Key-Based Credentials](#) or [Terminal Password-Based Credentials](#).
 - d. Under **Terminal**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Input Command(s): Enter the appropriate commands and inputs that a user can send to an open session.
 - ii. Ends with Special Character (Only If Send All the Lines As One Input Selected): Select the appropriate option to place at the end of the lines that is sent with the input from the dropdown list. Use options CTRL_A through CTRL_Z.
 - iii. Multiple Lines Option: Specify the following information:
 1. Send All the Lines As One Input: Select this radio button to send all lines in the plain text as one input.
 2. Send Next Line Only if Previous Line Succeeded: Select this radio button to send a line as an input if there is a previous line before the input.
 - iv. Individual Command Timeout (Seconds): Enter a value to specify the time frame to wait for an individual user input to be completed before timing out.
 - v. Expects (regex): Under Failed (Completed), click **+ADD** to enter the regex character.

Back to: [Terminal](#)

Unix/Linux System

Unix/Linux System

The Unix/Linux system provides the functionality to execute commands, scripts and session-based activities against a system or network device using SSH or Telnet. While SSH is more secure than telnet, many environments use a telnet connection and using a SSH connection against such devices will not be possible. The Unix/Linux system allows you the flexibility to execute against those devices.

The Unix/Linux system allows Action Orchestrator to run commands and script activities on a system or network device that has Secure Shell (SSH) enabled. The Unix/Linux system also contains three session-based activities that allow you to open new SSH/Telnet sessions and interact with the previously opened sessions.

SSH and Telnet leverage the same command execution activities differentiated by the target type they are deployed against. For example, an IOS target can have SSH or telnet optionally configured. Action Orchestrator requires SFTP to be configured on the Unix/Linux system.

The following sections display UNIX/LINUX System activities:

- [Execute Linux/Unix SSH Command](#)
- [Execute Linux/Unix SSH Script](#)
- [Write File](#)

Execute Linux/Unix SSH Command

Execute Linux/Unix SSH Command

Use the Execute Unix/Linux SSH Command activity to specify a SSH command to execute. To properly run this activity, Cisco Orchestration Process requires SFTP to be configured on the SSH server. This activity is only supported against the Unix/Linux system target. Korn Shell is also required.

Pipe is not supported by the Execute Unix/Linux SSH Command activity. If the user needs to execute pipe in an activity, it is recommended that the user places the pipe in the Execute Unix/Linux SSH Script activity.

For example, you can enter `ps -ef` in the Execute Unix/Linux SSH Command activity, but if you need to execute `ps -ef | grep myusername` then, that information should be placed in the Execute Unix/Linux SSH Script activity.

When the Execute Unix/Linux SSH Command activity is launched, the results of the executed SSH command are displayed from the Operations Workspace activity instance view.

1. In the Workflow Editor Toolbox, choose **Unix/Linux System > Execute Linux/Unix SSH Command** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Execute Linux/Unix SSH Command activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the drop-down list. For more information, see [Unix/Linux Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Click this radio button to use the target's default account key.
 - ii. Override Account Key: Click this radio button to override the workflow account key. You can select the appropriate account key or **+ADD NEW** from the drop-down list. For more information, see [Terminal Key-Based Credentials](#) or [Terminal Password-Based Credentials](#).
 - d. Under **Unix/Linux**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Input Command: Enter the actual command to execute an activity on the SSH server. See [Command Line Examples](#).
 - ii. Individual Command Timeout (Seconds): Enter a value to specify the time frame to wait for an individual user input to be completed before timing out.
 - iii. Expects (regex): Under **Failed (Completed)**, click **+ADD** to enter the regex character.

Command Line Examples

The following are Terminal adapter command line examples.

Example:

If your local working directory is:

```
/home/myusername/myappdata
```

and the command is

```
/myAppPath/myShellScript.sh
```

the full path is:

```
/home/myusername/myappdata/myAppPath/myShellScript.sh.
```

Example:

on Unix systems:

```
ls  
/usr/bin/ls
```

If your command is located at the directory of:

```
/myCommandPath  
and the command is  
myCommand
```

the full path is:

```
/myCommandPath/myCommand
```

Back to: [Unix/Linux System](#)

Execute Linux/Unix SSH Script

Execute Linux/Unix SSH Script

Use the Execute Unix/Linux SSH Script activity to specify a SSH script argument to execute.

When the Execute Unix/Linux SSH Script activity is launched, the results of the executed SSH script argument are displayed from the Operations Workspace activity instance view.

 To properly run this activity, SFTP must be configured on the SSH server.

1. In the Workflow Editor Toolbox, choose **Unix/Linux System** > **Execute Linux/Unix SSH Script** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Execute Linux/Unix SSH Command activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the drop-down list. For more information, see [Unix/Linux Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Click this radio button to use the target's default account key.
 - ii. Override Account Key: Click this radio button to override the workflow account key. You can select the appropriate account key or **+ADD NEW** from the drop-down list. For more information, see [Terminal Key-Based Credentials](#) or [Terminal Password-Based Credentials](#).
 - d. Under **Unix/Linux**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Local Working Directory on Target: Enter the path to the local working directory on the SSH server where the script will be executed.
 - ii. Script Arguments: Click **+ADD** to enter the collection of argument values for the script. See [Script Argument Example](#).
 - iii. Script to Execute on Target: Enter the actual script code to use to execute in the specified local working directory.
 - iv. Expects (regex): Under **Failed (Completed)**, click **+ADD** to enter the regex character.

Script Argument Example

The following is an example of a script containing four arguments.

Script to Execute

```
#!/bin/csh
echo ${0}
echo Number of arguments is $#argv
echo $2
echo $argv[2-3]
echo $argv[$]
exit
```

Script Arguments

```
% argex.csh hello world 42 3.14159 (300:400,~100)
```

Script Output

```
argex.csh
Number of arguments is 4
42
42 3.14159
(300:400,~100)
```


Back to: [Unix/Linux System](#)

Write File

Write File

Use the Write File activity to append to existing file, overwrite existing file, and not to overwrite if file exists using the encoding options such as ASCII, UTF-16, UTF-32, etc.

1. In the Workflow Editor Toolbox, choose **Unix/Linux System > Write File** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Write File activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [Unix/Linux Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the dropdown list. For more information, see [Terminal Key-Based Credentials](#) or [Terminal Password-Based Credentials](#).
 - d. Under **Unix/Linux**, specify the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Local File Name: Enter the file path along with the local file name in which the contents is written. For example, /root/file.txt
 - ii. Content: Enter the appropriate contents to be added in the file.

 The maximum number characters is limited to 1048576.
 - iii. Encoding: Select the appropriate encoding class from the dropdown list:
 1. ASCII: An encoding for the ASCII (7-bit) character set.
 2. UTF-16: An encoding object for the UTF-16 format using little endian format byte format.
 3. UTF-32: An encoding object for the UTF-32 format using little endian format byte format.
 4. UTF-7: An encoding format is less robust and secure than UTF-8, UTF-16, or UTF-32.
 5. UTF-8: An encoding for the UTF-8 format.
 - iv. Options: Select the appropriate action from the dropdown list. The following action is used when saving the file:
 1. Append to existing file
 2. Do not overwrite if file exists
 3. Overwrite existing file

Back to: [Unix/Linux System](#)

Web Service

Web Service

Web services are components on a Web server that a client application can call by making HTTP requests across the Web. The Action Orchestrator Web Service adapter is designed to support general web service calls. The adapter allows users to send requests using web service methods and other parameters to generate an XML output. Web Targets allow activities to execute against a web site or web service that is hosted by several machines.

The following sections display Web Service activities:

- [HTTP Request](#)
- [Swagger HTTP Request](#)


HTTP Request

HTTP Request

Use the Web HTTP Request activity to send a request for a file based on a URL, HTTP headers, or Cookies data. This request generates a response in an output file provided by the web server.

This activity supports generic HTTP operations, such as POST and GET, and is used to retrieve a web page and then examine the results to ensure there are no errors. The activity can be used to perform synthetic transactions against portals or other web sites.

1. In the Workflow Editor Toolbox, choose **Web Service** > **HTTP Request** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name: Enter the unique display name for the activity.
 - ii. Description: Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for HTTP Request activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target: Check this radio button to use the workflow target.
 - ii. Override Workflow Target: Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [HTTP Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key: Check this radio button to use the target's default account key.
 - ii. Override Account Key: Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the dropdown list. For more information, see [HTTP Basic Authentication](#) or [HTTP Client Certificate Authentication](#).
 - d. Under **HTTP Request**, enter the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Relative URL: Enter the relative URL to be requested. The base URL will be determined by the web target combined with the relativeURL during the activity execution. Use slash (/) before the URL, for example: /system/v1/auth/login
 - ii. Method: Select the method to be performed on the resource identified by the Request-URI from the dropdown list such as GET, POST, PUT, and so forth.
 - iii. Request Body: Enter the message body to be carried in the HTTP request.

 You will be able modify the request body formats using Format option in the right bottom such as JSON, Text, XML, and so forth.
 - e. Under **Headers**, enter the following information:
 - i. Content Type: Select the appropriate value for the content type used to define the structure of the outputs such as HTML, JSON, Plain Text, and so forth.
 - ii. Accept: Enter the value of the Accept HTTP header.
 - iii. User-Agent: Enter the value of the User-agent HTTP header.
 - iv. Custom Headers: Click **+ADD**, to enter the **Header** and **Value**.
 - v. Cookie: Click **+ADD**, to enter the cookie to be accepted from HTTP request.
 - f. Under **Behavior**, specify the appropriate information:
 - i. Allow auto redirect: Check this check box to allow the header request to be redirected automatically. It is checked by default.
 - ii. Continue on HTTP Error Status Code: Check this check box to allow the header request to continue on HTTP Error Status Code.

Back to: [Web Service](#)

Swagger HTTP Request

Swagger HTTP Request

Use the Swagger HTTP Request activity to send a request for a file based on a URL, HTTP headers, or Cookies data.

1. In the Workflow Editor Toolbox, choose **Web Service** > **Swagger HTTP Request** and drag and drop the activity onto the Workflow pane.
2. On the Workflow Properties pane, enter the following information:
 - a. Under **General**, specify the following information:
 - i. Display Name - Enter the unique display name for the activity.
 - ii. Description - Enter the brief description about the activity.
 - iii. Activity Timeout (Seconds): Enter the number of seconds to wait for Swagger HTTP Request activity to fail because it timed out.
 - iv. Check the **Continue Workflow Execution on Failure** check box to continue the workflow execution on failure of the activity.
 - b. Under **Target**, specify the following information:
 - i. Use Workflow Target - Check this radio button to use the workflow target.
 - ii. Override Workflow Target - Check this radio button to override the workflow target. You can select the appropriate target or **+ADD NEW** from the dropdown list. For more information, see [HTTP Endpoint](#).
 - iii. Use Workflow Target Group: Check this radio button to use the workflow target group.
 - iv. Override Workflow Target Group Criteria: Check this radio button to override the workflow target group criteria.
 - c. Under **Credentials**, specify the following information:
 - i. Use Target's Default Account Key - Check this radio button to use the target's default account key.
 - ii. Override Account Key - Check this radio button to override the workflow account key. You can select the appropriate Account key or **+ADD NEW** from the dropdown list. For more information, see [HTTP Basic Authentication](#) or [HTTP Client Certificate Authentication](#).
 - d. Under **Browse APIs**, enter the **Swagger URL** to be requested or click **Browse** icon to choose your URL.
 - e. Under **HTTP Request**, enter the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Relative URL - Enter the relative URL to be requested. The base URL will be determined by the web target combined with the relative Url during the activity execution.
 - ii. Method - Select the method to be performed on the resource identified by the Request-URI from the dropdown list such as Get, Post, Put, and so forth.
 - iii. Request Parameters - Enter the message parameters to be carried in the HTTP request.
 - iv. Request Body - Enter the message body to be carried in the HTTP request.
- f. Under **Headers**, enter the following information or click [Variable Reference](#) icon to choose any variable:
 - i. Content Type: Select the appropriate value from the dropdown list to be used for defining the structure of the outputs such as HTML, JSON, Plain Text, and so forth.
 - ii. Custom Headers: Click **+ADD**, to enter the **Header** and **Value**.
 - iii. Cookie: Click **+ADD**, to enter the cookie to be accepted from HTTP request.
- g. Under **Behavior**, check the **Continue on HTTP Error Status Code** check box to allow the header request to continue on HTTP Error Status Code.



You will be able to modify the request parameters and body formats using Format option in the right bottom such as JSON, Text, XML, and so forth.

Back to: [Web Service](#)

Creating an Atomic Workflow

Creating an Atomic Workflow

The atomic workflows allow you to group the workflows in a group name under the activities. This helps you to drag and drop the workflows as activities from the customized group name. The following procedure provides information on creating an atomic workflow in Action Orchestrator:



Conditions for Atomic Workflow

- The users with *Adapter Author* role only would be able to create atomic workflows. These options would not be enabled for other roles. For more information on Roles and Permissions, see [Action Orchestrator Roles](#).
- A workflow with trigger can't be marked as atomic workflow.
- An atomic workflow can only be edited by users with *modify* permission for that workflow.
- An atomic workflow instances are stored if **Delete Instance After execution** is not selected in the parent workflow.
- An atomic workflow instances are accessible to users with *modify* permission for the corresponding atomic workflow.
- An atomic Action tab is visible to users with *tenant_admin* role. The *tenant_admins* have *manage* permission for the atomic workflows created by Adapter Authors.
- An atomic workflow inside an atomic workflow is not allowed that is nested atomic workflow is not allowed.



Identify any drag and drop objects in the toolbox that will be required by your new atomic workflow.

1. Choose **Workflows > Atomic Workflows > NEW WORKFLOW**.
2. On the Workflow Properties panel, define the workflow properties (see [Adding Workflow Properties](#)).
3. From the Activities pane, drag and drop the appropriate items onto the workflow pane (see [Activities Panel](#)).
4. On the Properties panel, define the properties for each object selected on the workflow pane. The available property pages are determined by the selected objects (see [Activities](#)).
5. When all of the property pages are complete, click **VALIDATE** on the header to validate the workflow.



If the workflow is not valid, click on activities that are orange and determine warnings in the upper right corner of the Properties pane. Enter the required information and validate again.

6. Once the workflow is successfully validated, click **Commit** on the header to export the workflow to your repository.
 - On the **Commit** panel, enter the **File Name** and **Commit Message**.
 - Click **Commit**, to export the workflow.



This is an optional step.

For more information on workflow export, see [Export Workflows](#).

For more information on repository, see [Git Repositories](#).

7. Once the workflow is successfully validated, click **RUN** on the header to execute the workflow.
8. Once the workflow execution starts, you will be taken to the **Runs** page where you can observe the workflow:
 - a. Status: Such as Running, Success, and Failed in the top left next to the workflow name.
 - b. Auto-Refresh: You can switch **ON** or **OFF** the auto refresh using the **Switch** icon on the top right.
 - c. Cancel Run: Click **Cancel Run** on the top right to cancel the running workflow.
 - d. Run time: Displays the time taken for the completion of the workflow on the top right.



For more information, see [Runs](#).

9. Click **Edit Workflow** on the top right of the **Runs** page to edit the workflow. This option will be enabled only after workflow completion.

Adding Logic Components to a Workflow

Adding Logic Components to a Workflow

Insert logic components into a workflow to support or configure the workflow logic and provide control over the workflow execution.

The following table summarizes the types of logic components and when to use them.

Activity Type	Purpose
Break	It terminates the current loop and resumes execution on the next activity. The break logic can be used in both While and For Each loops.
Completed	Signal the completion of an activity and terminate the workflow. The component ends the workflow and sets the state of the workflow to Succeeded, Failed (Completed), or Failed (Not Completed).
Condition Block	Execute one of the defined Condition Branches in a workflow. It checks conditions for each of the branches, in order from left to right, and executes the first Condition Branch whose condition is true.
For Each	Add the activities to the workflow that should be executed one time for each item in the target source.
Group	Run activities in a block in a sequential order. Group block is used mainly to group a set of actions logically and the block can be collapsed or expanded in the workflow designer. Group block should be able to move inside other logic blocks just like an action.
Parallel Block	Run two or more branches of a workflow simultaneously. The component consists of two or more sequential block components that execute their activities in parallel.
Start Point	Indicate points within a workflow (in addition to the top of the workflow) at which you can start the workflow. You will always be able to start the workflow from the beginning. However, if a workflow contains a Start Point component, then you can start the process from the location of the Start Point within the workflow.
While Loop	Execute a sequence of child activities (contained in the While Block) that repeats as long as the specified condition is true.

To add logic components to a process:


1. In the Workflow Editor, choose **Logic** tab from the Left pane, then highlight and drag the appropriate logic component to the Workflow pane.
2. On the component property pages, define the properties.

Variable Reference

Variable Reference

The Variable Reference icon displayed next to a text field indicates that the field can be populated by referencing a defined variable or the property of another activity or workflow or Environments. Use the Browse Variables dialog box to select a defined variable or reference an object to populate a field. The **SAVE** button does not activate until a valid property or variable is selected. The different types of data that you can refer:

- ENV: You can choose environment settings as variables such as **ACTION ORCHESTRATOR_LOOP_LIMIT**.
- Global: You can choose global variables that you have created such as Date Time, Table, Boolean, and so forth.
- Workflow: You can choose output of the workflow as variables such as Instance ID, Start Time, and so forth.
- Activities: You can choose the activity properties as variables such as End time, Start time, Succeeded, and so forth.
- Trigger: You can choose the trigger properties as variables.

 Depending on the object type, some of these variables might not be available.

Reference Variable	Description
Name	Display name of the object
Columns	Column of the table variable
Items	Items in the variable
First	The first name and age in the variable
Last	The name and age in the variable
Start Time	Date and time the activity was started
End Time	Date and time the activity stopped
Results	Results of the activity
Instance ID	ID number of the Action Orchestrator workflow instance
Body	Body of the activity
Succeeded	Indicates the activity has succeeded

Share Workflow

Share Workflow

Use the Share option from the workflow dropdown to share object permission to other users or groups.



To share a workflow, you must be an owner of the workflow or user with Manage permissions such as system admin. You won't see this option if you are not having the required permissions. For more information on roles and permissions, see [Action Orchestrator Roles](#).

1. In the default home page, choose **Share** from the workflow dropdown.



Hover your mouse cursor over the created workflow card and click the dropdown list to view the Share option.

2. In the **Share Permissions** dialog box, specify the following information:
 - a. The share permissions dialog box displays the **Users** and **Groups** having access to the workflow.
 - b. Under **Add Users**, select the users from the dropdown list or just type in few letters of the name to choose the required user. You can also invite the user using **Invite By Email** option.
 - i. **Shared With**: Displays the name of the user with share permissions.
 - ii. **Access**: Select the appropriate permission from the dropdown list such as View, Modify, and Manage.
 - iii. **Can Run**: Enable or disable the Run permission using the switch icon.
 - iv. **Actions**: You can delete the user from the actions column.
 - c. Click **Save**, to save the sharepermissions.

Runs

Runs

The Runs page is used to monitor the state of workflow runs that are cancelled, created, failed, running, successful, and total. You will also be able to filter the runs on the basis of workflow run days such as all, yesterday, 30 days, 10 Days, and so forth.

The Action Orchestrator workflow executions are queued and executed asynchronously.

In workflow you have to start API and pass query parameter (`sync=true`) to execute workflow in synchronous mode. This API call provides you the status of the workflow stating if the workflow is running or Success or Failed. Based on the workflow status, you can poll to get the workflow execution is success.

For example: You can gather values for an input field in the catalog or another workflow to run the workflows synchronously.

- The **Filter** icon allows you to filter the workflow runs based on the following
 - **Workflow Name:** Choose the workflow name from the drop-list by checking the appropriate workflow check box.
 - **Last Run Status:** Choose the status in the runs page by checking the check box under Last Run Status such as Cancelled, Created, Failed, and so forth.
 - **Owner:** Choose the owner name by checking the appropriate owner check box.
- The **Search** icon allows you search for the workflow runs based on the names.
- The **Auto-Refresh** switch icon allows you to switch **ON** or **OFF**. This enables or disables auto refresh of the workflow during the execution of each activity of the workflow.
- The page displays the following information of the existing or filtered workflows:
 - **Display Name:** Displays the workflow name along with the number of times the workflow is executed such as Run 0, Run 1, and so on. The color codes along with the workflow name denotes the status:
 - Green: Denotes Success.
 - Red: Denotes Failed.
 - Orange: Denotes Running.
 - **Version:** Displays the Action Orchestrator version number.
 - **Status:** Displays the status of the workflow such as running, success, failed, and so forth.
 - **Started On:** Displays the start date and time of the workflow execution.
 - **Ended On:** Displays the end date and time of the workflow execution.
 - **Actions:** By using the dropdown icon in actions column, you can delete the workflow being displayed in the Runs page.

Configuring Targets

Configuring Targets

- [Overview Targets](#)
- [Targets](#)
- [Target Groups](#)
- [Add Target Type](#)

Overview Targets

Adding Targets and Target Groups

When you create a workflow, you must specify where you want the workflow to run. You can also specify that the workflow runs on a specific target or target group.

The target group can be defined once and reused in several workflows. For example, you might have a database maintenance workflow that is scheduled to run every month on all database servers. Instead of scheduling the workflow multiple times to run on each database server, you can create a target group that includes all the database servers and schedule the workflow to run on all the servers at the same time.

If you choose to execute the workflow on a target group, you can further specify to run the workflow on all objects that are included in the target group, or run the workflow on a specific object within the target group.

Service instances are targets. A target type allows you to define a new service; all new targets are created based on a target type.

- [Targets](#)
- [Target Groups](#)

Targets

Targets

The following sections display list of targets:

- [Targets Overview](#)
- [AMQP Endpoint](#)
- [AWS Endpoint](#)
- [Amazon Device Endpoint](#)
- [Ansible Tower Endpoint](#)
- [CloudCenter Endpoint](#)
- [Google Cloud Platform Endpoint](#)
- [HTTP Endpoint](#)
- [IMAP Endpoint](#)
- [JDBC Database Server](#)
- [KAFKA Endpoint](#)
- [Meraki Endpoint](#)
- [Microsoft Windows Endpoint](#)
- [POP3 Endpoint](#)
- [Prime Service Catalog Endpoint](#)
- [SMTP Endpoint](#)
- [Terminal Endpoint](#)
- [Unix/Linux Endpoint](#)

Targets Overview

Overview

Use **Targets > Targets** to view the defined targets. From this view, you can create new target by clicking **New Target**, modify the properties of a target, and delete targets. You can also add the target from the workflow or activities properties pane. You can define a target once and then reuse it in multiple processes. These are the following targets that can be created from Action Orchestrator:

AMQP Endpoint

AMQP Endpoint

On the **ADD NEW TARGET** Panel, perform the following procedure to add an AMQP Endpoint target:

1. Under **Target Type**: Select the **AMQP Endpoint** target type from the drop-down list.
2. Under **General**, specify the appropriate information:
 - a. **Display Name**: Enter the unique display name for the target.
 - b. **Description**: Enter the brief description about the target.
3. Under **Account Key**, select the appropriate existing Account Key or click **ADD NEW** from the drop-down list, see [AMQP Certificate-Based Credentials](#), [AMQP Password-Based Credentials](#), or [AMQP Password-Less Certificate-Based Credentials](#).
4. Under **AMQP**, specify the appropriate information:
 - a. **Host/IP Address**: Enter the host name or IP address for the AMQP Endpoint.
 - b. **Port**: Enter the AMQP protocol port number; the default port is 5671.
 - c. **Virtual Host**: Enter the virtual host name or IP address for the AMQP Endpoint.

A Virtual Host is a namespace for objects like Exchanges, Queues and Bindings.
 - d. **SSL enabled**: Indicates whether SSL is enabled on the AMQP Endpoint.
 - e. **Ignore Certificate Errors**: Ignore the certificate error messages when attempting to connect to the service portal.
5. Click **Submit**, to add and save the Target.

AWS Endpoint

AWS Endpoint

On the **ADD NEW TARGET** Panel, perform the following procedure to add AWS Endpoint target:

1. Under **Target Type**: Select the **AWS Endpoint** target type from the dropdown list.
2. Under **General**, specify the appropriate information:
 - a. **Display Name**: Enter the unique display name for the target.
 - b. **Description**: Enter the brief description about the target.
3. Under **Account Key**, select the appropriate existing Account Key or click **ADD NEW** from the dropdown list, see [AWS Credentials](#).
4. Under **AWS**, enter the Amazon Web Services **Region**.
5. Click **Submit**, to add and save the Target.

Amazon Device Endpoint

Amazon DeviceEndpoint

On the **ADD NEW TARGET** Panel, perform the following procedure to add Amazon Device Endpoint target such as Alexa, Echo Dot, etc.

1. Under **Target Type**: Select the **Amazon DeviceEndpoint** target type from the drop-down list.
2. Under **General**, specify the appropriate information:
 - a. Display Name: Enter the unique display name for the target.
 - b. Description: Enter the brief description about the target.
3. Under **Account Key**, select the appropriate existing Account Key or click **ADD NEW** from the drop-down list, see [Amazon Alexa Device Credentials](#).
4. Under **IOT**, enter the following information:
 - a. Device ID: Enter the device id of the Amazon device.
 - b. Device Serial Number: Enter the unique identification number of the device.
5. Click **Submit**, to add and save the Target.

Ansible Tower Endpoint

Ansible Tower Endpoint

On the **ADD NEW TARGET** Panel, perform the following procedure to add Ansible Tower Endpoint target:

1. Under **Target Type**: Select the **Ansible Tower Endpoint** target type from the dropdown list.
2. Under **General**, specify the appropriate information:
 - a. **Display Name**: Enter the unique display name for the target.
 - b. **Description**: Enter the brief description about the target.
3. Under **Account Key**, select the appropriate existing Account Key or click **ADD NEW** from the dropdown list, see [Ansible Tower Credentials](#).
4. Under **Ansible Tower Endpoint**, enter the following information:
 - a. **Protocol**: Select the appropriate protocol from the dropdown list.
 - i. HTTP
 - ii. HTTPS
 - b. **Host/IP Address**: Enter the host name or IP address for the Ansible Tower Endpoint.
 - c. **Port**: Enter the Ansible Tower port number.
 - d. **Disable server certification validation**: Indicates if server certification validation is disabled on the Ansible Tower Endpoint.
5. Click **Submit**, to add and save the Target.

CloudCenter Endpoint

CloudCenter Endpoint

On the **ADD NEW TARGET** Panel, perform the following procedure to add CloudCenter Endpoint target:

1. Under **Target Type**: Select the **CloudCenter Endpoint** target type from the dropdown list.
2. Under **General**, specify the appropriate information:
 - a. Display Name: Enter the unique display name for the target.
 - b. Description: Enter the brief description about the target.
3. Under **Account Keys**, select the appropriate existing Account Key or click **ADD NEW** from the dropdown list, see [CloudCenter Suite Explicit User](#).
4. Under **CloudCenter Suite**, enter the following information:
 - a. Protocol: Select the appropriate protocol from the dropdown list.
 - i. HTTP
 - ii. HTTPS
 - b. Host/IP Address: Enter the host name or IP address for the CloudCenter Endpoint.
 - c. Port: Enter the CloudCenter port number.
5. Click **Submit**, to add and save the Target.

Google Cloud Platform Endpoint

Google Cloud Platform Endpoint

On the **ADD NEW TARGET** Panel, perform the following procedure to add Google Cloud Platform (GCP) Endpoint target:

1. Under **Target Type**: Select the **Google Cloud Platform Endpoint** target type from the dropdown list.
2. Under **General**, specify the appropriate information:
 - a. **Display Name**: Enter the unique display name for the target.
 - b. **Description**: Enter the brief description about the target.
3. Under **Account Key**, select the appropriate existing Account Key or click **ADD NEW** from the dropdown list, see [Google Cloud Platform Authentication](#).
4. Under **Google Cloud Platform**, specify the following information:
 - a. **Protocol**: Select the appropriate protocol from the dropdown list.
 - b. **Host/IP Address**: Enter the host name or IP address for the GCP Endpoint.
 - c. **Scope**: Enter the appropriate scope to request an access token from Google authorization server to access protected resources such as read-only, read-write, full-control, and so forth.
5. Click **Submit**, to add and save the Target.

HTTP Endpoint

HTTP Endpoint

On the **ADD NEW TARGET** Panel, perform the following procedure to add HTTP Endpoint target:

1. Under **Target Type**: Select the **HTTP Endpoint** target type from the dropdown list.
2. Under **General**, specify the appropriate information:
 - a. Display Name: Enter the unique display name for the target.
 - b. Description: Enter the brief description about the target.
3. Under **Account Key**, specify the appropriate information:
 - a. Select **True** or **False** from the **No Account Key** dropdown list.
 - b. select the appropriate Account Key or click **ADD NEW** from the **Default Account Key** dropdown list, see [HTTP Basic Authentication](#) or [HTTP Client Certificate Authentication](#).
4. Under **HTTP**, enter the following information:
 - a. Protocol: Select the appropriate protocol from the dropdown list.
 - i. HTTP
 - ii. HTTPS
 - b. Host/IP Address: Enter the host name or IP address for the HTTP Endpoint.
 - c. Port: Enter the HTTP port number; the default port is 9092.
 - d. Path: Enter the HTTP path.
 - e. Disable server certificate validation: Indicates if server certification validation is disabled on the HTTP Endpoint.
5. Under **Proxy**, enter the following information:
 - a. Proxy URL: Enter the URL of the proxy server.
 - b. User Name: Enter the user name of the proxy server.
 - c. Password: Enter the password of the proxy server.
6. Click **Submit**, to add and save the Target.

IMAP Endpoint

IMAP Endpoint

The IMAP email server allows an email client, such as Microsoft Outlook, to retrieve email on a remote mail server.

On the **ADD NEW TARGET** Panel, perform the following procedure to add IMAP Endpoint target:

1. Under **Target Type**: Select the **IMAP Endpoint** target type from the dropdown list.
2. Under **General**, specify the appropriate information:
 - a. **Display Name**: Enter the unique display name for the target.
 - b. **Description**: Enter the brief description about the target.
3. Under **Account Key**, select the appropriate existing **Account Key** or click **ADD NEW** from the dropdown list, see [Email Credentials](#).
4. Under **IMAP**, enter the following information:
 - a. **IMAP Server**: Name of the email server that relays email to the mailbox.
 - b. **IMAP Port**: The port number for the IMAP server. Default is 143.
 - c. **Protocol**: Display-only field of the type of email protocol being used by the email server
 - d. **TLS Authentication Enabled**: If checked, the authorization of the Email server will use TLS.
 - e. **Ignore Certificate Errors**: If checked, any errors regarding the certificate will be ignored.
 - f. **Polling Interval (SEC)**: Specify the interval time period in seconds. Default is 10 seconds.
5. Click **Submit**, to add and save the Target.

JDBC Database Server

JDBC Database Server

On the **ADD NEW TARGET** Panel, perform the following procedure to add a JDBC data server target:

1. Under **Target Type**: Select the **JDBC Database Server** target type from the dropdown list.
2. Under **General**, specify the appropriate information:
 - a. Display Name: Enter the unique display name for the target.
 - b. Description: Enter the brief description about the target.
3. Under **Account Key**, select the appropriate existing Account Key or click **ADD NEW** from the dropdown list, see [JDBC Login Credentials](#).
4. Under **Database**, specify the appropriate information:
 - a. Database server type: Select the appropriate database server type from dropdown list:
 - i. MYSQL
 - ii. Microsoft SQL Server
 - iii. Oracle Server
 - iv. SAP HANA
 - b. Server IP Address: Enter the Host address or the IP address of the database server.
 - c. Port: Enter the port number used to access the SQL database.
 - d. Database Name: Enter the name of the database.
5. Click **Submit**, to add and save the Target.

KAFKA Endpoint

KAFKA Endpoint

On the **ADD NEW TARGET** Panel, perform the following procedure to add Kafka Endpoint target:

1. Under **Target Type**: Select the **Kafka Endpoint** target type from the dropdown list.
2. Under **General**, specify the appropriate information:
 - a. Display Name: Enter the unique display name for the target.
 - b. Description: Enter the brief description about the target.
3. Under **Account Key**, specify the appropriate information:
 - a. Select **True** or **False** from the **No Account Key** dropdown list.
 - b. select the appropriate existing Account Key or click **ADD NEW** from the **Default Account Key** dropdown list, see [Kafka Authentication](#) or [Kafka Certificate Authentication](#).
4. Under **Kafka**, enter the following information:
 - a. Host/IP Address: Enter the host name or IP address for the Kafka Endpoint.
 - b. Port: Enter the Kafka port number; the default port is 9092.
 - c. SSL enable: Indicates if SSL is enabled on the Kafka Endpoint.
 - d. Disable server certification validation: Indicates if server certification validation is disabled on the Kafka Endpoint.
5. Click **Submit**, to add and save the Target.

Meraki Endpoint

Meraki Endpoint

On the **ADD NEW TARGET** Panel, perform the following procedure to add Meraki Endpoint target:

1. Under **Target Type**: Select the **Meraki Endpoint** target type from the dropdown list.
2. Under **General**, specify the appropriate information:
 - a. Display Name: Enter the unique display name for the target.
 - b. Description: Enter the brief description about the target.
3. Under **Account Key**, select the appropriate existing Account Key or click **ADD NEW** from the dropdown list, see [Meraki Credentials](#).
4. Under **Meraki**, enter the following information:
 - a. Protocol: Select the appropriate protocol from the dropdown list.
 - i. HTTP
 - ii. HTTPS
 - b. Host/IP Address: Enter the host name or IP address for the Meraki Endpoint.
 - c. Port: Enter the Meraki port number.
5. Click **Submit**, to add and save the Target.

Microsoft Windows Endpoint

Microsoft Windows Endpoint

On the **ADD NEW TARGET** Panel, perform the following procedure to add Microsoft Windows Endpoint target:

1. Under **Target Type**: Select the **Microsoft Windows Endpoint** target type from the dropdown list.
2. Under **General**, specify the appropriate information:
 - a. **Display Name**: Enter the unique display name for the target.
 - b. **Description**: Enter the brief description about the target.
3. Under **Account Keys**, select the appropriate Account Key or click **ADD NEW** from the **Default Account Keys** dropdown list, see [Microsoft Windows Credentials](#).
4. Under **Windows**, enter the following information:
 - a. **Protocol**: Select the appropriate protocol from the dropdown list.
 - i. HTTP
 - ii. HTTPS
 - b. **Host/IP Address**: Enter the host name or IP address for the HTTP Endpoint.
 - c. **Port**: Enter the HTTP port number; the default port is 5985.
5. Click **Submit**, to add and save the Target.

POP3 Endpoint

POP3 Endpoint

This target will allow a process or activity to execute against the an email account on an Post Office Protocol (POP3) email server.

On the **ADD NEW TARGET** Panel, perform the following procedure to add POP3 Endpoint target:

1. Under **Target Type**: Select the **POP3 Endpoint** target type from the dropdown list.
2. Under **General**, specify the appropriate information:
 - a. Display Name: Enter the unique display name for the target.
 - b. Description: Enter the brief description about the target.
3. Under **Account Key**, select the appropriate existing Account Key or click **ADD NEW** from the dropdown list, see [Email Credentials](#).
4. Under **POP3**, enter the following information:
 - a. POP3 Server: Name of the email server that relays email to the mailbox.
 - b. POP3 Port: The port number for the POP3 server. Default is 110.
 - c. Protocol: Display-only field of the type of email protocol being used by the email server
 - d. TLS Authentication Enabled: If checked, the authorization of the Email server will use TLS.
 - e. Ignore Certificate Errors: If checked, any errors regarding the certificate will be ignored.
 - f. Polling Interval (SEC): Specify the interval time period in seconds. Default is 10 seconds.
5. Click **Submit**, to add and save the Target.

Prime Service Catalog Endpoint

Prime Service Catalog Endpoint

On the **ADD NEW TARGET** Panel, perform the following procedure to add Prime Service Catalog Endpoint target:

1. Under **Target Type**: Select the **Prime Service Catalog Endpoint** target type from the dropdown list.
2. Under **General**, specify the appropriate information:
 - a. **Display Name**: Enter the unique display name for the target.
 - b. **Description**: Enter the brief description about the target.
3. Under **Account Keys**, select the appropriate Account Key or click **ADD NEW** from the **Default Account Keys** dropdown list, see [Cisco Prime Service Catalog Credentials](#).
4. Under **PSC**, enter the following information:
 - a. **Protocol**: Select the appropriate protocol from the dropdown list.
 - i. HTTP
 - ii. HTTPS
 - b. **Host/IP Address**: Enter the host name or IP address for the HTTP Endpoint.
 - c. **Port**: Enter the HTTP port number.
5. Click **Submit**, to add and save the Target.

SMTP Endpoint

SMTP Endpoint

On the **ADD NEW TARGET** Panel, perform the following procedure to add SMTP Endpoint target:

1. Under **Target Type**: Select the **SMTP Endpoint** target type from the dropdown list.
2. Under **General**, specify the appropriate information:
 - a. Display Name: Enter the unique display name for the target.
 - b. Description: Enter the brief description about the target.
3. Under **Account Key**, select the appropriate existing Account Key or click **ADD NEW** from the dropdown list, see [Email Credentials](#).
4. Under **Email**, enter the following information:
 - a. SMTP Server: Name of the email server to be used as the default server for sending email.
 - b. SMTP Port: The port number for the SMTP server.
 - c. Protocol: The default is SMTP protocol.
5. Click **Submit**, to add and save the Target.

Terminal Endpoint

Terminal Endpoint

On the **ADD NEW TARGET** Panel, perform the following procedure to add Terminal Endpoint target:

1. Under **Target Type**: Select the **Terminal Endpoint** target type from the dropdown list.
2. Under **General**, specify the appropriate information:
 - a. Display Name: Enter the unique display name for the target.
 - b. Description: Enter the brief description about the target.
3. Under **Account Key**, select the appropriate existing Account Key or click **ADD NEW** from the dropdown list, see [Terminal Key-Based Credentials](#) or [Terminal Password-Based Credentials](#).
4. Under **Connection Settings**, enter the following information:
 - a. Protocol: Select the appropriate protocol from the dropdown list.
 - i. SSH
 - b. Host: Enter the host name or IP address of the network device.
 - c. Port: Enter the port number used to access the appropriate terminal target port (Default: SSH server: 22).
5. Under **Terminal Interaction Patterns (regex)**, enter the following information:
 - a. Prompt: Enter the system prompt pattern in regular expression.
 - b. Additional Succeeded Prompts: Click **+ADD** to enter additional system prompt patterns in regular expressions.
6. Click **Submit**, to add and save the Target.

Unix/Linux Endpoint

Unix/Linux Endpoint

On the **ADD NEW TARGET** Panel, perform the following procedure to add Unix/Linux Endpoint target:

1. Under **Target Type**: Select the **Unix/Linux Endpoint** target type from the drop-down list.
2. Under **General**, specify the appropriate information:
 - a. **Display Name**: Enter the unique display name for the target.
 - b. **Description**: Enter the brief description about the target.
3. Under **Account Key**, select the appropriate existing Account Key or click **ADD NEW** from the drop-down list, see [Terminal Key-Based Credentials](#) or [Terminal Password-Based Credentials](#).
4. Under **Unix/Linux**, enter the following information:
 - a. **Host**: Enter the host name for the Unix/Linux Endpoint.
 - b. **Port**: Enter the Unix/Linux port number; the default port is 22.
 - c. **Default Bash Shell Path**: Enter the default bash shell path, the default is /bin/bash.
5. Click **Submit**, to add and save the Target.

Target Groups

Target Groups

Target groups are collections of targets. Often automation might need to run against all machines in a collection, or against one of the machines in a collection. Target groups provide this functionality.

Use **Targets > Target Groups** to view the defined target groups. From this view, you can create new target groups by clicking **New Target Group**, modify the properties of a target group, and delete target groups.

Add Target Group

On the **ADD NEW TARGETGROUP** Panel, perform the following procedure to add a new target group:

1. Under **General**, specify the appropriate information:
 - a. Display Name: Enter the unique display name for the target group.
 - b. Description: Enter the brief description about the target group.
2. Under **Selected Targets**, click **Add Target Type** to add target type. For more information, see [Add Target Type](#).

You will be able to edit and delete the created target type by using the drop-down icon from the actions column.
3. Click **Submit**, to add and save the Target Group.

Add Target Type

Add Target Type

Using Add Target Type you will be able to create Target Type Group, Using queries of their attributes, the Action Orchestrator provides type-based groupings of targets. For example, use a target group to group all targets of a given type, or to perform additional filtering to pattern match against a field in the target definition.

On the **Edit Target Type Panel**, perform the following procedure to add/edit a target type:

1. Under **General**, specify the appropriate information:
 - a. Under **Target Type**, select the appropriate target type from the drop-down list.
 - b. **Include All Targets of this Type**: Check this check box to include all targets of the selected target type.
2. Under **Add Conditions**, click **+ADD** to specify the condition, enter the following information:
 - i. **Left Operand**: Enter the value for the left operand.
 - ii. **Operator**: From the dropdown list, choose the operator to use for comparing the value:
 1. **Does not match wildcard**: Determines if the item does not match all items in the wildcard example
 2. **Equal**: Determines if the left side equals the right side.
 3. **Equal (case-insensitive)**: Determines if the left side equals the right side (if this is a string comparison, this is case-insensitive)
 4. **Greater Than**: Determines if a value is greater than another value.
 5. **Greater Than or Equal to**: Determines if a value is greater than or equal to another value.
 6. **Less Than**: Determines if a value is less than another value.
 7. **Less Than or Equal to**: Determines if a value is less than or equal to another value.
 8. **Match regular expression**: Determines if the left side matches the regular expression specified on the right side.
 9. **Matches wildcard**: Determines if the left side matches the wildcard specified on the right side.
 10. **Not equals**: Determines if the left side does not equal the right side.
 - iii. **Right Operand**: Enter the value for the right operand.
3. Under **Include Individual Targets**, select the specific target to be included of the selected target type.

This only includes the specific selected target and excludes all the other targets of the selected target type.

This option is disabled, if the Include All Targets of this Type option is enabled.

4. Click **OK**, to save the target type.

Back to: [Target Groups](#)

Configuring Account Keys

Configuring Account Keys

The following sections display list of account keys:

- [Account Keys Overview](#)
- [Amazon Alexa Device Credentials](#)
- [AMQP Certificate-Based Credentials](#)
- [AMQP Password-Based Credentials](#)
- [AMQP Password-Less Certificate-Based Credentials](#)
- [Ansible Tower Credentials](#)
- [Cisco Prime Service Catalog Credentials](#)
- [CloudCenter Suite Explicit User](#)
- [AWS Credentials](#)
- [Email Credentials](#)
- [Git Password-Based Credentials](#)
- [Google Cloud Platform Authentication](#)
- [HTTP Basic Authentication](#)
- [HTTP Client Certificate Authentication](#)
- [JDBC Login Credentials](#)
- [Kafka Authentication](#)
- [Kafka Certificate Authentication](#)
- [Meraki Credentials](#)
- [Microsoft Windows Credentials](#)
- [Terminal Key-Based Credentials](#)
- [Terminal Password-Based Credentials](#)

Account Keys Overview

Account Keys Overview

An account key record stores information about the user security context and passes this information to the adapters for activity execution, event monitoring, and some target operations (such as availability monitoring and discovery). Account keys instances can be shared across targets and workflows. For example, if a single set of credentials can be used to access a set of network devices, only one account key instance must be created. When it is time to change the credentials, users can go to the Account Keys list and edit the single instance to change the credentials. This greatly reduces the configuration load when credentials tend to change often in some environments.. Account Keys hold the security credentials that are assigned to workflows and activities.

Account Key credentials can be used in a workflow, but no workflow can retrieve credentials. If your workflow must access credentials, use hidden string variables.

The account keys concept allows the product to implement delegation. For example:

1. An IT help desk operator comes to Action Orchestrator to run a workflow.
2. This operator is presented with a list of workflows that Action Orchestrator's role-based access control allows them to run. These workflows might include activities that require a level of security permission that the operator does not natively have.
3. The operator can perform actions as a part of the established workflow that are not possible for them to perform manually.

This concept can also be leveraged to reveal where operators make changes outside of a workflow. By examining auditing logs such as Windows logs for things being done under the operators credentials rather than the Action Orchestrator account key credentials, it is possible to determine how the operator is doing things outside of a workflow and determine how to close things down. So a side effect of Action Orchestrator automation is that customers might be able to tighten security in their environment.

Amazon Alexa Device Credentials

Amazon Alexa Device Credentials

1. Under **Account Key Type**: Select the **Amazon Alexa Device Credentials** from the dropdown list.
2. Under **General**, specify the appropriate information.
3. Under **Credentials**, specify the following information:
 - a. Client ID: Enter the Client ID.
 - b. Client Secret: Enter the Client secret password.
 - c. Access Token: Enter the access token for the Amazon device.
 - d. Refresh Token: Enter the refresh token to be used for the amazon device.
4. Click **SUBMIT** to apply the new changes.

AMQP Certificate-Based Credentials

AMQP Certificate-Based Credentials

1. Under **Account Key Type**- Select the **AMQP Certificate-Based Credentials** key type from the drop-down list.
2. Under **General**, specify the appropriate information.
 - a. Display Name - Enter the unique display name for the AMQP Credentials.
 - b. Description - Enter the brief description about the AMQP Credentials.
3. Under **AMQP**, Specify the following information:
 - a. UserName - Enter the AMQP user name.
 - b. Password - Enter the appropriate password.
 - c. CA CRT File - Enter the certificate file from certificate authority. You can also browse the file from your local.
 - d. CRT File - Enter the certificate file. You can also browse the file from your local.
 - e. Key File - Enter the Key file. You can also browse the file from your local.
 - f. Passphrase - Enter the appropriate passphrase.
4. Click **SUBMIT** to apply the new changes.

AMQP Password-Based Credentials

AMQP Password-Based Credentials

1. Under **Account Key Type**: Select the **AMQP Password-Based Credentials** key type from the dropdown list.
2. Under **General**, specify the appropriate information.
 - a. Display Name: Enter the unique display name for the AMQP Credentials.
 - b. Description: Enter the brief description about the AMQP Credentials.
3. Under **AMQP**, specify the following information:
 - a. UserName: Enter the AMQP user name.
 - b. Password: Enter the appropriate password.
4. Click **SUBMIT** to apply the new changes.

AMQP Password-Less Certificate-Based Credentials

AMQP Password-Less Certificate-Based Credentials

1. Under **Account Key Type**: Select the **AMQP Password-Less Certificate-Based Credentials** key type from the drop-down list.
2. Under **General**, specify the appropriate information.
 - a. Display Name: Enter the unique display name for the AMQP Credentials.
 - b. Description: Enter the brief description about the AMQP Credentials.
3. Under **AMQP**, specify the following information:
 - a. CA CRT File: Enter the certificate file from certificate authority. You can also browse the file from your local.
 - b. CRT File: Enter the certificate file. You can also browse the file from your local.
 - c. Key File: Enter the Key file. You can also browse the file from your local.
 - d. Passphrase: Enter the appropriate passphrase.
4. Click **SUBMIT** to apply the new changes.

Ansible Tower Credentials

Ansible Tower Credentials

1. Under **Account Key Type**: Select the **Ansible Tower Credentials** key type from the dropdown list.
2. Under **General**, specify the appropriate information:
 - a. Display Name: Enter the unique display name for the Ansible tower credentials.
 - b. Description: Enter the brief description about the Ansible tower credentials.
3. Under **Credentials**, specify the following information:
 - a. UserName: Enter the Ansible Tower user name.
 - b. Password: Enter the appropriate password.
4. Click **SUBMIT** to apply the new changes.

Cisco Prime Service Catalog Credentials

Cisco Prime Service Catalog Credentials

1. Under **Account Key Type**: Select the **Cisco Prime Service Catalog Credentials** from the dropdown list and enter the following information:
2. Under **General**, specify the appropriate information.
 - a. Display Name: Enter the unique display name for the Cisco Prime Service Catalog Credential.
 - b. Description: Enter the brief description about the Cisco Prime Service Catalog Credential.
3. Under **PSC**, specify the following information:
 - a. UserName: Enter the PSC user name.
 - b. Password: Enter the PSC password.
4. Click **SUBMIT** to apply the new changes.

CloudCenter Suite Explicit User

CloudCenter Suite Explicit User

1. Under **Account Key Type**: Select the **CloudCenter Suite Explicit User** type from the dropdown list.
2. Under **General**, specify the appropriate information:
 - a. Display Name: Enter the unique display name for the CloudCenter Suite Explicit User.
 - b. Description: Enter the brief description about the CloudCenter Suite Explicit User.
3. Under **CloudCenter Suite**, specify the following information:
 - a. UserName: Enter the CloudCenter Suite user name.
 - b. Password: Enter the appropriate password.
 - c. Tenant ID: Enter the appropriate tenant ID.
4. Click **SAVE** to apply the new changes.

AWS Credentials

AWS Credentials

1. Under **Account Key Type**: Select the **AWS Credentials** from the dropdown list.
2. Under **General**, specify the appropriate information.
 - a. Display Name: Enter the unique display name for the AWS Credentials.
 - b. Description: Enter the brief description about the AWS Credentials.
3. Under **AWS Keys**, specify the following information:
 - a. Access Key: Enter the AWS access key ID.
 - b. Secret Key: Enter the AWS secret access key.
4. Click **SUBMIT** to apply the new changes.

Email Credentials

Email Credentials

1. Under **Account Key Type**: Select the **Email Credentials** from the dropdown list.
2. Under **General**, specify the appropriate information.
 - a. Display Name: Enter the unique display name for the Email Credentials.
 - b. Description: Enter the brief description about the Email Credentials.
3. Under **Email**, specify the following information:
 - a. From: Enter the valid email id.
 - b. Password: Enter the appropriate password.
4. Click **SUBMIT** to apply the new changes.

Git Password-Based Credentials

Git Password-Based Credentials

1. Under **Account Key Type**: Select the **Git Password-Based Credentials** from the dropdown list and enter the following information:
2. Under **General**, specify the appropriate information.
 - a. **Display Name**: Enter the unique display name for the Git Password-Based Credential.
 - b. **Description**: Enter the brief description about the Git Password-Based Credential.
3. Under **Git**, specify the following information:
 - a. **UserName**: Enter the Git user name.
 - b. **Password**: Enter the Git password.
4. Click **SUBMIT** to apply the new changes.

Google Cloud Platform Authentication

Google Cloud Platform Authentication

1. Under **Account Key Type**: Select the **Google Cloud Platform Authentication** from the drop-down list.
2. Under **General**, specify the appropriate information.
3. Under **Credentials**, enter the **Service Account Key File (JSON)** or click on **Browse for Service Account Key File (JSON)** to browse the key file from the local.
4. Click **SUBMIT** to apply the new changes.

HTTP Basic Authentication

HTTP Basic Authentication

1. Under **Account Key Type**: Select the **HTTP Basic Authentication** from the dropdown list.
2. Under **General**, specify the appropriate information.
 - a. Display Name: Enter the unique display name for the HTTP Basic authentication.
 - b. Description: Enter the brief description about the HTTP Basic authentication.
3. Under **Credentials**, specify the following information:
 - a. UserName: Enter the HTTP user name.
 - b. Password: Enter the appropriate password.
4. Click **SUBMIT** to apply the new changes.

HTTP Client Certificate Authentication

HTTP Client Certificate Authentication

1. Under **Account Key Type**: Select the **HTTP Client Certification Authentication** from the dropdown list.
2. Under **General**, specify the appropriate information.
 - a. Display Name: Enter the unique display name for the HTTP client certification authentication.
 - b. Description: Enter the brief description about the HTTP client certification authentication.
3. Under **Credentials**, specify the following information:
 - a. CRT File: Enter the certificate file. You can also browse the file from your local.
 - b. Key File: Enter the Key file. You can also browse the file from your local.
 - c. Passphrase: Enter the appropriate passphrase.
4. Click **SUBMIT** to apply the new changes.

JDBC Login Credentials

JDBC Login Credentials

1. Under **Account Key Type**: Select the **JDBC Login Credentials** from the dropdown list.
2. Under **General**, specify the appropriate information.
 - a. Display Name: Enter the unique display name for the JDBC login Credentials.
 - b. Description: Enter the brief description about the JDBC login Credentials.
3. Under **Database**, specify the following information:
 - a. UserName: Enter the database user name.
 - b. Password: Enter the appropriate password.
4. Click **SUBMIT** to apply the new changes.

Kafka Authentication

Kafka Authentication

1. Under **Account Key Type**: Select the **Kafka Authentication** from the dropdown list.
2. Under **General**, specify the appropriate information.
 - a. Display Name: Enter the unique display name for the Kafka Authentication.
 - b. Description: Enter the brief description about the Kafka Authentication.
3. Under **Credentials**, specify the following information:
 - a. UserName: Enter the Kafka user name.
 - b. Password: Enter the appropriate password.
4. Click **SUBMIT** to apply the new changes.

Kafka Certificate Authentication

Kafka Certificate Authentication

1. Under **Account Key Type**: Select the **Kafka Certificate Authentication** from the drop-down list.
2. Under **General**, specify the appropriate information.
 - a. Display Name: Enter the unique display name for the Kafka Authentication.
 - b. Description: Enter the brief description about the Kafka Authentication.
3. Under **Credentials**, specify the following information:
 - a. CRT File: Enter the certificate file. You can also browse the file from your local.
 - b. Key File: Enter the Key file. You can also browse the file from your local.
 - c. Passphrase: Enter the appropriate passphrase.
 - d. CA CRT File: Enter the certificate file from certificate authority. You can also browse the file from your local.
 - e. UserName: Enter the Kafka user name.
 - f. Password: Enter the appropriate password.
4. Click **SUBMIT** to apply the new changes.

Meraki Credentials

Meraki Credentials

1. Under **Account Key Type**: Select the **Meraki Credentials** from the dropdown list.
2. Under **General**, specify the appropriate information.
 - a. Display Name: Enter the unique display name for the Meraki Credential.
 - b. Description: Enter the brief description about the Meraki Credential.
3. Under **Meraki**, enter the **X-CISCO-MERAKI-API-KEY**.
4. Click **SUBMIT** to apply the new changes.

Microsoft Windows Credentials

Microsoft Windows Credentials

1. Under **Account Key Type**: Select the **Microsoft Windows Credentials** from the dropdown list and enter the following information:
2. Under **General**, specify the appropriate information.
 - a. Display Name: Enter the unique display name for the Microsoft Windows Credential.
 - b. Description: Enter the brief description about the Microsoft Windows Credential.
3. Under **Windows**, specify the following information:
 - a. UserName: Enter the Windows user name in the following format *domain\username*.
 - b. Password: Enter the Windows password.
4. Click **SUBMIT** to apply the new changes.

Terminal Key-Based Credentials

Terminal Key-Based Credentials

1. Under **Account Key Type**: Select the **Terminal Key-Based Credentials** from the dropdown list.
2. Under **General**, specify the appropriate information.
 - a. **Display Name**: Enter the unique display name for the Terminal key based credentials.
 - b. **Description**: Enter the brief description about the Terminal key based credentials.
3. Under **Terminal**, specify the following information:
 - a. **UserName**: Enter the AMQP user name.
 - b. **Private Key**: Enter the appropriate private key.
 - c. **Passphrase**: Enter the appropriate passphrase.
4. Click **SUBMIT** to apply the new changes.

Terminal Password-Based Credentials

Terminal Password-Based Credentials

1. Under **Account Key Type**: Select the **Terminal Password-Based Credentials** from the dropdown list.
2. Under **General**, specify the appropriate information.
 - a. **Display Name**: Enter the unique display name for the Terminal password based credentials.
 - b. **Description**: Enter the brief description about the Terminal password based credentials.
3. Under **Terminal**, specify the following information:
 - a. **UserName**: Enter the Terminal user name.
 - b. **Password**: Enter the appropriate password.
4. Click **SUBMIT** to apply the new changes.

Configuring Variables

Configuring Variables

- [Adding Variables](#)
- [Creating Global Variables](#)
- [Creating Variable Type](#)

Adding Variables

Adding Variables

The variables feature provides a storage area for information that is used on a regular basis to avoid having to specify the same information in several places. Data stored in a variable can be altered to affect process execution behavior. The Variables in Action Orchestrator work in the same way as variables of any other programming language.

To add a global variable, choose **Variables > Global Variables > NEW Variable**. From this view, you can create new global variable, modify the properties of a variable, and delete variables. You can also add the variable from the workflow or activities properties pane. For more information, see [Creating Global Variables](#).

Variable type provide a way to define a new user defined variable type that is not represented by any default variable type. To add a variable type, choose **Variables > Variable Types > New Variable Type**. From this view, you can create new variable type, modify the properties of a variable type, and delete variable types. You can also add the variable type from the workflow or activities properties pane. For more information, see [Creating Variable Type](#).

The following sections describe how you can use variables in Action Orchestrator:

- [Activity Configuration](#)
- [Workflow Control Components](#)
- [Workflow Parameters](#)
- [Formulas as Variable Values](#)
- [Common Use of Variables](#)
 - [Named Variables](#)
 - [Workflow or Activity Property Variables](#)
 - [Status Tracking](#)
 - [Summary Variables](#)

Activity Configuration

One of the most common uses of variables is to define activity configurations. Any field in an activity can refer to a variable value rather than an explicit value. For example, you can use a variable to:

- Specify the start date of the process operations window as a parameter to an operating system command.
- Specify a condition, such as a file that should not exist after a job is initially triggered by the arrival of that file where a prior activity should have deleted the file.

Workflow Control Components

A Workflow can use variables to define the control components. For example, you can use a variable to define:

- A Conditional activity to look at the exit code of a prior activity.
- A While Loop activity to loop until a query fails or loop for a number of times corresponding to a number of objects pulled from a query.

Workflow Parameters

Variables can be parameterized so that a workflow definition can be flexible enough to be reused in multiple places and the specifics can remain undefined so that they can be defined by the person or workflow that invokes the workflow or activity.

For example, a workflow called notify server owner might use a variable server for the name of the server that has a problem. The workflow retrieves the email address of the owner of the server and sends an email.

This workflow might be called from multiple places; a step in a server maintenance job fails, so the maintenance job populates the Server variable and invokes the notify server owner process. Another process might notify the server owner when a backup completes.

Formulas as Variable Values

You can specify a formula anywhere a variable value is used. For example, an operating system command's parameter might be formed from concatenating two variables' values or from parsing the output of a prior command.

Variables are used to store or pass a value between executions of a process or between steps within a single workflow.

Common Use of Variables

The most common types of variables in Action Orchestrator are name variables and process or activity property variables.

Named Variables

The most common use of variables is a name that has a changeable value. For example, you can use a global variable to store information used in processes such as:

- Locations of files and directories

- Email addresses
- Order numbers
- User names

Workflow or Activity Property Variables

- In a Workflow or activity definition, you can refer to the workflow properties or the properties of a prior activity in the workflow. In this scenario, the properties of the workflow or activity may also refer to associated objects.
- One of the most common uses of variables is to define activity configuration. Any field in an activity with a Reference tool can refer to a variable value rather than an explicit value.

Status Tracking

Another common use of variables is to track state. For instance, you can use variables as a loop counters to store the number of times a loop has executed and know the current loop iteration running.

Summary Variables

You can also use a variable to build up a 'summary' message. For each thing event happens, you can append 'what just happened' to the variable. At the end of a process, the result will be the contents of this variable as an entire summary of the workflow.

Creating Global Variables

Creating Global Variables

Variables can be used as a reference value used for multiple objects. They can also be used to store or pass a value between executions of a process or between steps within a single process.

- Use the Boolean variable to indicate the set of elements that should be true or false.
- Use the DateTime variable to define a variable as date.
- Use the Decimal variable to define a variable containing a decimal number (positive and negative).
- Use the Integer variable to define a variable containing an integer value (positive and negative).
- Use the Secure String variable to define a variable as encrypted.
- Use the String variable to define a variable containing a string of text.

On the **New Variable** panel, specify the appropriate information:

1. **Data Type:** Select the appropriate data type from the dropdown list. You will be able to select data types such as Boolean, Date, String, and so forth.

To create new data type, click **+ADD NEW** from the dropdown list. For more information, see [Creating Variable Type](#).

2. Under **General**, specify the appropriate information:

- a. **Display Name:** Enter the unique display name for the variable.
- b. **Description:** Enter the brief description about the variable.
- c. **Scope:** Select the scope from the drop-down list. Valid values are: local, input, output, static, and so forth.



This is applicable only when you create the variable from the Variables page, select the scope from the dropdown list such as Global and Environment.

- d. **Value:** Enter or select the appropriate value. For example: For Boolean global variable, you can select either true or false as the value.
3. Click **SUBMIT** or **SAVE** in the appropriate pages.


Creating Variable Type


Creating Variable Type

Variable type provide a way to define a new user defined variable type that is not represented by any default variable type.

Under the **New Variable Type** panel, select the type from the dropdown list (default is Table Type) and specify the appropriate information:

1. Under **General**, specify the appropriate information:
 - a. Display Name: Enter the unique display name.
 - b. Description: Enter the brief description about the data type.
2. Under **Columns**, specify the following information:
 - a. Required: Choose **Yes** using the toggle button to make the column a required column (Default is No).
 - b. Field Name: Enter the field name.
 - c. Field Title: Enter the field title to be displayed in the columns.
 - d. Field Type: Select the appropriate type from the dropdown list such as Boolean, Date Time, Decimal, Integer, and String.

 Specify the maximum length of the string, when you choose string as the field type.

 Specify the minimum and maximum number, when you choose number as the field type.

3. Click **Save**, to save the new type.

Configuring Calendars

Configuring Calendars

- [Configuring Calendars](#)
 - [Adding Calendar](#)

Calendars are reusable for schedules within many processes. For example, you can define a calendar for Saturdays. When defining a workflow that you want to run on Saturdays, you reference the Saturday calendar. Other examples include a calendar that includes weekends and company holidays when IT might perform scheduled maintenance, or the last week of a fiscal quarter when IT might exclude non-essential automation or deny change requests.

The calendars feature defines the calendar to be associated with a schedule, time, or condition. This feature simplifies:

- Reusing calendar definitions across workflows
- Building complex calendars from other calendars
- Viewing the workflows that run based on a specific calendar

The **Calendars** page displays the **Display Name** (along with the type), **Owner**, and **Last Modified** details. You can delete the Calendars by performing the **Delete** action and **Change Owner** using the dropdown from the **Actions** column. Calendars are reusable for schedules within many workflows.

- **Date List:** Specify an explicit list of dates. The processes to which this calendar definition is assigned will execute on the specified dates in the calendar. You might want to use this type of calendar for workflows that run on specific days of a specific month.
- **Group:** Specify a collection of other defined calendar types, such as inclusion of date list or a recurring calendar within the group calendar definition. The group calendar can contain defined recurring calendars, other group calendars, and date list calendars. You select the calendars to include or exclude in the group calendar definition. You can also add dates to or exclude dates from a group calendar.
- **Recurring:** Specify a starting date for the subsequent dates and recurrence frequency. You can specify the calendar to repeat on a daily, weekly, monthly, or yearly basis.

Adding Calendar

Perform the following procedure to add a new calendar:

1. Under **Calendar Type**, select the appropriate calendar type from the dropdown list and enter the following information:
 - a. Date list calendar
 - b. Group calendar
 - c. Recurring calendar
2. Under **General**, enter the name and description for the calendar.



According to the calendar type chosen in step 1, you have to follow either step 3 or step 4 or step 5.

3. Under **Dates**, click **+ADD**, to add dates to the calendar.
4. Under **Group Calendars**, specify the following information:
 - a. Under **Starts**, specify the start date either by entering manually or by selecting the date from calendar icon.
 - b. Under **Ends**, specify the end date either by entering manually or by selecting the date from calendar icon.
 - c. Select **Includes** or **Excludes** dates from following calendars such as All, Every Saturday, Weekdays, and so forth.
5. Under **Recurring**, specify the following information:
 - a. Under **Starts**, specify the start date either by entering manually or by selecting the date from calendar icon.
 - b. Under **Ends**, specify the end date either by entering manually or by selecting the date from calendar icon.
 - c. Under **Repeats**, select the appropriate information such as daily, weekly, monthly, or yearly from the dropdown list.
 - i. **Daily:** Enter the days count for daily repeat.
 - ii. **Weekly:** Enter the weeks count for weekly repeat. You can also specify the following days by selecting the days under **the following days** such as Sunday, Monday, and so forth.
 - iii. **Monthly:** Enter the monthly count for monthly repeat.
 - Under **ON**, select the appropriate information such as Day, First, Second, and so forth.
 - Enter or select the appropriate information from next dropdown list such as Day, Weekday, WeekendDay, and so forth.
 - iv. **Yearly:** Enter the yearly count for yearly repeat by selecting month from the dropdown list.
 - Under **ON**, select the appropriate information such as Day, First, Second, and so forth.
 - Enter or select the appropriate information from next dropdown list such as Day, Weekday, WeekendDay, and so forth.
6. Click **SUBMIT**, to save the changes.

Configuring Tasks

Configuring Tasks

The Tasks page is used to monitor the state of tasks that are created, pending, overdue, and completed. You will also be able to filter the tasks on basis of response (Approve or Reject), status (Created, Pending, Overdue, and Completed), Priority (Low, Normal, and High), due date, and so forth.

- The **Filter** icon allows you to filter the tasks based on the following
 - Response: Choose the **Approve** or **Reject** response by checking the appropriate check box.
 - Status: Choose the status in the tasks page by checking the appropriate check box such as **Created, Pending, Overdue, and Completed**.
 - Priority: Choose the priority such as **Low, Normal, and High** by checking the appropriate check box.
 - Due Date: Check the check box and choose the required date from the calendar.
- The **Search** icon allows you search for the tasks based on the names.
- The **Refresh** icon allows you to refresh the task page.
- The page displays the following information of the existing or filtered tasks:
 - Display Name: Displays the name of the tasks.
 - Status: Displays the status of the tasks such as created, pending, overdue, and completed.
 - Priority: Displays the priority of the tasks such as low, normal, and high.
 - Due Date: Displays the due date and time of the tasks.
 - Task Requestor: Displays the email ID of the task requestor.
 - Task Owner: Displays the email ID of the task owner.
 - Task Assignees: Displays the email ID of the task assignee.
 - Last Modified: Displays the last task modified date and time.
 - Actions: By using the dropdown icon in actions column, you can either **Approve** or **Reject** the task.

Configuring Schedules

Configuring Schedules

Schedules allow triggering processes at some time by leveraging another object called a calendar. Calendars define which days something can occur. Calendars can be selected days or sequences of dates such as weekly or monthly, they can represent dates like fiscal quarter end, or they can be combined hierarchically. Schedules then associate a time with a calendar. When the day is in the calendar, the time is evaluated. Times can be explicit or repeating (for example, hourly).

The Schedules page displays the **Display Name** (along with the type), **Owner**, and **Last Modified** details. You can see the schedules **Used by** details, delete the added schedule by performing the **Delete** action, and **Change Owner** using the dropdown from the **Actions** column. To add a new schedule, click on **New Schedule**.

Perform the following procedure to add schedule:

1. Under **Select Type**, select **Generic Schedule** from the dropdown list.
2. Under **General**, enter the name and description for calendar. And enter the following information:
 - a. Under **Calendar**, select an existing calendar or choose the appropriate options from the dropdown list such as Every Saturday, Weekdays, Workdays, etc. For more information to create new calendar, see [Configuring Calendars](#).
 - b. Under **Timezone**, select the appropriate information from the dropdown list.
3. Under **Schedule**, specify the following information:
 - a. Under **Start Time**, specify the start time either by entering manually or by adjusting the time by using the up and down arrow buttons or by using mouse scroll option.
 - b. Under **Number of Runs Per Day**, specify the number of times the activity or task has to run per day.
 - c. Under **Time Interval (Run Every)**, specify the time interval in hours and Minutes. The activity run every hours and minutes mentioned in the time interval.
4. Click **SUBMIT**, to save the changes.

Configuring Events

Configuring Events

- [Events Overview](#)
- [AMQP Event](#)
- [Approval Task Event](#)
- [Email Event](#)
- [KAFKA Event](#)

Events Overview

Events Overview

The Action Orchestrator can monitor for events from the environment, and you can specify triggers that initiate workflows when the subscribed event occurs. For example, an event might be an incoming stop trap or a fault on a Unified Computing System (UCS). You can use events to watch for patterns in these services, enabling policy-driven automation. Targets and target types have events. These can be internal process events or the open Advanced Message Queuing Protocol (AMQP) protocol. Triggering processes in response to patterns in underlying processes provides policy.

The Events page displays the **Display Name** (along with the type), **Target**, **Owner**, and **Last Modified** details. You can see the event Used by details, delete the added event by performing the **Delete** action, and **Change Owner** using the dropdown from the **Actions** column. To add a new event, click on **New Event**.

AMQP Event

AMQP Event

The Advanced Message Queuing Protocol (AMQP) is an open standard application layer protocol for message-oriented middleware. It delivers message orientation, queuing, routing (including point-to-point and publish-and-subscribe), reliability and security. AMQP came out of the financial industry, and is proven highly scalable in demanding environments (refer <http://www.amqp.org/>).

AMQP is the emerging standard for messaging and events in the cloud. For example:

- vCloud Director can publish vCloud Messages, also known as blocking tasks, notifications, or call-outs, related to different provisioning. An orchestrator can not only receive these events, but can also respond to them to delay execution.
- AMQP is supported with vCloud Orchestrator.
- OpenStack selected AMQP as the messaging technology for OpenStack.

AMQP is integrated with more than 70 developer platforms, providing a nice framework for event-oriented integrations.

AMQP enables event-driven capabilities of Enterprise Service Bus-style designs. It enables queuing, so automation can fetch messages when there is capacity. You can use asynchronous methods servicing requests as capacity allows when possible, and reserve real-time, synchronous methods only when absolutely needed. AMQPs open platform is a natural choice for event and message design patterns.

Action Orchestrator can trigger processes in response to messages placed on AMQP queues/exchanges. Processes can also read messages from queues/exchanges one at a time if they want to respond to messages one at a time rather than in parallel, to operate more as a queue. Processes can submit messages to queues/exchanges.

JMS is another possible integration enabled through AMQP. AMQP has providers to place JMS messages on queues/exchanges.

To create a new AMQP event perform the following procedure:

1. Under **Select Type**, select **AMQP Event** from the dropdown list.
2. Under **General**, specify the following information:
 - a. **Display Name**: Enter the unique display name for the AMQP event.
 - b. **Description**: Enter the brief description about the AMQP event.
 - c. **Target**: Select the target from the dropdown list. To add a new target, click **+ADD NEW** from the dropdown list. For more information, see [AMQP Endpoint](#).
3. Under **Criteria**, specify the following information:
 - a. **Queue Name**: Enter the name of the queue.
 - b. **Conditions**: Click **+ADD** to specify the condition, enter the following information:
 - i. **Left Operand**: Enter the value for the left operand.
 - ii. **Operator**: From the dropdown list, choose the operator to use for comparing the value:
 1. **Does not match wildcard**: Determines if the item does not match all items in the wildcard example
 2. **Equal**: Determines if the left side equals the right side (if this is a string comparison, this is case-insensitive)
 3. **Match regular expression**: Determines if the left side matches the regular expression specified on the right side.
 4. **Matches wildcard**: Determines if the left side matches the wildcard specified on the right side.
 5. **Not equals**: Determines if the left side does not equal the right side
 - iii. **Right Operand**: Enter the value for the right operand.
4. Click **Submit**, to save the changes.

Approval Task Event

Approval Task Event

The approval task event allows you to create conditions for your task event. To create an approval task event perform the following procedure:

1. Under **Select Type**, select **Approval Task Event** from the dropdown list.
2. Under **General**, specify the following information:
 - a. Title: Enter the unique title for the Approval task event.
 - b. Description: Enter the brief description about the event.
3. Under **Criteria**, specify the appropriate conditions:
 - a. Left Operand: Enter the value for the left operand or click on [Variable Reference](#) icon to choose variable such as approval choices, Assignee Responses, Add Task Assignees, and so forth.
 - b. Operator: From the dropdown list, choose the operator to use for comparing the value:
 - i. Does not match wildcard: Determines if the item does not match all items in the wildcard example
 - ii. Equal: Determines if the left side equals the right side (if this is a string comparison, this is case-insensitive)
 - iii. Match regular expression: Determines if the left side matches the regular expression specified on the right side.
 - iv. Matches wildcard: Determines if the left side matches the wildcard specified on the right side.
 - v. Not equals: Determines if the left side does not equal the right side
 - c. Right Operand: Enter the value for the right operand.
4. Click **Submit**, to save the changes.

Email Event

Email Event

Use the Email Event trigger to specify the basic criteria for the mail server to be monitored and the email conditions that will trigger the workflow.

To create a new Email event perform the following procedure:

1. Under **Select Type**, select **EmailEvent** from the dropdown list.
2. Under **General**, specify the following information:
 - a. **Display Name**: Enter the unique display name for the Email event.
 - b. **Description**: Enter the brief description about the Email event.
 - c. **Target**: Select the target from the dropdown list. To add a new target, click **+ADD NEW** from the dropdown list. For more information, see [MAP Endpoint](#) or [POP3 Endpoint](#).
3. Under **Criteria**, specify the following information:
 - a. **Folder**: Enter the name of the folder where the message is to be moved. If the folder is a subfolder, then enter the file path for the folder location (for example, project/issues/connections).
 - b. **Conditions**: Click **+ADD** to specify the condition, enter the following information:
 - i. **Left Operand**: Enter the value for the left operand.
 - ii. **Operator**: From the dropdown list, choose the operator to use for comparing the value:
 1. **Does not match wildcard**: Determines if the item does not match all items in the wildcard example
 2. **Equal**: Determines if the left side equals the right side (if this is a string comparison, this is case-insensitive)
 3. **Match regular expression**: Determines if the left side matches the regular expression specified on the right side.
 4. **Matches wildcard**: Determines if the left side matches the wildcard specified on the right side.
 5. **Not equals**: Determines if the left side does not equal the right side
 - iii. **Right Operand**: Enter the value for the right operand.
4. Under **What to do with the message**, select the option to specify the action to be taken after the criteria has been met on the Exchange server.
 - a. **Mark message read**: The message will be marked as read. This option is not available for POP3 email systems.
 - b. **Move message to folder**: The message will be moved to a designated folder.
 - c. **Delete message**: The email will be deleted. This is the only option available for a POP3 type of email connection.
5. Click **Submit**, to save the changes.

KAFKA Event

KAFKA Event

To create a new Kafka event perform the following procedure:

1. Under **Select Type**, select **Kafka Event** from the dropdown list.
2. Under **General**, specify the following information:
 - a. Display Name: Enter the unique display name for the Kafka event.
 - b. Description: Enter the brief description about the Kafka event.
 - c. Target: Select the target from the dropdown list. To add a new target, click **+ADD NEW** from the dropdown list. For more information, see [KAFKA Endpoint](#).
3. Under **Criteria**, specify the appropriate information:
 - a. Topic Name: Enter the associated topic name.
 - b. Conditions: Click **+ADD** to specify the condition, enter the following information:
 - i. Left Operand: Enter the value for the left operand.
 - ii. Operator: From the dropdown list, choose the operator to use for comparing the value:
 1. Does not match wildcard: Determines if the item does not match all items in the wildcard example
 2. Equal: Determines if the left side equals the right side (if this is a string comparison, this is case-insensitive)
 3. Match regular expression: Determines if the left side matches the regular expression specified on the right side.
 4. Matches wildcard: Determines if the left side matches the wildcard specified on the right side.
 5. Not equals: Determines if the left side does not equal the right side
 - iii. Right Operand: Enter the value for the right operand.
4. Click **Submit**, to save the changes.

Admin

Admin

- [Admin Overview](#)
- [Action Orchestrator Roles](#)
- [Integrations](#)
- [Schemas](#)
- [Categories](#)

Admin Overview

Overview

Use the admin space to perform administrative actions such as:

- [Action Orchestrator Roles](#)
- [Integrations](#)
- [Schemas](#)
- [Categories](#)



The availability of this space is subject to roles and permissions, it will be applicable only for admin users. For more information, see [Action Orchestrator Roles](#).

Action Orchestrator Roles

Action Orchestrator Roles

- [Overview](#)
- [Predefined Security Roles](#)
- [Adding Custom Roles](#)
- [Roles and Permissions](#)

Overview

In Action Orchestrator, authorization is performed using a Role-Based Access Control System (RBAC). Roles are a collection of permissions, each permission pairs a set of operations that can be performed over some set of Action Orchestrator objects such as workflows, targets, account keys, variables, and so forth. A user assignment gives end users the ability to perform the action. Access rights include Create, View, Update, Delete, Run, and so forth.

A role is assigned to user groups in Action Orchestrator. When Action Orchestrator becomes a part of CloudCenter Suite or another Cisco product, the common RBAC component shall provide APIs to map roles in the host applications to the Action Orchestrator roles.

Typically, roles are defined according to a standardized job function within IT. Examples might include Level 1 Helpdesk, Level 2 Helpdesk, Human Resources, Network Configuration, SAP Basis Expert, and so on. Security groups already in the directory for the users in these job functions are then typically assigned to the roles.

For more information on roles, see [Understand Roles](#).

Predefined Security Roles

Action Orchestrator provides predefined security roles that ship with the product and cannot be modified. Custom user roles (see [Adding Custom Roles](#)) can be created using the Administration view, but the following roles are defined by default:

Role	Description
Tenant Admin	These users have almost access to all functionality in the product. Users can view or modify or change owner of any workflow or setting such as automation packs, calendar, category, global variable, queue resource, and so forth.
Content Author	This is a user who can define workflows. The user cannot update administration settings.
Operator	This is a classic role for a level 1 Service Desk employee, executing workflows.
System Admin	Only a small number of users are assigned this role. These users have permissions to modify adapter settings.
Adapter Author	These users have access to enable or disable atomic workflows in the product.

For more information, see [Roles and Permissions](#).

Adding Custom Roles

To add a new role, choose **Admin>Roles>New Role**.

In the **New Role** panel, perform the following procedure to add a new role.

1. Under **General**, specify the appropriate information:
 - a. Display Name: Enter the unique name to be displayed in the roles page.
 - b. Name: Enter the unique name for the role.
 - c. Description: Enter the brief description about the role.
 - d. Role Type: By default the role type is custom.
2. Under **Permissions**, specify the appropriate action:
 - a. Use the toggle buttons to activate or deactivate the list of permissions to be included and/or to be made available for inclusion into the security role.
 - b. Click play icon, on the appropriate object type and choose the appropriate powers for the security role from the dropdown list. For more information, see [Roles and Permissions](#).
3. Click **Submit**, to add and save the Role.

Roles and Permissions

Object Level Permissions


Object level Permissions define what operations can be performed over workflows. This is similar to file permissions (such as read or update). You can have permissions for each user to access and can be shared to multiple users. When you are logged into Action Orchestrator, you can only access the objects which you have permissions.

Whenever the object shared among users and groups, Action Orchestrator creates a link document in uses collections with the users and groups information with the permission types to that object.

The following table contains information about the permission type and the type of actions supported:

Permission Type	Type of action supports
View	Read
Modify	View, Update
Manage	View, Update, Delete, Share
Run	View, Execute, Stop

The following table contains information about the predefined permissions given to thesecurity roles:

 The "x" denotes the permission available to the user role.

Object Type	Object Permissions	Tenant Admin Role	Content Author Role	Operator Role	System Admin Role	Adapter Author
Adapter	View	x	x	x		
	Modify					
	Manage				x	x
	Change Owner				x	
Calendar	View			x		
	Modify					
	Manage	x	x			x
	Change Owner	x				
Category	View		x	x		x
	Modify					
	Manage	x				
	Change Owner	x				
Global Variable	View			x		
	Modify					
	Manage	x	x			x
	Change Owner	x				
Role (Tenant specific)	View		x	x		x
	Modify					
	Manage	x			x	
	Change Owner	x			x	
Account Key	View			x		
	Modify					
	Manage	x	x			x
	Change Owner	x				
Schedule	View			x		
	Modify					
	Manage	x	x			x
	Change Owner	x				

Event	View			x		
	Modify					
	Manage	x	x			x
	Change Owner	x				
Target	View			x		
	Modify					
	Manage	x	x			x
	Change Owner	x				
Target Group	View			x		
	Modify					
	Manage	x	x			x
	Change Owner	x				
Workflow definition	View			x		
	Modify					
	Manage	x	x			x
	Run	x	x	x		x
	Change Owner	x				
Workflow instance	View			x		
	Modify					
	Manage	x	x			x
	Cancel	x	x	x		x
	Change Owner	x				
User/role Assignment	View					
	Modify					
	Manage	x				
	Change Owner	x				
Variable Type	View			x		
	Modify					
	Manage	x	x			x
	Change Owner	x				
System	View		x	x		x
	Modify	x				
	Manage				x	
	Change Owner	x				
Atomic Workflow	View	x	x	x		
	Modify					
	Manage				x	x
	Change Owner					
Repository (Git Repo)	View		x	x	x	x
	Modify					
	Manage	x				
	Change Owner	x				

Integrations

Integrations

- [Integrations Overview](#)
- [Git Repositories](#)
- [Add Git Repository](#)

Integrations Overview

Integrations Overview

The Action Orchestrator provides integrations with various technologies and can integrate with repositories such as [Git Repositories](#).

Git Repositories

Git Repositories

This page displays the already existing Git Repositories and allows you to modify or create new Git repository from this page. You will be able to do the following actions from this page:

- Create a new Git repository by clicking on the **New Git Repository**. For more information, see [Add Git Repository](#).
- Modify the repository information by clicking on the appropriate repository name.
- Delete the existing repository by using the **Delete** option by clicking the dropdown icon in actions column.



To modify the existing Git repository, click on the appropriate repository name. The Edit Git repository page is similar to AddGit repository page. For more information, see [Add Git Repository](#).

Add Git Repository

Add Git Repository

Use the **Add/Edit Git Repository** page to create or modify Git repository properties such as automation pack repositories, and so forth. An example of properties include values such as repository URL, repository user, branch and code path.



The users with *Tenant Admin* role only would be able add a new repository. For more information on Roles and Permissions, see [Action Orchestrator Roles](#).



The example repository mentioned in this procedure is *Cisco public repository*, it is a read only repo. You will not have permission to commit your workflows to Cisco repository.

1. To create a new Git repository, choose **Admin>Integrations>Git Repositories**.
2. Under **General**, specify the appropriate information:
 - a. Display Name: Enter the unique name for the Git repository.
 - b. Description: Enter the brief description about the repository.
3. Under **Account Keys**, specify the appropriate information:
 - a. No Account Keys: Select **True** or **False** from the dropdown list.



For Example:

If you are using a read only Cisco public repository, you do not require any credentials while adding a new repository. choose *No Account Keys* as *True*.

- b. Default Account Keys: Select the appropriate account key from the dropdown list or click **ADD NEW** from the dropdown list, see [Git Password-Based Credentials](#).
4. Under **Git**, enter the following information:
 - a. Protocol: Select the appropriate protocol from the dropdown list:
 - i. HTTP
 - ii. HTTPS
 - b. Rest API Repository: Enter the Rest API Git URL of the repository.



For Example:

The Rest API Git URL for the Cisco public repository is api.github.com/repos/cisco/ActionOrchestratorContent.

- c. Branch: Enter default branch name **master**. As you initially make commits, you are given a master branch that points to the last commit you made.
 - d. Code Path: Enter the code path. The code path is folder structure required to locate the workflow in the specific folder or sub-folder in the Git repository.



For Example, the following are the two different code paths of Cisco Public Repository:

The Code path for *atomic actions* in the Cisco public repository is */atomic-actions*.

The Code path for *workflow examples* in the Cisco public repository is */workflow-examples*.



You can only add one code path while adding Git repository. If you want to configure with two or more code paths, perform the same procedure separately for each code path.

5. Click **Submit**, to create/edit and save the Git repository.

Schemas

Schemas

- [Schemas Overview](#)
- [Manage Schemas](#)
- [Creating Schema](#)

Schemas Overview

Overview

The Action Orchestrator User Interface is completely driven by schema definitions of object types. For example, Use Interfaces of all adapter objects, including adapters, targets, account keys, activities, and events, are driven by their corresponding schemas. Each object type has its own schema definition. Each object types schema includes both data schema and view schema.

1. **Data Schema:** Data schema contains the data attributes of each object type. A database schema is the skeleton structure that represents the logical view of the entire database. It defines how the data is organized and how the relations among them are associated. For example, data schema of a target describes all target configuration property names and data types of those properties.
2. **View Schema:** The view schema is used to describe how an object should be rendered properly in an UI. For example, view schema of a target describes how those configuration properties will be rendered on the UI. That is which UI component should be used to render a property, display name of a property, position of a property in UI, which UI section a property belongs to, and so forth.

Manage Schemas

Manage Schemas

This page displays the already existing schema base types and allows you to modify or create new schema from this page. For more information, see [Creating Schema](#).

The filter icon allows you to filter for the schema base types based on the following:

- Account Key
- Activity
- Adapter
- Event
- Target



To modify the existing schema, click on the appropriate schema display name. The Edit Schema page is similar to Add Schema Page. For more information, see [Creating Schema](#).

Creating Schema

Creating Schema

1. To create a new schema, choose **Admin>Manage Schemas>New Schema**.
2. In the **New Schema** panel, perform the following procedure to add a new schema.
3. Under **Select Type**, select the appropriate schema data type from the dropdown list:
 - a. [Account Key](#)
 - b. [Activity](#)
 - c. [Adapter](#)
 - d. [Event](#)
 - e. [Target](#)
4. Click **Submit**, to create and save the Schema.



There are dependencies among adapter schemas. When executing schema, the schemas should be created in the order of Account Key schema, Activity schema, Adapter schema, Event Schema, and Target schema.

Activity

Activity

Use the following procedure to create activity schema:

1. Under **General**, specify the appropriate information:
 - a. Display Name: Enter the unique name to be displayed in the schema page.
 - b. Schema Type: Enter the schema type.
 - c. Description: Enter the brief description about the schema.
 - d. Group Name: Enter the group name for new schema.
2. Under **Access Meta**, specify the appropriate action:
 - a. Adapter: Choose the appropriate adapter from the dropdown list.
 - b. Targets: Choose the appropriate target from the dropdown list.
3. Under **Input Properties**, click **+Add** to add input property. For more information, see [Add Input Property](#).
4. Under **Output Properties**, click **+Add** to add output property. For more information, see [Add Output Property](#).
5. Click **Submit**, to create and save the Schema.

Back to: [Creating Schema](#)

Add Input Property

Add Input Property

Use the following procedure to add an input property while creating a schema:

1. Under **General**, enter the following information:
 - a. Field Label: Enter the Field label.
 - b. Field Name: Enter the unique field name.
 - c. Data Type: Select the data type from the dropdown list such as Boolean, Decimal, Integer, and String.
 - d. Component: Select the appropriate component from the dropdown list such as Check box, Password, Picker, Radio, and so forth.
 - e. Is Required: Check this checkbox to provide value for the input property.
 - f. Under **Optional Parameters**, enter the following information:
 - i. Optional Key: Select the appropriate key from the dropdown list such as Max Length, Maximum, Min Length, and so forth.
 - ii. Optional Value: Enter the required value for the parameter.
2. Click **SAVE**, to save the changes.

Back to: [Creating Schema](#)

Add Output Property

Add Output Property

Use the following procedure to add an output property while creating a schema:

1. Under **General**, enter the following information:
 - a. Field Label: Enter the Field label.
 - b. Field Name: Enter the unique field name.
 - c. Data Type: Select the data type from the dropdown list such as Boolean, Decimal, Integer, and String.
 - d. Component: Select the appropriate component from the dropdown list such as Check box, Password, Text Area, and so forth.
2. Click **SAVE**, to save the changes.

Back to: [Creating Schema](#)

Adapter

Adapter

Use the following procedure to create adapter schema:

1. Under **General**, specify the appropriate information:
 - a. Display Name: Enter the unique name to be displayed in the schema page.
 - b. Schema Type: Enter the schema type.
 - c. Under **Access Meta**, select the appropriate **Account Key** from the dropdown list.
 - d. Description: Enter the brief description about the schema.
 - e. Is Microservice: Check the check box if the schema is a microservice.
2. Under **Cloud Type**, select the appropriate Cloud Type from the dropdown list.
3. Under **Lambda Name**, enter the lambda name.
4. Under **Region**, select the appropriate region from the dropdown list.
5. Click **Submit**, to create and save the Schema.

Back to: [Creating Schema](#)

Event

Use the following procedure to create event schema:

1. Under **General**, specify the appropriate information:
 - a. Display Name: Enter the unique name to be displayed in the schema page.
 - b. Schema Type: Enter the schema type.
 - c. Description: Enter the brief description about the schema.
2. Under **Access Meta**, specify the appropriate action:
 - a. Adapter: Choose the appropriate adapter from the dropdown list.
 - b. Targets: Choose the appropriate target from the dropdown list.
3. Under **Input Properties**, click **+Add** to add input property. For more information, see [Add Input Property](#).
4. Under **Output Properties**, click **+Add** to add output property. For more information, see [Add Output Property](#).
5. Click **Submit**, to create and save the Schema.

Back to: [Creating Schema](#)

Account Key

Account Key

Use the following procedure to create account key schema:

1. Under **General**, specify the appropriate information:
 - a. Display Name: Enter the unique name to be displayed in the schema page.
 - b. Schema Type: Enter the schema type.
 - c. Description: Enter the brief description about the schema.
2. Under **Input Properties**, click **+Add** to add input property. For more information, see [Add Input Property](#).
3. Click **Submit**, to create and save the Schema.

Back to: [Creating Schema](#)

Target

Target

Use the following procedure to create target schema:

1. Under **General**, specify the appropriate information:
 - a. Display Name: Enter the unique name to be displayed in the schema page.
 - b. Schema Type: Enter the schema type.
 - c. Description: Enter the brief description about the schema.
2. Under **Input Properties**, click **+Add** to add input property. For more information, see [Add Input Property](#).
3. Under **Access Meta**, specify the appropriate action:
 - a. Adapter: Choose the appropriate adapter from the dropdown list.
 - b. Account Keys: Choose the appropriate account key from the dropdown list.
4. Click **Submit**, to create and save the Schema.

Back to: [Creating Schema](#)

Categories

Categories

- [Categories Overview](#)
- [Adding Category](#)

Categories Overview

Categories Overview

The Categories feature in Action Orchestrator provides a way to organize your workflows based on your organizational or functional requirements. The categories are tags for grouping workflows within the UI. Action Orchestrator ships with predefined categories, but provides the capability for you to create your own business-specific categories. When creating a workflow, you can assign zero or more categories to the workflow in the Properties section of that workflow.

The Categories page under Admin allows you to create and edit your own categories.



To modify the existing category, click on the appropriate category display name. The Edit Category page is similar to New Category Page. For more information, see [Adding Category](#).

Adding Category

Adding Category

To create a new category perform the following procedure:

1. To create a new category, choose **Admin>Categories**.
2. In the **New Category** panel, perform the following procedure to add a new Category.
3. Under **Select Type**, select the appropriate category type from the dropdown list. Default is Generic Category.
4. Under **General**, specify the display name and brief description for the category.
5. Click **Submit**, to save the Category.

File Operations Overview

File Operations Overview

The file operations enables Action Orchestrator to handle files in the process of a workflow. The file operations allows you to include a file as an input while running a workflow.

Files are a type of object that can be mapped by the variable browser only to certain actions. The file operations that require file access integrates directly with the file handler adapter. File type objects are either declared as inputs to a workflow or as parameters of an action and have a label associated with them. The file operations action implementing file type objects must require the user to add a custom label, which can be a variable enabled field.

The UI allows you to browse local system for the file or for the workflow to pass a file from a parent workflow to a child workflow. Extensions of this feature can be added to other adapters that have to use files such as the web service adapter or the Terminal/SSH adapter.

The file operations create an ephemeral storage in Kubernetes that gets deleted when the workflow completes.

The file operations allow access to the file while running the workflow only by actions explicitly created by this operation. Other adapters cannot write custom actions to access or handle files through the file operations.

The file operations does not support any storage of files beyond running the workflow. The file objects present in a workflow cannot be accessed by any action outside the workflow, even if these actions are run by the same user in the same tenant. The subworkflows/child workflows can access the files from parent as input variable to it. Workflow instance cannot be resumed if any files are associated to the instance because pausing/canceling the workflow will delete the associated files

The file operations does not allow any form of execution of a file and forces all files to a strict read/write permission. All access to the file object is handled by the file operations. The file operations is the only service with access to the ephemeral storage used while running the workflow.

The file operations does not have any outbound access to the internal networking of the cluster.

If the workflow accepts any files as input variables, use `/api/v1.1/workflows/start` API to run the workflow. For more details, refer to the [Synchronous and Asynchronous Calls](#).

You can download files that are up to 10 MB through HTTP API and sendEmail or EMail Event.

A dedicated volume of space will be mounted to the File Operations. All the downloaded files should be kept in unique path based on `tenantId`, `workflowInstanceId` and `actionInstanceId`. The path of the file should be stored as a reference in action output.

For example: `1/01BB6ALS3QRYK0A5nqmip8gBeNS7M09sKk7/01BB6ALS3QRYK0A5nqmip8gBeNS7M09sKI8/{filename}`

Any executables, dlls, and so on should not be downloaded. All the downloaded files must have strict Read Only permission.

You can upload file through HTTP API and sendEmail or EMail Event.

Creating Custom Adapters

Creating Custom Adapters

- [Creating Custom Adapters Overview](#)
- [Python Adapter](#)
- [Golang Adapter](#)
- [Java Adapter](#)

Creating Custom Adapters Overview

Creating Custom Adapters Overview

The following sections provide information on how to create custom adapters in Action Orchestrator. You can use these adapters in the workflow.



You need access to the Git files for creating a custom adapter in Action Orchestrator. For access, contact [CloudCenter Suite Support team](#).

Python Adapter

Python Adapter

- [Create Custom Adapter in Python](#)

Create Custom Adapter in Python

Create Custom Adapter in Python

This section provides information on creating custom adapter in Python:



Important

Windows is not supported anymore. It is not possible to run python adapter locally on windows. Template now supports running commands in jail environment and uses some specific libraries

1. To set up Git access to the Action Orchestrator Bitbucket repositories, contact [CloudCenter Suite Support team](#).
2. Install Python wheel package locally, perform the following:
 - a. On **Mac or Linux**, run **sudo pip install wheel**.
3. Fetch source code of Python template adapter, perform the following:
 - a. **git clone**, see [Python Adapter Template](#).
 - b. Under the template folder, **git checkout dev**.
4. Make a clone of the **adapter-template python** folder. Rename the folder to appropriate custom adapter name.
5. To create schema for adapters from UI, see [Creating Schema](#).
 - Follow the schema creation order described in Create Schemas doc.
 - When creating adapter schema please remember that the name of **MICROSERVICE NAME** should be the same as **demo-adapter-name** used when building docker container.
 - When creating target schema please notice that **SCHEMA TYPE** should be the same as used in adapter **BasicConstants.TARGET_NAME**.
 - When creating activity schema please notice that **SCHEMA TYPE** should be the same as used in adapter **BasicConstants.ACTIVITY_x_NAME**.
6. Open the custom adapter project in an IDE like Visual Studio Code or another IDE and update the following files:
 - a. Under **activities_python\actions** folder, rename **action_helloworld.py** to appropriate activity name, update activity inputs and outputs using proper convention used while creating activity schema. By default **action_helloworld.py** supports two input properties (**input_one**, **input_two**) and two output properties (**output_one**, **output_two**).
 - b. Under **activities_python\constants** folder:
 - i. Update **basic_constants.py** using proper convention used while creating schemas.
 - c. Under **activities_python\actions** folder, update **verify_target.py** for target and account key verification.
 - d. Under **activities_python\events** folder, update **event_resolve.py** to import proper classes.
 - e. Under **yaml** folder, replace all **demo-adapter** occurrences with the custom adapter name **demo-adapter.yaml**.
 - f. Under **activities_python\common\factories** folder, update description in **parser.py** where **parser = argparse.ArgumentParser(description='Template Python activities adapter.'**)
7. On command line, under custom adapter folder add the custom adapter project directory to PYTHONPATH using the following command: **export PYTHONPATH=PathToCustomPythonAdapterProject**
8. On command line, go under the custom adapter folder and perform the following:
 - a. Update **setup.py** to include any additional libraries in the **setup_requires** section:

```
setup_requires=['pytest-runner']
```
 - b. Run the following python setup command to create a wheel package of the custom adapter:

```
python setup.py bdist_wheel
```
 - c. Run docker build command to build a docker image. Change **demo-adapter-name** in the command to proper adapter name defined in **demo-adapter.yaml**:

```
docker build -t demo-adapter-name -f Dockerfile
```
 - d. Run the following kubectl command to deploy the custom adapter in Kubernetes cluster:

```
kubectl create -fyaml/demo-adapter.yaml -n orch-platform
```
9. Open Action Orchestrator UI and create custom adapter target and account key.
10. Create **New Workflow**. Make sure that the custom adapter activities show up in the Workflow Editor toolbox and validate those activities.

Python Adapter Template

Python Adapter Template

Overview

This template can be used to create a python based adapter. The template is written in Python.



Template has three actions:

- hello_world
- create_template
- run_script

There is also one action which is supposed to be by default in every adapter, verify_target. Usually verify_target action is used to verify connection and credentials to the target during its creation in UI.

Run adapter locally

1. Install required packages: python-dotenv, six, requests, and responses.

2. Create self-signed certificates in the custom python adapter projectfolder:

- Run **make create-certs**: This will create all needed certificates to run adapter https service locally.
 - After running certificate creation commands you will have the following files created:

```
secrets/ssl/cert/certificate.pem
secrets/ssl/cert/private_key.pem
```

- If you want to use your own certificates, then add following environment variables:

```
export CERTFILE=path_to_certificate.pem
export PKEYFILE=path_to_private_key.pem
export CAFILE=path_to_ca_certificate.pem
```

3. Prepare JAIL environment:

- Download Jailkit package and follow the INSTALL.TXT instructions.

Here are common commands to install Jail environment:

- `wget http://olivier.sessink.nl/jailkit/jailkit-2.20.tar.gz`
- `tar -xzf jailkit-2.20.tar.gz`
- `cd jailkit-2.20;./configure && make && make install`
- `mkdir /jail (or use some other directory)`
- `jk_init -j /jail jk_lsh`
- `PYTHON_PATH=$(which python)`
- `PYTHON_LIB_PATH=$(python -c "import os, inspect; print os.path.dirname(inspect.getfile(inspect))")`
- `jk_cp -j /jail $PYTHON_PATH`
- `jk_cp -j /jail $PYTHON_LIB_PATH`
- `groupadd script_executer`
- `adduser script_executer -G script_executer`
- `jk_jailuser -n -j /jail script_executer`

- Export environment variables needed to run the adapter:

- `export JAIL_DIR=/jail`
- `export JAIL_USERNAME=script_executer`
- `export JAIL_GROUPNAME=script_executer`

4. Add the custom adapter project directory to PYTHONPATH using the following command:**export**

```
PYTHONPATH=PathToCustomPythonAdapterProject
```

5. Run adapter: `python worker/activities-worker`

(worker/activities-worker is the main entry point to run the adapter)

Files

1. `setup.py`, `setup.cfg`,`requires.txt`: Used for building python package
2. `Dockerfile`: Used to create adapter docker container Example commands:`cd 'cloned adapter repo folder', python setup.py bdist_wheel, docker build -t ad-template (ad-template - container name for the adapter)`

3. Jenkinsfile, Jenkinsfile-lambda: Used in jenkins jobs
4. event-json: Contains sample api calls to run some actions

activities_python Folders

Actions folder contains four template actions and sample test files:

1. Hello World: Represents an action to demonstrate input and output parameters.
2. Create Template: Represents an action with api POST request. `BasicConstants.ACTION_2_URL` is api relative URL for the action2.
3. Run Script: Represents an action to run python script in jail env.
4. Verify Target: Represents an action for verifying target.

common folder: Is a common adapter library.

constants folder files: You can change the values of these constants to customize your adapter.

events/event_resolver.py: Type resolver for incoming requests. We have four event types with corresponding actions.

pythonutils: Contains different models used in actions.

Other folders/files:

functions/lambda_function_name/handler.py is used to run adapter as aws lambda function. The name **lambda_function_name** should be the same as name in adapter lambda schema.

To create schema for adapters from Action Orchestrator UI, see [Manage Schemas](#).

scripts/run_test.sh: Script is used in build to run tests.

worker/activities-worker: Is used to run adapter as microservice.



For more information on Python adapter template, contact Action Orchestrator support team.

Related Topics

- [Manage Schemas](#)
- [Action Orchestrator Schemas](#)

Back to: [Create Custom Adapter in Python](#)

Golang Adapter

Golang Adapter

- [Create Custom Adapter in Golang](#)

Create Custom Adapter in Golang

Create Custom Adapter in Golang

This section provides information on creating a custom adapter in GoLang:

1. Set up Git access to the Longhorn Bitbucket repositories, contact [CloudCenter Suite Support team](#).
2. Install Golang locally, see <https://golang.org/doc/>.
3. Fetch source code of Golang template adapter by performing the following:
 - a. **git clone**, see [GoLang Adapter Template](#).
 - b. Under the template folder, **git checkout dev**.
4. Make a clone of the **adapter-template-go** folder. Rename the folder to an appropriate custom adapter name.
5. Open the custom adapter project in an IDE like Visual Studio Code and update the following files:
 - a. Under **actions** folder, rename **DemoAction.go** to appropriate activity name, then update activity inputs and outputs using proper convention.
 - b. Under **actions** folder, update **verify_target.go** for target and account key verification.
 - c. Under **events** folder, update **events.go** to import proper classes.
 - d. Under **yaml** folder, replace all **demo-adapter** occurrences with the custom adapter name **demo-adapter.yaml**.
6. To create schema for adapters from UI, see [Manage Schemas](#).
7. On command line, go under the custom adapter folder and perform the following:
 - a. Update **Vendor** folder to include any additional libraries:
go vendor init

go vendor fetch +e
 - b. Run docker build command to build a docker image. Change **demo-adapter-name** in the command to proper adapter name defined in **demo-adapter.yaml**:

docker build . -t demo-adapter-name -f Dockerfile
 - c. Run the following kubectl command to deploy the custom adapter in Kubernetes cluster:

**kubectl create -f
yaml/demo-adapter.yaml -n orch-platform**
8. Open Action Orchestrator UI and create custom adapter target and account key.
9. Create **New Workflow**. Make sure that the custom adapter activities show up in the Workflow Editor toolbox and validate those activities.

Related Topic

- [Schema Generation Utility](#)
- [GoLang Adapter Template](#)

Schema Generation Utility

Schema Generation Utility

Overview

This repo can be used to generate schemas for template adapter. The utility is written in Golang and you can simply run it like: `go run schema.go template.go`



The utility will generate five sample schemas. The schemas are adapter, runtime_user, target, and two action schemas.

1. If you want to generate your own schemas with different parameters you need to modify **schema.go** file.
2. Schema.go file has five object with sample data. The objects are AdapterRequest, CredentialsRequest, TargetRequest, ActionRequest1, and ActionRequest2.
3. The object use constants as input parameters for the schema, you can modify either constants or objects values directly. For more information see, [Action Orchestrator Schemas](#).

Folders

constants folder:

1. actions_constants: Used mostly to generate actions schemas
2. adapter_constants: Used to generate adapter schema
3. credentials_constants: Used to generate runtime user schema
4. target_constants: Used to generate target schema
5. basic_constants: Used in actions

schemas folder:

Placeholder for generated schema files

Files

schema.go - main file template.go - go template used to parse data from schema.go and return data in json format.

Back to: [Create Custom Adapter in Golang](#)

GoLang Adapter Template

GoLang Adapter Template


Overview

This template can be used to create a golang api based adapter. The template is written in Golang.

 Template has two actions:


- `get_template`
- `create_template`.

There is also one action which is supposed to be by default in every adapter, `verify_target`. Usually `verify_target` action is used to verify connection and credentials to the target during its creation in UI.

 The response of this API request will be the response of the action. Here, we have assumed that every action performs only one API call to the target.

Run adapter locally

Run `worker/main.go`.

 `worker/main.go` is the main entry point to run the adapter.

Files

1. Makefile - Used to compile the adapter
2. Dockerfile - Used to create adapter docker container
3. Jenkinsfile and Jenkinsfile-lambda - Used in jenkins jobs
4. event-json - Contains sample api calls to run each action

Golang Packages

Actions folder contains three template actions and target and sample test files:

1. common folder: It is a common adapter library.
2. constants folder files: You can change the values of these constants to customize your adapter.
3. events/events.go: Type resolver for incoming requests. We have 4 event types with corresponding actions.
4. utils - Contains different models used in actions.

Other folders/files:

- `functions/lambda_function_name/main.go` is used to run adapter as aws lambda function. The name `lambda_function_name` should be the same as name in adapter lambda schema.
- `scripts/run_test.sh - script` is used in build to run tests.
- `worker/main.go` is used to run adapter as microservice.

 For more information on Golang adapter template, contact Action Orchestrator support team.

Related Topics

- [Manage Schemas](#)
- [Action Orchestrator Schemas](#)

Back to: [Create Custom Adapter in Golang](#)

Java Adapter

Java Adapter

- [Create Custom Adapter in Java](#)

Create Custom Adapter in Java

Create Custom Adapter in Java

This section provides information on creating custom adapter in Java:

1. To set up Git access to the Longhorn Bitbucket repositories, contact [CloudCenter Suite Support team](#).
2. Install Java JDK locally, see https://docs.oracle.com/javase/8/docs/technotes/guides/install/install_overview.html.
3. Fetch source code of Java template adapter, perform the following:
 - a. **git clone**, see [Java Adapter Template](#).
 - b. Under the template folder, **git checkout dev**.
4. Make a clone of the **adapter-template-java** folder. Rename the folder to appropriate custom adapter name.
5. Open the custom adapter project in an IDE like Visual Studio Code or another IDE and update the following files:
 - a. Under **actions** folder, rename **ActionJsonPathQuery.java** to appropriate activity name, update activity inputs and outputs using proper convention.
 - b. Under **events** folder, update **EventResolver.java** to add switch case to make a call to appropriate action class.
 - c. Under Project Directory **adapter-template-java**, replace all **adapter-template-java** name with custom adapter name and add required dependencies for custom adapter in **pom.xml**.
6. Under **constants** folder, update **Constants.java** to include input configurations.
7. To create schema for adapters from UI, see [Manage Schemas](#).
8. On command line, go under the custom adapter folder and perform the following:
 - a. Update **Vendor** folder to include any additional libraries.
 - b. Create class files that should be overridden under the same path of the library where the actual class files exists.
 - c. Run docker build command to build a docker image. Change **adapter-template-java** in the command to appropriate adapter name defined in **demo-adapter.yaml**: **docker build . -t adapter-template-java-f Dockerfile**
 - d. Run the following kubectl command to deploy the custom adapter in Kubernetes cluster: **kubectl create -f yaml/demo-adapter.yaml -n orch-platform**
9. Open Action Orchestrator UI.
10. Create **New Workflow**. Make sure that the custom adapter activities show up in the Workflow Editor toolbox and validate those activities.

Java Adapter Template

Java Adapter Template

This template can be used to create a Java api based adapter. The template is written in Java.

Run adapter locally

Runfunctions/core/Main.java.



functions/core/Main.java is the main entry point to run the adapter.

Files

1. Makefile: Used to compile the adapter.
2. Dockerfile: Used to create adapter docker container.
3. Jenkinsfile and Jenkinsfile-lambda: Used in jenkins jobs.
4. event-json: Contains sample api calls to run each action.

Folders

Below are the different folders included in the adapter template:

1. actions folder: It contains java code for sample action and a junit test file to test the action.
2. constants folder files: You can change the values of these constants to customize your adapter.
3. coreutils: This folder contains Event.java file which defines format for input payload.
4. events: This folder contains file EventResolver.java, which defines code to resolve the specific event in the input request and invoke the corresponding action code.
5. resources: This folder contains files to define the properties for the applications in the adapter.
6. schemas: This folder contains json files which define schemas for adapter and sample actions.

Related Topics

- [Manage Schemas](#)
- [Action Orchestrator Schemas](#)

Back to: [Create Custom Adapter in Java](#)

Action Orchestrator Schemas

Schemas

- [Overview](#)
- [Data Schema](#)
- [View Schema](#)
- [Sample Schema](#)
- [JSON Standard Keywords](#)

Overview

Overview

The Action Orchestrator uses schemas to define its user interface (UI). This is useful in that schema definitions can be easily created and modified for customer purposes. The schemas exist in the system's database as JSON data structures, and there are both View and Data schemas for each UI page. Outside the database, schemas exist in .json format files, with the view and data sections being in the same file.

The [Manage Schemas](#) page helps to view and modify existing schemas, as well as create new schemas in a UI setting without editing JSON text directly, and separates the view and data sections of the schemas seamlessly. Within Manage Schema, user interfaces of all adapter objects, including adapters, targets, account keys, activities, and events, are driven by their corresponding schemas. Each object type has its own schema definition. Each object types schema includes both [Data Schema](#) and [View Schema](#).

1. **Data Schema:** Data schema contains the data attributes of each object type. A database schema is the skeleton structure that represents the logical view of the entire database. It defines how the data is organized and how the relations among them are associated. For example, data schema of a target describes all target configuration property names and data types of those properties.
2. **View Schema:** The View schema is used to describe how an object should be rendered properly in a UI. For example, view schema of a target describes how those configuration properties will be rendered on the UI. That is which UI component should be used to render a property, display name of a property, position of a property in UI, which UI section a property belongs to, etc.
3. **Sample Schema:** Displays the sample schema, to be used for reference only.
4. **JSON Standard Keywords:** Displays the list of JSON standard keywords used by Action Orchestrator.

Data Schema

Data Schema

The following validation keywords in a schema impose requirements for successful validation of an instance. The following are the Validation Keywords used in Action Orchestrator:

- [enum](#)
- [format](#)
- [lhd_reference](#)
- [lhd_table](#)
- [lhd_secret](#)

enum

Type-The value of this keyword is an **array**.

Description-The enum keyword is used to restrict a value to a fixed set of values. It must be an array with at least one element, where each element is unique.

Possible Values-null, string, number, Boolean

Schema Example:

```
{litem
  "category": {2items
    "type": string"string"
    "enum": [2items
      0: string"cisco"
      1: string"amazon"
    ]
  }
}
```



The schema state that category field value can be either Cisco or Amazon.

format

Type-The value of this keyword string.

Description-It is used to parse the field value based on specified format such as date, time, date-time, etc.

Possible Values-date, date-time, ipv4, ksuid, lgh-time, time, email, lgh-hostname

lhd_reference

Type- The value of this keyword boolean.

Description-The lhd_reference keyword specifies that a field value can be either number, integer, boolean or variable reference.

Possible Values-TRUE, FALSE

Schema Example:

```
{litem
  "timeout": {2items
    "type": string"integer"
    "lhd_reference": booltrue
  }
}
```



Applicable only for number, integer, and Boolean type fields.

lhd_table

Type- The value of this keyword boolean.

Description-The lhd_table keyword specifies that a field value will be of type table.

Possible Values-TRUE, FALSE

Schema Example:

```
{litem
  "input table": {3items
    "title": string"input table"
    "type": string"string"
    "lhd_table":booltrue
  }
}
```



The value of input_table field will be of type table. It instructs Longhorn console service to validate the field value against correct data type.

lhd_secret

Type- The value of this keyword boolean.

Description-The lhd_secret keyword specifies that a field value has secret information and instructs Longhorn console service to encrypts the value.

Possible Values-TRUE, FALSE

Schema Example:

```
{litem
  "password": {2items
    "type": string"string"
    "lhd_secret":booltrue
  }
}
```



The value of password field will be encrypted.

View Schema

View Schema

The following table provides the list of view schemas used in Action Orchestrator.

- title
- type
- Component
- Number Component Example
- required
- format
- maxlength
- minlength
- maximum
- minimum
- lhv_clearable
- lhv_inline
- lhv_inlineToNext
- lhv_inlinhideTitle
- lhv_placeholder
- lhv_section
- lhv_width
- lhv_mindate
- lhv_maxdate
- lhv_position
- lhv_maxfiles
- lhv_maxFileSize
- lhv_minFileSize
- lhv_options
- lhv_editorTypes
- lhv_optionsDynamicRef
- lhv_filterBy
- lhv_invisible
- lhv_renderAs
- lhv_multiSelect
- lhv_subTitle
- lhv_subTitlePosition
- lhv_disabled
- lhv_variable
- lhv_varTypeAnyOf
- lhv_help
- lhv_table
- lhv_accessColumnsFrom
- lhv_margin
- lhv_pattern
- lhv_trimWhiteSpaces

S. No	Name	Type	Description
1	title	String	The title keyword specifies label for the UI field.
2	type	String	The type keyword specifies type for the UI field.
3	Component	String	The component keyword specifies type of UI component for the field.
4	required	Array	The required keyword specifies all the required fields in the form
5	format	String	It is used to parsed the field value based on specified format. For example, date, time, date-time, and so forth.
6	maxlength	Integer	The maxLength keyword specifies maximum number of characters allowed for the field.
7	minlength	Integer	The minLength keyword specifies minimum number of characters allowed for the field.
8	maximum	Integer	The maximum keyword specifies maximum value allowed for the field.
9	minimum	Integer	The minimum keyword specifies minimum value allowed for the field.
10	lhv_clearable	Boolean	The lhv_clearable keyword is used to specify whether the select component can be cleared.
11	lhv_inline	Boolean	The lhv_inline keyword is used to render title and component in same line.
12	lhv_inlineToNext	Boolean	The lhv_inlineToNext keyword is used to render multiple fields in same line.
13	lhv_inlinhideTitle	Boolean	The lhv_inlinhideTitle keyword specifies to hide the title for the UI field.
14	lhv_placeholder	String	The lhv_placeholder keyword specifies placeholder text for the UI field.
15	lhv_section	String	The lhv_section keyword specifies the section to which UI field belongs to.

16	lhv_width	String	The lhv_width keyword specifies the width of UI field.
17	lhv_mindate	String	The lhv_minDate keyword specifies the minimum Date for Calendar component. The value should be in ISO string format.
18	lhv_maxdate	String	The lhv_maxDate keyword specifies the maximum Date for the Calendar component. The value should be in ISO string format.
19	lhv_position	Integer	The lhv_position keyword specifies the position of UI field in the form.
20	lhv_maxfiles	Integer	The lhv_maxFiles keyword specifies maximum number of files a user can upload using uploadfile component.
21	lhv_maxFileSize	Integer	The lhv_maxFileSize keyword specifies the maximum file size in bytes.
22	lhv_minFileSize	Integer	The lhv_minFileSize keyword specifies the minimum file size in bytes.
23	lhv_options	Array	The lhv_options keyword specifies the list of options for the select component.
24	lhv_editorTypes	Array	The lhv_editorTypes keyword used to specify the types supported by editor component.
25	lhv_optionsDynamicRef	Object	The lhv_optionsDynamicRef keyword specifies the properties and information needed to generate options asynchronously.
26	lhv_filterBy	Object	The lhv_filterBy keyword specifies dynamic filter attributes to filter options.
27	lhv_invisible	String	The lhv_invisible keyword specifies whether to hide the UI field from formOnly or formAndData.
28	lhv_renderAs	String	The lhv_renderAs keyword specifies to render field value as plain text or link or as count in ListWithModal component.
29	lhv_multiSelect	Boolean	The lhv_multiSelect keyword specifies to render dropdown as a multiselect.
30	lhv_subTitle	String	The lhv_subTitle keyword specifies subtitle for the picker component.
31	lhv_subTitlePosition	String	The lhv_subTitlePosition keyword specifies position of subtitle in picker component.
32	lhv_disabled	Boolean	The lhv_disabled keyword used to disabled the field.
33	lhv_variable	String	The lhv_variable keyword specifies that a field can be referenced by variables.
34	lhv_varTypeAnyOf	Array	The lhv_varTypeAnyOf keyword specifies types of variable a field can accept.
35	lhv_help	String	The lhv_help keyword specifies additional information related to UI field.
36	lhv_table	Boolean	The lhv_table keyword specifies output variable is of type table.
37	lhv_accessColumnsFrom	String	The lhv_accessColumnsFrom keyword specifies the field name from which UI field should get the columns from.
38	lhv_margin	String	The lhv_margin keyword specifies the margin for the UI field.
39	lhv_pattern	String	The lhv_pattern keyword specifies the pattern name for the field, against which field value will get validated.
40	lhv_trimWhiteSpaces	String	The lhv_trimWhiteSpaces keyword specifies the position from which blank spaces should be trimmed.

title

Type-The value of this keyword is a **String**.

Description-The title keyword specifies label for the UI field.

Possible Values-Value should be defined by user.

type

Type-The value of this keyword is a **String**.

Description-The type keyword specifies type for the UI field.

Possible Values-string, number, integer, boolean, object, and array.

String Example

If the field type is string then the value generated will be string.

Schema

```
{ 1 item
  "display_name" : { 1 item
    "type" : string "string"
  }
}
```

Payload

```
{ 1 item
  "display_name" : string "New Workflow"
}
```

Number Example:

If the field type is number then the value generated will be number.

Schema

```
{ 1 item
  "total" : { 1 item
    "type" : string "number"
  }
}
```

Payload

```
{ 1 item
  "total" : float 20.35
}
```

Integer Example:

If the field type is integer then the value generated will be integer.

Schema

```
{ 1 item
  "timeout" : { 1 item
    "type" : string "integer"
  }
}
```

Payload

```
{ 1 item
  "total" : int 5
}
```

Boolean Example

If the field type is integer then the value generated will be Boolean.

Schema

```
{ 1 item
  "isRequired" : { 1 item
    "type" : string "boolean"
  }
}
```

Payload

```
{ 1 item
  "isRequired" : bool true
}
```

Object Example

If the field type is integer then the value generated will be object.

Schema

```
{ 1 item
  "employee_details" : { 3 items
    "type" : string "object"
    "title" : string "Employee Details"
    "properties" : { 2 items
      "name" : { 2 items
        "type" : string "string"
        "title" : string "Employee Name"
      }
      "id" : { 2 items
        "type" : string "number"
        "title" : string "Employee Id"
      }
    }
  }
}
```

Payload

```
{ 1 item
  "employee_details" : { 2 items
    "id" : int 1
    "name" : string "Brown"
  }
}
```

Array Example

If the field type is array then the value generated will be either array of string or array of objects depending on the schema. Below sample json is for array of objects.

Schema

```
{ 1 item
  "queries" : { 4 items
    "type" : string "array"
    "title" : string "Json Queries"
    "component" : string "list"
    "items" : { 2 items
      "type" : string "object"
      "properties" : { 2 items
        "query_name" : { 2 items
          "type" : string "string"
          "title" : string "Query Name"
        }
        "query_type" : { 2 items
          "type" : string "string"
          "title" : string "Data Type"
        }
      }
    }
  }
}
```

Payload

```

{ 1 item
  "queries" : [ 2 items
    0 : { 2 items
      "query_name" : string "Name"
      "query_type" : string "string"
    }
    1 : { 2 items
      "query_name" : string "Id"
      "query_type" : string "integer"
    }
  ]
}

```

Component

Type-The value of this keyword is a **String**.

Description-The component keyword specifies type of UI component for the field.

Possible Values-string, number, integer, boolean, checkbox, radio, textarea, password, picker, switch, objectComponent, list, propertylist, dynamiclist, horizontallist, editor, calendar, uploadfile, and daterange.

String Component Example

If the component is string then input field of type text is rendered.

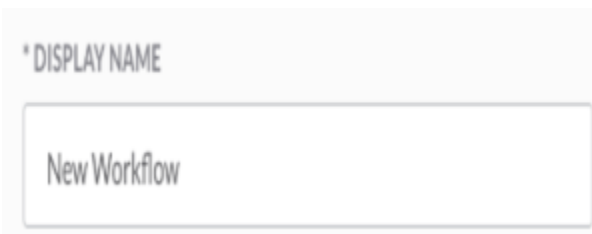
Schema

```

{ 1 item
  "display_name" : { 2 items
    "type" : string "string"
    "component" : string "string"
  }
}

```

Preview



If user want to render a text input then no need to explicitly mention component in schema. Longhorn UI will render text input by default if field type is string.

Number Component Example

If the component is number then input field of type number is rendered.

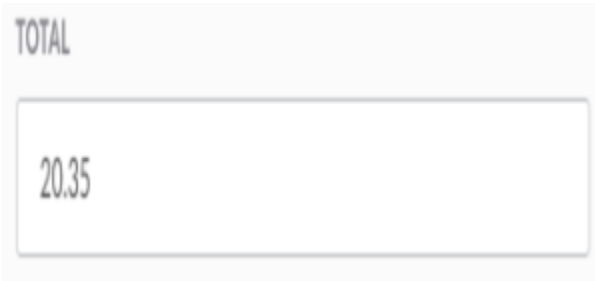
Schema

```

{ 1 item
  "total" : { 2 items
    "type" : string "number"
    "component" : string "number"
  }
}

```

Preview



A preview of a number input field. The label "TOTAL" is positioned above the input field. The input field contains the value "20.35".



If user want to render a number input then no need to explicitly mention component in schema. Longhorn UI will render number input by default if field type is number.

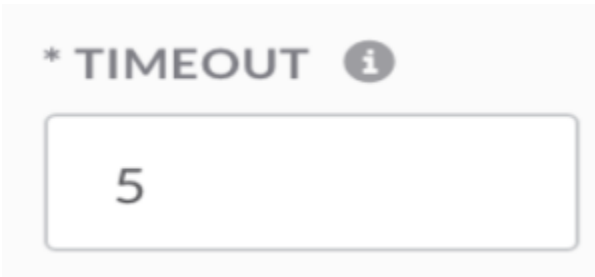
Integer Component Example

If the component is integer then input field of type number is rendered.

Schema

```
{ 1 item
  "timeout" : { 2 items
    "type" : string "integer"
    "component" : string "integer"
  }
}
```

Preview



A preview of an integer input field. The label "* TIMEOUT" is positioned above the input field, followed by an information icon (i). The input field contains the value "5".



If user want to render a integer input then no need to explicitly mention component in schema. Longhorn UI will render integer input by default if field type is integer. Difference between number and integer component is in integer component you cannot enter decimal numbers where as in number component you can.

Boolean Example

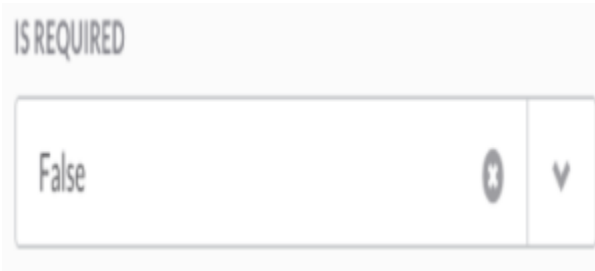
If the component is Boolean then a drop down component will be render with TRUE/FALSE option.

Schema

```
{ 1 item
  "isRequired" : { 2 items
    "type" : string "boolean"
    "component" : string "boolean"
  }
}
```

Preview

Boolean Component



Checkbox Example

Checkbox component is used for Boolean type fields.

Schema

```
{ 1 item
  "is_required" : { 2 items
    "type" : string "boolean"
    "component" : string "checkbox"
  }
}
```

Preview

Checkbox Component



Radio Example

Radio component is used for Boolean type fields.

Schema

```
{ 1 item
  "is_required" : { 2 items
    "type" : string "boolean"
    "component" : string "radio"
  }
}
```

Preview

Radio Component





If radio component is configured with `lhv_options` then Longhorn UI will render it as a radio group else it will be rendered as independent radio component.

TextArea Example

TextArea component is used when the value of the field is paragraph.

Schema

```
{ 1 item
  "description" : { 2 items
    "type" : string "string"
    "component" : string "textarea"
  }
}
```

Preview

TextArea Component

DESCRIPTION ⓘ

Password Example

Password component is used for secret values like accessKeys or User Password.

Schema

```
{ 1 item
  "access_key" : { 2 items
    "type" : string "string"
    "component" : string "password"
  }
}
```

Preview

Password Component

PASSWORD

Picker Example

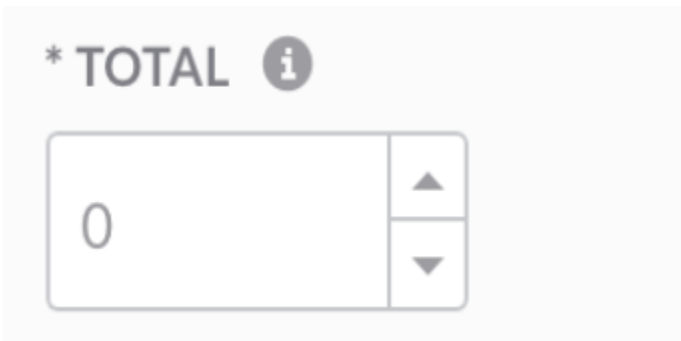
Picker component is used for number type fields. It extends Number component API and provides more features and behavior.

Schema

```
{ 1 item
  "total" : { 2 items
    "type" : string "string"
    "component" : string "picker"
  }
}
```

Preview

Picker Component



Switch Example

Switch component is used for Boolean type fields.

Schema

```
{ 1 item
  "total" : { 2 items
    "type" : string "boolean"
    "component" : string "switch"
  }
}
```

Preview

Switch Component



Object Example

Object component is used if user wants to render payload in object format.

Schema

```

{ 1 item
  "employee" : { 3 items
    "type" : string "object"
    "component" : string "objectComponent"
    "properties" : { 2 items
      "name" : { 2 items
        "type" : string "string"
        "lhv_margin" : string "0px 0px 0px 20px"
      }
      "id" : { 2 items
        "type" : string "integer"
        "lhv_margin" : string "0px 0px 0px 20px"
      }
    }
  }
}

```

Preview

Object Component

EMPLOYEE

ID

NAME

List Example

List component is used for array type fields.

Schema

```

{ 1 item
  "employees" : { 3 items
    "type" : string "array"
    "component" : string "list"
    "items" : { 2 items
      "type" : string "object"
      "properties" : { 2 items
        "name" : { 2 items
          "type" : string "string"
          "title" : string "Name"
        }
        "id" : { 2 items
          "type" : string "integer"
          "title" : string "Id"
        }
      }
    }
  }
}

```

Preview

List Component

EMPLOYEES

ID	NAME
Id	Name

ADD

Preview

List Component with add new

EMPLOYEES

ID	NAME
1	Matt
Id	Name
Required	Required

ADD

Property List Example

Property List component is used for array type fields.

Schema

```
{ 1 item
  "employees" : { 3 items
    "type" : string "array"
    "component" : string "propertylist"
    "items" : { 2 items
      "type" : string "object"
      "properties" : { 2 items
        "name" : { 1 item
          "type" : string "string"
        }
        "id" : { 2 item
          "type" : string "integer"
        }
      }
    }
  }
}
```

Preview

Property List Component

EMPLOYEES

ID ✕

Required

NAME

Required

➕ ADD

Dynamic List Example

Dynamic List component is used for array type fields.

Schema

```
{ 1 item
  "employees" : { 3 items
    "type" : string "array"
    "component" : string "dynamiclist"
    "items" : { 2 items
      "type" : string "object"
      "properties" : { 2 items
        "name" : { 1 item
          "type" : string "string"
        }
        "id" : { 2 item
          "type" : string "integer"
        }
      }
    }
  }
}
```



Its another way of representation in UI for array of objects field.

Preview

Dynamic List Component

EMPLOYEES

ID	NAME
1	Matt ✕
Id	Name

➕ ADD 1 MORE RECORD

Horizontal List Example

Horizontal List component is used for array type fields.

Schema

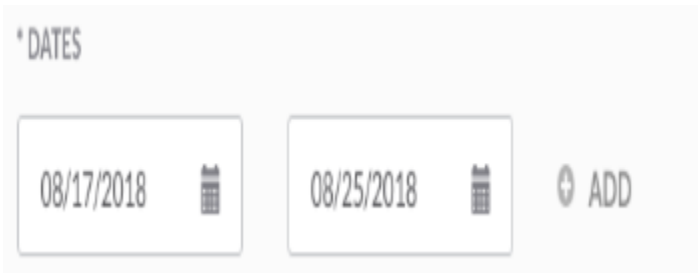
```
{ 1 item
  "date_list" : { 3 items
    "type" : string "array"
    "component" : string "propertylist"
    "items" : { 2 items
      "type" : string "string"
      "component" : string "calendar"
    }
  }
}
```



Its another way of representation in UI for array of strings field.

Preview

Horizontal List Component



Editor Example

Editor component is used to render text editor in UI.

Schema

```
{ 1 item
  "response" : { 4 items
    "type" : string "string"
    "component" : string "editor"
    "lhv_editorTypes" : [ 2 items
      0 : string "XML"
      1 : string "JSON"
    ]
  }
  "title" : string "API Response"
}
```



By default editor component support JSON, TEXT, XML and HTML editorTypes. If user want to render specific type of editor then set the component value to any of ['json', 'xml', 'html']. In addition, user can render editor with set of editorTypes by using lhv_editorTypes keyword in schema.

Preview

Editor Component



Calendar Example

Calendar component is used to render DatePicker in UI.

Schema

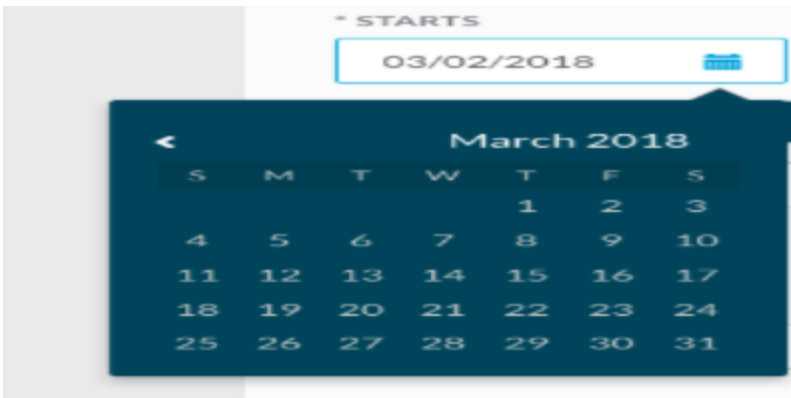
```
{ 1 item
  "start_date" : { 4 items
    "type" : string "string"
    "component" : string "calendar"
    "lhv_format" : string "date"
    "title" : string "Start Date"
  }
}
```



By default calendar component support MM/DD/YYYY dateFormat and it is non-editable. User can set maxDate and minDate using lhv_maxDate and lhv_minDate keywords and its value should be in ISO format. For date fields user must set lhv_format keyword to date in schema.

Preview

Calendar Component



Upload File Example

Upload File component is used to upload the file content. It is commonly used to upload certificate keys.

Schema


```
{ 1 item
  "key" : { 2 items
    "type" : string "string"
    "component" : string "uploadfile"
  }
}
```



This component can be configured using following keys: lhv_acceptedType, lhv_isMultiple, lhv_maxFiles, lhv_maxFileSize lhv_minFileSize.

Preview

Upload File Component

CA CRT FILE

Browse for CA CRT File

BROWSE...

Date Range Example

Date Range component is used to specify start date and end date.

Schema

```
{ 1 item
  "date_range" : { 4 items
    "type" : string "object"
    "title" : string "Date Range"
    "component" : string "daterange"
    "properties" : { 2 items
      "start_date" : { 2 items
        "type" : string "string"
        "component" : string "calendar"
      }
      "end_date" : { 2 items
        "type" : string "string"
        "component" : string "calendar"
      }
    }
  }
}
```



This component is only supported for object types fields with start-date and end-date properties.

Preview

Date Range Component

*** STARTS**

03/02/2018

ENDS

ends

required

Type-The value of this keyword is an **Array**.

Description-The required keyword specifies all the required fields in the form.

Possible Values-any required field name.

Required Example

In below schema display name is marked as required.

Schema

```

{ 2 items
  "required" : { 1 item
    0 : string "display_name"
  }
  "properties" : { 2 items
    "display_name" : { 2 items
      "type" : string "string"
      "maxLength" : int 30
    }
    "description" : { 1 item
      "type" : string "string"
    }
  }
}

```



UI will throw validation message if form is submitted with empty values for required field.

Preview

Required field

*** DISPLAY NAME**

Christmas

DESCRIPTION

format

Type-The value of this keyword is an **String**.

Description-It is used to parse the field value based on specified format. Eg: date, time, date-time, and so forth.

Possible Values-date, date-time, ipv4, ksuid, lgh-time, time, email, lgh-hostname.

maxlength

Type-The value of this keyword is an **Integer**.

Description-The maxLength keyword specifies maximum number of characters allowed for the field.

Possible Values-nonNegative integers.

Maximum Length Example

maxLength is applicable only for string type fields. It is used for Form validation.

Schema

```
{ 1 item
  "display_name" : { 2 items
    "type" : string "string"
    "maxLength" : int 30
  }
}
```

minlength

Type-The value of this keyword is an **Integer**.

Description-The minLength keyword specifies minimum number of characters allowed for the field.

Possible Values-nonNegative integers.

Minimum Length Example

minLength is applicable only for string type fields. It is used for Form validation.

Schema

```
{ 1 item
  "display_name" : { 2 items
    "type" : string "string"
    "minLength" : int 2
  }
}
```

maximum

Type-The value of this keyword is an **Integer**.

Description-The maximum keyword specifies maximum value allowed for the field.

Possible Values-nonNegative integers.

Maximum Example

Maximum is applicable only for integer and number type fields. It is used for Form validation.

Schema

```
{ 1 item
  "count" : { 2 items
    "type" : string "number"
    "maximum" : int 100
  }
}
```

minimum

Type-The value of this keyword is an **Integer**.

Description-The minimum keyword specifies minimum value allowed for the field.

Possible Values-nonNegative integers.

Minimum Example

Minimum is applicable only for integer and number type fields. It is used for Form validation.

Schema

```
{ 1 item
  "count" : { 2 items
    "type" : string "number"
    "minimum" : int 1
  }
}
```

lhv_clearable

Type-The value of this keyword is a **Boolean**.

Description-The lhv_clearable keyword is used to specify whether the select component is clearable or not.

Possible Values-TRUE, FALSE.

Clearable Example

If the value is set to true then the selected option can be cleared.

Schema

```
{ 1 item
  "category" : { 4 items
    "type" : string "string"
    "lhv_clearable" : bool true
    "component" : string "select"
    "options" : { 1 item
      0 : { 2 items
        "label" : string "cisco"
        "value" : string "cisco"
      }
    ]
  }
}
```

lhv_inline

Type-The value of this keyword is a **Boolean**.

Description-The `lhv_inline` keyword is used to render title and component in same line.

lhv_inlineToNext

Type-The value of this keyword is a **Boolean**.

Description-The `lhv_inlineToNext` keyword is used to render multiple fields in same line.

Possible Values-TRUE, FALSE.

Inline To Next Example

`lhv_inlineToNext` is used to render multiple form fields in single line.

Schema

```
{ 1 item
  "display_name" : { 2 items
    "type" : string "string"
    "lhv_inlineToNext" : bool true
  }
}
```

lhv_inlinetitle

Type-The value of this keyword is a **Boolean**.

Description-The `lhv_hideTitle` keyword specifies to hide the title for the UI field.

Possible Values-TRUE, FALSE.

Hide Title Example

`lhv_hideTitle` is used to hide title for the respective field in UI.

Schema

```
{ 1 item
  "display_name" : { 2 items
    "type" : string "string"
    "lhv_hideTitle" : bool true
  }
}
```

lhv_placeholder

Type-The value of this keyword is a **String**.

Description-The `lhv_placeholder` keyword specifies placeholder text for the UI field.

Placeholder Example

`lhv_placeholder` specifies a short hint that describes the expected value of an input field.

Schema

```
{ 1 item
  "display_name" : { 2 items
    "type" : string "string"
    "lhv_placeholder" : string "Display Name"
  }
}
```



The placeholder attribute works with the following input types: text, search, url, tel, email, and password.

lhv_section

Type-The value of this keyword is a **String**.

Description-The lhv_section keyword specifies the section to which UI field belongs to.

Section Example

lhv_section is used to group common behavior fields.

Schema

```
{ 1 item
  "display_name" : { 2 items
    "type" : string "string"
    "lhv_section" : string "Variable"
  }
}
```



If lhv_section keyword is not specified in schema then by default Longhorn UI add the field to General section.

lhv_width

Type-The value of this keyword is a **String**.

Description-The lhv_width keyword specifies the width of UI field.

Width Example

lhv_width is used to configure width of the field.

Schema

```
{ 1 item
  "display_name" : { 2 items
    "type" : string "string"
    "lhv_width" : string "medium"
  }
}
```



xsmall will be of 32px, small will be of 128px, medium will be of 160px, large will be of 256px and extraLarge will be of 400px.

lhv_mindate

Type-The value of this keyword is a **String**.

Description-The `lhv_minDate` keyword specifies the minimum Date for Calendar component. The value should be in ISO string format.

PossibleValues-2018-08-10T12:00:00.000Z

Minimum Date Example

It is used to configure calendar component.

Schema

```
{ 1 item
  "start_date" : { 3 items
    "type" : string "string"
    "component" : string "calendar"
    "lhv_minDate" : string "2018-08-10T12:00:00.000Z"
  }
}
```



Applicable only for calendar component.

lhv_maxdate

Type-The value of this keyword is a **String**.

Description-The `lhv_maxDate` keyword specifies the maximum Date for the Calendar component. The value should be in ISO string format.

PossibleValues-2019-05-19T12:00:00.000Z

Maximum Date Example

It is used to configure calendar component.

Schema

```
{ 1 item
  "start_date" : { 3 items
    "type" : string "string"
    "component" : string "calendar"
    "lhv_maxDate" : string "2019-05-19T12:00:00.000Z"
  }
}
```



Applicable only for calendar component.

lhv_position

Type-The value of this keyword is a **Integer**.

Description-The `lhv_position` keyword specifies the position of UI field in the form.

PossibleValues-nonNegative integers.

lhv_maxfiles

Type-The value of this keyword is an **Integer**.

Description-The `lhv_maxFiles` keyword specifies maximum number of files a user can upload using uploadfile component.

PossibleValues-nonNegative integers.

Maximum Files Example

It is used to configure uploadfile component.

Schema

```
{ 1 item
  "key" : { 3 items
    "type" : string "string"
    "component" : string "uploadfile"
    "lhv_maxfiles" : string "int 1"
  }
}
```



Applicable only for uploadfile component.

lhv_maxFileSize

Type-The value of this keyword is an **Integer**.

Description-The lhv_maxFileSize keyword specifies the maximum file size in bytes.

PossibleValues-nonNegative integers.

Maximum File Size Example

It is used to configure uploadfile component.

Schema

```
{ 1 item
  "key" : { 3 items
    "type" : string "string"
    "component" : string "uploadfile"
    "lhv_maxFileSize" : int 10000
  }
}
```



Applicable only for uploadfile component.

lhv_minFileSize

Type-The value of this keyword is an **Integer**.

Description-The lhv_minFileSize keyword specifies the minimum file size in bytes.


PossibleValues-nonNegative integers.

Minimum File Size Example

It is used to configure uploadfile component.

Schema


```
{ 1 item
  "key" : { 3 items
    "type" : string "string"
    "component" : string "uploadfile"
    "lhv_minFileSize" : int 10000
  }
}
```

 Applicable only for uploadfile component.

lhv_options

Type-The value of this keyword is an **Array**.

Description-The lhv_options keyword specifies the list of options for the select component.

PossibleValues-array of objects with label value attributes.

Options Example


It is used to configure select component.

Schema

```
{ 1 item
  "Category" : { 3 items
    "type" : string "string"
    "component" : string "select"
    "lhv_options" : [ 2 items
      0 : { 2 items
        "label" : string "Cisco"
        "value" : string "cisco"
      }
      1 : { 2 items
        "label" : string "Amazon"
        "value" : string "amazon"
      }
    ]
  }
}
```

Payload

```
{ 1 item
  "category" : string "cisco"
}
```

 Applicable only for select component.

lhv_editorTypes

Type-The value of this keyword is an **Array**.

Description-The lhv_editorTypes keyword used to specify the types supported by editor component.

PossibleValues-json, xml, and html.

Editor Types Example

It is used to configure editor component.

Schema

```
{ 1 item
  "Category" : { 3 items
    "type" : string "string"
    "component" : string "editor"
    "lhv_editorTypes" : [ 2 items
      0 : string "json"
      1 : string "xml"
    ]
  }
}
```

Payload

```
{ 1 item
  "response" : { 1 item
    "description" : string "hello Longhorn user"
  }
}
```



Applicable only for editor component.

lhv_optionsDynamicRef

Type-The value of this keyword is an **Object**.

Description-The lhv_optionsDynamicRef keyword specifies the properties and information needed to generate options asynchronously.

Options Dynamic Reference Example

It is used to configure select component asynchronously.

Schema

```
{ 1 item
  "swagger_url" : { 3 items
    "type" : string "string"
    "component" : string "select"
    "lhv_optionsDynamicRef" : { 4 items
      "endpoint" : string "invoke_adapter"
      "valuekey" : string "id"
      "labelkey" : string "name"
      "payload" : { 1 item
        "properties" : { 1 item
          "api_method" : string "web-service.swagger_verify_request"
        }
      }
    }
  }
}
```

Payload

```
{ 1 item
  "swager_url" : { 0 items
  }
}
```



Applicable only for select component.

lhv_filterBy

Type-The value of this keyword is an **Object**.

Description-The lhv_filterBy keyword specifies dynamic filter attributes to filter options.

Possible Values-Its an object type with filterkey and filterValue

FilterBy with static filterValue Example

It is used to configure select component.

Schema

```
{ 1 item
  "target_id" : { 4 items
  "type" : string "string"
  "component" : string "select"
  "lhv_optionsDynamicRef" : { 1 item
  "endpoint" : string "targets"
  }
  "lhv_filterBy" : { 2 items
  "filterkey" : string "type"
  "filterValue" : string "target.meraki"
  }
  }
}
```



Applicable only for asynchronous select component.

FilterBy with dynamic filterValue Example

It is used to configure select component.

Schema

```
{ 1 item
  "target_id" : { 4 items
  "type" : string "string"
  "component" : string "select"
  "lhv_optionsDynamicRef" : { 1 item
  "endpoint" : string "targets"
  }
  "lhv_filterBy" : { 2 items
  "filterkey" : string "type"
  "filterValue" : string "$schema.access_meta.targets[].type$"
  }
  }
}
```



filterValue can be a defined dynamically to get the value from same schema properties or accessMeta info. In Below sample schema, filterValue instructs the UI component to filter the target list based on current schema accessMeta targets type.

lhv_invisible

Type-The value of this keyword is a **String**.

Description-The lhv_invisible keyword specifies whether to hide the UI field from formOnly or formAndData.

Possible Values-formAndData, formOnly.

formAndData Example

It will hide the field from form and data.

Schema

```
{ 1 item
  "properties" : { 1 item
    "no_runtime_user" : { 4 items
      "type" : string "boolean"
      "component" : string "checkbox"
      "default" : bool true
      "lhv_invisible" : string "formAndData"
    }
  }
}
```

Payload

```
{ 1 item
  "properties" : { 0 items
  }
}
```

formOnly Example

It will hide the field from form only, but keeps its value in payload.

Schema

```
{ 1 item
  "properties" : { 1 item
    "no_runtime_user" : { 4 items
      "type" : string "boolean"
      "component" : string "checkbox"
      "default" : bool true
      "lhv_invisible" : string "formAndData"
    }
  }
}
```

Payload

```

{ 1 item
  "properties" : { 1 item
    "no_runtime_user" : bool true
  }
}

```

lhv_renderAs

Type-The value of this keyword is a **String**.

Description-The lhv_renderAs keyword specifies to render field value as plain text or link or as count in ListWithModal component.

PossibleValues-data, link, and count.

RenderAs Example

It is used to configure cell values in ListWithModal component. Each cell value can be render as normal data(text) or as a link to edit the row or as a count.

Schema

```

{ 1 item
  "properties" : { 1 item
    "queries" : { 4 items
      "type" : string "array"
      "title" : string "Json Queries"
      "component" : string "listwithmodal"
      "items" : { 2 items
        "type" : string "object"
        "properties" : { 3 items
          "query_name" : { 3 items
            "type" : string "string"
            "title" : string "Query Name"
            "lhv_renderAs" : string "link"
          }
          "query_type" : { 3 items
            "type" : string "string"
            "title" : string "Data Type"
            "lhv_renderAs" : string "data"
          }
        }
        "options" : { 4 items
          "type" : string "array"
          "component" : string "dynamiclist"
          "lhv_renderAs" : string "count"
          "items" : { 2 items
            "type" : string "object"
            "properties" : { 2 items
              "key" : { 1 item
                "type" : string "string"
              }
              "value" : { 1 item
                "type" : string "string"
              }
            }
          }
        }
      }
    }
  }
}

```



Applicable only for listwithmodal component

lhv_multiSelect

Type-The value of this keyword is a **Boolean**.

Description-The lhv_multiSelect keyword specifies to render drop down as a multiselect.

PossibleValues-TRUE, FALSE.

Multi Select Example

It is use to configure select dropdown to enable multiple selection.

Schema

```
{ 1 item
  "categories" : { 4 items
    "type" : string "array"
    "component" : string "select"
    "lhv_multiSelect" : booltrue
    "lhv_options" : [ 2 items
      0 : { 2 items
        "label" : string "Cisco"
        "value" : string "cisco"
      }
      1 : { 2 items
        "label" : string "Amazon"
        "value" : string "amazon"
      }
    ]
  }
}
```



Applicable only for select component.

lhv_subTitle

Type-The value of this keyword is an **String**.

Description-The lhv_subTitle keyword specifies subtitle for the picker component.

Sub Title Example

lhv_subTitle keyword is used to configure number or picker components.

Schema

```
{ 1 item
  "interval_hours" : { 3 items
    "type" : string "integer"
    "component" : string "picker"
    "lhv_subTitle" : string "HRS"
  }
}
```



Applicable only for number/integer and picker component.

lhv_subTitlePosition

Type-The value of this keyword is a **String**.

Description-The lhv_subTitlePosition keyword specifies position of subtitle in picker component.

Possible Values-right and left.

Sub Title Position Example

lhv_subTitlePosition keyword is used to configure number or picker components.

Schema

```
{ 1 item
  "interval_hours" : { 4 items
    "type" : string "integer"
    "component" : string "picker"
    "lhv_subTitle" : string "HRS"
    "lhv_subTitlePosition" : string "right"
  }
}
```



Applicable only for number/integer and picker component.

lhv_disabled

Type-The value of this keyword is a **Boolean**.

Description-The lhv_disabled keyword used to disabled the field.

Possible Values-TRUE and FALSE.

Disabled Example

lhv_disabled keyword is used to disabled UI field.

Schema

```
{ 1 item
  "display_name" : { 2 items
    "type" : string "string"
    "lhv_disabled" : bool true
  }
}
```



Applicable to all UI fields.

lhv_variable

Type-The value of this keyword is a **String**.

Description-The lhv_variable keyword specifies that a field is variable reference-able.


Possible Values-onlyVariable, onlyVariables, and variableAndInput.

Only Variable Example

If a field has lhv_variable set to onlyVariable then Longhorn UI will allow user to refer only single variable and restrict the user from inputting any plain text.

Schema

```
{ 1 item
  "subject" : { 2 items
    "type" : string "string"
    "lhv_variable" : string "onlyVariable"
  }
}
```


 Applicable only for primitive type fields.

Only Variables Example

If a field has lhv_variable set to onlyVariable then Longhorn UI will allow user to refer multiple variable and restrict the user from inputting any plain text.

Schema

```
{ 1 item
  "subject" : { 2 items
    "type" : string "string"
    "lhv_variable" : string "onlyVariables"
  }
}
```


 Applicable only for primitive type fields.

Variable and Input Example

If a field has lhv_variable set to variableAndInput then Longhorn UI will allow user to refer variables and input any plain text.

Schema

```
{ 1 item
  "subject" : { 2 items
    "type" : string "string"
    "lhv_variable" : string "variableAndInput"
  }
}
```

 Applicable only for primitive type fields.

lhv_varTypeAnyOf

Type-The value of this keyword is an **Array**.

Description-The lhv_varTypeAnyOf keyword specifies types of variable a field can accept.

Possible Values-string, number, integer, boolean, secure_string, array, and table.

Variable Type Any Of Example

In below schema subject field can refer string, number, integer, secure_string type variables.

Schema


```

{ 1 item
  "subject" : { 3 items
    "type" : string "string"
    "lhv_variable" : string "VariableAndInput"
    "lhv_varTypeAnyOf" : [ 5 items
      0 : string "string"
      1 : string "number"
      2 : string "boolean"
      3 : string "integer"
      4 : string "secure_string"
    ]
  }
}

```



Applicable only for primitive type fields.

lhv_help

Type-The value of this keyword is a **String**.

Description-The lhv_help keyword specifies additional information related to UI field.

lhv_table

Type-The value of this keyword is a **Boolean**.

Description-The lhv_table keyword specifies outout variable is of type table.

lhv_accessColumnsFrom

Type-The value of this keyword is a **String**.

Description-The lhv_accessColumnsFrom keyword specifies the field name from which UI field should get the columns from.

lhv_margin

Type-The value of this keyword is a **String**.

Description-The lhv_margin keyword specifies the margin for the UI field.

lhv_pattern

Type-The value of this keyword is a **String**.

Description-The lhv_pattern keyword specifies the pattern name for the field, against which field value will get validated.

lhv_trimWhiteSpaces

Type-The value of this keyword is a **String**.

Description-The lhv_trimWhiteSpaces keyword specifies the position from which blank spaces should be trimmed.

integer

Sample Schema

Sample Schema

This page displays the sample schema, to be used for reference only:

```
{
  "schema_type": "meta",
  "name": "lhdata",
  "title": "LHData",
  "description": "Longhorn Data Meta Schema",
  "base_type": "meta",
  "type": "meta.lhdata",
  "version": "1.0.0",
  "meta_schema": {
    "$schema": "http://cisco.com/lhdata-01/schema#",
    "$id": "http://cisco.com/lhdata-01/schema#",
    "title": "Longhorn data meta-schema",
    "definitions": {
      "schemaArray": {
        "type": "array",
        "minItems": 1,
        "items": {
          "$ref": "#"
        }
      },
      "nonNegativeInteger": {
        "type": "integer",
        "minimum": 0
      },
      "nonNegativeIntegerDefault0": {
        "allOf": [{
          "$ref": "#/definitions/nonNegativeInteger"
        },
        {
          "default": 0
        }
      ]
    },
    "simpleTypes": {
      "enum": [
        "array",
        "boolean",
        "integer",
        "null",
        "number",
        "object",
        "string"
      ]
    },
    "stringArray": {
      "type": "array",
      "items": {
        "type": "string"
      },
      "uniqueItems": true,
      "default": []
    }
  },
  "type": ["object", "boolean"],
  "properties": {
    "$id": {
      "type": "string",
      "format": "uri-reference"
    },
    "$schema": {
      "type": "string",
      "format": "uri"
    }
  },
}
```

```

"$ref": {
  "type": "string",
  "format": "uri-reference"
},
"$comment": {
  "type": "string"
},
"title": {
  "type": "string"
},
"description": {
  "type": "string"
},
"default": true,
"readOnly": {
  "type": "boolean",
  "default": false
},
"examples": {
  "type": "array",
  "items": true
},
"multipleOf": {
  "type": "number",
  "exclusiveMinimum": 0
},
"maximum": {
  "type": "number"
},
"exclusiveMaximum": {
  "type": "number"
},
"minimum": {
  "type": "number"
},
"exclusiveMinimum": {
  "type": "number"
},
"maxLength": {
  "$ref": "#/definitions/nonNegativeInteger"
},
"minLength": {
  "$ref": "#/definitions/nonNegativeIntegerDefault0"
},
"pattern": {
  "type": "string",
  "format": "regex"
},
"additionalItems": {
  "$ref": "#"
},
"items": {
  "anyOf": [{
    "$ref": "#"
  },
  {
    "$ref": "#/definitions/schemaArray"
  }
  ],
  "default": true
},
"maxItems": {
  "$ref": "#/definitions/nonNegativeInteger"
},
"minItems": {
  "$ref": "#/definitions/nonNegativeIntegerDefault0"
},
"uniqueItems": {
  "type": "boolean",
  "default": false
},

```

```

"contains": {
  "$ref": "#"
},
"maxProperties": {
  "$ref": "#/definitions/nonNegativeInteger"
},
"minProperties": {
  "$ref": "#/definitions/nonNegativeIntegerDefault0"
},
"required": {
  "$ref": "#/definitions/stringArray"
},
"additionalProperties": { "$ref": "#" },
"definitions": {
  "type": "object",
  "additionalProperties": {
    "$ref": "#"
  },
  "default": {}
},
"properties": {
  "type": "object",
  "additionalProperties": {
    "$ref": "#"
  },
  "default": {}
},
"patternProperties": {
  "type": "object",
  "additionalProperties": {
    "$ref": "#"
  },
  "propertyNames": {
    "format": "regex"
  },
  "default": {}
},
"dependencies": {
  "type": "object",
  "additionalProperties": {
    "anyOf": [{
      "$ref": "#"
    },
    {
      "$ref": "#/definitions/stringArray"
    }
  ]
}
},
"propertyNames": {
  "$ref": "#"
},
"const": true,
"enum": {
  "type": "array",
  "items": true,
  "minItems": 1,
  "uniqueItems": true
},
"type": {
  "anyOf": [{
    "$ref": "#/definitions/simpleTypes"
  },
  {
    "type": "array",
    "items": {
      "$ref": "#/definitions/simpleTypes"
    },
    "minItems": 1,
    "uniqueItems": true
  }
}
}

```

```

    ]
  },
  "format": {
    "type": "string"
  },
  "contentMediaType": {
    "type": "string"
  },
  "contentEncoding": {
    "type": "string"
  },
  "if": {
    "$ref": "#"
  },
  "then": {
    "$ref": "#"
  },
  "else": {
    "$ref": "#"
  },
  "allOf": {
    "$ref": "#/definitions/schemaArray"
  },
  "anyOf": {
    "$ref": "#/definitions/schemaArray"
  },
  "oneOf": {
    "$ref": "#/definitions/schemaArray"
  },
  "not": {
    "$ref": "#"
  },
  "reference": {
    "type": "boolean",
    "default": false
  },
  "lhd_reference": {
    "type": "boolean",
    "default": false
  },
  "lhd_table": {
    "type": "boolean"
  },
  "lhd_dataFormat": {
    "type": "string",
    "enum": ["xml", "json"]
  },
  "lhd_secret": {
    "type": "boolean",
    "default": false
  }
},
"default": true
}
}

```

JSON Standard Keywords

JSON Standard Keywords

The following are the list of JSON standard keywords used by Action Orchestrator:

- title
- type
- description
- default
- readOnly
- examples
- multipleOf
- maximum
- exclusiveMaximum
- minimum
- exclusiveMinimum
- maxLength
- minLength
- pattern
- items
- maxItems
- minItems
- uniqueItems
- contains
- maxProperties
- minProperties
- required
- properties
- enum
- format
- contentMediaType
- contentEncoding
- if
- then
- else
- allOf
- anyOf
- oneOf

- not



For more information, see this external page on [JSON Schema Validation](#).

Action Orchestrator API

Action Orchestrator API

- [API Overview](#)
- [API Authentication](#)
- [API Key](#)
- [Base URI Format](#)
- [HTTP Status Codes](#)
- [CSRF Token Protection](#)
- [API Permissions](#)
- [Synchronous and Asynchronous Calls](#)
- [Action Orchestrator Calls 5.2.0](#)
- [Import/Export API Calls 5.2.0](#)

API Overview

CloudCenter Suite API Overview

- [Overview](#)
- [CloudCenter Suite API Version](#)
- [Date Format](#)
- [HTTPS Request Methods](#)
- [Response Schema](#)
- [Resource URL and ID](#)
- [Pagination](#)
 - [Pagination Request Attributes](#)
 - [Pagination Response Attributes](#)
- [Sorting](#)
- [Searching](#)
- [HTTP Location URL](#)
- [Who Can Use CloudCenter Suite APIs?](#)

Overview

The payloads for the CloudCenter Suite APIs are visible in the API documentation section for each module.

CloudCenter Suite API Version

CloudCenter Suite APIs provide support for the CloudCenter Suite modules: [Suite Admin API](#), [Workload Manager API](#), [Action Orchestrator API](#), and [Cost Optimizer API](#).

The User, Groups, and Tenant APIs are part of the Suite Admin and each API using these services have an additional prefix in the URI. The payloads for the CloudCenter Suite APIs are visible in the API documentation section for each module.

The v2 APIs, where available, provide structured responses with minimum details and provides links for nested resources as well as improved search, sort, and pagination filters.

Date Format

The CloudCenter Suite API date and time values are formatted in [Unix time](#) to the millisecond level. The APIs are agnostic to dates and time zones.

HTTPS Request Methods

CloudCenter Suite APIs support the following request methods:

- **GET**: To query or view the server information based on a CloudCenter Suite deployment
- **PUT**: To replace the entire object for update operations
- **POST**: To perform a CloudCenter Suite task or creating the resource
- **DELETE**: To remove specific aspects of the CloudCenter Suite deployment

Response Schema

CloudCenter APIs issue responses for all APIs using both JSON and XML formats. You can set the response format by sending the appropriate Content-Type request headers:

- JSON (Default)

```
Content-Type: application/json Accept: application/json
```

- XML

```
Content-Type: application/xml Accept: application/xml
```

- CSV (Only for Reports)



The CSV format only applies to report-based APIs

Content-Type: application/csv Accept: text/csv

Resource URL and ID

For each API request, you see two common attributes displayed in the API response:

```
{
  "resource": "https://<HOST>:<PORT>/v1/users/",
  "size": 12,
  "pageNumber": 0,
  "totalElements": 12,
  "totalPages": 1,
  "users": [
    {
      "id": "2",
      ...
    }
  ]
}
```

- The **resource** URL: A unique URL that provides access to the requested *CloudCenter Suite Resource*.
- The POST and PUT API calls additionally provide an **id** attribute for each new *CloudCenter Suite Resource*.

Pagination

The pagination information differs based on the API version:

- **v1 APIs:** The GET (view or list) APIs support pagination by default. CloudCenter Suite APIs use the following attributes to provide paginated results:


```
{
  "resource": "https://<HOST>:<PORT>/v1/users/",
  "size": 12,
  "pageNumber": 0,
  "totalElements": 12,
  "totalPages": 1,
  "users": [
    {
      "id": "2",
      ...
    }
  ]
}
```

- **v2 APIs:** Requires the *page* and *size* attributes for any request. The default size for v2 APIs now list 50 records by default.

Pagination Request Attributes

page

- **Description:** The total number of pages in for the API listing.
 - Default = 0
 - If **size=0**, then the **page** value is ignored.
 - If not specified (**page=0&size=20**), the default **size** (default = 20) value displays the first 20 elements, which is equal to one page
 - If you specify both the page and the size values, the following applies:

If you specify...	...then
size=21	Elements numbered 21 - 40 entities are displayed, which is equal to 2 pages
page=0 (or not specified)	The first set of 20 elements in the list, elements 1 to 20 are displayed
page=1	The second set of 20 elements in the list, elements 21 to 40 are displayed
page=2	The third set of 20 elements in the list (the third page). <div style="border: 1px solid green; border-radius: 10px; padding: 5px; margin-top: 10px;"> if the page does not have more than 10 elements, then only those 10 elements are displayed.</div>
page=1&&size=10	A set of 10 elements, Elements 11 to 20 are displayed
page=1&&size=20	A set of 20 elements, Elements 21 to 40 are displayed
page=2&&size=10	A set of 10 elements, Elements 21 to 30 are displayed

- **Type:** Integer

size

- **Description:** Total number of records that any list page should contain. The default is:
 - v1 APIs = 20 records
 - v2 APIs = 50 records
- **Type:** Integer

Pagination Response Attributes

- v1 APIs:
 - **pageResource**
 - **Description:** Identifies the pagination information for each resource
 - **Type:** Sequence of attributes for v1 APIs

size (see above)
pageNumber <ul style="list-style-type: none">• Description: The page number that the client wants to fetch. Page numbers start with 0 (default).• Type: Integer
totalElements <ul style="list-style-type: none">• Description: The number resources that an API call returns• Type: Long
totalPages <ul style="list-style-type: none">• Description: The number of pages in a response• Type: Integer

- v2 APIs:
 - **pageResource**
 - **Description:** Identifies the pagination information for each resource
 - **Type:** Sequence of attributes for v2 APIs

resource <ul style="list-style-type: none">• Description: Unique URL to access this resource.• Type: String
size (see above)

status

- **Description:** Status of the operation. See the *APIs for the relevant module* to view a list of all job operations.
- **Type:** Enumeration

Enumeration	Description
SUBMITTED	The operation has been submitted
RUNNING	The operation is currently in progress
SUCCESS	The operation succeeded
FAIL	The operation failed

startTime/endTime

- **Description:** Start/Endtime for this resource. Unix epoch time in milliseconds.
- **Type:**
 - v1 APIs = Long
 - v2 APIs = Epoch time as a String

totalCost

- **Description:** Identifies the total cost per hour of the job for billing purposes. See the *Cost Optimizer APIs* section to view additional details.
- **Type:** Float

nodeHours


- **Description:** The number of VM hours for this resource. See the *Cost Optimizer APIs* section to view additional details.
- **Type:** Float

name

- **Description:** The name assigned for this *CloudCenter Suite Resource*. Valid characters are letters, numbers, underscores, and spaces.
- **Type:** String

deploymentEntity.name

- **Description:** Identifies evolving resource details about the deployment. The deploymentEntity attribute uses the *deploymentEntity.name* format, where **name** is a search value for deploymentEntity and deploymentEntity itself is a JSON object.

 Instead of placing the deployment name at the top level search and adding numerous query parameters, this format allows for nested search results. The top level **name** is the job name and deploymentEntity.name is the deployment name.

- **Type:** JSON objects

favoriteCreationTime

- **Description:** If the job was configured as a favorite job, then this attribute identifies the time when this configuration took place. See the *Favorite Deployments* section for the relevant release for additional context.
- **Type:** Epoch time as a String

Searching

This attribute is only available for v2 APIs.

search

- **Description:** Searches API responses based on the format specified.
- **Type:** String
 - Format: search=[field, searchType, SearchExpression1, SearchExpression2]
 - Example: search =[startTime, gt, 01/01/2016]
 - Search Expressions:
 - *pattern*: Provide a pattern using the format provided in these *searchType* table below.
 - searchTypes

searchType	Format
eq	==
ne	!=
el	LIKE <i>pattern</i> %
fl	LIKE % <i>pattern</i>

eln	NOT LIKE <i>pattern%</i>
fln	NOT LIKE <i>%pattern</i>
fle	LIKE <i>%pattern%</i> "
gt	> <i>searchValue</i>
lt	< <i>searchValue</i>
ge	>= <i>searchValue</i>
le	<= <i>searchValue</i>
gtlt	> <i>searchValue</i> && <i>searchValue</i>
gtelt	>= <i>searchValue</i> && < <i>searchValue</i>
gtlte	> <i>searchValue</i> && <= <i>searchValue</i>
gtelte	>= <i>searchValue</i> && <= <i>searchValue</i>
emp	Empty string
noemp	Not Empty string
nu	Null value
nn	Not Null Value

- searchValue:

searchValue	SearchType Availability
id	eq
startTime	eq, nu, gtlt
endTime	eq, nu, nn, gtlt
totalCost	eq, gt, ge, le, gtlt, gtlte, gtelte, gtelt
favoriteCreationTime	eq, nu, ,nn gtlt
jobStatusMessage	el, eln, fl, fln, fle, nn, emp, noemp
nodeHours	eq, gt, ge, le, gtlt, gtlte, gtelte, gtelt
name	eq, nn, eln, fle, fln, el, emp, noemp, fl
description	eq, nn, eln, fle, fln, el, emp, noemp, fl
deploymentEntity.name	eq, nn, eln, fle, fln, el, emp, noemp, fl
ownerEmailAddress	eq
cloudFamily	eq, nu
status	eq, nu

HTTP Location URL

The HTTP Status code and the Location URL (highlighted in blue in the following example) is provided in the Response Header when `CreatoresourceAPI` calls are successful:

```

curl -k -X POST -H "Content-Type: application/json" -H "Accept: application/json"
cliqradmin:D3DD6F7874E6B26B https://test.cliqr.com/v1/users -d '{
  "firstName": "User 02",
  "lastName": "Cliqr",
  "password": "cliqr",
  "emailAddr": "user.02@cliqr.com",
  "companyName": "Cliqr, Inc",
  "phoneNumber": "14085467899",
  "externalId": "",
  "tenantId": 1
}'
> POST /v1/users HTTP/1.1
> Authorization: Basic Y2xpcXJhZG1pbjpwEM0RENkY3ODc0RTZCMjZC
> User-Agent: curl/7.37.1
> Host: test.cliqr.com
> Content-Type: application/json
> Accept: application/json
> Content-Length: 217
>
< HTTP/1.1 201 Created
< Server: Apache-Coyote/1.1
< Set-Cookie: JSESSIONID=0E85227543C66D55E06449582091C2B4; Path=/; Secure; HttpOnly
< osmosix_content: true
< X-Frame-Options: SAMEORIGIN
< Pragma: no-cache
< Expires: Thu, 01 Jan 1970 00:00:00 GMT
< Cache-Control: no-cache
< Cache-Control: no-store
< Location: https://test.cliqr.com/v1/users/12
< Content-Type: application/json;charset=UTF-8
< Transfer-Encoding: chunked
< Vary: Accept-Encoding
< Date: Fri, 07 Aug 2015 20:59:18 GMT

```

Who Can Use CloudCenter SuiteAPIs?

Both admins and users can use CloudCenter Suite REST APIs.

Your login credentials determine if you are an admin (platform (root), tenant admin, or co-admin) or a user. If you do not have the required Permission Controllevel to access any *resource*, you receive the HTTP 403 status error mentioned in the [HTTP Status Codes](#) section.

Back to:

- [Suite Admin API](#)
- [Workload Manager API](#)
- [Action Orchestrator API](#)
- [Cost Optimizer API](#)

API Authentication

API Authentication

- [Overview](#)
- [Authentication Format in CURL Requests](#)
- [Successful Authentication](#)
- [Session Timeout Length](#)

Overview

CloudCenter Suite APIs require the following authentication details for each API call:

- Username
- API access key



The authentication HTTP header is not required when making standalone REST API calls using the username/API Key credentials.

Authentication Format in CURL Requests

Standalone CURL Request Example:

```
curl -H "Accept:application/json" -H "Content-Type:application/json" -u writer:BED74F4D9BFE0DA0 -X GET https://<HOST>:<PORT>/v1/users/27
```

In this CURL request example:

- **writer1** is the username
- **BED74F4D9BFE0DA0** is the API access key

Your tenant administrator can retrieve the username and API access key from the UI. See [API Key](#) for additional details.

Successful Authentication

On successful authentication, CloudCenter Suite sends a browser cookie to maintain the authentication session. The cookie forwards the information to the server for each API call so you do not need to authenticate each time you make an API call. If you do not want to maintain cookies in your browser, you can send the authentication information for each API request. Once authenticated, you can begin making API calls.

Session Timeout Length

The CloudCenter Suite authentication session times out after 15 minutes. If you use a REST client to make API calls by authenticating through the UI's, this session timeout applies to the REST client as well.

However, if you add and save the REST client authentication headers or if you issue CURL commands with the authentication details, you can circumvent the session timeout restriction.

Back to:

- [Suite Admin API](#)
- [Workload Manager API](#)
- [Action Orchestrator API](#)
- [Cost Optimizer API](#)

API Key

Generate API Key

- [Overview](#)
- [UI Process to Generate Your Own API Key](#)
- [UI Process to Generate API Key for Another User](#)
- [API Process to Generate a New API Key](#)

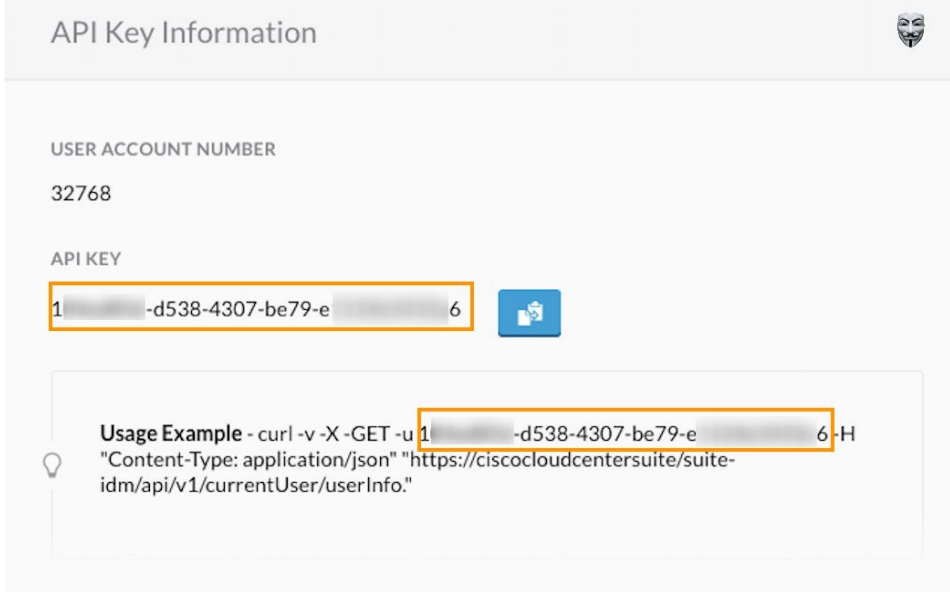
Overview

You need an **API key** to use CloudCenter Suite APIs. Suite administrators or tenant administrator (for their respective tenants) can generate/regenerate an API key by using the Suite Admin UI or the `user_api_key` API call.

UI Process to Generate Your Own API Key

To generate the API key from the UI for yourself, follow this procedure:

1. Navigate to the [Suite Admin Dashboard](#) and click your account profile dropdown.
2. Click the **Generate API Key** link to generate a new API key.
3. Click **Yes** to replace the API key. You can now use this key to make REST API calls as listed in the Usage Example in the following screenshot.



API Key Information

USER ACCOUNT NUMBER
32768

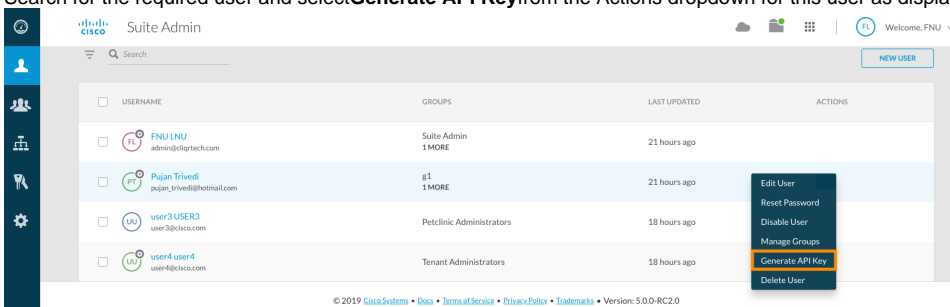
API KEY
1 [redacted] -d538-4307-be79-e 6

Usage Example - curl -v -X GET -u 1 [redacted] -d538-4307-be79-e 6 -H "Content-Type: application/json" "https://ciscocloudcentersuite/suite-idm/api/v1/currentUser/userInfo."

UI Process to Generate API Key for Another User

To generate the API key from the UI for another user, follow this procedure:

1. Navigate to the [Suite Admin Dashboard](#) > **Users**.
2. Search for the required user and select **Generate API Key** from the Actions dropdown for this user as displayed in the following screenshot.



USERNAME	GROUPS	LAST UPDATED	ACTIONS
<input type="checkbox"/> FNU LNU admin@lartech.com	Suite Admin 1 MORE	21 hours ago	
<input type="checkbox"/> Pujan Trivedi pujan_trivedi@hotmail.com	g1 1 MORE	21 hours ago	
<input type="checkbox"/> user3 USER3 user3@ciscc.com	Petclinic Administrators	18 hours ago	
<input type="checkbox"/> user4 user4 user4@ciscc.com	Tenant Administrators	18 hours ago	Generate API Key

3. Click the **Generate API Key** link to generate a new API key. This user can now make REST API calls using new API key.

API Process to Generate a New API Key

To generate the API key using the Suite Admin API call, follow this procedure:

1. Issue the [Password Service API Calls](#) > `/api/v1/users/{userId}/user_api_key` API POST call to generate/regenerate the API key for yourself or for any other user.

```
POST https://host-port/suite-password/api/v1/users/1/user_api_key
```

2. Retrieve the `apiKey` from the response for this API.

```
{
  "userId": 1,
  "apiKey": "1.....-d538-4307-be79-e.....6",
  "accountNumber": "32768"
}
```

3. Use this `apiKey` to make REST API calls.

Back to:

- [Suite Admin API](#)
- [Workload Manager API](#)
- [Action Orchestrator API](#)
- [Cost Optimizer API](#)

Base URI Format

Base URI Format

- [Overview](#)
- [Host Name](#)
- [Port Usage](#)
- [API Version](#)
- [Parameters](#)
- [Parameter Types](#)

Overview

The base URI format is **https:// <host>:<port>/**

Host Name

The host is generally represented as <HOST> in all CloudCenter APIs. It represents the IP address or the DNS name.

The host differs based on your DNS or IP address and port usage.

Port Usage

The port is generally represented at <PORT> in all CloudCenter APIs. It represents the port used to connect to theCCO server for the API connection. The <PORT> in the REST endpoint is **optional**. You can decide if you want to use the port for each API call. All CloudCenter API requests and responses display <PORT> in all examples.

```
curl -H "Accept:application/json" -H "Content-Type:application/json" -u \
cloudcenteradmin:40E45DBE57E35ECB -X GET https://<HOST>:<PORT>/...
```



If you do not specify the port, **then API requests default to Port 443 for a HTTPS connection** when accessing CloudCenter Suite REST APIs.

API Version

The CloudCenter Suite 5.0.0 API version can be v1 or v2 as applicable. The version is identified for each API, where applicable.

Parameters

Parameters used to make the API call are displayed after the APIs and are called out after the description.

Parameter Types

Attribute Type	Description
String	Any combination of characters. Maximum of 255 characters.
Integer	A whole number value. Restricted to 32-bit values.
Long	A whole number value. Restricted to 64-bit values.
Float	A number with or without a decimal point. Displayed as a string in the response.
Boolean	A logical true or false value. May be passed to API requests as true or false or 1 or 0.
Enumeration	A predefined list of values, for example STANDARD or TENANT describes the possible values for each type. Only listed values are permitted, other values result in an error.
JSON Object	A method to parse JavaScript Object Notation (JSON) and return the object value to which a specified name is mapped.

Name-Value Pair	A namevalue pair whereeach element is an attributevalue pair.
Array	A sequential collection of like elements corresponding to the element's data type. The type of the array is determined by the types of the elements (can be String, Integer, Name-Value Pair Type)
Perms List	Lists the permissions for specific user if the user is logged in. An empty response is <i>also</i> indicative of the resource not being currently supported.
Metadata	Metadata information associated with the cloud provider.

Back to:

- [Suite Admin API](#)
- [Workload Manager API](#)
- [Action Orchestrator API](#)
- [Cost Optimizer API](#)

HTTP Status Codes

HTTP Status Codes

CloudCenter APIs return one or more of the following HTTPS status codes for all (synchronous and asynchronous) API requests:

HTTP Response Code	Status	Description
200	Success	Successful GET and PUT
201		Successful POST (when a resource is created)
202		Request accepted for a time-consuming task (asynchronous update and created requests). See Shared 5.1 Synchronous and Asynchronous APIs for more details You can issue GET calls until the request completes.
204		Successful DELETE
30x	Redirection	Only displays if a client calls an API using HTTP instead of HTTPS
400	Client failure	Validation error. This category has additional error codes in the response body for each API (as applicable).
401		Not authenticated
403		Forbidden. You do not have the required permission level to access the <i>CloudCenter Resource</i>
404		Resource not found
500	Server failure	Server error: The server failed to respond to this request due to an internal error

Back to:

- [Suite Admin API](#)
- [Workload Manager API](#)
- [Action Orchestrator API](#)
- [Cost Optimizer API](#)

CSRF Token Protection

CSRF Token Protection

- [Overview](#)
- [The 403 Forbidden Error for Some APIs](#)
- [Setting the CSRF Token](#)
- [Retrieving the CSRF Token](#)
- [Using the CSRF Token](#)

Overview

Cisco provides CSRF protection for all API calls. When an API call is made by you or the CloudCenter Suite, be aware that a CSRF token is required for the following scenarios:

- If the request method is **POST**, **PUT**, or **DELETE** and
- If the request **Content-Type** is not **application/json**

For example, the following functions require the CSRF token:

- Suite Admin Resource Management Service API Calls that use the following functions:
 - Company logo upload
 - User avatar upload
- Workload Manager API Calls that use the following functions
 - Application profiles
 - Logo upload
 - Services logo upload
 - Import applications
 - Cloud account management API calls
 - DELETE calls that change the database contents

The 403 Forbidden Error for Some APIs

If the CSRF token is missing or incorrect, you will see a 403 error due to the CSRF token protection.

If you see this error, you must first set the CSRF token in the request header for the affected API.

Setting the CSRF Token

To set a CSRF token, add **X-CSRF-TOKEN** to the header name (case sensitive, all uppercase).

Retrieving the CSRF Token

To obtain the CSRF token, follow this procedure.

1. You must first pass authentication. See [API Authentication](#) for details.
2. Once authenticated, use one of the following APIs to retrieve the CSRF token from the response body (**csrfToken** attribute). See [Authentication Service API Calls](#) for details.
 - a. Login API (/suite-auth/login)
 - b. Token Refresh API (/suite-auth/api/v1/token)
 - c. CSRF Token API (/suite-auth/api/v1/csrfToken)

Using the CSRF Token

See the following request for examples of using a CSRF Token.

Java Rest Client Example

```
WebResource.Builder builder = webResource.type(MediaType.APPLICATION_JSON).header("X-CSRF-TOKEN", "<TOKEN>");
```

Python Example

```
headers = {'content-type': 'application/json', 'X-CSRF-TOKEN': '<TOKEN>'}  
  
requests.delete(url, headers = headers, verify=False)  
  
requests.post(url, json=jobJson, headers = headers, verify=False)
```

Where **<TOKEN>** is retrieved as specified in the *Retrieving the CSRF Token* section above.

Back to:

- [Suite Admin API](#)
- [Workload Manager API](#)
- [Action Orchestrator API](#)
- [Cost Optimizer API](#)

API Permissions

API Permissions Allowed Roles

- [Overview](#)
- [Current User Permissions](#)
- [Suite Level Permissions](#)
- [Workload Manager Roles](#)
- [Action Orchestrator Roles](#)
- [Cost Optimizer Roles](#)

Overview

Each API identifies the permissions and roles required to execute that API call. Permissions for each API are governed by Role Based Access Control (RBAC) as explained in [Understand Roles](#) and user level as explained in [Understand User Levels](#).

Current User Permissions

Users can find their permission level by executing the `GET /suite-idm/api/v1/currentUser/userInfo` API listed in the [DM Service API Calls > User Controller](#) section.

Suite Level Permissions

Based on the current user's permissions the Suite Admin APIs display enumerations for the **Allowed Role(s)** described in the following table.

Allowed Role(s) Enumeration	Description
SUITE_ADMIN	The initial administrator described in Initial Administrator Setup . This user can perform the following tasks: <ul style="list-style-type: none">• Module Lifecycle Management• Manage Clusters
SUITE_TENANT_ADMIN	The tenant administrator set up as part of the root tenant configuration described in Manage Tenants . This user can perform the following tasks: <ul style="list-style-type: none">• Manage sub-tenants• Create, update, and delete sub-tenant users (including <code>createTenantWithAdmin</code> atomic operation)• Tenant resource management including Email Settings, Branding Information, and so forth
SUITE_USER	Any user added to the CloudCenter Suite. A newly-added user can only view the Suite Admin Dashboard , if not assigned to a group.
SUITE_USER_ADMIN	ASUITE_ADMIN can promote any SUITE_USER to the SuiteAdmin group as described in Create and Assign Groups . This user can perform the following tasks: <ul style="list-style-type: none">• Manage users and groups• Create, update, delete users and groups• Assign roles to users and groups• Manage passwords for users
SUITE_OUTOFBOX_USER	ASUITE_ADMIN can promote any SUITE_USER to be a SUITE_OUTOFBOX_USER, which basically implies that this user has been added to one or more OOB Suite Admin Groups .
SUITE_RESET_PASSWORD	Users with SUITE_ADMIN permissions and/or SUITE_TENANT_ADMIN for this tenant as described in Create and Manage Users > User Actions . This user can perform the following tasks: <ul style="list-style-type: none">• Edit any user's profile by changing the first/middle/last name and email• Configure metadata details• Configure groups• Reset password• Disable a user

Workload Manager Roles

See [OOB Groups, Roles, and Permissions](#) for details.

Action Orchestrator Roles

See [Action Orchestrator Roles](#) for details.

Cost Optimizer Roles

See [Access and Roles](#) for details.

Back to:

- [Suite Admin API](#)
- [Workload Manager API](#)
- [Action Orchestrator API](#)
- [Cost Optimizer API](#)

Synchronous and Asynchronous Calls

Synchronous and Asynchronous Calls

- [Overview](#)
- [Synchronous](#)
- [Asynchronous](#)
 - [Call States](#)
 - [Operation ID Availability](#)

Overview

CloudCenter Suite APIs support both synchronous and asynchronous calls. Some APIs return data in the response body and others will only return an HTTP status. For example, CloudCenter DELETE calls return a **Status204 No Content** after deleting the *resource* in the background.

Synchronous

Synchronous APIs indicate that the program execution waits for a response to be returned by the API. The execution does not proceed until the call is completed. The real state of the API request is available in the response.

Asynchronous

Asynchronous APIs do not wait for the API call to complete. Program execution continues, and until the call completes, you can issue GET requests to review the state after the submission, during the execution, and after the call completion. Use the **Get Operation Status** API to retrieve the status of an asynchronous operation.

As asynchronous calls may take some time to complete, they return HTTP Status Codes responses containing information with an HTTP Status Code, which allows you to retrieve the progress, status, response, and other information for the call.

After submitting an asynchronous API call:

1. Retrieve the resource URL from the HTTP Status Codes.
2. Use this location URL and query the system using GET calls. While the call is in progress and you issue the GET request, you get additional details of the operation being performed. These details are only available while the operation is in various states of execution (RUNNING, SUCCESS, FAILED).
3. When the asynchronous API call completes successfully, issue a GET request to view the SUCCESS state and the resource URL for this operation.

Call States

In the following example of a **Create Cloud Account** API:

- The various states of execution (RUNNING, SUCCESS, FAILED) are highlighted in corresponding colors
- The first and last GET requests are in bold to show the sequence of events

```
Location: https://test.cliqr.com/v1/operationStatus/f503c52a-d13b-4b62-840d-0faa22ccbb78
{ "operationId": "f503c52a-d13b-4b62-840d-0faa22ccbb78", "status": "RUNNING", "msg": "Updating Image permissions...", "progress": 50, "timestamp": 1438850245522, "additionalParameters": null, "operationHistory": [ ], "subtaskResults": null, "resourceUrl": "https://test.cliqr.com/v1/operationStatus/f503c52a-d13b-4b62-840d-0faa22ccbb78" }
curl 'https://test.cliqr.com/v1/operationStatus/f503c52a-d13b-4b62-840d-0faa22ccbb78' -H 'Accept: application/json'
{ "status": "RUNNING", "msg": "Updating Image permissions...", "resource": "https://test.cliqr.com", "additionalParameters": [ ] }
...
curl 'https://test.cliqr.com/v1/operationStatus/f503c52a-d13b-4b62-840d-0faa22ccbb78' -H 'Accept: application/json'
{ "status": "RUNNING", "msg": "Saving cloud account...", "resource": "https://test.cliqr.com/https://test.cliqr.com/v1/operationStatus/f503c52a-d13b-4b62-840d-0faa22ccbb78", "additionalParameters": [ ] }
curl 'https://test.cliqr.com/v1/operationStatus/f503c52a-d13b-4b62-840d-0faa22ccbb78' -H 'Accept: application/json'
{ "status": "SUCCESS", "msg": "Cloud Account is saved successfully.", "resource": "https://test.cliqr.com/https://test.cliqr.com/v1/operationStatus/f503c52a-d13b-4b62-840d-0faa22ccbb78", "additionalParameters": [ ] }
```

Operation ID Availability

Operation IDs (displayed below the Location URL in the above image) allow you to query the status of asynchronous APIs and are only available for a brief period as identified in the following table:

Operation ID Availability	Description
5 minutes	The Operation ID is available for five minutes if the operation completes (regardless of success or failure).
1 hour	The Operation ID is available for one hour if the operation times out and does not complete.

Back to:

- [Suite Admin API](#)
- [Workload Manager API](#)
- [Action Orchestrator API](#)
- [Cost Optimizer API](#)

Action Orchestrator Calls 5.2.0

Action Orchestrator API Calls for 5.2.0

Download the API Swagger file from https://www.cisco.com/content/dam/en/us/td/docs/cloud-systems-management/cloudcenter-suite/Action-Orchestrator/52_AO_Swagger.zip.



AO-5.2.0-console...er_API,json,json

Import/Export API Calls 5.2.0

Import/Export API Calls for Action Orchestrator 5.2.0

Download the API Swagger file from https://www.cisco.com/content/dam/en/us/td/docs/cloud-systems-management/cloudcenter-suite/Action-Orchestrator/52_AO_Swagger.zip.



AO-5.2.0-import...swaggerAPI.json