CloudCenter Platform Documentation

First Published: October 05, 2021

Last Modified: November 08, 2021

Suite Admin 5.4

Suite Admin 5.4.0 Release Notes

Release Date

First Published: April 2022

Updating Modules

CloudCenter Suite Admin 5.4.0 is only supported as an upgrade from Suite Admin 5.3.1. Please ensure that you follow the procedural steps below to correctly update your CloudCenter installation.

1. You must upgrade the Suite Admin module to version 5.4.0 before you upgrade any other CloudCenter Suite module.
2. After the Suite Admin upgrade has been completed, upgrade the other CloudCenter modules to a supported configuration.
   a. Workload Manager required version - 5.5.2
   b. Cost Optimizer required version - 5.5.2
   c. Action Orchestrator required version - 5.2.5
3. Upgrade the respective CloudCenter modules that you use to the most current versions. After performing the upgrade, follow the directions below to upgrade your kubernetes cluster.

> ⓘ **Note**
>
> Before updating any module, verify that you have twice the required CPU/Memory in your cluster. A module-update scenario requires additional resources for the old pod to continue running until the new pod initializes and takes over. This additional resource requirement is temporary and only required while a module update is in progress. After the module is updated, the additional resources are no longer needed.
>
> Update only one module at at time. If you simultaneously update more than one module, your update process may fail due to limited resource availability. See Prepare Infrastructure for additional context.

Backup and Restore

There are two ways to upgrade the kubernetes cluster. Ensure you take backup of the kubernetes cluster before upgrading the cluster.

1. Upgrade the existing kubernetes cluster or
2. Spin up a new kubernetes cluster with the Suite 5.4.0 installer. On this new cluster restore the backup.

> ⚠ Elasticsearch data will not be backed up during a normal backup session

Please follow the instructions documented here to backup before upgrading the cluster.

Kubernetes Cluster Upgrade from v1.18.12 to 1.19.5

Customers running CCS v5.3.1 can now upgrade their kubernetes cluster from v1.18.12 to v1.19.5 using the v5.4.0 installer. However customers need to follow a few required steps to start upgrading the kubernetes version to 1.19.5.
Customers running on kubernetes version 1.16.x **would first** need to use the CCS v5.3.1 installer to upgrade the kubernetes version to 1.18.12. Please refer Suite Admin 5.3.1 release notes.

1. Upgrade the Suite Admin module to version 5.4.0 and also update the other CCS modules used to their most recent versions. Please refer Suite Admin 5.4#Updating Modules.
2. Use v5.4.0 installer to upgrade the kubernetes cluster
3. After upgrading the cluster, users can use the "Take me to Suiteadmin" link to go back to the Suite Admin UI. Please note that this address might change for DHCP based clusters.

Kubernetes upgrade from v1.16.1x to v1.18.12 after upgrading Suite Admin chart to 5.4.0

If you have upgraded only the Suite Admin chart(and not kubernetes cluster) to v5.4.0 you'll see an error in the installer UI:

```
"Failed to validate the user login info:Err: Cluster is NOT running Common-Framework Suite Admin v5.3.x .Please
upgrade the Suite Admin chart to v5.3.x before upgrading kubernetes"
```

You'll need to run a workaround on Installer v5.3.1 to be able to upgrade from k8s v1.16.12 to v1.18.12 using installer v5.3.1.

```
Workaround to be executed on installer v5.3.1:

1. SSH in the installer v5.3.1
2. Run command
kubectl --record deployment.apps/suite-k8s-mgmt set image deployment.v1.apps/suite-k8s-mgmt suite-k8s-
mgmt=devhub-docker.cisco.com/multicloudsuite-dev/suite-k8s-mgmt:5.3.1-2990 -n ccp

Wait for around 5 mins till the new suite-k8s-mgmt pod in ccp namespace becomes Running.
DO NOT restart the installer after this change as it'll replace the image again.

Continue with the cluster ugprade on the installer UI.
```

After completing the full upgrade you'll be able to upgrade kubernetes version from v1.18.12 to v1.19.15 using installer v5.4.0 as mentioned in the previous step.

Kubernetes Cluster Installation

CCS Installer drops support for Public clouds (AWS, GKE & Azure) for new cluster installation and upgrades , however, the "existing cluster" mode of installation is still supported. Users can bring a GKE/Azure based kubernetes cluster and install suite admin using the v5.4.0 installer.

CCS v5.4.0 does not support installer images for public clouds. Only OVA and QCOV2 appliances are published.

Security Management

No updates

Suite UI

No updates.

Deprecated

- CCS Installer drops support for upgrades of cluster on public clouds(GKE & Azure)

Documentation

The following documentation changes were implemented in CloudCenter Suite5.4.0:

- Support for New Kubernetes Version 1.19.x

Known Issues

CloudCenter Suite 5.4.0 has the following known issues

- CPSGCORE-4445:Two elasticsearch client pods can be seen post common-framework chart upgrade

```
Step 1: Find replicasets with 0 DESIRED, 0 CURRENT and 0 READY count.

kubectl get replicasets -n cisco| grep "elasticsearch-client"
Step 2: Delete the replicasets which are not in READY state from step 1

kubectl delete replicaset $RS -n cisco
Step 3: (This is only required if the cluster is upgraded from v5.2.4->5.3.1->5.4.0)

If there are still 2 elasticsearch-client replicasets that are both running, please delete the
replicaset with older image which can be listed by:

kubectl describe replicaset $RS -n cisco | grep Image
Delete the older replicaset using Step 2.
```

Resolved Issues

CloudCenter Suite 5.4.0 has the following resolved issues:

- **CSCwb84925:**Upgrade CCP from v8.0.3 to v9.0.1
- **CSCwb84860:** kube-state-metrics could not list resource metrics
- **CSCwb84921**: Updatejdk-8-infosec baseimage and update suite-cryptoservice reference
- **CSCwb84921**: Upgrade node-exporter from v0.15.2 to v1.2.2-cisco7
- **CSCwb85226**: Upgrade prometheus from v2.2.1 to v2.30.2-cisco3
- **CSCwb84926**: Upgrade nginx ingress controller from v0.25.0 tov0.49.3-cisco4
- **CSCwb84955**:CCP v9 k8s upgrades from k8s 1.18.12 to 1.19.x for vsphere
- **CSCwb84952**:CCP v9 k8s upgrades from k8s 1.18.12 to 1.19.x for openstack
- **CSCwb84925**:Update log4j to 2.17.1, alpine to 3.15
- **CSCwb84922**: Upgrade the baseimage of installers.

Suite Admin API

Suite Admin API

Suite Admin 5.4.0 API Calls

Suite Admin 5.4.0 API Calls

- Resource Management Service API Calls 5.4.0
- Product Registry Service API Calls 5.4.0
- Password Service API Calls 5.4.0
- Suite Notification Service API Calls 5.4.0
- Monitor Service API Calls 5.4.0
- Logs Service API Calls 5.4.0
- License Service API Calls 5.4.0
- IDM Service API Calls 5.4.0
- Email Service API Calls 5.4.0
- Authentication Service API Calls 5.4.0

Resource Management Service API Calls 5.4.0

ResourceManagement Service API Calls for Suite Admin 5.4.0

Download the API Swagger file from https://www.cisco.com/content/dam/en/us/td/docs/cloud-systems-management/cloudcenter-suite/Suite-Admin /51_SA_swagger.zip.

suite-res-mgmt_swagger.json

Back to: Suite Admin API

Product Registry Service API Calls 5.4.0

Product Registry Service API Calls for Suite Admin 5.4.0

Download the API Swagger file from https://www.cisco.com/content/dam/en/us/td/docs/cloud-systems-management/cloudcenter-suite/Suite-Admin/51_SA_swagger.zip.

suite-prod-regi...wagger_540.json

Back to: Suite Admin API

Password Service API Calls 5.4.0

Password Service API Calls for Suite Admin 5.4.0

Download the API Swagger file from https://www.cisco.com/content/dam/en/us/td/docs/cloud-systems-management/cloudcenter-suite/Suite-Admin/51_SA_swagger.zip.

suite-password_...wagger_540.json

Back to: Suite Admin API

Suite Notification Service API Calls 5.4.0

Suite NotificationService API Calls for Suite Admin 5.4.0

Download the API Swagger file from https://www.cisco.com/content/dam/en/us/td/docs/cloud-systems-management/cloudcenter-suite/Suite-Admin/51_SA_swagger.zip.

suite-notificati...swagger_540.json

Back to: Suite Admin API

Monitor Service API Calls 5.4.0

Monitor Service API Calls for Suite Admin 5.4.0

Download the API Swagger file from https://www.cisco.com/content/dam/en/us/td/docs/cloud-systems-management/cloudcenter-suite/Suite-Admin /51_SA_swagger.zip.

suite-monitor_swagger_540.json

Back to: Suite Admin API

Logs Service API Calls 5.4.0

Logs Service API Calls for Suite Admin 5.4.0

Download the API Swagger file fromhttps://www.cisco.com/content/dam/en/us/td/docs/cloud-systems-management/cloudcenter-suite/Suite-Admin[/51_SA_swagger.zip](https://www.cisco.com/content/dam/en/us/td/docs/cloud-systems-management/cloudcenter-suite/Suite-Admin/51_SA_swagger.zip).

suite-logs_swagger_540.json

Back to: Suite Admin API

License Service API Calls 5.4.0

License Service API Calls for Suite Admin 5.4.0

Download the API Swagger file from https://www.cisco.com/content/dam/en/us/td/docs/cloud-systems-management/cloudcenter-suite/Suite-Admin/51_SA_swagger.zip.

suite-license_swagger_540.json

Back to: Suite Admin API

IDM Service API Calls 5.4.0

IDM Service API Calls for Suite Admin 5.4.0

Download the API Swagger file from https://www.cisco.com/content/dam/en/us/td/docs/cloud-systems-management/cloudcenter-suite/Suite-Admin /51_SA_swagger.zip.

suite-idm_swagger_540.json

Back to: Suite Admin API

Email Service API Calls 5.4.0

Email Service API Calls for Suite Admin 5.4.0

Download the API Swagger file from https://www.cisco.com/content/dam/en/us/td/docs/cloud-systems-management/cloudcenter-suite/Suite-Admin/51_SA_swagger.zip.

suite-email_swagger_540.json

Back to: Suite Admin API

Authentication Service API Calls 5.4.0

AuthenticationService API Calls for Suite Admin 5.4.0

Download the API Swagger file from https://www.cisco.com/content/dam/en/us/td/docs/cloud-systems-management/cloudcenter-suite/Suite-Admin /51_SA_swagger.zip.

suite-auth_swagger_540.json

Back to: Suite Admin 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

API Permissions

API Permissions Allowed 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 IDM 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: • Module Lifecycle Management • Manage Clusters
SUITE_TENANT_AD MIN	The tenant administrator set up as part of the root tenant configuration described in Manage Tenants. This user can perform the following tasks: • Manage sub-tenants • Create, update, and delete sub-tenant users (including createTenantWithAdmin 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	A SUITE_ADMIN can promote any SUITE_USER to the SuiteAdministrator group as described in Create and Assign Groups. This user can perform the following tasks: • Manage users and groups • Create, update, delete users and groups • Assign roles to users and groups • Manage passwords for users
SUITE_OUTOFBOX_ USER	A SUITE_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_PAS SWORD	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: • 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](#)

CSRF Token Protection

CSRF Token Protection

-

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

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 *CloudCenter Resource*
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

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 *also* 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

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
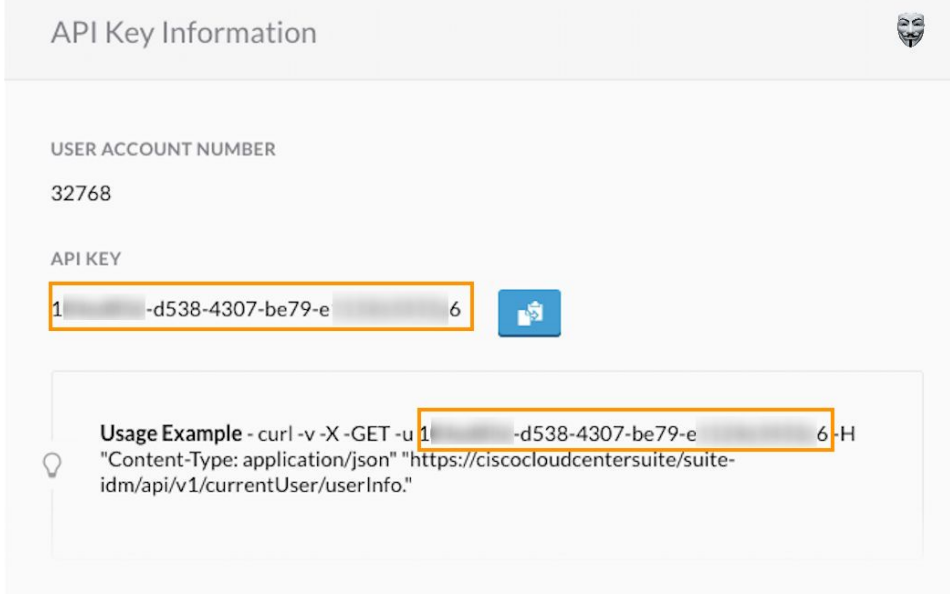
Overview

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
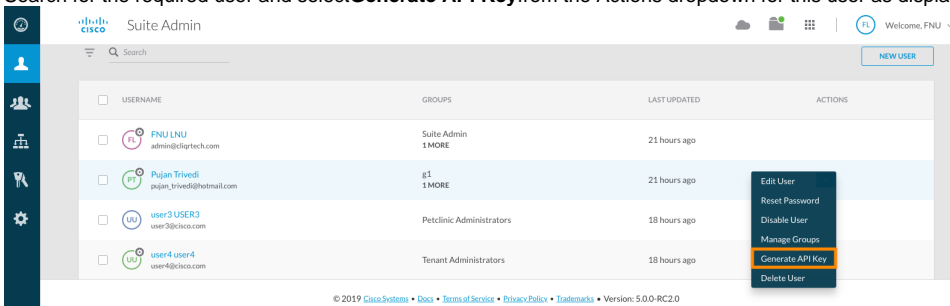
API KEY

1 -d538-4307-be79-e 6

Usage Example - curl -v -X -GET -u 1 -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.

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

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
- APIaccess 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 theusername
- **BED74F4D9BFE0DA0**is the APIaccessKey

Yourtenant administratorcan 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 Overview

CloudCenter Suite API Overview

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 theCloudCenter 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 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 inUnix timeto 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 Suitetask 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:

- 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:

- **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). ✓ if the page does not have more than 10 elements, then only those 10 elements are displayed.
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 = 20records
    - 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
  • **Description**: The page number that the client wants to fetch. Page numbers start with 0 (default).
  • **Type**: Integer

totalElements
  • **Description**: The number resources that an API call returns
  • **Type**: Long

totalPages
  • **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
  • **Description**: Unique URL to access this resource.
  • **Type**:String

size (see above)

pageNumber
- **Description**: The page number that the client wants to fetch. Page numbers start with 0 (default).
- **Type**: Integer

totalPages
- **Description**: The number of pages in a response
- **Type**: Integer

jobs
- **Description**: Array of JSON objects that use **jobs** as the key.
- **Type**: Array of JSON objects

previousPage
- **Description**: A resource link to the previous page.
- **Type**: URI as a string

nextPage
- **Description**: A resource link to the following page.
- **Type**: URI as a string

lastPage
- **Description**: A resource link to the last page.
- **Type**: URI as a string

Sorting

- **v1 APIs**: All list APIs support sorting by default and use the query-string parameters to provide sorted results with a comma-separated set of property names.

    - Sorting Order:

        - Ascending order: Default when you specify the property.
        - Descending order: Append a dash ⛔ to the property.
    - Example:

        - **sort=id,name**: Sort by ID property in ascending order and then sort by name property in ascending order.
        - **sort=id,name-,description**: Sort by ID property in ascending order, then sort by name property in descending order, and finally sort by description in ascending order.
    - Property name validation: Property names in sort parameters are validated. For example, APIs that return a list of users can sort only on properties exposed by the user object as sortable.
    - The following example displays the use of sorting and pagination attributes in the same API request.

```
curl -k -X GET -H "Accept: application/json" -u cliqradmin:D3DD6F7874E6B26B "https://test.cliqr.com/v1/users?
detail=true&page=0&size=30&sort=firstName

> GET /v1/users?detail=true&page=0&size=30&sort=firstName HTTP/1.1
> Authorization: Basic Y2xpcXJhZG1pbjpEM0RENkY3ODc0RTZCMjZC
> User-Agent: curl/7.37.1
> Host: test.cliqr.com
> Accept: application/json
>
< HTTP/1.1 200 OK
```

- **v2 APIs**: Requires the *sort* attributes for any request.

    sort
    - **Description**: Sorts API responses based on the format specified.
    - **Type**: String

        - Sorting order:

            - Ascending order = ASC
            - Descending order = DESC
        - Default: Sort criteria is based on *startTime* and DESC order.
        - Format: sort=[*attribute*,*order*]
        - Example: [endTime,ASC]
        - Sorting attributes:

            id
            - **Description**: Unique, system-generated identifier for this *resource*.
            - **Type**: String

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 *deployment Entity.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 the *searchTypes* table below.
    - searchTypes

searchType	Format
eq	==
ne	!=
el	LIKE *pattern%*
fl	LIKE *%pattern*

eln	NOT LIKE *pattern*%
fln	NOT LIKE %*pattern*
fle	LIKE %*pattern*%"
gt	> *searchValue*
lt	< *searchValue*
ge	>= *searchValue*
le	<= *searchValue*
gtlt	>*searchValue* &&*searchValue*
gtelt	>=*searchValue* && <*searchValue*
gtlte	>*searchValue* && <=*searchValue*
gtelte	>=*searchValue* && <=*searchValue*
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 Create*resource*API 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 Y2xpcXJhZGlpbjpEM0RENkY3ODc0RTZCMjZC
> 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 requiredPermission Controllevel to access any*resource,*you receive the HTTP 403 status error mentioned in theHTTP Status Codessection.

Back to:

- Suite Admin API
- Workload Manager API
- Action Orchestrator API
- Cost Optimizer API

Troubleshoot Suite Admin

Troubleshoot Suite Admin

Overview

This sectionlists some of the issues that you may encounter and suggests workarounds.

Download Log File

SeeMonitor Modules > *Download Logs.*

Kibana UI (Log Search)

SeeMonitor Modules > *View Logs in Kibana.*

Grafana dashboards Alerts

SeeMonitor Modules>*Configure Grafana Dashboard Alert*.

Module Failure during Installation or Upgrade
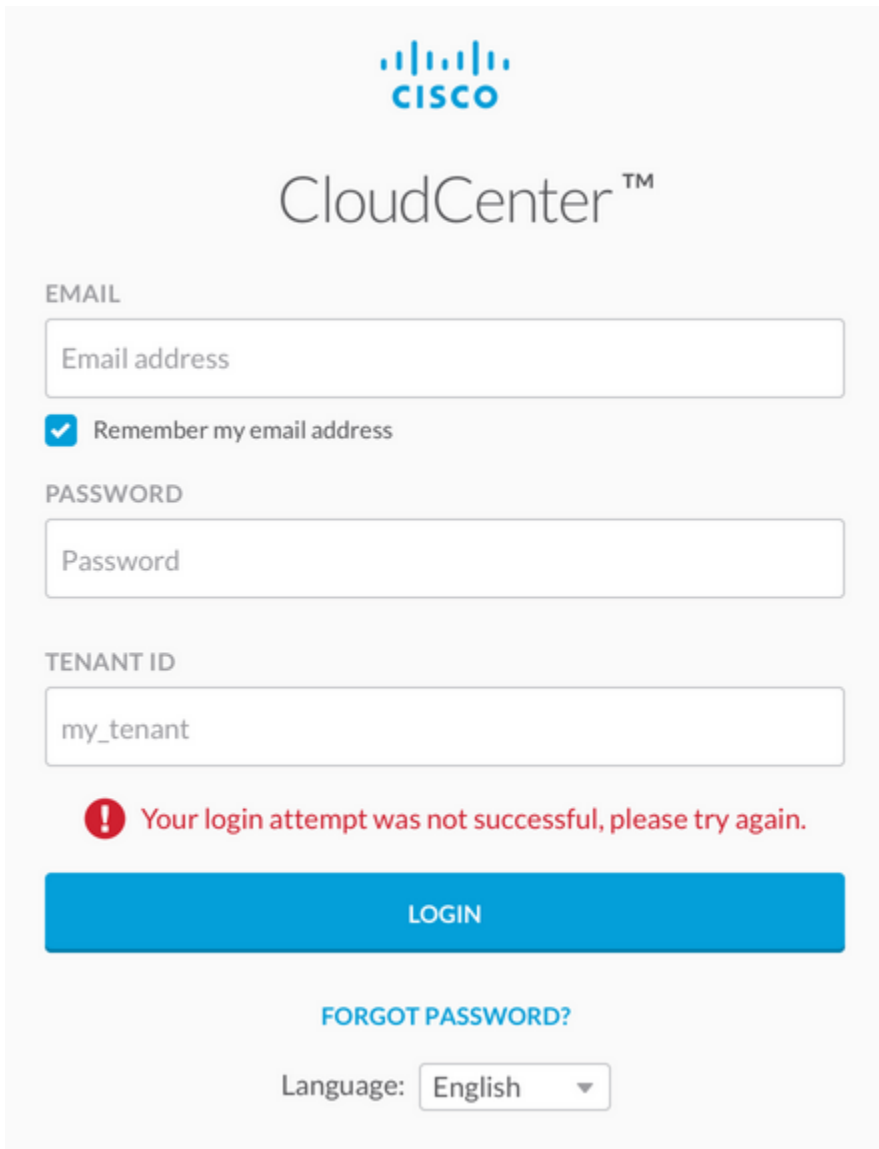
When installing the CloudCenter Suite for aOpenStack Installation or aVMware vSphere Installation, you have the option to configureNTP server details. If you do not provide the NTP details, workers and nodes may not have their time synchronized with each other. This can potentially cause modules to fail during an installation or upgrade as displayed in the following screenshot.
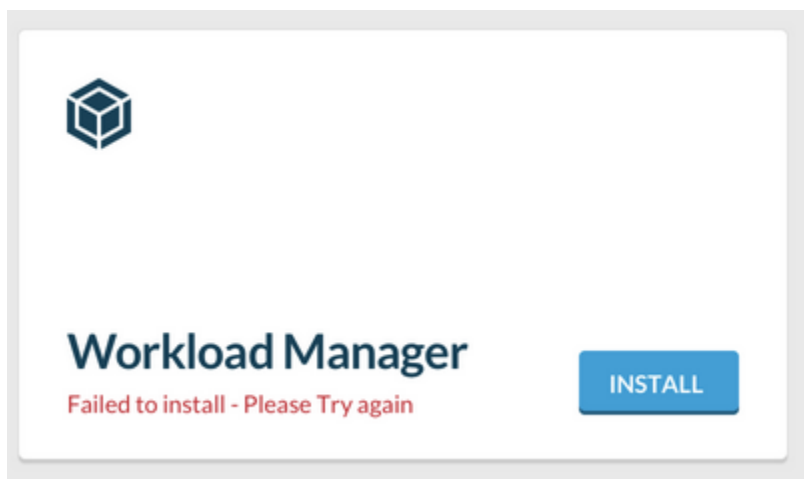
To workaround this issue, be sure to synchronize the server time for all instances running the CloudCenter Suite.

Log in Failure Due to Session Timeout

If your session has timed out during an idle session, you may sometimes see the message displayed in the following screenshot even if you have entered the right credentials. Try logging in again.

If you are unable to login due to a wrong password as visible in the following screenshot, contact your suite administrator to reset the password (see Create and Manage Users > User Actions for details).
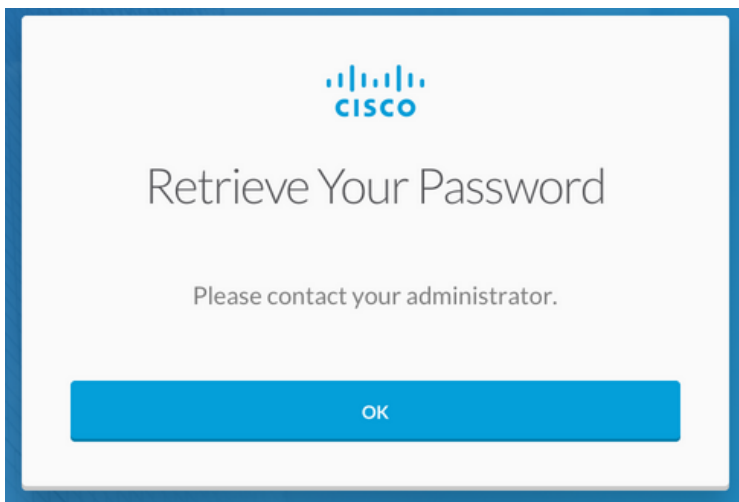
Blank Screen when Logging into Suite Admin

A user who only belong to one group is abandoned if the group was only specific to one module and if that module was uninstalled. In this case, the abandoned user must follow up with one of the CloudCenter Suiteadministrators based on their enterprise policies. If a user does not have any active roles, this user may see a blank screen on log in.

SSO Setup Resulting in Login Failure

If you log in as root admin, configure SSO, and was subsequently timed out, you may not be able to log back in. This is because the ADFS user may not have the roles mapped and will not be able to access any modules. This user may not be able tologin by using the direct URL (ui/auth/login).

To address this issue, be sure tocomplete theSSO Setup, add the ADFS user to the Suite Admin Group *before* any session timeout.

Deployment Repo Uses the Public Repo Even if Kubernetes was Restarted

If you initially use the public repository to install the CloudCenter Suite, the repo for deployments and other activities may continue to point to the public repository. If so, your deployments may continue to reference the public repo even for cases where the Kubernetes nodes were restarted.

After an offline repo is registered with the CloudCenter Suite, users may expect Deployments to **automatically and immediately** pickup images from the offline repo. This is not the natural behavior.

During product installation/upgrade events, the repository settings are set to Helm (the package manager for Kubernetes). Consequently, offline repository settings are only registered after the next upgrade or new product installation event.

To workaround this natural behavior, you can opt to start a new cluster with the offline repository during the first event to ensure that your environment continues to use this offline repository.

PVC Cleanup

When you uninstall the Workload Manageror Cost Optimizer modules in the Suite Admin, theKubernetes Persistent Volume Claims (PVCs)are not deletedthey are retainedas is for the Suite Administrator to take appropriate steps to backup or manually delete the PVC. The secrets for the Workload Managerand the Cost Optimizerare not deleted when you uninstall the product. To work around this issue, the Suite Administrator must clean up their instances using one of the following suggestions.

- Backup PVC: Take a snapshot of the volume backing up the PVC or just the data contained within. Refer to the Kubernetes Documentation for additional details.
- Delete PVC: Manually delete the PVCs by running the following command:

```
kubectl delete pvc -n <namespace>
```

Admin Menu

Admin Menu

- Currency Conversion
- SSO Setup
- Log Archive
- Offline Repository Configuration
- Base URL Configuration
- Email Settings
- Proxy Settings
- Backup

Currency Conversion

CurrencyConversion

- [Overview](#)
- [Process](#)

Overview

The CloudCenter Suite provides support for the following currencies to analyze cost reports, billing units, or savings functions used in the Workload Manager and Cost Optimizer modules:

- AED = United Arab Emirates Dirham
- AUD = Australian Dollar
- BRL = Brazilian Real
- CAD = Canadian Dollar
- CHF = Swiss Franc
- CNY = Chinese Yuan Renminbi
- EUR = European Euro
- GBP = British Pound
- HKD = Hong Kong Dollar
- IDR = Indonesian Rupiah
- INR = Indian Rupee
- JPY = Japanese Yen
- KWD = Kuwaiti Dinar
- MXN = Mexican Peso
- RUB = Russian Ruble
- SEK = Swedish Krona
- SGD = Singapore Dollar
- SAR = Saudi Riyal
- TRY = Turkish Lira
- USD = US Dollar (default)

> ⓘ All User input fields accept and display values in USD.

Requirements

Once you select the currency option of choice, you must also enter the conversion factor for this currency.

> ⚠ Changing from the default USD currency to any other currency in this list may impact billing for environments as currency information is used by and not limited to the multiple features in the CloudCenter Suite.

Process

To configure the conversion rate to the selected currency, follow this procedure.

1. Navigate to the Suite Admin Dashboard>**Admin**.
2. Click **Currency** in the left tree pane to view the Currency page.
3. Select the currency from the dropdown list.
4. Assign the conversion rate for this currency for 1 USD.
5. Click **Save** to register your changes.

SSO Setup

Single Sign On (SSO) Setup

Overview

Some enterprises have their own Active Directory (AD) or other similar setup and prefer to use those credentials to login into the external applications and platforms. The Cloud Center Suite does not support direct AD authentication, and instead supports integration using a Single Sign On (SSO) setup between the Suite Admin as a Service Provider (SP) and a customer's Identity Provider (IdP) such as ADFS.

Requirements

You should have already configured the Base URL Configuration for the root tenant in order to use this functionality. This URL is used to download the service provider metadata. You can retrieve the data by clicking on the URL and accessing the metadata for the IdP attributes.

The Cloud Center Suite only supports AD through a SSO IdP that supports SAML 2.0 protocol (for example, Ping Identity, ADFS, Shibboleth, and so forth).

Each tenant can point to its own SSO:

- Tenant Admins can configure each tenant to have a dedicated alias hostname and use an external IdP to authenticate its users.
- Each tenant and user has a **Tenant Login ID** to associate with an external organization and user.

Handling Deleted Users

If you delete a user from the IdP database, the deleted user cannot log into the Cloud Center Suite, but any configuration and associated dependencies continue to remain in the Suite Admin.

High-Level Process

To configure SSO, perform this procedure.

1. Navigate to the Suite Admin Dashboard>**Admin**.
2. Click **Single Sign On** in the left tree pane to display the Single Sign On page.
3. Toggle the switch to enable (disabled by default) users to use Single Logout.

   > ⓘ If you do not enable single log out, be aware that users cannot logout until the token expires.

4. Configure the IdP URL for the Metadata in the **IdP Settings** section using HTTP or HTTPS protocol.
5. Toggle the switch if you prefer users to have a **Single Logout** from the IdP to log out of each session.

   > ⓘ SSO Sessions in different browsers are independent of each other. Enabling the **Single Logout** switch does not terminate all sessions.
   >
   > By terminating the current SSO or IdP session, you are only terminating that session on that browser. The remaining sessions remain active until their JWT token expires or the user explicitly logs out of each session.

6. Provide the IdP mapping attributes to connect the Suite Admin properties to the IdP properties.
7. Click **Save** to save your changes.

ADFS SAML SSO Sample Integration and Setup

This flow provides the required information to setup ADFS in *Windows* 2016 for a vSphere environment.

⚠

⚠️ This is a sample setup flow and you can adapt the information to your environment based on your requirements.

Setup ADFS in Your Environment

To setup ADFS in *Windows* 2016 for a vSphere environment, follow these steps.

1. Create a new Windows 2016 VM in your vSphere environment.

   ✅ You can clone a new VM using the base_windows2016 template from *CliqrTemplate*.

   To use this template, you must login using administrator credentials contact CloudCenter Suite Support to obtain the administrator credentials.

2. Login into the administrator account using the default password.
3. Configure the VM Network settings.

   a. Access **Control panel** > **Network and Internet (View network status and tasks)** > **Change adapter settings** and right click **Ethernet0**.
   b. Select **Properties**.
   c. Select **Internet Protocol Version 4** > **Properties** as reflected in the following screenshot.
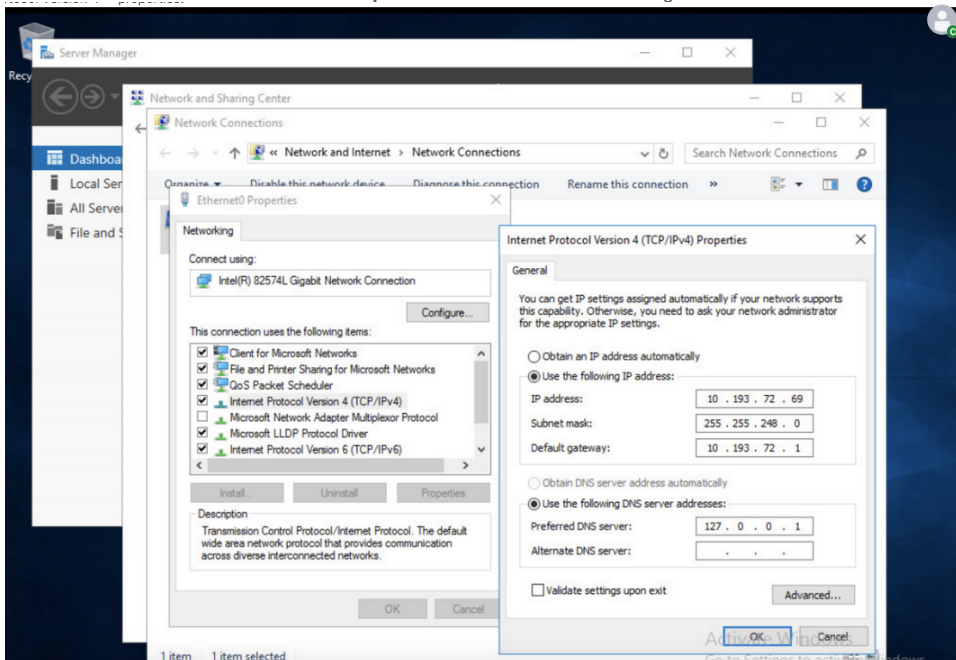
   d. Assign the static IP address, default gateway, subnet mask, and DNS.

4. Change the hostname.

   a. Access **Server Manager** > **Local Server**.
   b. Update the computer/host name.
   c. Enable **Remote Desktop** and turn off **IE Enhanced Security**.
   d. Save your changes and restart the VM for the changes to apply.

5. Synchronize the System Date and Time.
6. Install Active Directory Domain Services.

   a. Access **Server Manager** > **Manage** > **Add Roles and Features** as reflected in the following screenshot.
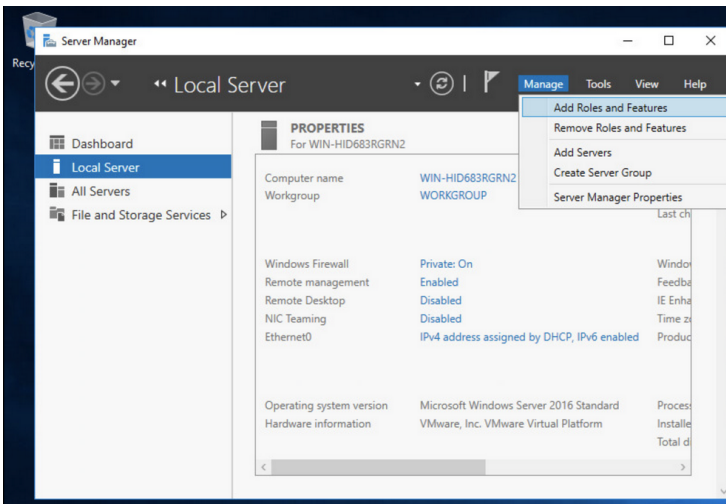
b. Select the type of Installation as reflected in the following screenshot.
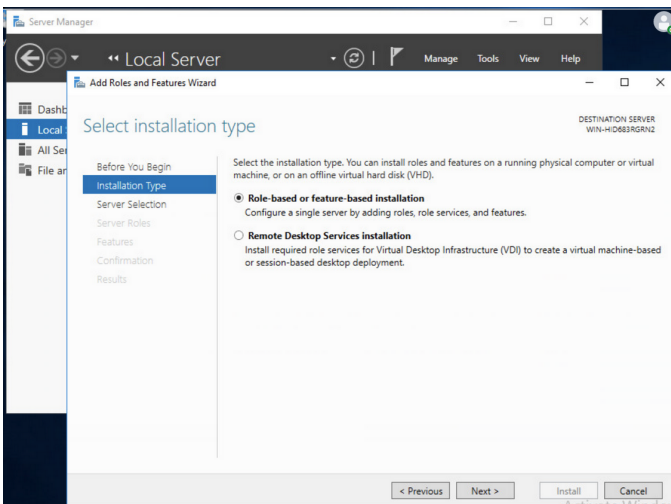
c. Select the destination server as reflected in the following screenshot.
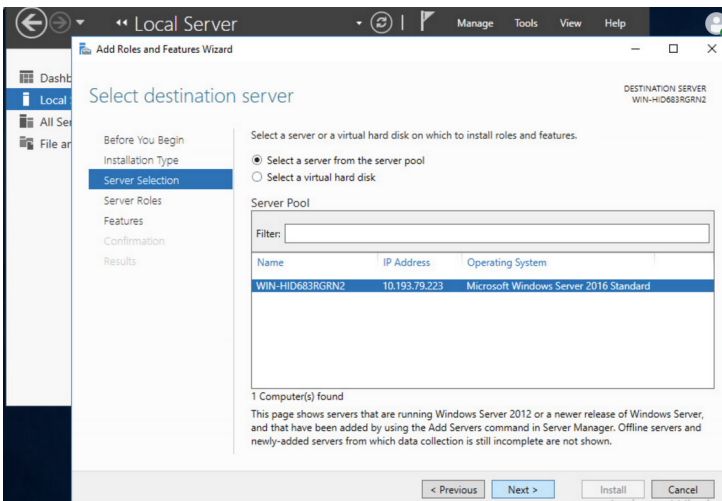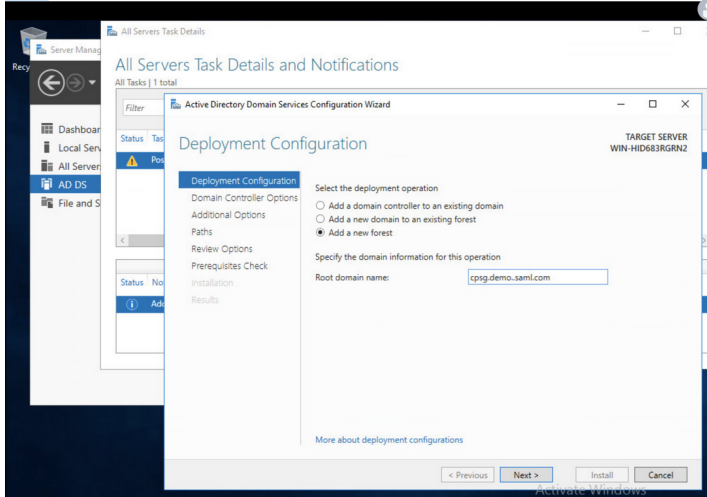

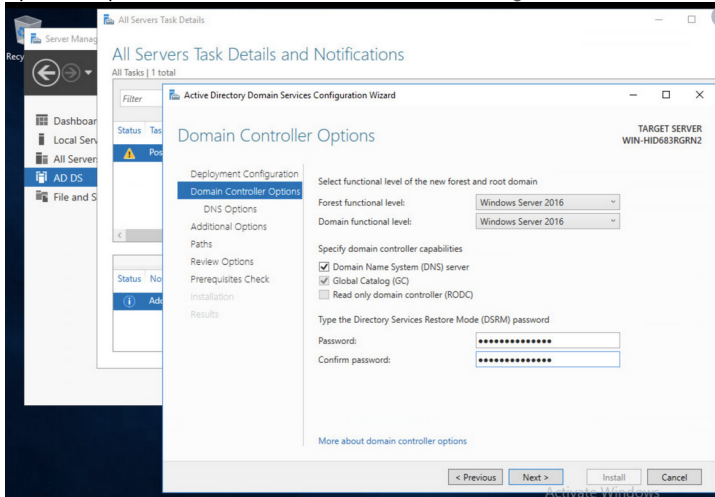d. Select **Active Directory Domain Services** asreflected in the following screenshot.
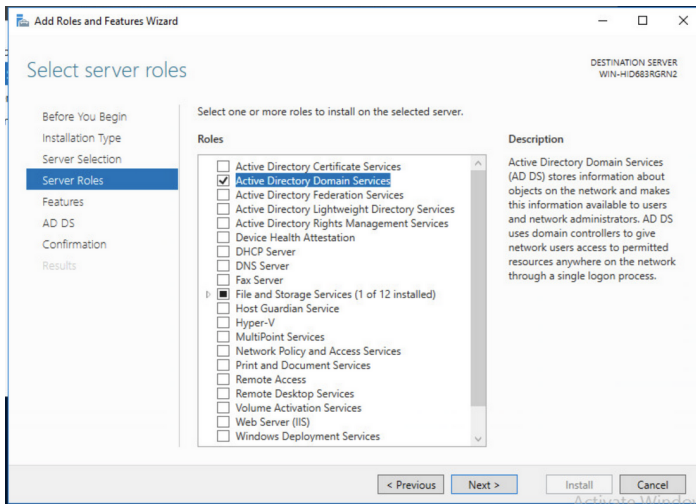
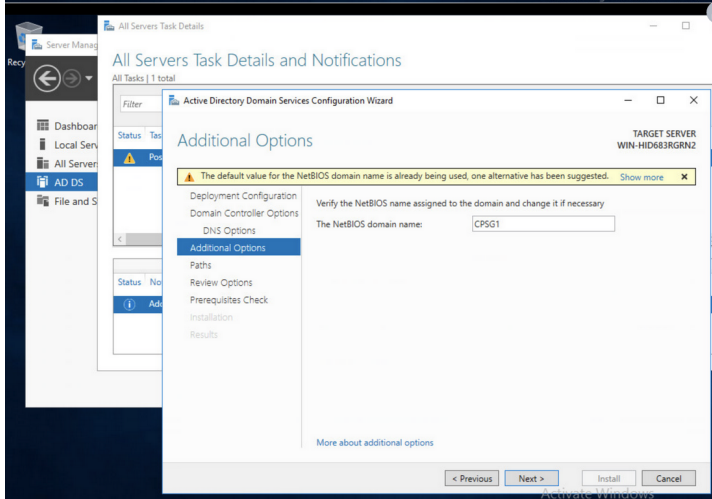   e. Follow the default configuration steps.

7. Configure the AD DS.

    a. Create new forest and provide a **Root domain name** as reflected in the following screenshot.

    b. Update the password for DSRM as reflected in the following screenshot.

c. Complete the remaining fields using the default settings asreflected in the following screenshot.

d. Save your configuration and restart the VM.

8. Install a DNS Server.

       i. Access **Server Manager** > **Manage** > **Add Roles and Features**> **DNS Install**.
      ii. Complete the configuration using the default values for the remaining fields.

9. Install the Web Server (IIS Manager)

a. Access**Server Manager**>**Manage**>**Add Roles and Features**>**IIS Manager Install**.
b. Complete the configuration using the default values for the remaining fields.
c. From the Windows **Start** menu, go to **Run** (or press **Window + R** keys, for MACs press **Command + R** keys) to open the Run window.
d. Type **inetmgr**, and click **OK**. This will open the IIS Manager asreflected in the following screenshot.
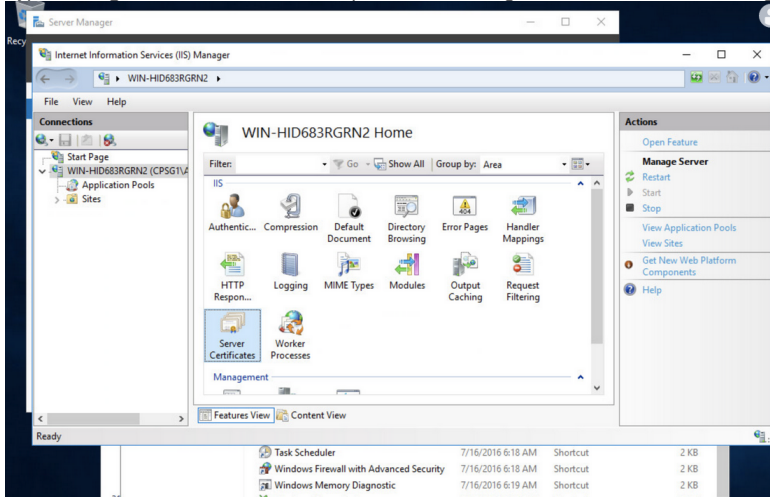
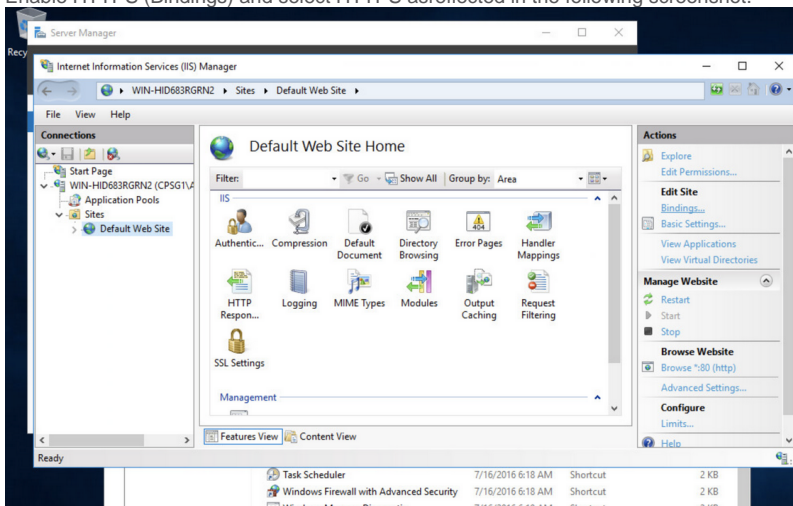
e. Click the **IIS server name** (below the **Start Page** option in the left pane) asreflected in the following screenshot.
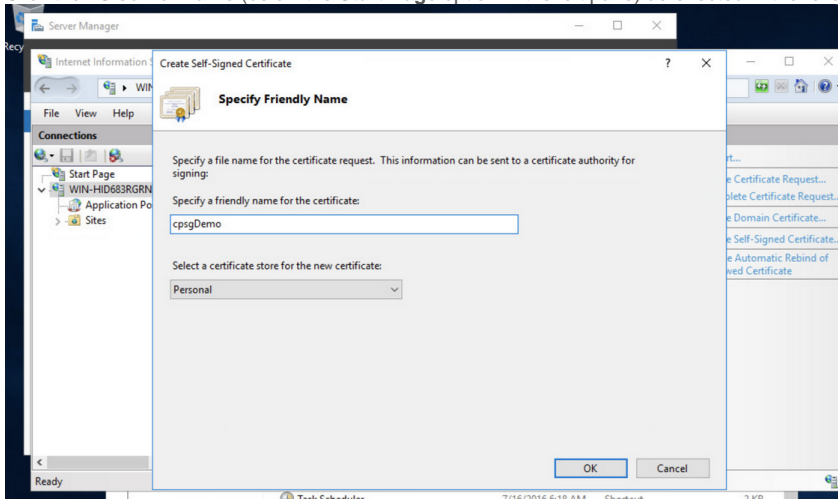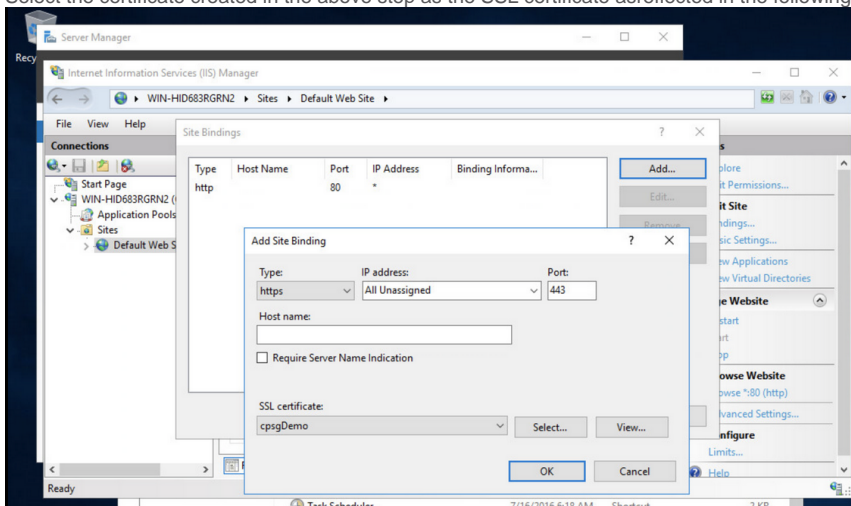
f. Create Self signed certificate by accessing **Create server certificates ▸ New self-signed** asreflected in the following screenshot.
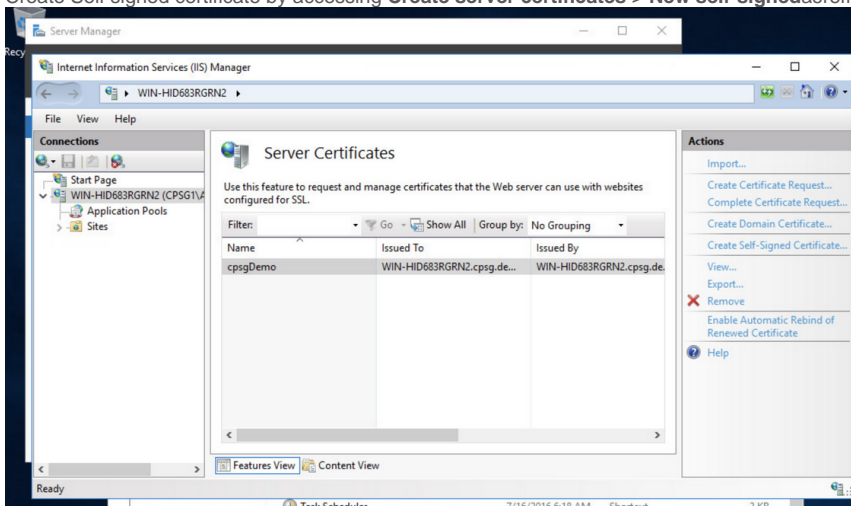
g. Enable HTTPS (Bindings) and select HTTPS asreflected in the following screenshot.

h. Select the certificate created in the above step as the SSL certificate asreflected in the following screenshot.

i. Click **OK** and close the window.

10. Install ADFS (connect ADFS to ADDS).

a. Access**Server Manager**>**Manage**>**Add Roles and Features**>**ADDS Install**asreflected in the following screenshot.
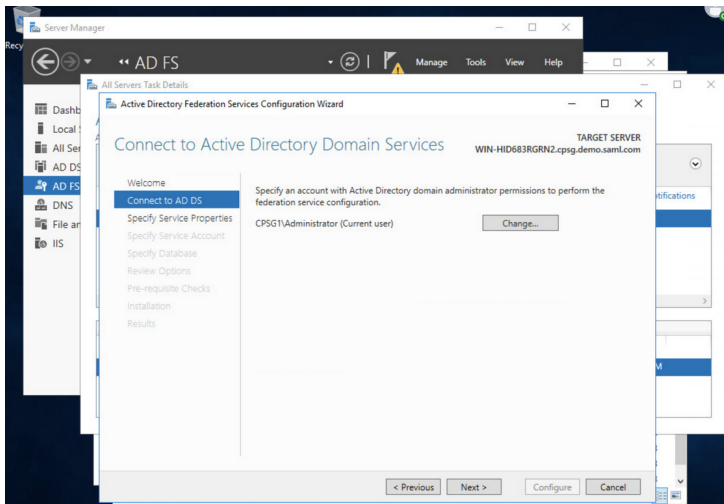
b. Select Create the first federation server.
   i. Select the SSL Cert from the drop down and provide the ADFS display name (any) asreflected in the following screenshot.
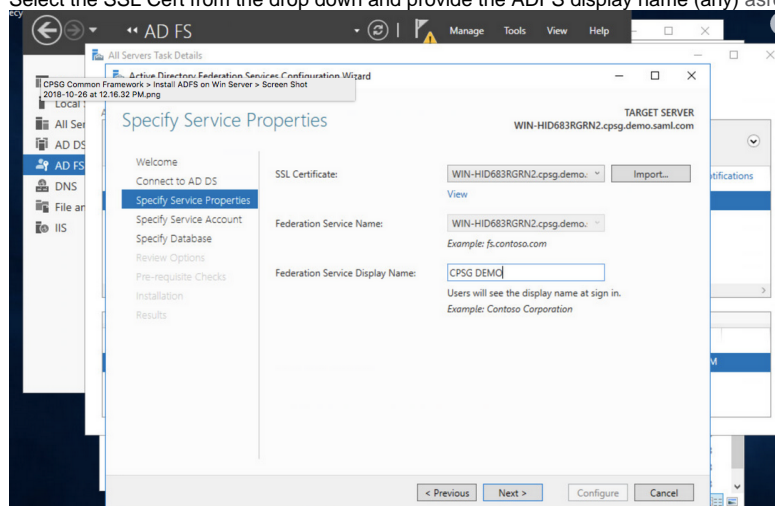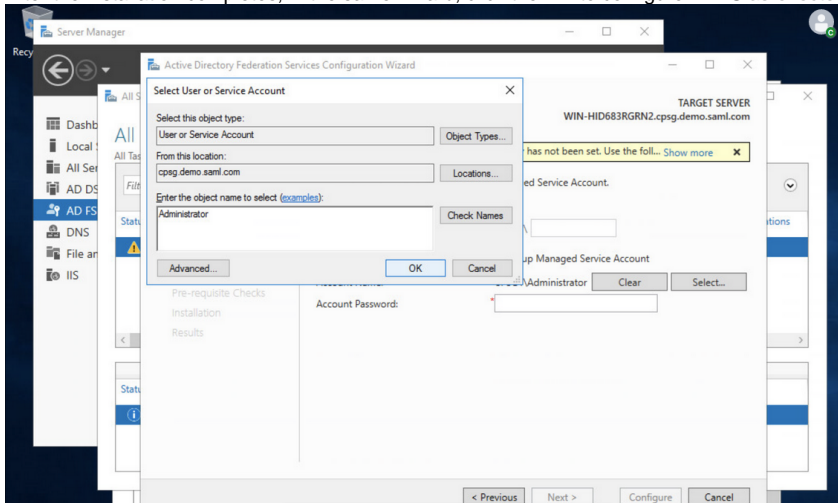

   ii. Select theUse an existing domain user account...button asreflected in the following screenshot.
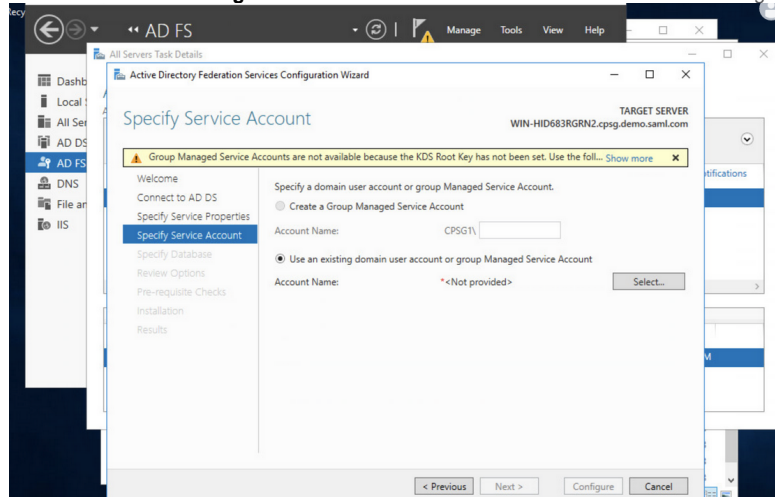
   iii. Complete the installationusing the default values for the remaining fields.

c. After the installation completes, in the same wizard, click the link to configure ADFS asreflected in the following screenshot.

11. Enable IpdInitiatedSingleSignOn:

    a. Access PowerShell
    b. Enable IPD initiated single sign-on and verify using the following commands.

```
# Set-AdfsProperties -EnableIdPInitiatedSignOnPage $true
# Get-AdfsProperties
```

12. Verify the AD FS installation:
    a. Check if you can download the metadata using the following URL format.

```
https://<IP_Address>/FederationMetadata/2007-06/FederationMetadata.xml
```

    b. Check if you canaccess the Single Sign On (SSO) page using the following URL format.

```
https://<IP_Address>/adfs/ls/IdpInitiatedSignon.aspx
```

You have now setup ADFS in *Windows* 2016 for a vSphere environment.

Establish a Third-Party Trust for SSO

You must establish a trust between the service provider and ADFS to ensure SSO. To perform this task, add the Suite Admin to the third-party trust using its metadata file by following these steps.

⚠️ **For ADFS to authenticate, the Base URL must match the IP address and port number in the metadata file.**

When you configure the Suite Admin to Enable SSO, enter the IP address and port number of your Suite Admin in the Base URL Configuration.

1. Access ADFS and right-click **Relying Party Trusts** as reflected in the following screenshot
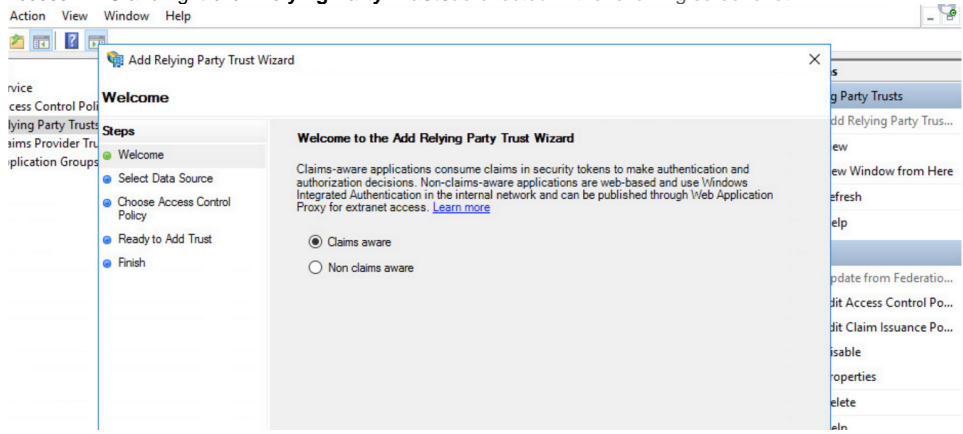
2. Select the **Add Relying Party Trust...** option as reflected in the following screenshot.
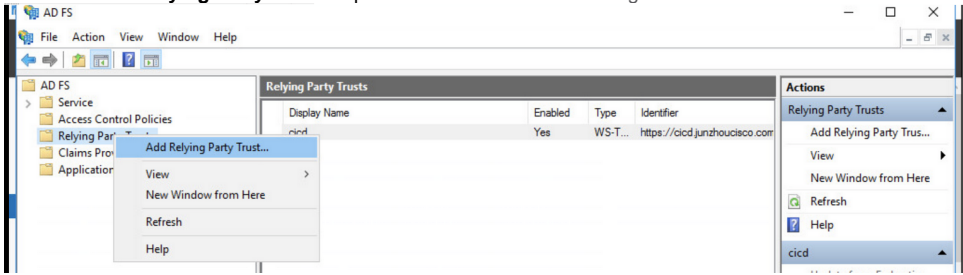
3. Download the Suite Admin's metadata file using the following URL and save it on the local disk of your Windows server.

> ✅ The *tenant_host_name* and *port_number* are the defined in tenant's Base URL Configuration.
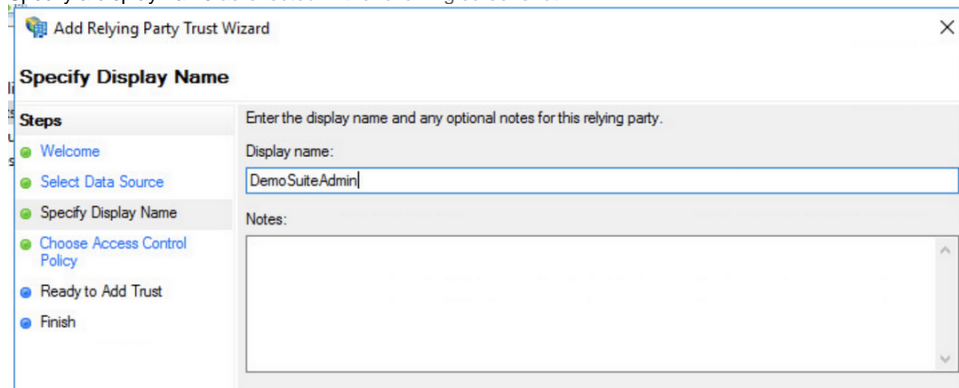
```
https://<tenant_host_name>:<port_number>/suite-saml/saml/metadata
```

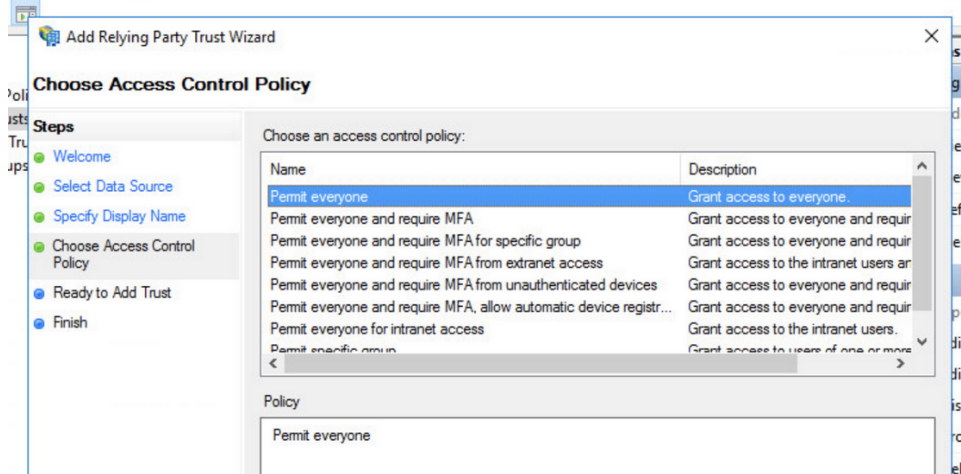4. Upload the metadata file to the Relying Party Trust by following these steps.
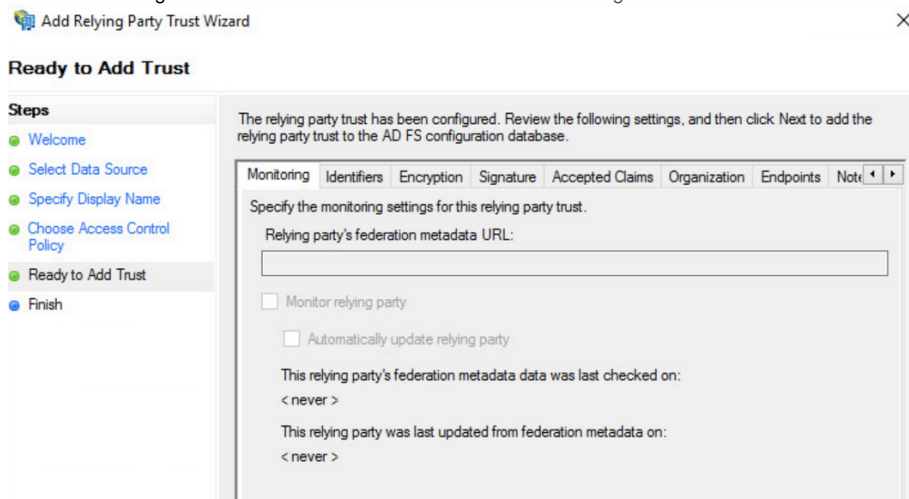   a. Add Relying Party Trusts as reflected in the following screenshot.
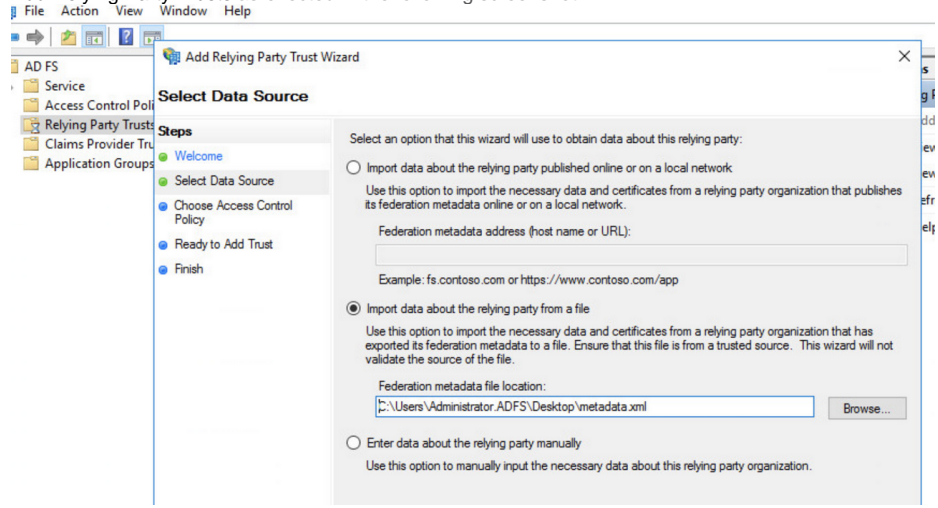
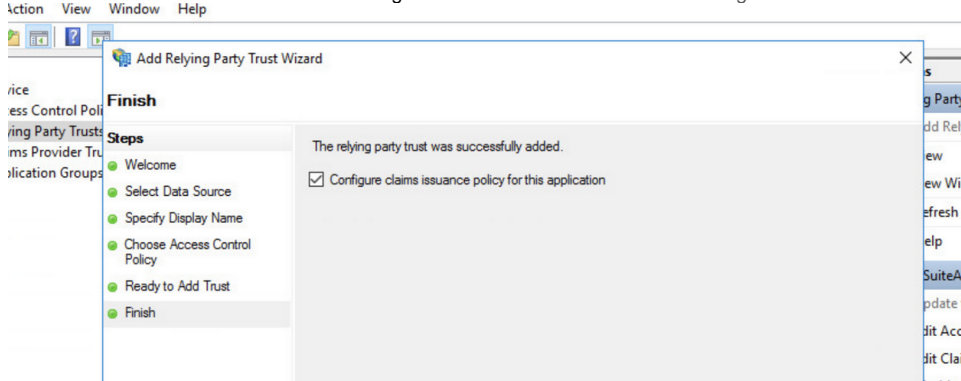b. Specify a display name asreflected in the following screenshot.

c. Select an access control policy asreflected in the following screenshot.

d. Review the configuration and add the trust asreflected in the following screenshot.

e. The trust addition is reflected in the following screenshot asreflected in the following screenshot.

You have now established a trust between the service provider and ADFS.

Adding Claims

To setup claim rules (**LDAP and Transform rules**) so you can transform the IdP properties to suite properties and vice versa, follow this procedure.

1. Create rule 1: Send LDAP attributes as claims When you use the **Send LDAP Attributes as Claims** rule template, you can select attributes from an LDAP attribute store, such as Active Directory or ADDS to send their values as claims to the relying party. This rule essentially maps specific LDAP attributes from an attribute store that you define to a set of outgoing claims that can be used for authorization.

   a. Edit the claim issuance policy (displayed in the following screenshot).
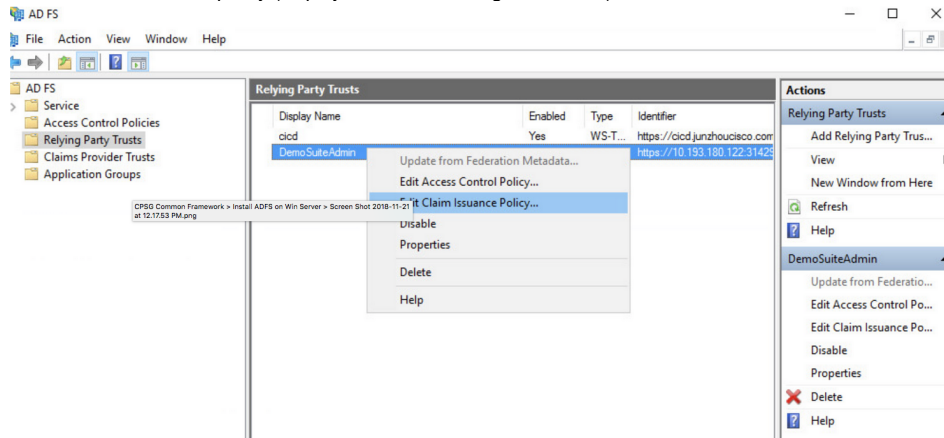
   b. Choose the rule type (displayed in the following screenshot).
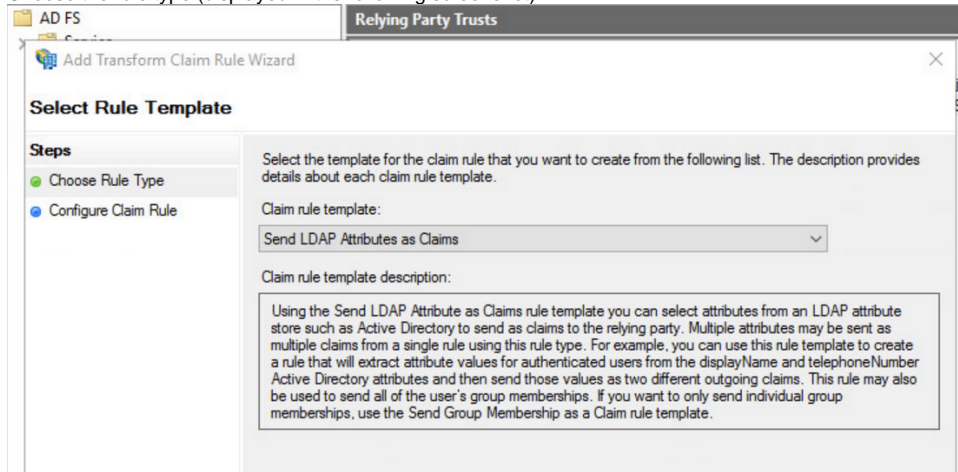
   c. Edit the rule (displayed in the following screenshot).

2. Create Rule 2:Transform an Incoming Claim By using the**Transform an Incoming Claim**rule template in ADFS, you can select an incoming claim, change its claim type, and optionally change its claim value.

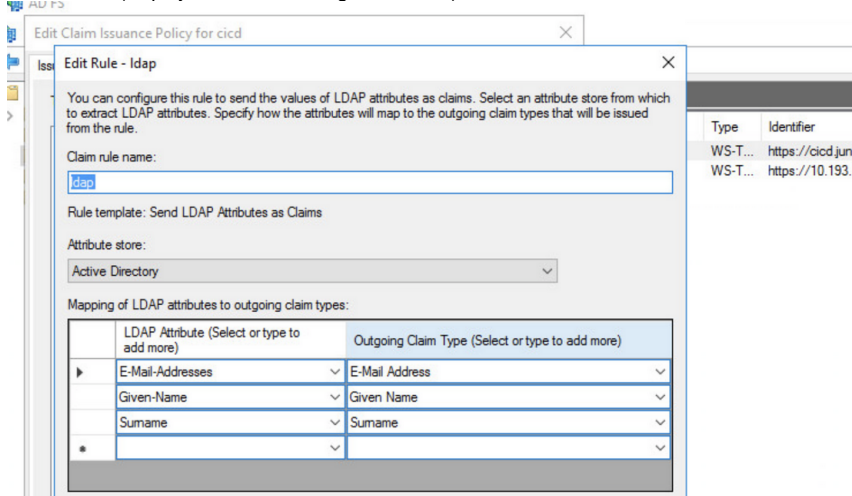a. Edit the claim issuance policy (displayed in the following screenshot).
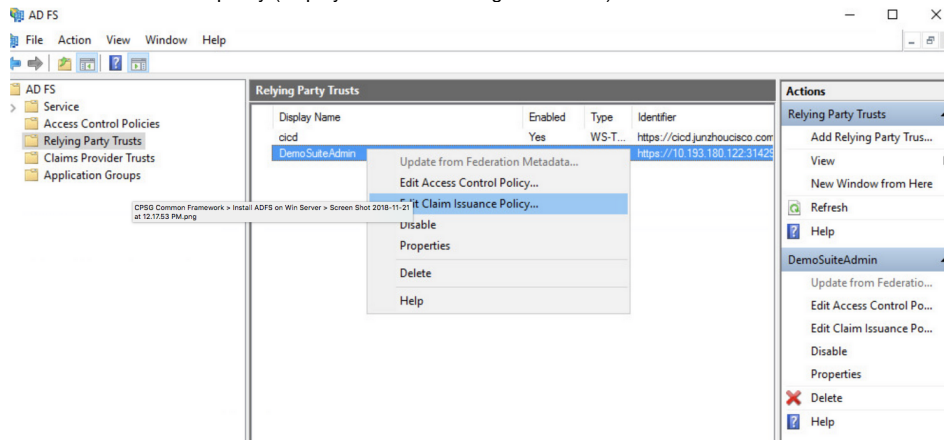
b. Specify the database (displayed in the following screenshot).
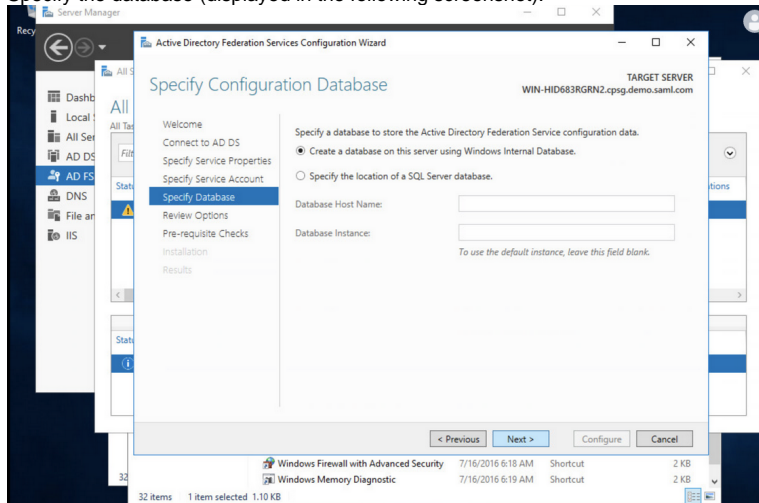
c. Edit the rule (displayed in the following screenshot).
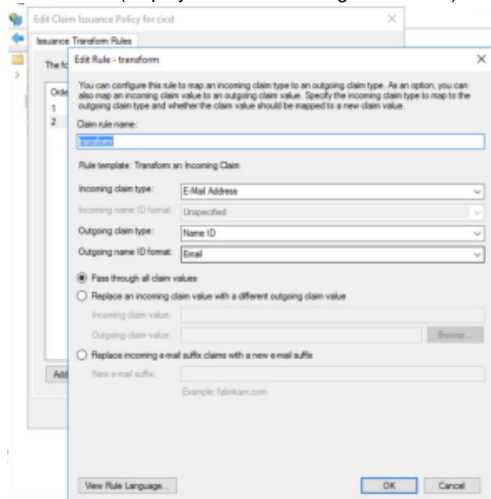
d. Make note of the following items so you can use the same information in the Suite AdminSSO Configuration page.

   i. Access the claims sent to the relying party (displayed in the following screenshot).

Edit Claim Issuance Policy for AZ894CCSQASSOSuiteAdmin

Issuance Transform Rules

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims
1	LDA	E-Mail Address,Given Na...
2	TransforIncoming	Name ID

Add Rule...   Edit Rule...   Remove Rule...

OK   Cancel   Apply
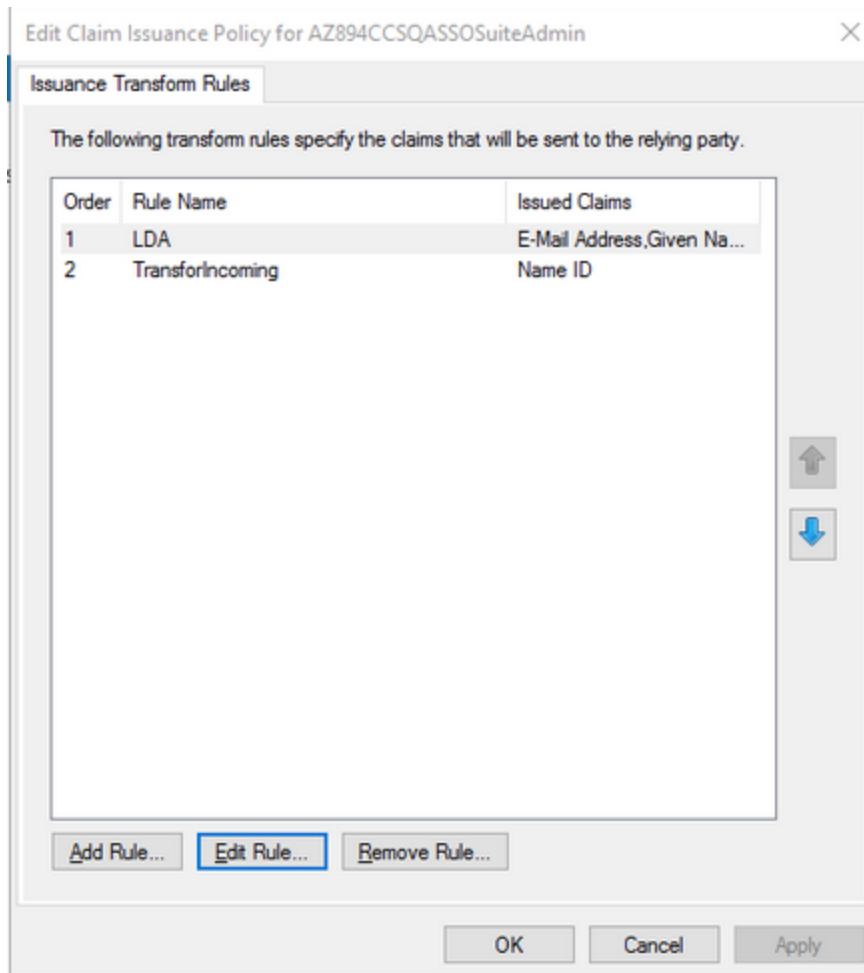
ii. LDAP attribute mapping to outgoing claim types (displayed in the following screenshot).

Edit Rule - LDA

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

LDA

Rule template: Send LDAP Attributes as Claims

Attribute store:

Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	E-Mail-Addresses	E-Mail Address
	Given-Name	Given Name
	Surname	Surname
	Company	Group
*		

View Rule Language...   OK   Cancel

iii. AD paths in exactly as listed in the Claim rule language (displayed in the following screenshot).

Edit Rule - LDA

You can use the following claim rule language to build a custom rule. To do this, copy the text below, create a new custom rule using the Send Claims Using a Custom Rule template, and then paste the text into the Custom Rule text box on the Configure Rule Template page in the Add Rule Wizard.

Claim rule language:

```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windows
accountname", Issuer == "AD AUTHORITY"]
 => issue(store = "Active Directory", types =
("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd
ress",
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
",
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname",
"http://schemas.xmlsoap.org/claims/Group"), query =
";mail,givenName,sn,company;{0}", param = c.Value);
```

OK

You have now setup claim rules totransform the IdP properties to suite properties and vice versa.

Update the Local host to Resolve ADFS and Tenant Hostname

To make domain name of ADFS to be resolvable, add it to /etc/hosts file.

```
# sudo vi /etc/hosts
<IP_address_adfs> win-qa-adfs.cpsg.qa.saml.com
<Kubernetes_IP_address> <tenant_host_name>
```

Creating a New User in ADDS

✅ The system time for the ADFS server and the Suite Adminsa server must be synchronized before authentication.

If the time difference between these two systems are different, then the authentication might fail.

To create a new user in ADDS, follow this procedure.

1. From the Server Manager, go to **Active Directory Users and Computers** (displayed in the following screenshot).
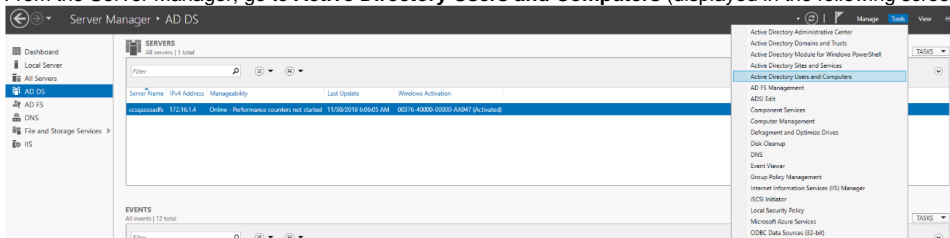
2. Create a new user (displayed in the following screenshot).
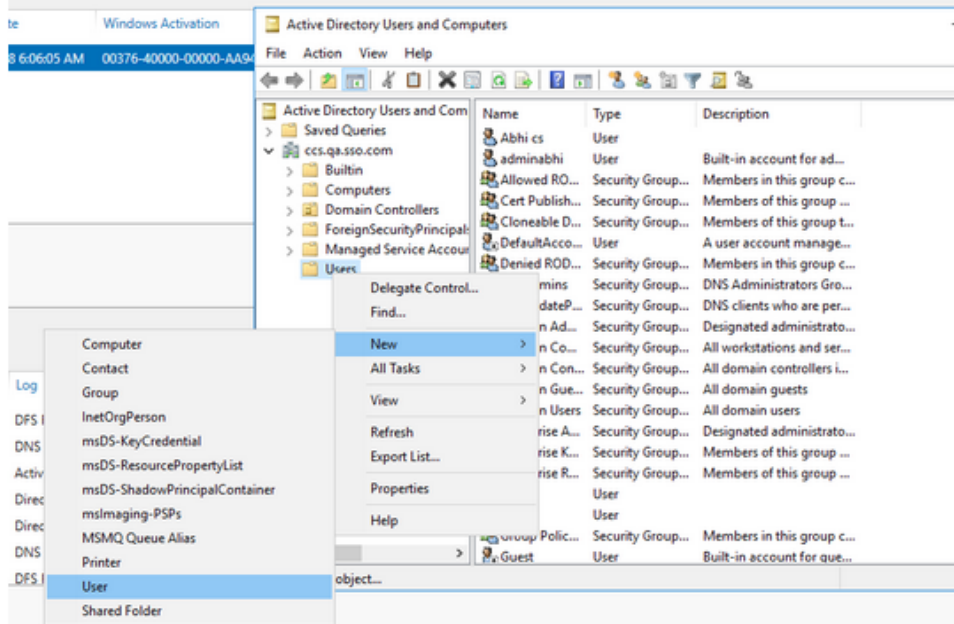
3. Enter the following details:
   a. First Name
   b. Last Name
   c. User logon name
4. Click **Next>** Enter the password and finish the user creation.

5. Right-click and access the properties for the created user.

6. Enter the email this information isused for authentication when this user tries login from the ADFS

Sample Flow to Setup SSO from the Suite Admin

To set up SSO from the Suite Admin, perform this procedure.

1. After the Initial Administrator Setup, login into Suite Admin as the root user.
2. Locate the base URL for this server.
3. Go to Base URLpage in the Configuration menu and enter the Base URL from Step 2.
4. For private clouds, enter the port for the node port service (leave it blank for public clouds).
5. Save your changes.
6. Set up ADFS as listed in the *ADFS SAML SSO Sample Integration and Setup* above.
7. Once you configure Suite Admin with ADFS, note the details to map each field in theSuite Admin as listed in the previous sections.
8. Create one user in ADFS as listed in the previous sections.
9. Login into Suite Adminas the root user and access the SSO Setup page in the Suite Admin UI.
10. Enable SSO.
11. Enter the appropriate IdP metadata details in each field as identified in the *Accessing Claims* section above.
12. Open the https://<**IP_Address**>/FederationMetadata/2007-06/FederationMetadata.xmllink.
13. From this file, get the information for the First Name, Last Name, Email, User Group, and Tenant Id based on the appropriate mapping provided in the *Creating a New User in ADDS* section above. The following path are merely some examples you must find theactual values when creating the user and claim mappings.

    - First Name:http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
    - Last Name:http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
    - email:http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
14. Populate the SSO fields, and click **Save**.

15. Logout and execute the BASE URL. The expected outcome is that the Base URL will redirect the user to the ADFS page https://<**IP_Address**>/adfs/ls/IdpInitiatedSignon.aspx

⚠ The Suite Admin login page is not displayed when you execute the Base URL, instead the configured ADFS sign on page is displayed.

⚠️

16. Enter the username/password of the user created in ADFS. Click the **Submit/Login** button.The expected outcome is that theuser can login to the Suite Admin and view the Product Dashboard page base on this user's permission level (seeUnderstand User Levels for details).
17. To generate certificates for the new domain, follow these steps:

    a. Install the certbot tool by running the following command to get the certbot package.

    ```
    brew install certbot
    ```

    b. Use AWS Route53 to create a domain name for the IP.

    ```
    sudo certbot certonly --server https://acme-v02.api.letsencrypt.org/directory --manual --preferred-
    challenges dns -d '<preferreddomain.name.com>'
    ```

    c. Once this command is executed, you see a message similar to the following message:

    ```
    Please deploy a DNS TXT record under the name_acme-challenge.pujt.oneqaciscocpsgtesting.com with
    the following value: FU5........................JWR4gy.......gno
    ```

    d. Before continuing, verify that the record is deployed.
    e. Now in AWS Route53, add this informationagain in the record.
    f. Wait for 2-3 minutes for it to replicate so that the record can be reached by letsencrypt.org.
    g. Now press **Enter** so the private key and certs are created and a message similar to the following message is presented to you.

    ```
    - Congratulations! Your certificate and chain have been saved at: /etc/letsencrypt/live/user.
    oneqaciscocpsgtesting.com/fullchain.pem Your key file has been saved at: /etc/letsencrypt/live
    /user.oneqaciscocpsgtesting.com/privkey.pem Your cert will expire on 2019-03-04. To obtain a new
    or tweaked version of this certificate in the future, simply run certbot again. To non-
    interactively renew *all* of your certificates, run "certbot renew" - If you like Certbot, please
    consider supporting our work by: Donating to ISRG / Let's Encrypt: https://letsencrypt.org/donate
    Donating to EFF: https://eff.org/donate-le
    ```

    h. Copy the certs and then use this information to create the Base URL Configuration.

    ⊘ You do not need to create this user in Suite admin, as the authentication is performed by ADFS.

You have now configured the ADFS SAML SSO integration.

Workaround for Configuring SSO

The workaround for configuring SSO is the following procedure:

1. After upgrading Suite Admin from version 5.2.3 to 5.2.4.
2. Run the database update command on postgres pod.

```
PGPASSWORD=$(cat /tmp/secrets/postgres-password) PGDATABASE=suite-saml psql --host=$POSTGRES_HOST --
username=$POSTGRES_USER -c "UPDATE public.saml_infra_config SET cert_source='cert_manager' WHERE id=1;"
```

3. Delete the saml-tls secret and the saml pod.

```
kubectl delete secret suite-saml-sso-tls -n cisco
kubectl delete pod suite-saml-pod -n cisco
```

4. Configure baseurl again, download the new metadata and reconfigure the relying party trust in ADFS.
5. Reconfigure SSO.

After performing these steps, you may see the following error:

```
Caused by:org.opensaml.common.SAMLException:NameIDelement must be present as part of the Subject in the
Response message, please enable it in the IDP configuration
```

⚠️

Note that the Transform Incoming Rule andLDAPrules get deleted from the Relying party trust object sometimes. In this case, redefine/add the Transform Incoming Claim rule. If both rules aredeleted, add them both again.

Log Archive

Log Archive

Overview

The temporarily stored logs on the CloudCenter Suite server are automatically purged on a regular basis. This log file location is not configurable from the CloudCenter Suite.

To store logs for a longer period, you can configure an archive location for your AWS S3 region if you configure an archive location for your AWS S3 region, the CloudCenter Suite logs can also be saved to the AWS S3 region besides the temporary location on the CloudCenter Suite server. If so, you can enable the archive of log files from the Suite Admin UI to the AWS S3 region using the S3 bucket name and AWS credentials.

Requirements

You should have already configured the AWS S3 region. Refer to https://docs.aws.amazon.com/AmazonS3/latest/dev/ServerLogs.html for details.

Each zip file saved in the S3 bucket is assigned a numeric value and saved with a time stamp.

Process

To enable log archives, follow this process.

1. Navigate to the Suite Admin Dashboard>**Admin**.
2. Click **Log Archive** in the left tree pane to display the Log Archive page as displayed in the following screenshot.
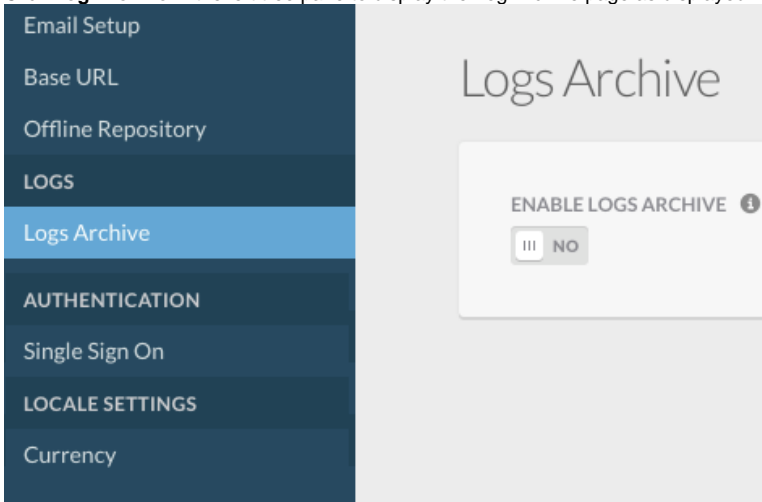
3. Toggle the **Enable Logs Archive** switch to enable (disabled by default) the archive of log files.
4. Configure the **AWS Region**, **S3 Bucket**, **AWS Access Key ID**, and **AWS Secret Key Access** details.

5. Click **Connect** to save your changes as displayed in the following screenshot.

Once connected, the CloudCenter Suite logs are collected in the configured S3 bucket as displayed in the following screenshot.

Disabling Log Archives

You can disable the log archives at any time by toggling the **Enable Logs Archive** switch and confirming your actions in the resulting popup. Disabling the configuration will only save future logs to the temporary CloudCenter Suite location where they are automatically purged.

Log Retention

By default, CloudCenter Suite stores logs locally for seven days. You cannot change or modify the log retention value from the SuiteAdmin user interface or API. If you find the seven-day retention value too restrictive, you can change value by adding more days or specifying a limit on the size of retained log files.

Offline Repository Configuration

Offline RepositoryConfiguration

- [Overview](#)
- [Connectivity Icon](#)
- [Process](#)

Overview

A repository connection enables access from one of the %ccsVMs to a local **Cisco Products Repository**. This default repository is only accessible if you have internet access.SeeOffline Repositoryfor details.

If your %ccs instance does not have internet access, you will not be able to view any dashboard in the %ccs even after you log in.

Connectivity Icon

The suite administrator's ability to view a configured repo is indicated by the green circle on the**folder icon**.

- If the%ccs is able to connect to theCisco Products Repository, then you'll see a green circle displayed in theSuite Admin Dashboardheader. If
- not, then you must first setup the offline repository, and then configure the Suite Admin to connect to the offline repository (displayed in the following screenshot).

Clicking this icon (displayed in the screenshot above)allows you to enable a local repository connection if you are operating in an environment with no internet access.

The color of the circle on the folder icon identifies the status of the repository(even if it is the default Cisco repository) connectedto the %ccs as identified in the following table.

Folder Icon Color	Description
Green	The offline repository connection is successful.
Red	The offline repository connection failed.

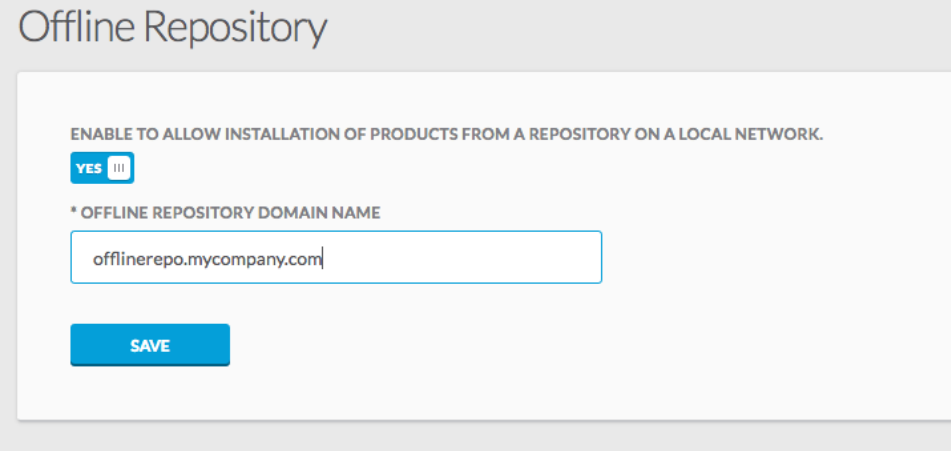The offline repository connection in disabled by default and must be explicitly enabled to configure the DNS or IP address of the local repository.

Process

To configure the connection to a local network repository, follow this procedure.

1. Click the folder icon to re-configure the proxy settings.
   Optional. Navigate to the Suite Admin Dashboard> **Admin**and click **Offline Repository**.

2. Toggle the switch (disabled by default) to enable access to the %ccs via a local repository (displayed in the following screenshot).

Offline Repository

ENABLE TO ALLOW INSTALLATION OF PRODUCTS FROM A REPOSITORY ON A LOCAL NETWORK.

YES |||

* OFFLINE REPOSITORY DOMAIN NAME

offlinerepo.mycompany.com

SAVE

3. Provide the DNS of the offline repositoryserver in the URL field.
4. Click **Save** to save your changes.
5. Go to the Module Dashboard icon to view the repo listing the offline repository similar to the display in the following screenshot:

cisco Suite Admin

REPO PROXY CONNECTIVITY

Modules

Connected to
offline9853.oneqaciscocpsgtestin
g.com products repository.
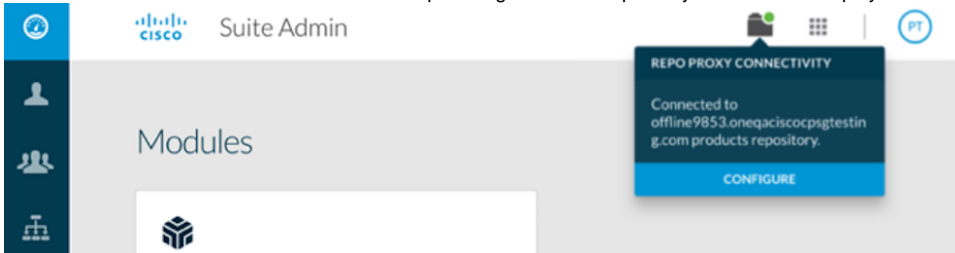
CONFIGURE

Base URL Configuration

Base URL

- Overview
- Requirements
- Process
- Re-Adding the Transform Incoming Claim Rule

Overview

The Base URL provides a DNS entry, instead of an IP address, to access the %ccs.

Functions like Email Settings and SSO Setup require the Base URL to be configured.

Requirements

If you do not configure the Base URL for a particular tenant, then the Suite Admin uses the parent-level configuration details to set the host/port link.

If a tenant does not have a Base URL configured, the URL is inherited from the immediate parent where the Base URL is configured.

Prior to %ccs 5.1.2, admins did not have the option to configure a specific parent/ancestor's Base URL for a tenant.

Effective %ccs 5.1.2, tenants admins can configure the Base URL of any of their ancestor tenants. The only caveat is that the admin cannot set the Base URL of child tenant for a parent tenant.

Process

To configure the Base URL, follow this procedure.

1. Navigate to the Suite Admin Dashboard>**Admin**.
2. Click **Base URL** in the left tree pane.
3. In the Base URL settings page, enter the **DNS/IP Address** and **Port** number that should be displayed in the Base URL.
4. Copy and paste the **Private Key** and/or **Certificate** details for the DNS provided in the previous step.
5. Click **Save** to save your changes and enable a direct connection to the IDP server.

Re-Adding the Transform Incoming Claim Rule

In some instances after configuring the Base URL, the Transform Incoming Rule and LDAP rules are deleted from the Relying party trust defined in the Active Directory Federation Services (ADFS) server. If these deletions occur, reconfigure the Base URL and SSO and add both rules again. The following error message indicates the rules have been deleted.

```
Caused by: org.opensaml.common.SAMLException: NameID element must be present as part of the Subject in the
Response message, please enable it in the IDP configuration
```

Email Settings

EmailSettings

- Overview
- Requirements
- Process

Overview

Email settings are required to communicate with %ccs userswhen triggering the reset password function or the password auto-generation function the emailsettings are used to construct the links when resetting a password for new or existing users.

> ✅ The Suite Admin does not support TLS ports itonly supports SSL ports to configure SMTP mail servers.

You can enable the*SMTPS*protocolto secure SMTP at the transport layer. SMTPS uses port 465 to indicate that the client and server communicate using normal SMTP at the application layer, but the connection is secured by SSL or TLS.

> ⚠️ If the SMTP settings are not configured for a sub-tenant, then the parent tenant's SMTP settings are used to send emails to users.

Requirements

To use this function:

- The enterprise should have already setup an SMTP server.
- The user must have tenant administrator permissions.
- The SMTP configuration must be authenticated and that you are able to send and receive emails before setting up your email communication.

> ⚠️ When a cloud is configured in a different region using some carriers (for example, GMAIL), the carrier may assume this configuration as a suspicious activity and block the email sending functionality. This is an example of an issue with your carrier's SMTP settings.
>
> Example: If you send an email using GMAIL from different region/machines, then GMAIL may trigger emails for suspicious activity and stops sending emails. In this case, you must resolved this issue by following this procedure.
>
> 1. Login into this email from gmail.com to access your account.
> 2. In thehttps://myaccount.google.com/?utm_source=OGB&utm_medium=actpage, click Security in the left pane.
> 3. Search for **Access allowed for less secure apps** and turn it on to ensure that you allow access for this application.
> 4.You can now configure your GMAIL email in the Email Setup page in Suite Admin.
>
> Be sure to resolve these issues before proceeding with the configuration.
>
> In AWS Environments, you must configure the application password to configure GMAIL in AWS cluster.

- You should have already configured the Base URL Configurationand completed theEmail Settings to ensure that the URL is accessible and that an email can be sent to the user.

Process

To configure SMTP details in the Suite Admin, follow this procedure.

1. Navigate to theSuite Admin Dashboard>**Admin**.
2. Click**SMTP**in the left tree pane to display the SMTP Settings page.
3. Toggle the switch to enable(disabled by default)**SMTP** settings.
4. Optional. Toggle the switch to enable **SMTPS** (Secure SMTP) at the transport level.
5. Optional. Toggle the switchto enable **TLS**security protocol if required by your SMTP server.
6. Provide the **Username**, **Password**, IP address or DNS for the **SMTP Host**, the **Port** Number, the From Address, and the From Alias to enable SMTP authentication.

> ℹ️ The the From Address, and the From Alias fields are available effective Suite Admin 5.2.2.

7. Click **Save** to save your edits.

ℹ️

When you save the SMTP settings, be aware that you are only saving the configuration parameters to the %ccs database and that the connection is still pending connection verification. As soon as the connection is verified by the %ccs, the current user (who changed the SMTP configuration) is notified in the notification pane (see Suite Admin Dashboard > *Notifications*) about the connection status with details on the SMTP connection check passing/failing.

Proxy Settings

Proxy Settings

-

Overview

The Suite Admin uses proxy settings for licensing and module configuration purposes. Proxy settings are disabled by default.If not provided, thenno proxy configuration is set!

> ⚠ Web service calls are routed through the proxy. When proxy settings are modified on the Suite Admin, the %ccs management pod is rebooted to apply the configuration.

Guidelines

Adhere to these guidelines if you decide to use a proxy server to connect to the internet:

- Only the suite administrator can configure the proxy protocol and provide the user authentication details.
- Set up the proxy server before starting the module installation processes.

Suite Administrator Proxy Configuration

To configure the internal proxy settings, follow this procedure after you have set up your proxy server and retrieve the DNS details and port number required by the proxy server.

1. Navigate to theSuite Admin Dashboard>**Admin**.
2. Click**Proxy**in the left pane to configure the enable proxy settings (disabled by default)as displayed in the following screenshot.

3. Switch on the required protocol to enable(disabled by default) your proxy setting: **HTTPS** or **HTTP**.
4. Provide the DNS name or IP address for the **HTTP Proxy Host** along with the **Port** number.
5. *Optional*. Identify if the proxy server requires the admin to be authenticated each time. If yes, provide the **User Name** and **Password** to access the Proxy server.
6. *Optional*. To bypass the proxy settings, provide a comma separate string of values in the **ByPass Proxy Settings** field as displayed in the following codeexample:

✓

Depending on the environment where you have installed the %ccs, you many need to include the required environments that you wish to bypass in order to access service endpoints. For example, if you are operating in a Cisco environment, include *.**cisco** to the following list. This is only an example and what you add is dependent on your environment.

When you enter a value in the HTTP or HTTPS field and if you also enter the IP/FQDN in the**ByPass Proxy Settings** field, then after setting up %ccs, the connection to this IP/FQDN will bypass the Proxy value when %ccs tries to connect to this IP/FQDN, the proxy entered during installation will not be used.

To bypass the proxy settings, provide a comma separated string of values in the **ByPass Proxy Settings** field as displayed in the following _examples_:

```
localhost.*,127.0.0.1:42

# Or, to bypass specific environments. The following is another example - what you add is dependent on
your environment.

localhost.*,127.0.0.1:42,*.cisco
```

7. Click**Save**to save the proxy settings.

Backup

Backup Approach

- [Overview](#)
- [Limitations](#)
- [What Data Is Backed Up?](#)
- [Requirements](#)
- [Process](#)
- [Actions after Configuring the Backup](#)

Overview

You may sometimes need to backup your CloudCenter Suite setup so you have the option to recover the data when required. When you have a cluster running, it can go into a bad state for a number of reasons (resource shortage, application unavailability, infrastructure changes,undependable state and so forth). In these cases, backing up the data allows you a to recover data when required.

> ⓘ The backup/restore feature is only available on*new*CloudCenter Suite clusters installed using CloudCenter Suite installers and *not on* existing Kubernetes clusters.

Limitations

> ✅ For isolated, air gap, environments, that do not have internet access, or to back up to a local system, a manual backup procedure is available see [Private Cloud](#) for additional details.

Before proceeding with a backup, adhere to the following limitations:

- **Supported Clouds**: You can backup data to one of the following locations:

    - Google Cloud Storage (use the procedure below)
    - AWS S3 (use the procedure below)
- **Switching between Clouds and Cloud Accounts**:

    - While editing the storage location in the CloudCenter Suite, if you switch to a new cloud type or cloud account within the same cloud type, be aware that backups in the previously configured storage location will no longer be accessible from the CloudCenter Suite.
    - The backup files from the previously configured storage location will continue to be available via your cloud console.
- **Restoring to a Different Cluster**:

    - This feature is only supported for clusters launched by theCloudCenter Suite installer.
    - You cannot backup from and restore to the same cluster you **can only** backup to one cluster and restore to a different cluster.
    - The backed up cluster and the target restore cluster should both be on the same cloud.
- **User Credentials**:

    - The credentials are specific to your service account in the cloud and only the user with those credentials can configure and initiate the backup.
    - If you change the credentials you will see a warning message to indicate that you cannot access previous backups.

What Data Is Backed Up?

> ⚠ The CloudCenter Suite does NOT provide a granular option to backup Kubernetes resources or application-specific databases.
>
> Additionally, you CANNOT take volume snapshots.

The CloudCenter Suite uses the *latest* cloud/cloud account and bucket configurations to retrieve the list of existing backups, displayed in the table in the **Admin** > **Backup** page (under the Data Recovery section in the Suite Admin UI).

> ⓘ If you update the existing configuration for any reason, users cannot manage the backups from the earlier cloud/cloud account and bucket configuration.

The backup action backs up the ENTIRE *cisco* namespace.

- **Backed Up**:

- Any data under the Cisco (*cisco*) name space.
- This includes users, groups, and roles for all modules.
- This also includes but is not restricted to the Kubernetes resources with associated application data, pod data, secrets, PersistentVolumeClaim (PVC) data, PersistentVolume (PV) data, and other relevant data associated with these sub-systems
- **Not Backed Up**: Any data that is not under the Cisco (*cisco*) name space.

  - Action Orchestrator Nuances:

    - The backup and restore procedures do not back up Action Orchestrator-specific data like workflows, targets, and so forth.
    - This type of Action Orchestrator-specific data is stored in arangoDB and requires arangodump and arangorestore to backup and restore the data.
    - To backup the date (Without internet access or proxy), theArangodump should occur *before* you install the new Action Orchestrator version. See for additional details onPrivate Cloud >*Action Orchestrator-Specific Post-Restore Procedure* for additional details.
    - Action Orchestrator Backup Requirements:

      1. Backup the Action Orchestrator database using the arangodump tool.
      2. Uninstall Action Orchestratorfrom the CCS cluster.
      3. Backup Suite Admin, Workload Manager, and Cost Optimizer using Velero.
    - Action Orchestrator Restore Requirements:

      1. Restore Suite Admin, Workload Manager, and Cost Optimizerusing Velero
      2. Reinstall Action Orchestrator.
      3. Restore the Action Orchestrator databaseusing arangorestore tool

Requirements

Before proceeding with a backup, adhere to the following limitations:

- **General**: When configuring a backup for the first time, verify that the storage bucket is empty before scheduling any backups.
- **GCP**:

  - Configure a Storage Bucket with the required permissions: The following screenshot displays a sample storage bucket in a GCP environment:
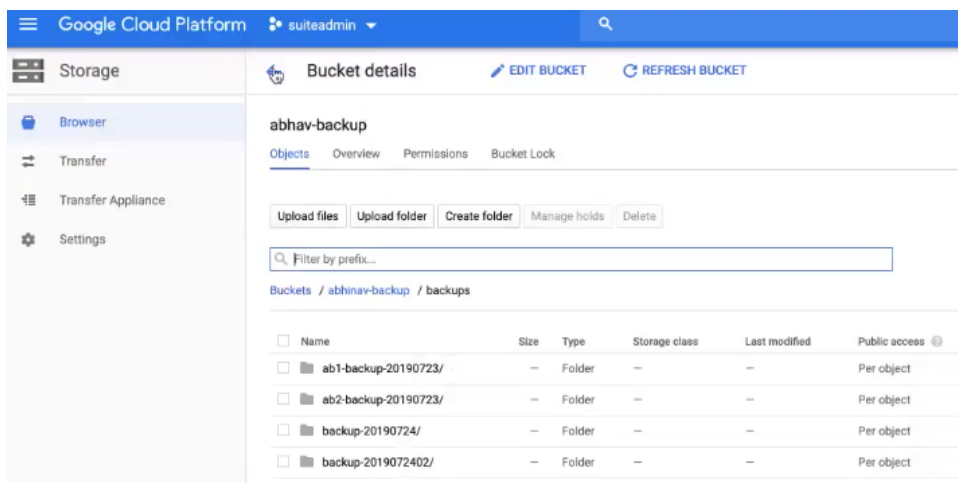
  - The cloud account used to configure the backup must have an empty **storage.bucket.list.**
  - The bucket must have its ACL set to **storage.objects(create,delete,get,list).**

- **AWS:**

  - The storage bucket in your AWS S3 environment must be empty with the applicable ACL permission.
  - The IAM user permissionsdefine the user privilege on the S3 bucket as listed in the following screenshot:

    > ✓ In the following code block, the bucket name is defined as **_velero-cisco_ this is just an example**! Be sure to change this value to reflect the name of your own bucket!

```json
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Effect":"Allow",
            "Action":[
                "ec2:DescribeRegions",
                "ec2:DescribeVolumes",
                "ec2:DescribeSnapshots",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot"
            ],
            "Resource":"*"
        },
        {
            "Effect":"Allow",
            "Action":[
                "s3:GetObject",
                "s3:DeleteObject",
                "s3:PutObject",
                "s3:AbortMultipartUpload",
                "s3:ListMultipartUploadParts"
            ],
            "Resource":[
                "arn:aws:s3:::velero-cisco/*"
            ]
        },
        {
            "Effect":"Allow",
            "Action":[
                "s3:ListBucket"
            ],
            "Resource":[
                "arn:aws:s3:::velero-cisco"
            ]
        },
        {
            "Effect":"Allow",
            "Action":"s3:ListAllMyBuckets",
            "Resource":[
                "arn:aws:s3:::*"
            ]
        }
    ]
}
```
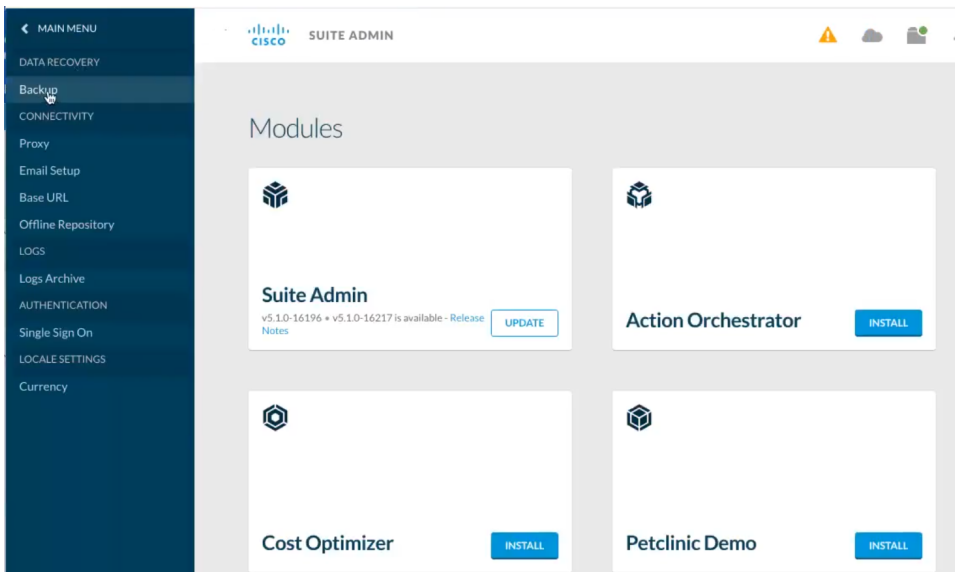
Process

To backup the CloudCenter Suite data, follow this procedure.

1. Navigate to the Suite Admin Dashboard.
2. Click **Admin** > **Backup** (under the Data Recovery section) to access the Backup page as displayed in the following screenshot.

3. Click the **cog** icon in the Backup page (as displayed in the following screenshot) to configure a new backup storage location.

4. Select the required cloud in the Configure a Backup Storage Location page as displayed in the following screenshot.
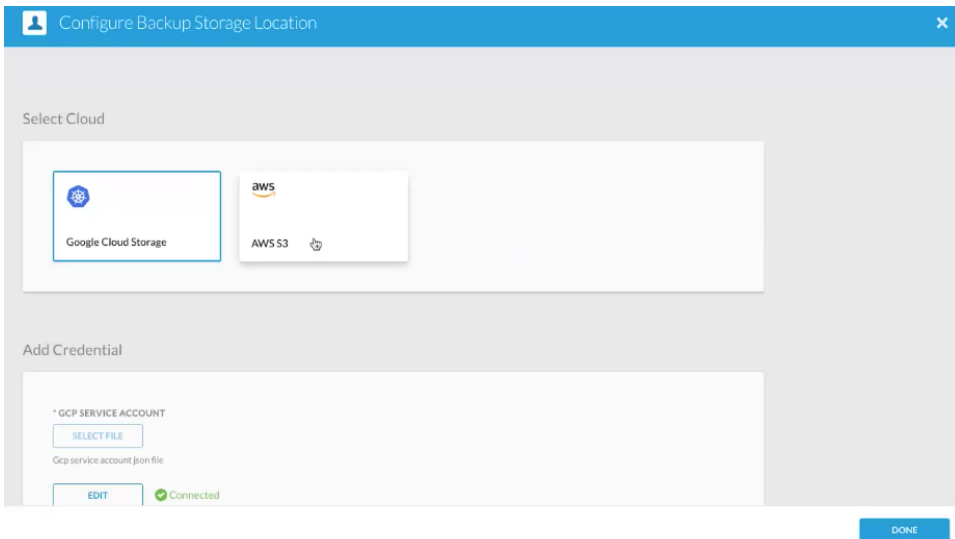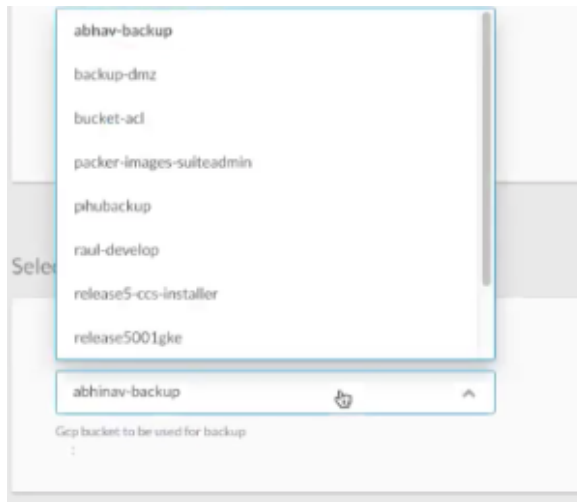

5. Depending on the selected cloud, the Add Credential section differs:
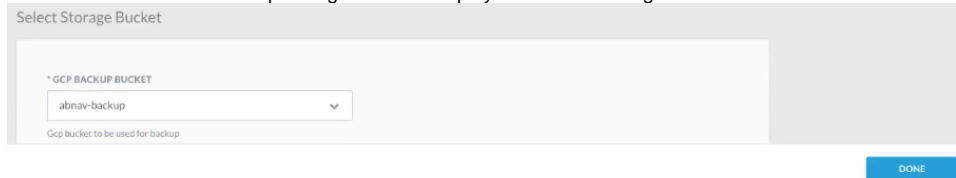
   - GCP:

     a. Select the file containing the credentials is displayed in the following screenshot.

     b. Select the Storage bucket as displayed in the following screenshot.

c. Click **Done** to save the backup configuration as displayed in the following screenshot.

- AWS S3:

    a. Select the file containing the credentials as displayed in the following screenshot.

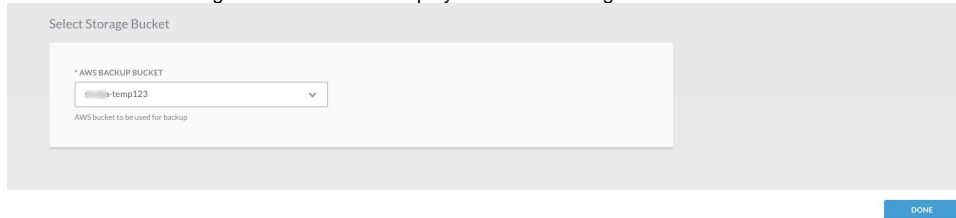   b. Select the Storage bucket as displayed in the following screenshot.

    c. Click **Done** to save the backup configuration as displayed in the following screenshot.
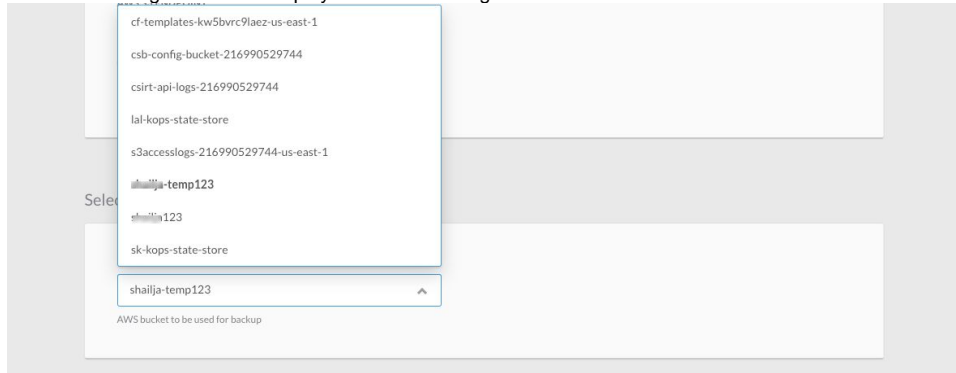
6. Once configured, click **Backup** in the Backup page to initiate the data backup. Until you initiate the first backup, this page will be empty. Once you have initiated one or more backups, they are automatically listed in this page as visible in the following screenshot.

7. In the Backup Name popup, assign a unique name (by default, the current date is listed) for this backup task and click **OK** as displayed in the following screenshot.

You have now backed up the CloudCenter Suite data to a cloud of choice.

Actions after Configuring the Backup

Once you have configure one or more backup settings in the Backup page, you may see the following actions in the Actions column.

- **Delete**: You can delete the configured backup as visible in the following screenshot:
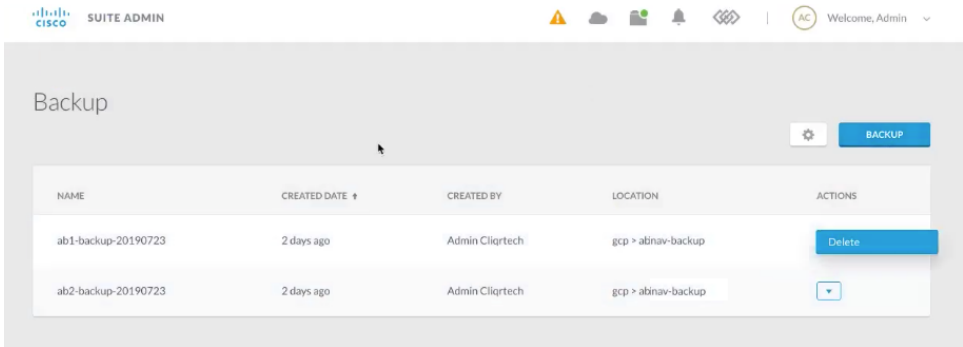
- **Cancel**: You will only see the **Cancel** option when you are in the process of backing up a storage location. After you create the location, the only option you will see is **Delete**.

Back to: Public Cloud

User Tenant Management

User Tenant Management

- Manage Module-Specific Content
- Manage Tenants
- Understand User Levels
- Understand Roles
- Custom Groups by Admin
- OOB Suite Admin Groups
- Create and Assign Groups
- Create and Manage Users

Manage Module-Specific Content

Manage Module-Specific Content

- [Overview](#)
- [Associate Modules](#)
- [Characteristics](#)
- [Process](#)

Overview

Each module in the CloudCenter Suite may have content that is specific to just that module. The suite administrator can manage these settings at the tenant level and the user level.

> ✓ Currently, the workload manager is the only module that uses this feature. See Tenant Management in the workload manager documentation for an example.

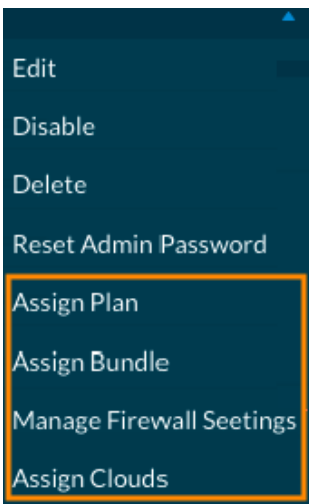The actions displayed for each module is a fluid list based on which module-specific actions were created and made available for each tenant or user within the module **this information is configured from the module**.

The configured content is **visible** from the %sa's **Tenants** list page or the **Users** list page, which displays the configured action for each tenant or user within the Actions dropdown list.

The following screenshot displays content that is specific to the %wm at the tenant level. The first few actions are specific to the Suite Admin and the module-specific actions are listed at the end of the dropdown.

Edit
Disable
Delete
Reset Admin Password
Assign Plan
Assign Bundle
Manage Firewall Seetings
Assign Clouds

The following screenshots display content that is generally available to different users. This screenshot does not include any module-specific actions as they have not been configured.

Edit User
Reset Password
Disable User
Manage Groups
Generate API Key
Delete User

Delete
Associate Modules
WORKLOAD MANAGEMENT
Manage Plan
Manage Cloud Group
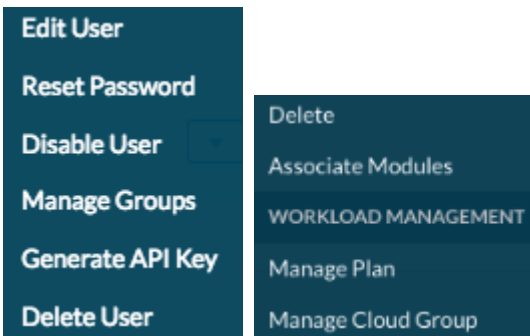
Associate Modules

After you add tenants (see Manage Tenants), you can provide access to modules at any time by clicking the Associate Modules option from the Actions dropdown. If you do, you will see a popup similar to following screenshot.
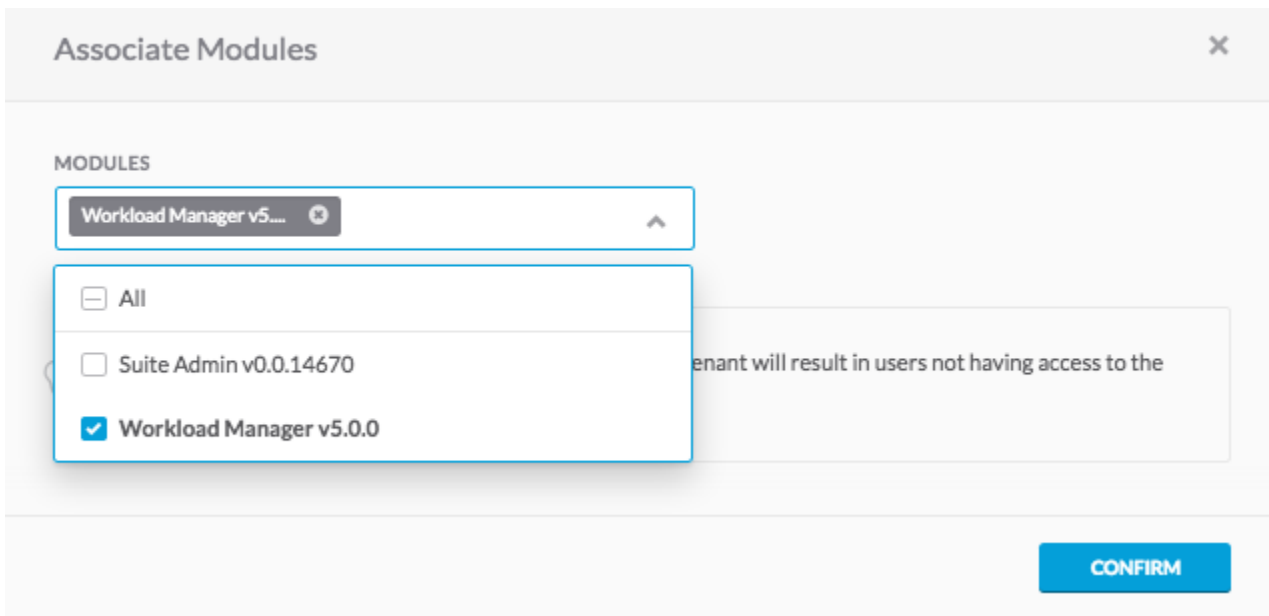
Characteristics

To configure module-specific content for a particular module, you must perform the configuration from the module for each applicable tenant or user.

This configured content for each module has the following characteristics:

- Can be made available at the tenant level for any user.
- Is *not* inherited from the parent tenant.
- Each tenant administrator can override this information for their respective tenants.

Process

To manage content at the tenants and user levels, follow this procedure.

1. Navigate to the Suite Admin Dashboard>**Tenants** page or **Users** page.
2. Click the **Actions** dropdown for the required tenant or user.
3. Select the action from the dropdown list for the required tenant or user.
4. Proceed with the action as listed in the module documentation. The general description of each setting and action is specified in the module documentation.

Manage Tenants

Manage Tenants

- Overview
- Tenants List Page
- General Settings Tab
- Branding Information Tab
- User Password Rules Tab
- Predefined Tenant Actions

Overview

By default, the suite administrator belongs to the root tenant. The suite administrator can perform the following tasks at this level:

- Create sub-tenants
- Modify the root tenant

Each task is explained in the context of configuration tabs that are explained in the following sections.

Tenants List Page

When you navigate to the **Tenant** page from the Suite Admin Dashboard, you see the following details:

- **My Tenant**: This is always the parent tenant from each CloudCenter Suite user's perspective! The suite administrator always belongs to the root tenant that was configured during the Initial Administrator Setup.
- **Sub-Tenants**: Each tenant admin can configure sub-tenants as required. If configured, they are listed in this section. Once configured, the sub-tenant admin receives an automatic *welcome* email.

The Tenant ID and the administrator's email is also listed in this page for both the My Tenant and the Sub-Tenants sections.

General Settings Tab

The root tenant configuration in this section is restricted to modifying the Tenant Name and Tenant Login ID. Root tenant users cannot disable or delete themselves.

When configuring sub-tenants, a tenant admin can configure the following details:

- **Tenant Settings**: Tenant Name and Tenant Login ID
- **Tenant Admin Settings**: First and Last Names, Email, and Auto Generate Password (default) to trigger a new message to this user (not available for the root tenant).

> ⓘ If you disable the **Auto Generate Password** switch, you must manually create a password and manually send an email to this user.
>
> The eye icon besides making the password visible also monitors the password rule check to ensure that you set an acceptable password based on the listed rules. The password rules are configured by the suite administrator as specified in the *User Password Rules Tab* section below.
>
> The SMTP settings must be set up on a per-tenant basis as required for your enterprise. See Email Settings for additional context.
>
> Either way, when the user's password expires, the user sees this alert when logging in for the first time, along with a link to change the assigned password. Be sure to change the password and then dismiss the alert. The user has 30 days to act on this message and use the link to change the password.

- **Module Assignment**: Select the modules that this tenant user can access by virtue of being in this tenant. The Initial Administrator can manage modules for sub-tenants at the root-tenant level

Branding Information Tab

This tab is only available at the **My Tenant** level. The information in this tab is inherited from the parent tenant, if configured. However, tenant admins can overwrite this information for their respective sub-tenants.

To configure branding information at the My Tenant level, follow this procedure.

1. Click the *link* in the Tenant Name column to open the **Editing tenant *Tenant Name*** form. This form has three tabs.
2. Click the **General Settings** tab, if required.
3. Click the **Branding Information** tab to configure the product branding, terms of service, privacy policy, and trademark details as listed in the form. All details in this form are optional and the default Cisco settings are identified in the Suite Admin Dashboard > **Footer** section.
4. Click the **User Password Rules,** if required.
5. Click **Done**.

User Password Rules Tab

This tab is only available at the **My Tenant** level. The information in this tab is inherited from the parent tenant, if configured. However, tenant admins can overwrite this information for their respective sub-tenants.

Predefined Tenant Actions

On the Tenant list page, the **Actions** column displays a dropdown list of actions that each Tenant admin can perform based on group membership and permissions.

The following table identifies the actions available at the Tenant Level.

Tenant-Level Action	Description
Edit	Available at the My Tenant and Sub-Tenant levels.
Enable /Disable	Once disabled, you must first enable a user to assign the user to a group and to see other Actions for this user.
Delete	When you attempt to delete a tenant or sub-tenant, the Suite Admin triggers a confirmation process to verify (with each module) that the resource can be deleted. If all product modules confirm the deletion, then the tenant or sub-tenant deletion is permitted to proceed. If the resource cannot be deleted the module returns a failure message with information about associated resources.
Associate Modules	This action provides the tenant admin with the ability to associate or disassociate one or more installed modules for users in this tenant. See Manage Module-Specific Content > *Associate Modules* for additional details. If you disable all modules for a tenant, then users in this tenant are abandoned and cannot view an information in the CloudCenter Suite.
Impersonate User	A suite administrator or a tenant administrator can temporarily sign into the CloudCenter Suite as a different user. See Create and Manage Users > *Impersonate User* for additional details.
Module-Specific Actions	This is a fluid list based on which module-specific actions were made available for each tenant, user, and module. See Manage Module-Specific Content for additional details.

Understand User Levels

Understand User Levels

- [Overview](#)
- [Suite Level](#)
- [Tenant Level](#)
- [Sub-Tenant Level](#)
- [Tasks Available at Each User Level](#)

Overview

The term *user level* refers to the user's permission level. Each user level requires explicit permissions to perform specific tasks at the suite level, the cluster level, the module level, the tenant level, or the sub-tenant level.
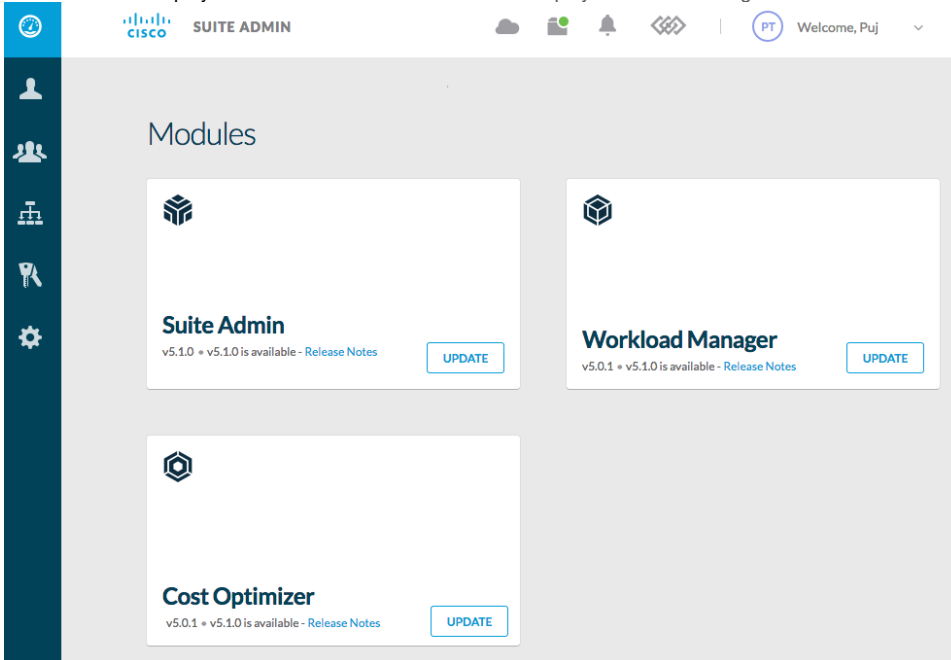
Suite Level

The following screenshots displays the information presented to a user with suite-level permissions:

- The Information displayed at the browser landing page level as displayed in the following screenshot:
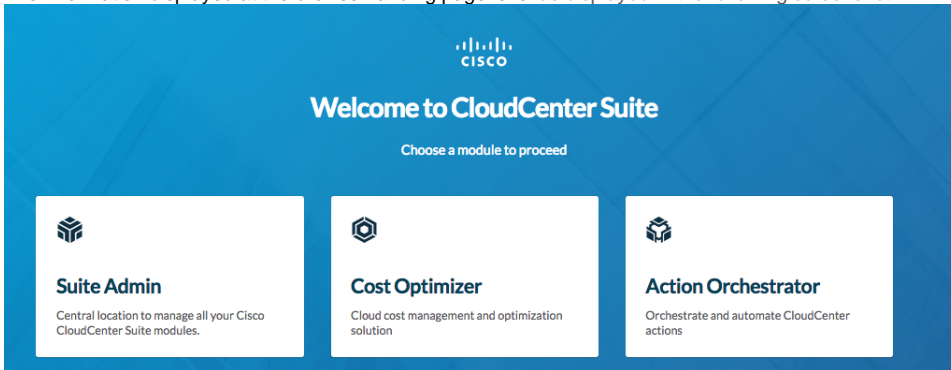
- The information displayed at this user's dashboard level as displayed in the following screenshot:

The suite administrator and/or tenant administrator has access to all installed modules as well as the Suite Admin Dashboard. Additionally, this user also has all options displayed in the Left Tree Pane.

Tenant Level

The following screenshot displays information presented to a user with tenant level permissions to specific modules.

A tenant level user only has access to the permitted modules at the landing page level as well as the Dashboard level. Additionally, this user only has tenant-level options displayed in the left tree pane based on permitted user levels.

Sub-Tenant Level

Thefollowing screenshots displays theinformation presented to a user with suiteadministrator permissions:

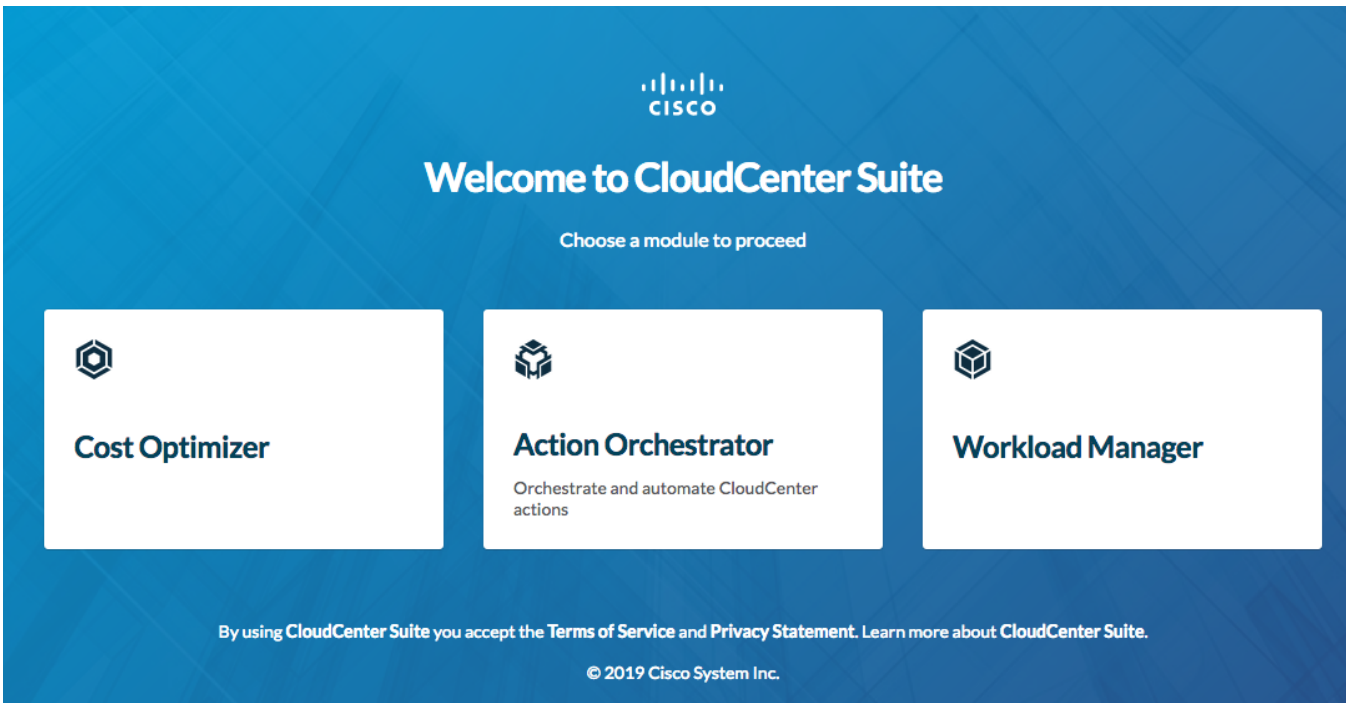- The Information displayed at the browser landing page level is displayed in the following screenshot:
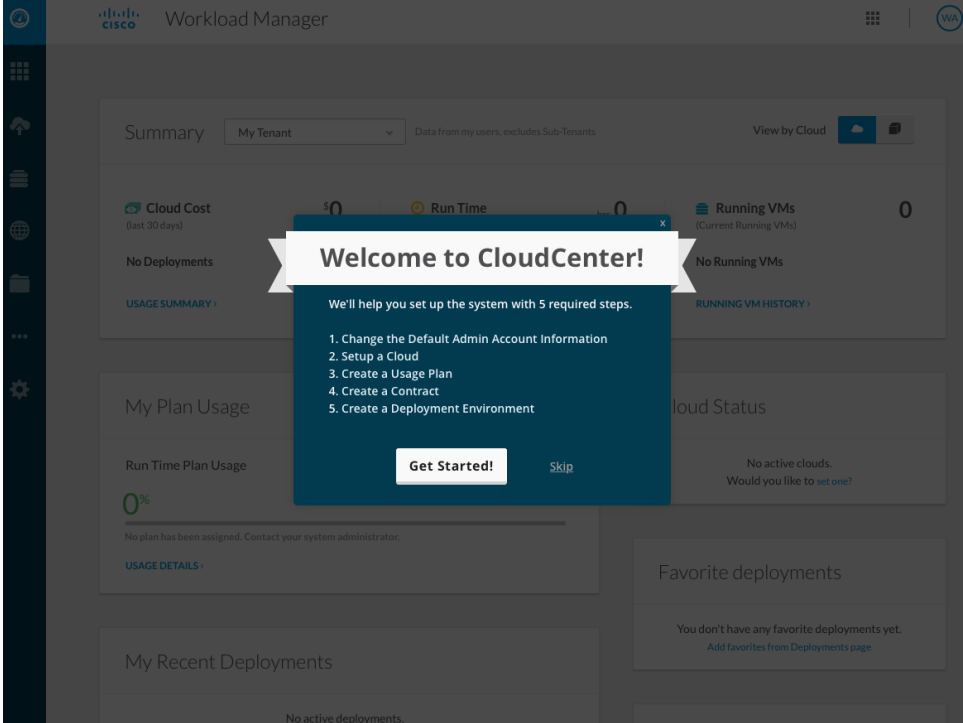
- The information displayed at the user's dashboard level is displayed in the following screenshot:
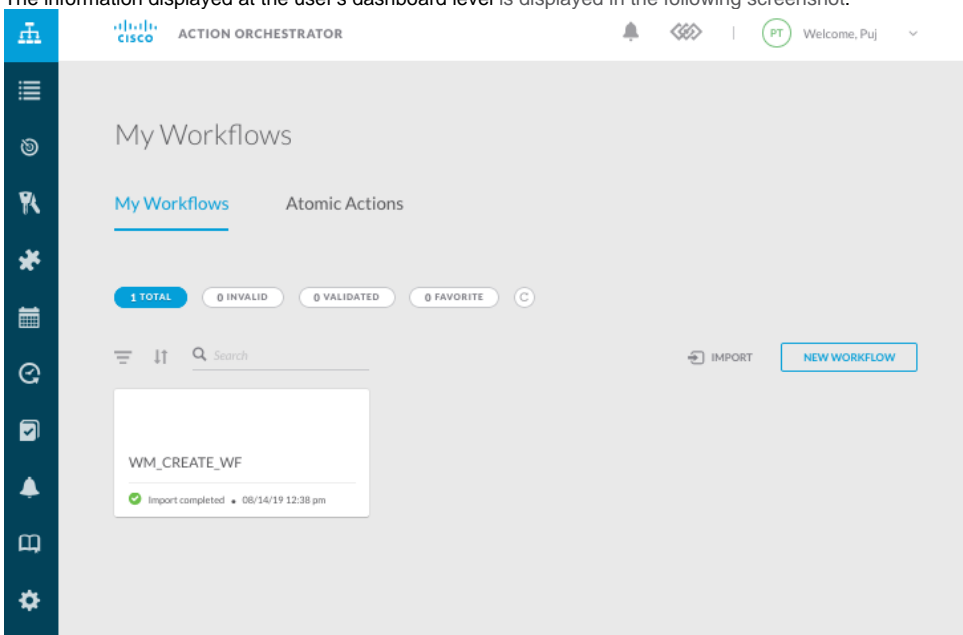

Note that this sub-tenant level user, has direct access into the only permitted module at the landing page level as well as the Dashboard level this user will not be able to see any suite-level options and will only see the module-level options (in this case, the workload manager) displayed in the Left Tree Pane based on the user level.

Tasks Available at Each User Level

The following table lists the task available to each user level and identifies the permission level as follows:

- ✅ = Permitted
- ❌ = Not permitted
- ⭐ = Permitted based on tenant ownership (if tenant owner or if sub-tenant owner)

Task	SuiteAdministrator	Tenant Admin	Sub-Tenant Admin	Module Admin
Module Lifecycle Management (Self-Hosted)				
Install Module	✅	❌	❌	❌
Update Module	✅	❌	❌	❌
Monitor Modules	✅	❌	❌	❌
Configure Smart Licenses	✅	❌	❌	❌
Admin Menu				
Backup	✅	❌	❌	❌
SSO Setup	✅	⭐	⭐	❌
Proxy Settings	✅	❌	❌	❌
Email Settings	✅	⭐	⭐	❌
Base URL Configuration	✅	⭐	⭐	❌
Offline Repository	✅	❌	❌	❌
Currency Conversion	✅	❌	❌	❌
Kubernetes Cluster Management (Self-Hosted)				
Cluster Status	✅	❌	❌	❌
Manage Clusters	✅	❌	❌	❌
User Tenant Management				
Create and Manage Users	✅	⭐	⭐	❌
Create and Assign Groups	✅	⭐	⭐	❌

Custom Groups by Admin	✅	❌	❌	❌
Manage Tenants	✅	⭐	⭐	❌
Manage Module-Specific Content	✅	⭐	⭐	✅

Understand Roles

Understand Roles

- [Overview](#)
- [Role-Based Access Control (RBAC)](#)
- [Predefined, Default Roles](#)
- [Custom Roles](#)
- [Predefined Roles for Each Module](#)

Overview

Roles are a collection of permissions provided to a OOB Suite Admin Group. The users within each group can perform *permitted functions* on *permitted resources* by virtue of being part of the group.

- *Permitted function* refers to configuration functions like create, view, update, delete, run, and so forth.
- *Permitted resources* differ based on the module where users in a group perform these actions. As the resources differ between modules, each user can only perform actionspermitted within the authorized group.

> ⊘ *You cannot assign a role to a specific user in any group.*

*Permissions*identify what operations can be performed on which resources based ontenant association,module restriction, anduser level (see Understand User Levels).

Role-Based Access Control (RBAC)

Authorization is based on Role-Based Access Control (RBAC), but restricted to groups in this release.

> ⚠ The RBAC function is inherent and cannot be configured on a per role/user basis. It is inherent because of the group association to users.

Roles are *only* associated withuser groups. Coupled with permissions andAccess Control Lists (ACL, see the documentation for each module for related details), roles offer the ability to perform specific tasks and view corresponding data.

Permissions can be configured and controlled by different types of roles:

- *Predefined, default roles*
- *Custom roles*are controlled by the modules to which these roles belong. These roles may be required to provide additional granularity for a resource. These roles can be configured for each module.Onlythe Action Orchestrator allows custom role creation.

Default/custom roles are**visible**from the %sa's**Tenants**list page or the**Users**list page, which displays the configured action for each tenant or user.

SeeAction Orchestrator Rolesfor contentspecific to Action Orchestrator at the tenant level.

Predefined, Default Roles

Predefined,default rolesare provided OOB by the Suite Admin for each modules. These roles cover 90% of the functionality required for you to get started with the CloudCenter Suite. These roles cannot be configured as they provide specific permission to specific resources.

Each module in the CloudCenter Suite also has default OOB roles that is specific to just that module. The suite administrator can manage these settings at the tenant level and the user level.

> ⊘ Currently, the Action Orchestrator is the only module that uses the custom role configuration function. See Action Orchestrator Roles for details.

The actions displayed for each moduleis a fluid list that is created and made available for each tenant or user within the module.

Custom Roles

Custom roles are **configured from the module**:

- Module admins can create custom roles within the module.

⊘

> ✓ Currently, the Action Orchestrator is the only module that uses the custom role configuration function. See Action Orchestrator Roles for details.

> ⚠ The workload manager and Cost Optimizer do not allow custom role creation as all required roles are already available through this user's group membership.

- Custom roles are available to suite administrators as the administrator can associate each new or existing user with one or more roles. See Custom Groups by Admin > *Create a Custom Group* for details.
- When module admins Create a Group, they can assign custom roles for the new group. See Custom Groups by Admin for additional details.

Predefined Roles for Each Module

The OOB ACLs, permissions, and roles that are predefined for each module are explained in the corresponding module documentation. See the pages identified in the following table for additional details.

Module	Page Reference
workload manager	See OOB Groups, Roles, and Permissions
Action Orchestrator	See Action Orchestrator Roles
Cost Optimizer	See Access and Roles

Custom Groups by Admin

Custom Groups by Admin

- Overview
- Create a Custom Group
- Deleting Custom Groups

Overview

If the pre-defined roles and groups listed in OOB Suite Admin Groups are not sufficient for your environment, suiteadministrators have the flexibility to create custom groupsand manage user membership for different modules.

> ⚠ A suiteadministrator **cannot** be added to *any* custom group!

Create a Custom Group

To create a custom group, follow this procedure.

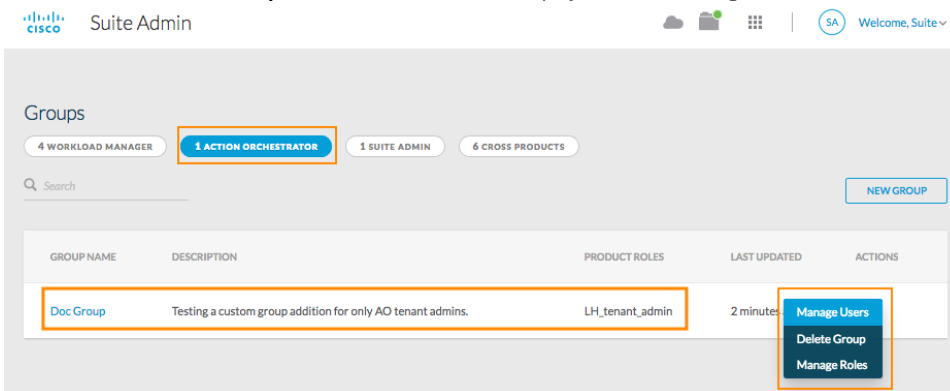1. Navigate to theSuite Admin Dashboard>**Groups**page.
2. Click **New Group**.
3. Provide a **Group Name** and **Description**.
4. Select the roles to be assigned to this group from the **Assign Roles** dropdown.

> ✅ Each CloudCenter Suite module has *default roles* provided OOB by the CloudCenter Suite. Additionally, Action Orchestrator is the only module that allows administrators to create *custom roles*. See Understand Roles for details.
>
> Custom Roles are only available for Custom groups and you can only view the **Manage Roles** action for a group's dropdown list this case. See Create and Assign Groups for details.
>
> To create a custom role, see Action Orchestrator Roles in the Cost Optimizer documentation section. Once created in the Action Orchestrator, the suite administrator can select a custom role and assign it to a custom group at any time.

5. Select the users to be added to this group from the **Associate Users** dropdown. The selected users are listed in the summary just below this field.
6. Click **Done** to save the new group. The status in the Groups list page displays the status of the custom group addition.
7. Click the Module for which you created this custom group. The following screenshot highlights the module for which a new custom group was added. As a Suite Admin user, you will also see the actionsdisplayed in the following screenshotfor this custom group.

Thesuiteadministrator can manage both the users and the roles associated with the new group as well as delete the group at will.

Deleting Custom Groups

A tenant administrator can manage custom groups for their tenant. If deleted, the users in the deleted custom group will no longer have access to any roles associated with that group. Users will not receive any warning messages or alerts about the deletion of this custom group.Once deleted, all users revert to their default permissions and groups.

OOB Suite Admin Groups

OOB Suite Admin Groups

Overview

Default out-of-box (predefined) groups provide a majority of the required functionality to module users. As such, enterprises will not need to create custom groups unless, this group is extremely specific to their environments. At each level, any CloudCenter Suite user can be assigned to one of the following predefined groups:

- Suite Level: The Suite Administrator Group
- Tenant Level: The Tenant Administrator Group
- Module Level: The Module Administrator Group

The Suite Admin Group

The Suite Admin group can execute the following roles and functions:

- User Tenant Management
- Module Lifecycle Management
- Kubernetes Cluster Management

Users in this group have access to the entire Suite Admin functionality. Additionally, if a user in this group installs a module, the default roles for that module are also assigned to this user.

The suite administrator can add any user to the Suite Admin.

The Tenant Admin Group

The Tenant Admin group can execute the roles and function for User Tenant Management **at the tenant level** (for tenant or sub-tenant, depending on permissions and ownership).

Users in this group manage all users, groups, and sub-tenants within their own tenant. Additionally, if a user in this group installs a module, the default roles for that module are also assigned to this user.

The Module Admin Group

The Module Admin group can execute the roles and function for User Tenant Management **at the module level** (not for a tenant or sub-tenant).

Users in this group have access to module-specific functionalities. A user in this group can automatically manage all users and groups for this module. For example, a workload manager admin can create a custom service and restrict that service to some users, but cannot delete or create a tenant.

Admin User Restrictions

No administrator can perform the following functions:

- Remove themselves from a default group
- Disable or delete a default group
- Reset their own password
- Create a new group with a suite administrator role

Active Directory Mapping

As a module admin, be aware that you can use SAML configuration for Active Directories to map existing enterprise users to the default Suite Admin groups or to default module group(s). See SSO Setup for additional context.

Create and Assign Groups

Create and Assign Groups

- [Overview](#)
- [The Groups List Page](#)
- [Default Suite Admin Groups](#)
- [Default Module Groups](#)
- [Assign a User to a Group](#)
- [Assign a Tenant Administrator to a Group](#)
- [Assign a Module Administrator to a Group](#)
- [Group Actions](#)

Overview

A CloudCenter Suite user must belong to at least one group to be able to view resources authorized for that group. A user without a group can only view the landing page and not be able to navigate anywhere else!

The Groups List Page

When you navigate to the Groups page from the Suite Admin Dashboard, you see a summary of configured groups at the top of the page which displays the following details:

- The total number of CloudCenter Suite groups
- The total number of Suite Admin groups
- The total number of workload manager groups
- The total number of Action Orchestrator groups
- The total number of Cost Optimizer groups
- The total number of cross-module groups groups with access to multiple CloudCenter Suite modules.

Any user who is a member of the Suite Admin, Product Admin, or Module Admin groups are identified by the admin icon attached to their profile display.

The **Groups** column identifies the groups to which each admin belongs.

The **Group Name column** displays **Default** next to each out-of-box, predefined group.

Default Suite Admin Groups

Two default groups are available to the suiteadministratorout-of-box:

- The **suiteadministrator** group
- The **tenant admin** group

Default Module Groups

When the suiteadministratorinstalls any module, additional, default out-of-box groups become available. These groups vary based on the module.

It is the responsibility of the module admins to administer andleverage the functionality of these module-level, default groups.

By installing the module, the suiteadministrator:

- Automatically inherits the module admin role.
- Can add three more module admins.

A module administratorrole allows the module admin to monitor and manage the module.

Assign a User to a Group

When you add a user to the CloudCenter Suite, you must assign the user to at least one group to ensure that the user can view resources

at a minimum. To assign a user to a group, follow this procedure.

1. Navigate to theSuite Admin Dashboard>**Users**page and verify that the user is listed in the Users page.
2. Navigate to the**Groups**page.
3. Locate and click the group to which you want to add this user.
4. Assign the newly added user to the group.

Promote a User to be a Suite Admin

A suiteadministrator can promote any user to the Suite Administrator group!

To assign a user to a group, follow the procedure listed in the *Assign a User to a Group* section above*.*

Assign a Tenant Administrator to a Group

A Tenant Administrator can promote any user to the Tenant Administrator group!

To assign a user to the Tenant Administrator group, follow the procedure listed in the *Assign a User to a Group* section above.

Assign a Module Administrator to a Group

A Module Admin can promote any user to the Module Admin group!

To assign a user to the Module Admin group, follow the procedure listed in the *Assign a User to a Group* section above.

Group Actions

On the Groups list page, the **Actions** column displays a dropdown list of actions that each group member can perform based on group membership and permissions. The list display begins with the available Suite Admin action for this group followed by the module-level actions.

The following table identifies the actions available at the Suite Level.

Suite-Level Actions	Description
Manage Users	Group members with suiteadministrator permissions and/or tenant administrator permissions for the tenant can manage user membership by associating users to this group. See Create and Manage Users for additional context.
Delete Group	
Manage Roles	This action is only visible for custom groups. It is not available for Default, predefined groups. Users with suiteadministrator or tenant administrator permissions can associate roles for each module by assigning those roles to this group. See Understand Roles for additional context.
Module-Level Actions	This is a fluid list based on which module-specific actions were made available for each tenant, user, and module. See Manage Module-Specific Content for additional details.

Create and Manage Users

Create and Manage Users

Overview

From the Suite Admin perspective, a user refers to two main roles: the suiteadministratorand the tenant administrator.

The Users List Page

When you navigate to the Users page from theSuite Admin Dashboard, you see a summary of configured users at the top of the page which displays the following details:

- The total number of CloudCenter Suite users
- The total number of Suite Admin users
- The total number of workload manager users
- The total number of Action Orchestrator users
- The total number of Cost Optimizer users
- Thetotal number ofcross-module users users who can access multiple CloudCenter Suite modules.
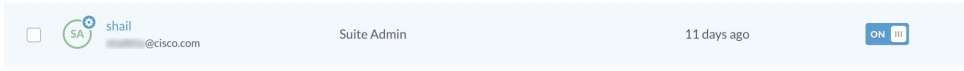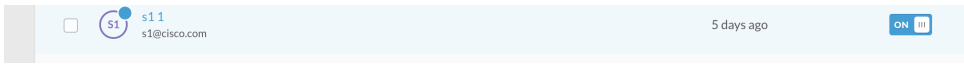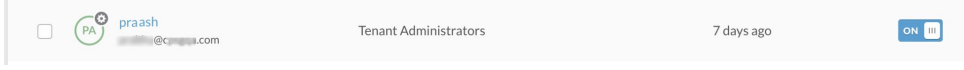
Any user who is a member of the Suite Admin, Product Admin, or Module Admin groups are identified by the admin icon (displayed in the following screenshot) attached to their profile display.

TheGroupscolumn identifies the groups to which each admin belongs.

Similarly, the icon for each user differs based on their permissions as identified in the following screenshots:

Type of %ccs User	Icon in the Suite Admin UI			
Suite Administrator	☐ (SA) shail ▓▓▓@cisco.com	Suite Admin	11 days ago	ON ⫿⫿⫿
Suite User	☐ (S1) s1 1 s1@cisco.com		5 days ago	ON ⫿⫿⫿
SSO User	☐ (PA) praash ▓▓▓@c▓▓▓▓.com	Tenant Administrators	7 days ago	ON ⫿⫿⫿

The Suite Administrator

The suiteadministrator:

- Is configured as part of the Initial Administrator Setup process.
- Is responsible for all user roles for all modules. As such, all %ccs of modules share the same user base.
- Can add other suiteadministrators.

> ⚠ Suite Administrator must exercise control over the number of suiteadministrator configured for the %ccs as they have the highest level of permissions and privileges in the %ccs!

You can add additional users in the Suite Admin or for each module beyond the OOB Suite Admin Groups. These users can be assigned to any module, group, or tenant depending on why they were added in the first place.

> ⓘ Groups have roles and depending on the group to which a user is added, that user inherits the roles associated with the assigned group.

Tenant Administrator

A user created with administrative permission at the tenant level is referred to as a *Tenant Admin.* A tenant admin does not have visibility into the Suite Admin Dashboard.

- While each user can be assigned a specific role with access to individual modules, each module also has its' own pre-defined roles and groups.
- The Suite Admin leaves it to the tenant admin to manage these roles and groups at the tenant level for each module.
- While a suiteadministrator can add unlimited tenant admins, it is better to have close control on the number of tenant admins for each module as they have the highest level of permissions and privileges for that module.

Tenant admins can perform the following tasks:

- Manage users, groups and tenants WITHIN their tenant hierarchy.
- Access modules made available for their tenant(s).
- Execute a subset of tasks as permitted by the suiteadministrator or their parent tenant.

The following image identifies a sample multi-tenant environment.
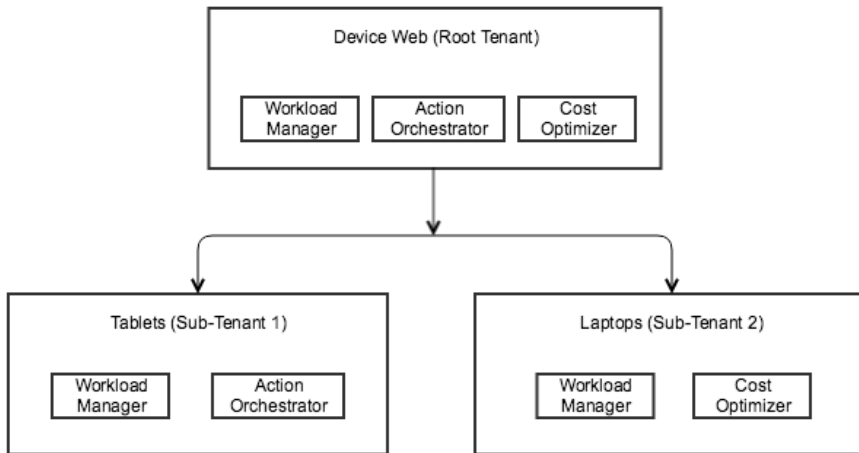
Each (sub)tenant does not have any default **suite admin** group andcannot executeModule Lifecycle Management or Kubernetes Cluster Management functions they can only executeUser Tenant Management functions at their tenant level.

Create a User

To create a %ccs user, follow this procedure.

1. Navigate to theSuite Admin Dashboard> **Users** page.
2. Click **Add User**.
3. Enter the details for this user in the Add User form.
4. *Optional.* Disable the **Auto Generate Password** switch if you prefer to provide your own password. If enabled, the system sends an email to the user with the link so the user can generate the password.

> ✅ To use this feature, you should have already configured the Base URL and the Email Setup to ensure that the URL is accessible and that an email can be sent to the user. See Base URL Configuration and Email Settings for additional details.

> ⚠️ Be sure to configure these two functions before opting to send an email to the user as this information is required to construct the links to reset the password for a new or existing user.

5. *Optional.* Provide name-value pairs for the field to be displayed and the value to be provided so the user can add more information at a later point. Some examples of name-value pair can beDesignation, Badge ID, Location, Department,Phone, and other details.
6. Select the group(s) to which this user must belong.

> ✅ A user without a group can only view the landing page and not be able to navigate anywhere else!

7. Click **Save**. The newly added user can now be added to any group.

Until you add this newly-created user to a group, this user will have no role or ability to perform any actions.

Create Another Suite Administrator

To create another suite administrator for the Suite Admin, besides the administrator created as part of the Initial Administrator Setup process, follow this procedure.

1. Follow the process above to *Create a User*.
2. Navigate to the Suite Admin Dashboard> **Groups**page.
3. Locate the suiteadministratorgroup to which you want to add this user.
4. Assign the newly added user to the suiteadministratorgroup.

This newly-assigned suiteadministratornow has all administrative abilities associated with the suiteadministratorgroup.

Create a Tenant Administrator

To create a tenant admin, follow this procedure.

1. Follow the process above to *Create a User*.
2. Navigate to the Suite Admin Dashboard>**Groups**page.
3. Locate the tenant admin group to which you want to add this user.
4. Assign the newly added user to the tenant admin group.

This newly-assigned tenant admin now has all administrative abilities associated with the tenant admin group.

Create a User with a Module-Specific Role

A module administrator refers to a user who can administer any of the %ccs modules. The suite administrator can add a user to a module-specific role to make this user a module administrator.SeeUnderstand Roles for details.

Importing User Data

To import Active Directory data, you must followa manual process toimport user data. SeeSSO Setup for additional details.

Disabled Users

Only an user administrator can disable a user. Once disabled, the user's profile updates to display this state.

User Actions

On the Users list page, the **Actions** column displays a dropdown list of actions (displayed in the following screenshot) that each user can perform based on group membership and permissions. The list display begins with the available Suite Admin action for this user followed by the module-level actions.
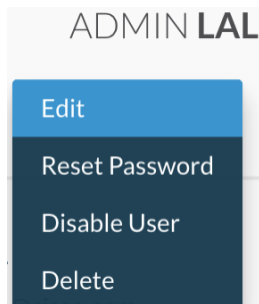
The following table identifies the actions available at the Suite Level.

Suite-Level Actions	Multi-Select Action?	Description
Edit User	No	Users with suiteadministrator permissions and/or tenant administrator permissions for this tenant can edit any user's profile by changing the first/middle/last name and email, Configure metadata details, Configure groups, Reset password, or disable the user.
Reset Password	No	
Disable /Enable User	No	Once disabled, you must first enable a user to assign the user to a group and to see other Actions for this user.
Delete User	No	As each user/tenant/sub-tenant may have a separate set of dependencies, multi-selection is not possible for this action. See the *Delete User* section below for additional details. ⚠ While this function is possible in this release, selecting multiple users to delete at the same time may lead to unpredictable consequences. Only delete one user at a time.
Impersonate User	No	A suite administrator or a tenantadministrator can temporarily sign into the %ccs as a different user. See the *Impersonate User* section below for additional details.
Manage Groups	No	Users with suiteadministrator permissions and/or tenant administrator permissions for this tenant can manage groups. See Custom Groups by Admin for additional details.

| Module-Level Actions	This is a fluid list based on which module-specific actions were made available for each tenant, user, and module. See Manage Module-Specific Content for additional details
Generate API Key	A suite administrator can generate an API key for any user. See API Key for details.

Disable/Enable User

The Enable column allows administrators to individually enable or disable %ccs users. Any user is enabled by default.

If a user deletion is in process, this user is automatically moved to the Disabled state as described in the *Delete User* section below.

Delete User

When you, as the administrator, attempt to delete a %ccs user (or tenant or sub-tenant), the Suite Admin triggers a confirmation process to verify (with each module) that the resource can be deleted. If all product modules confirm the deletion, then the user (or tenant or sub-tenant) deletion is permitted to proceed. If the resource cannot be deleted the module returns a failure message with information about associated resources.

As this process confirms with each module, the notification in the UI header continues to remain in the spinning state until the verification process is complete. This latency is based on the number of modules associated with this user. During this process, the user is placed in a disabled state (Delete Pending) until the deletion can be confirmed by all modules as displayed in the following screenshot.
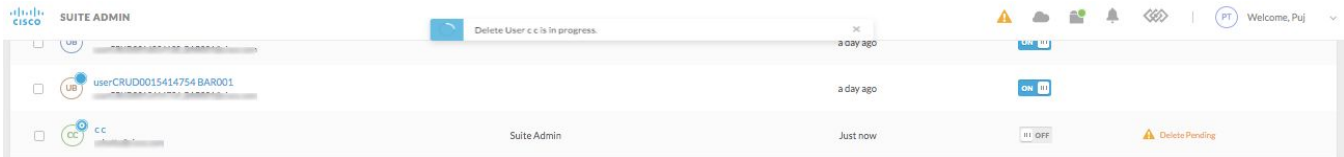
Impersonate User

User impersonation allows you to temporarily sign into any %ccs module as a different user. Suite and tenant administrators can impersonate all other users in their tenants and sub-tenants and take any action, regardless of the permission level of the user being impersonated.

There are a number of reasons why you might want to impersonate a user:

- To help another user troubleshoot an issue.
- To make changes on behalf of another user (for example, a user is away on vacation and you want to manage content managed by the user on vacation).

Restrictions

When impersonating another user, be aware of the following restrictions:

- Impersonators appear as themselves in the change history.
- You can only impersonate one user at a time.
- If the user you impersonate has permission to modify your role, you cannot modify your own %ccs role access for the duration of the impersonation.
- A tenant admin can impersonate a user within the entire sub-tenant tree this behavior supports multiple troubleshooting and content management scenarios.
- A tenant admin can not impersonate a suite admin.
- Module Admins who manage user/groups for their module(s) are not allowed to impersonate users.
- When impersonating an Admin user (who has permission to manage groups, disable user, or delete user), then these actions cannot be performed for the originally logged in user even if this user is an admin.

Logs

In the history and log files, the Tenant ID and email of the admin who impersonated a user will be displayed for the actions taken during the impersonation session.

When an administrator impersonates another user and performs any operation, the log files will display the original User ID, the impersonated User ID, and the impersonated users Tenant ID in the POD details for the corresponding service as visible in the following DEBUG snippet:

```
./common-framework-suite-idm-85dc97c79f-zjf4l:[[originalUserId=1&userId=2&tenantId=1]] 2019-07-23 19:14:39,742
DEBUG com.cisco.cpsg.idm.controller.helper.UserHelperImpl [http-nio-8080-exec-4] - product list for user 2:
[com.cisco.cpsg.prodregistry.api.v1.dto.ProductDto@77771337, com.cisco.cpsg.prodregistry.api.v1.dto.
ProductDto@2c1c70b0]
./common-framework-suite-idm-85dc97c79f-zjf4l:[[originalUserId=1&userId=2&tenantId=1]] 2019-07-23 19:14:40,161
DEBUG com.cisco.cpsg.idm.controller.helper.UserHelperImpl [http-nio-8080-exec-6] - product list for user 2:
[com.cisco.cpsg.prodregistry.api.v1.dto.ProductDto@620f9219, com.cisco.cpsg.prodregistry.api.v1.dto.
ProductDto@63c2a6be]
```

Process

To create a %ccs user, follow this procedure.

1. Navigate to theSuite Admin Dashboard and click youraccount profile dropdown and click the **Impersonate User** link (displayed in the following screenshot) to initiate the process.
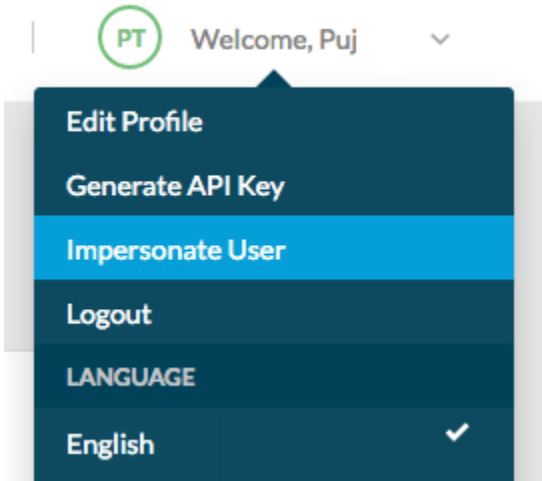
Alternately, you can navigate to the **Users** page and click the Actions dropdown (displayed in the following screenshot) for the required user.
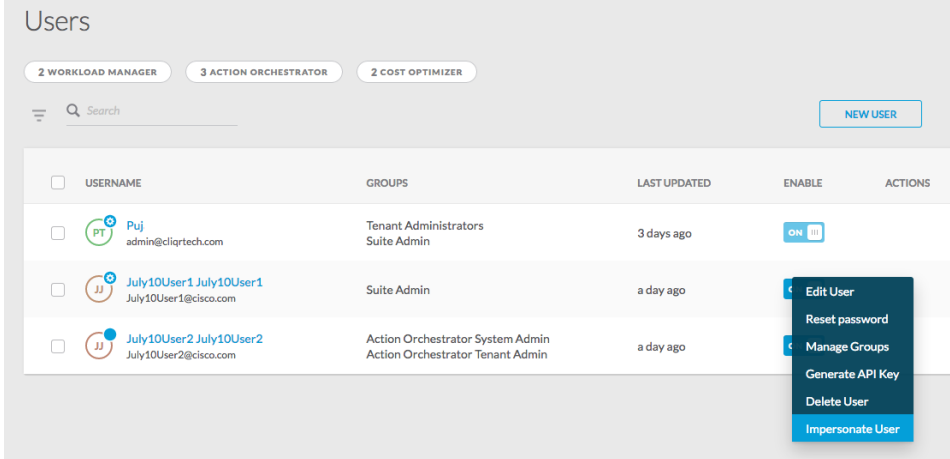
2. In the Impersonate User popup displayed in the following screenshot, enter the Tenant Login ID and email address for the user to be impersonated.

3. Click **Start** to begin the impersonation session and click **Confirm** to confirm the impersonation for this user.

4. Once you confirm, you see a new header in the UI to indicate that you are impersonating the identified user. The Last Login session details changes based on the impersonation details as displayed in the following screenshot.

You can exit the impersonation session in one of two ways:

- Click **Logout** in youraccount profile dropdown to exit the impersonation mode and log out of the Suite Admin UI.
- Click **Exit Impersonation** in the impersonation header to exit the impersonation mode and continue to work in the Suite Admin UI.

Suite Admin Dashboard

Suite Admin Dashboard

Overview

The Suite Admin Dashboard displays the following information:

- The Suite Admin to administer the Cloud Center Suite as described in Initial Administrator Setup.
- Additional modules that you can install on an as-needed basis.

Who Can Access the Suite Admin Dashboard?

The Suite Admin Dashboard is visible to suite administrators configured by the Initial Administrator.

Navigating to the Suite Admin Dashboard

To access the Dashboard, bookmark the page to ensure easy navigation. During the course of using the Suite Admin documentation, you will see instructions to *na vigate to the Suite Admin Dashboard.* This step implies that the suite administrator must access this home page to perform the remaining procedure!

Contents of the Suite Admin Dashboard

The Suite Admin Dashboard is made up of multiple panes:
- Personal Information Banner
- The header
- The left tree pane
- The main display pane
- The footer

Personal Information Banner

Effective CloudCenter 5.2.1, the following Personal Information banner is visible in the %ccs UI.

Unless you are being requested by Cisco to input your personal information, including identifiers (ie., email and contact details) to enable your use of the Cisco CloudCenter Suite features, please avoid or minimize inputting additional personal information.

While you can acknowledge and dismiss this banner by clicking the **Acknowledge** button, be aware of the following nuances:

- This banner is only visible in the Cloud Center Suite UI, not in any API call.
- If you dismiss the banner in the Suite Admin, it does not display in other modules when those are opened at a later time.
- The banner dismissal information is stored in a user's local browser storage.When a user logs in and dismisses the banner in a one browser, like Chrome from a laptop, it will not display again in Chrome on the laptop. However, it will display on another browser, like Firefox.

The Header

The %ccs uses the same header for all modules installed by the Suite Admin. As such, the following items are displayed for all modules in their respective dashboards:

Edit Profile

Your account profile is based on the user configuration setup as displayed in the following screenshot.
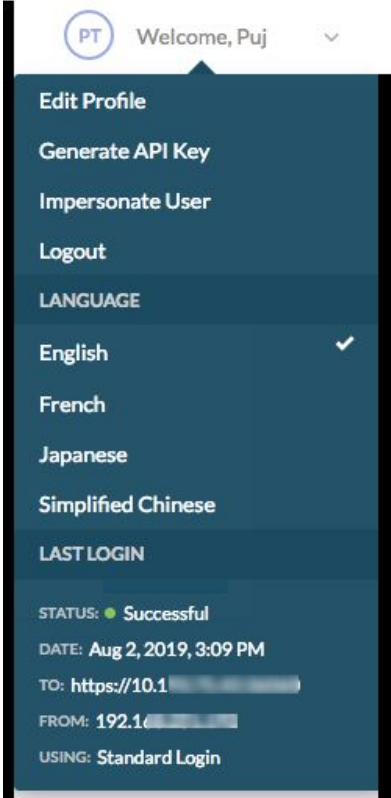

- When you click the **Profile**link, you see the profile settings based on your user level and user configuration:

    - If a user was created in the Suite Admin, then that user can edit profile details available in the Actions dropdown as displayed in the following screenshot.
    - If a user was created using SSO setup, then this SSO user cannot reset password after logging into the Cloud Center Suite.

        - SSOusers can only changing their photo in their profile page.
        - The options displayed in the above screenshots are not be available to SSO users.
- If you need an API keyto use Cloud Center Suite APIs, click **Generate API Key**. The suiteadministrator can generate/regenerate the API management key for any user within their tenant). SeeAPI Key for details.
- Besides, **English**, you have multiple language options to view the %ccs UI. SeeUI Language Availability for additional details.
- Suite Administrators:

    - Must provide the following information either with the AD setup or when adding users individually:First Name, Last Name, and Email.
    - Can configure one or more of the following details as name-value pairs or from an AD setup: Name,Designation, Location, Department, Phone, Group, Type, and other details. Once configured, users can change the details displayed in the following screenshot:
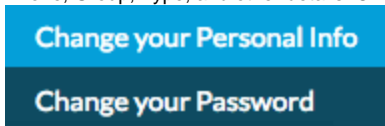
        - Personal profile information by clicking **Actions** > **Change your Personal Info**
        - User Password by clicking**Actions**>**Change your Password**

Last Login Indicator

The log session history information for each Cloud Center Suite session provides details on the last login time, the type of login, and the location (IP address) of the person logging into the session as visible in the following screenshots.
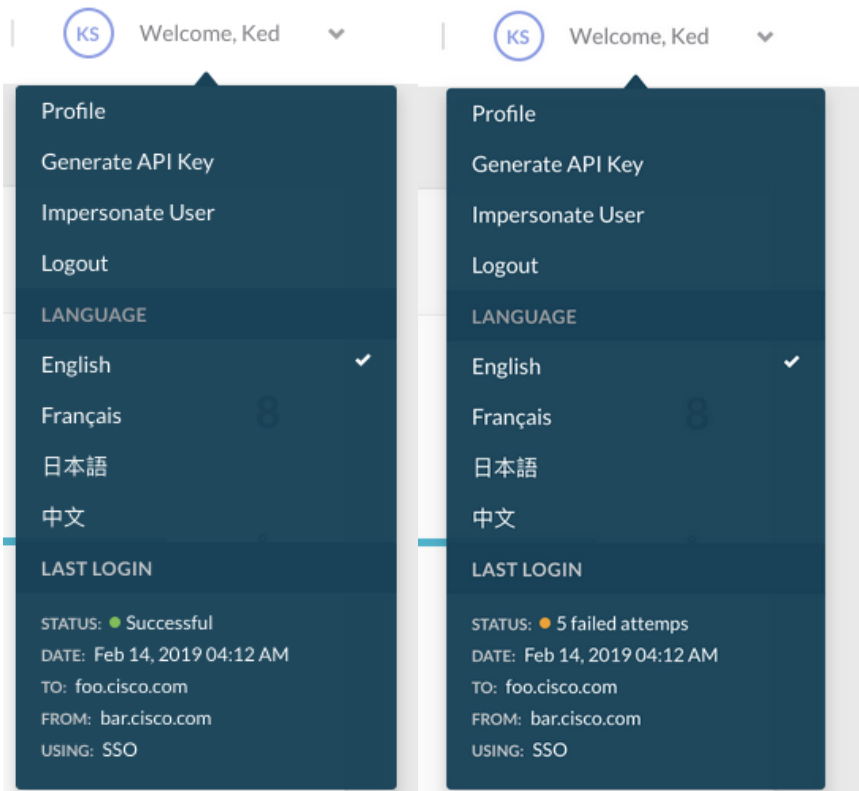
The following table identifies the last login details provided in this section.

| Field	Possible Values	Description
Status	• Successful • Failed (number of failed attempts)	The number of failed attempts provides a point of verification and allows the user to notice unauthorized use of the % ccs system at any given time. The remaining attempts are included in the number listed, but the details are only provided for the last login attempt. After 10 failed attempts, the system is locked out for 10 minutes. This user can log back in after 10 minutes.
Date	Month, day, year, and time	The full date and time format of this event is listed here.
To	The address of your %ccs system	The DNS or IP address of the Suite Admin UI.
From	The address of the person accessing your system	The DNS or IP address of the event origination endpoint.
Using	• SSO • Standard • Impersonation	This field lists the type of login. If the event was not accessed as an SSO event or an impersonation event, you see *Standard* login displayed in this field. • See SSO Setup for additional details on SSO. • See Create and Manage Users > *Impersonate User* for additional details on impersonation.

Module Navigation

To switch back and forth between the module dashboards and/or the Suite Admin dashboard as displayed in the following screenshot. SeeModule Lifecycle Management for details.
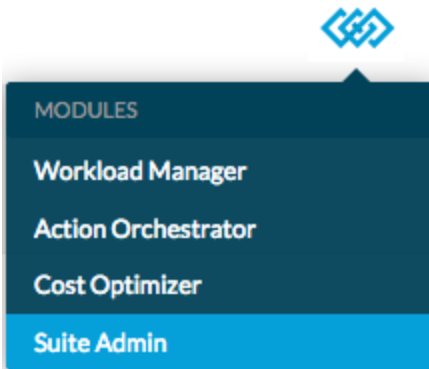
Offline Repo

After you create a VM from the OVA, you can use theVM as an offline repository server.If you set up this connection, the icon displays a green status circle as displayed in the following screenshot. SeeOffline Repository Configuration for details.
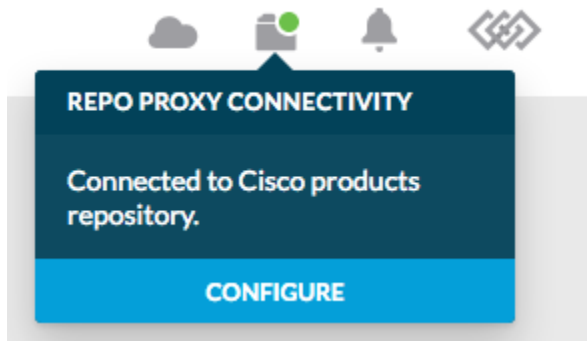
Notifications

> ⓘ This feature is available for all modules, however, the notification content feed is only triggered by the Action Orchestratorand Cost Optimizer modules.

The Notifications feature is accessible from any page and can be triggered at any time.

- If triggered (bell icon), you receive the notification stream for selective events within the module.
    - Cost Optimizer Events: For example, trend and budget alerts. See Alerts Page for a complete list of notifications.
    - Action Orchestrator Events: For example, overspending alerts. See System Elements > *Workflow Events* for details.
- Each notification contains the following details:
    - The event title.
        - Notifications are listed as an aggregation for all modules.
        - The new tab icon indicates that a new tab will be opened for that notification.
    - The event details, if available, for each event.
    - The created timestamp on each notification displays the relativetime (for example, 4 hours, 2 days, and so forth) if within 4 weeks and the absolute time (for example, August 10, 2019) if later than 4 weeks.
- An end user can view module-specific notifications based on their role and access level within the %ccs.
- The grey, bell icon displays a blue circle (displayed in the following screenshot) when unread notification(s) become available for a module.

- To view notifications, click the bell icon to open the Notifications Pane to display messages as displayed in the following screenshot. The pane, by default, displays the unread (most recent notification first) notifications tab.
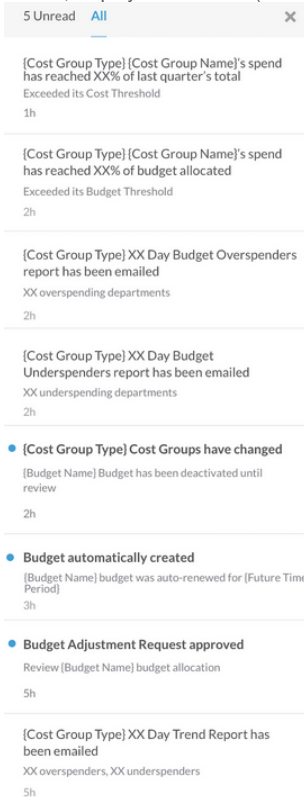
- To close the Notifications Pane click the **X** or click *outside* the pane, within the UI.

Cluster Management

The Suite Admin dashboard also lists *Cluster Management* icons and notifications. See Kubernetes Cluster Management for details.

The Tree Pane

The Tree pane is displayed to the left of your screen and displays a list of items that you can configure as the suiteadministrator. The options in the tree pane differ based on your module selection and your user level.

From this pane, the suiteadministrator for example, can perform the following tasks:

- User Management
- Group Management
- Tenant Management
- Smart License Management
- Admin Options Management

The Display Pane

The default view for the Display pane is a list of modules to administer:

- The Suite Admin Continue reading this section for additional details.
- The Workload Manager See Workload Manager 5.1 for additional details.
- The Action Orchestrator See Action Orchestrator 5.1 for additional details.
- The Cost Optimizer See Cost Optimizer 5.1 for additional details.

Each module represents your ability to install and administer each module. While the Suite Admin is not a typical module, it alerts the suiteadministrator to additional configuration capabilities.

The Footer

The footer provides links to the main Cisco website while the footer configuration defaults to Cisco, the Suite Administrator can change the following items as described in Manage Tenants>*Branding Information Tab.*

- %ccs Documentation
- Terms of Service

- Online Privacy Policy
- Trademark information
- The Cloud Center Suite being used

See the following release notes for version-specific information:

- The Cloud Center Suite release notes
- The Suite Admin Release Notes

UI Language Availability

UI LanguageAvailability

- [Overview](#)
- [Language Options](#)
- [Browser Language Detection](#)
- [Language Configuration](#)

Overview

Cisco provides *English* as the only language option for %ccs documentation.

You have multiple language options when you view the %ccs UI.

> ⓘ In %ccs 5.1.0, the UI for theinstallation process (from running the installer up to the [Initial Administrator Setup](#)) is only available in *English* you cannot change the language, not does Cisco detect your browser language at that time.
>
> The first point where you can change the language and where Cisco detects your browser language, is in the Suite Admin login page as listed in the sections below.

Language Options

Cisco provides the following language choices to view the %ccs UI:

- English
- French
- Japanese
- Simplified Chinese

Browser Language Detection

The %ccs detects your browser's language of choice and automatically displays the %ccs UI in the same language provided it is one of the language options listed in the above section.

Regardless of the detected browser language or the administrator settings at the time of %ccs installation, each end user can change the language at any time from the module to which each user has access.

Language Configuration

You can set your language of choice in one of two configuration screens:

- Administrative Level: When you configure the suite administrator. See [Initial Administrator Setup](#) > *Configure an Admin User and Tenant* for details.
- User Level: When you edit your user profile. See [Suite Admin Dashboard](#) > *The Header* for details.