CloudCenter Suite Admin 5.2 Documentation

First Published: May 9, 2020

Last Modified: January 22, 2021

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

Suite Admin 5.2 Home

CloudCenter Suite Administration Documentation

Cisco released the following Suite Admin releases:

- Suite Admin 5.2.0 released on May 9, 2020
- Suite Admin 5.2.1 released on June 8, 2020
- Suite Admin 5.2.2 released on September 4, 2020
- Suite Admin 5.2.3 released on October 13, 2020
- Suite Admin 5.2.4 released on January 22, 2021

Release Notes

Suite Admin Release Notes

- Suite Admin 5.2.4
- Suite Admin 5.2.3
- Suite Admin 5.2.2
- Suite Admin 5.2.1
- Suite Admin 5.2.0

Suite Admin 5.2.4

Suite Admin 5.2.4 Release Notes

First Published: January 28, 2021

Suite Admin 5.2.4 is available for ALL components for all supported clouds. Suite Admin 5.2.4 is a module update that uses the CloudCenter Suite 5.2.3 installers. Contact the CloudCenter Suite Support team for additional details on installers.

> Suite Admin 5.2.4 is dependent on the underlying CloudCenter Suite Kubernetes cluster which runs Version 5.2.2 or higher for private clouds. The ***underlying requirement before upgrading to Suite Admin 5.2.4*** is to ensure that the CloudCenter Suite Kubernetes cluster is Version 5.2.2 or above.
>
> If you prefer to upgrade the cluster from various previous CloudCenter Suite versions, see the Determining the Current CloudCenter Suite Kubernetes Cluster Version section provided below for additional details.

Backup and Restore

No updates

No updates

While you can update just the modules without upgrading the Kubernetes cluster, you will continue to see the new CloudCenter Suite 5.2 features for each module. See Update Module for additional details.

> - 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.
> - You must update the Suite Admin module before you update any other CloudCenter Suite module.
> - **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.**
> - You may see one or more error messages during the update process. Be aware that these messages will not affect the update itself.

See SaaS Access for FAQs on updating SaaS environments.

Public and private clouds have different cert-manager versions for CloudCenter Suite clusters. This section explains the nuances and differences.

Public Clouds and Self-Hosted Kubernetes Clusters

You must explicitly update the cert-manager on public clouds or self hosted Kubernetes clusters to **cert-manager v0.7.x or newer versions**, *but not later than v0.10.1*.

> As the upgrade process specified in the cert-manager documentation does not in Cisco's test environment, Cisco recommends the following process:

1. Ensure that you only have ONE cert-manager for the CloudCenter Suite cluster – this cert-manager ***must*** already be using the older v.0.5.x version.
2. Backup your certificate manifest file –including the CRDs and Kubernetes secrets from your current CloudCenter Suite cluster.

```
kubectl get -o yaml         --all-namespaces issuer, clusterissuer, certificates > cert-manager-backup.
yaml
```

3. Un-install the old cert-manager.

   ```
   kubectl delete crd certificates.certmanager.k8s.io  clusterissuers.certmanager.k8s.io  issuers.
   certmanager.k8s.io   --all-namespaces
   kubectl delete namespace cert-manager
   ```

4. Install the new cert-manager.

   ```
   kubectl apply -f https://github.com/jetstack/cert-manager/releases/download/v0.10.1/cert-manager.yaml
   ```

5. Restore the certificate manifest file.

   ```
   kubectl apply -f cert-manager-backup.yaml
   ```

   The CloudCenter Suite cluster should now have the required cert-manager along with the mandatory certificates for the CloudCenter Suite cluster.

Private Clouds

Private cloud environments already have the required cert-manager version or the cert-manager upgrade taken care of in the following cases:

> When moving to a later Suite Admin version, Cisco recommends that you **migrate existing CloudCenter Suite clusters to the latest cluster using the Suite Admin 5.2.3** installer ***before installing*** Suite Admin 5.2.4.

- From Suite Admin 5.0.x: Migrate from 5.0.x to 5.2.x using the backup and restore process in Suite Admin 5.2.x by using the latest Suite Admin 5.2.3 installer.
- From Suite Admin 5.1.1: This release has 2 cert-managers (v0.5.x and v0.5.7). Migrate from Suite Admin 5.1.1 to Suite Admin 5.2.x using the backup and restore process provided for the Suite Admin 5.2.3 installer.
- Effective Suite Admin 5.2.x: All releases have the required cert-managers (v0.10.1).

Suite Admin 5.2.4 provides the following certificate management features:

- Post upgrade, Helm hooks can handle x.509 certificates issues.
- A new common-framework-suite-cert-mgmt pod is introduced in this release to manually troubleshoot and renew certificates.

Prerequisite

Effective Suite Admin 5.2.4, all CloudCenter Suite clusters **must use** cert-manager v0.7.x or newer versions, but not later than v0.10.1!

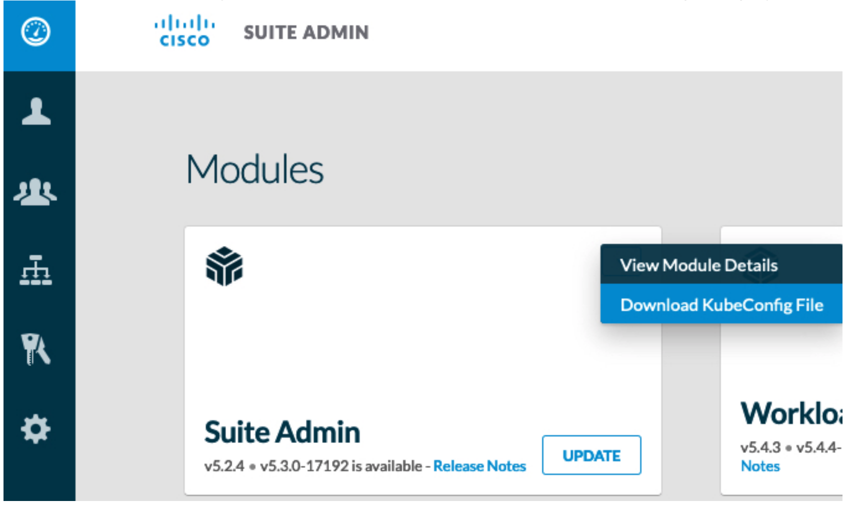
The upgrade process takes care of this certificate regeneration:

- The upgrade process disables the certificate in the **cert-manager** namespace, if there are 2 instances of cert-manager running in both **cert-manager** and **ccp** namespaces.
- The upgrade process patches the Kubernetes certificate manifests to have an accurate **duration** attribute.
- The upgrade process automatically renews the Suite Admin and/or module certificates issued by cert-manager to ensure that they have at least a 1-year validity.
- The upgrade process performs a rolling restart of the pods that consume the new certificates.

Determining the Current CloudCenter Suite Kubernetes Cluster Version

To determine the current CloudCenter Suite Kubernetes cluster version in your environment, follow this procedure.

1. Download the kubeconfig file from the current environment's Suite Admin UI (as displayed in the following UI image).



2. Run the following Shell command.

```
export KUBECONFIG=<PATH_TO_KUBECONFIG_FILE>
```

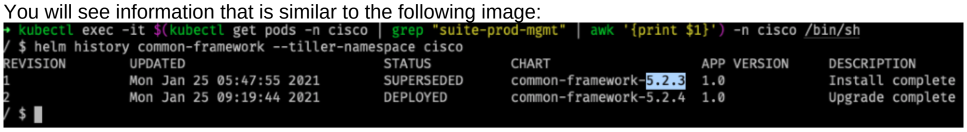
3. SSH into the suite-prod-mgmt pod using the following command.

```
kubectl exec -it $(kubectl get pods -n cisco | grep "suite-prod-mgmt" | awk '{print $1}') -n cisco /bin
/sh
```

4. Run the following command.

```
helm history common-framework --tiller-namespace cisco
```

You will see information that is similar to the following image:



```
→ kubectl exec -it $(kubectl get pods -n cisco | grep "suite-prod-mgmt" | awk '{print $1}') -n cisco /bin/sh
/ $ helm history common-framework --tiller-namespace cisco
REVISION        UPDATED                         STATUS          CHART                   APP VERSION     DESCRIPTION
1               Mon Jan 25 05:47:55 2021        SUPERSEDED      common-framework-5.2.3  1.0             Install complete
2               Mon Jan 25 09:19:44 2021        DEPLOYED        common-framework-5.2.4  1.0             Upgrade complete
/ $ █
```

Suite Admin versions are suffixed with *common-framework* under the CHART output – the oldest version displayed in this output must reflect **common-framework-5.2.3**.

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

Suite Admin 5.2.3

Suite Admin 5.2.3 Release Notes

First Published: October 13, 2020

Updated:

- December 4, 2020: Added the SaaS EOS section.
- January 22, 2021: Updated the *Documentation* section to include a list of pages that were updated.

Cisco announces the end-of-sale and end-of-life dates for the Cisco CloudCenter Suite SaaS. The last day to order the affected product(s) is May 7, 2021. Refer to https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/cloudcenter-suite/eos-eol-notice-c51-744446.html for additional details.

CloudCenter Suite 5.2.3 is available as installers for ALL components for all supported clouds. Contact the CloudCenter Suite Support team for additional details**.**

Suite Admin 5.2.3 addresses potential configuration issues observed with its' Elasticsearch component in Suite Admin 5.2.2. If you have already installed Suite Admin 5.2.2, we suggest you upgrade to this release. If you have not upgraded or installed Suite Admin 5.2.2, we suggest you directly install or upgrade to Suite Admin 5.2.3.

No updates

No updates

While you can update just the modules without upgrading the Kubernetes cluster, you will continue to see the new CloudCenter Suite 5.2 features for each module. See Update Module for additional details.

> ⚠
>
> - 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.
> - You must update the Suite Admin module before you update any other CloudCenter Suite module.
> - **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.**
> - You may see one or more error messages during the update process. Be aware that these messages will not affect the update itself.

See SaaS Access for FAQs on updating SaaS environments.

Suite Admin 5.2.3 does not support Azure cloud installation/upgrade in the CloudCenter Suite. This change is due to the new Kubernetes versions supported by Azure requiring all modules to change their installed version of Kubernetes.

The following documentation changes were implemented in CloudCenter Suite 5.2.3:

- Private Cloud (added notes to emphasis repetition for each backup)
- Public Cloud (changed the title for this page from *With Internet Access*)
- Private Cloud (changed the title for this page from *Without Internet Access*)
- End-of-Sale and End-of-Life Announcement for Cisco CloudCenter Products (added this page to replace the earlier *End of Support Notices* page)
- Backup Approach (added emphasis to specify new backups and updated the *What Data Is Backed Up?* section by adding additional Action Orchestrator Nuances for both backup and restore)
- SaaS Access (added the notification for the date when the CloudCenter Suite SaaS platform will be completely decommissioned)

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

Suite Admin 5.2.2

Suite Admin 5.2.2 Release Notes

First Published: September 4, 2020

Updated:

- September 25, 2020: Added a note to the *Updating Modules* section.
- November 18, 2020: Updated the *Documentation* section to include the list of changed pages.

CloudCenter Suite 5.2.2 is available as installers for ALL components for all supported clouds. Contact the CloudCenter Suite Support team for additional details**.**

You may see the following cert-manager error on the destination cluster during the Suite Admin restore process. However, you can ignore this error as the module data operations function as designed on the restored cluster.

```
Velero:     <none>

Cluster:  error restoring customresourcedefinitions.apiextensions.k8s.io/certificates.certmanager.k8s.io:
CustomResourceDefinition.apiextensions.k8s.io "certificates.certmanager.k8s.io" is invalid: metadata.annotations
[api-approved.kubernetes.io]: Required value: protected groups must have approval annotation "api-approved.
kubernetes.io", see https://github.com/kubernetes/enhancements/pull/1111
error restoring customresourcedefinitions.apiextensions.k8s.io/issuers.certmanager.k8s.io:
CustomResourceDefinition.apiextensions.k8s.io "issuers.certmanager.k8s.io" is invalid: metadata.annotations[api-
approved.kubernetes.io]: Required value: protected groups must have approval annotation "api-approved.
kubernetes.io", see https://github.com/kubernetes/enhancements/pull/1111
```

Kubernetes Cluster Upgrade

No updates

If you have already updated the module to Suite Admin 5.2.2, contact the CloudCenter Suite Support team for assistance with applying a required configuration change.

While you can update just the modules without upgrading the Kubernetes cluster, you will continue to see the new CloudCenter Suite 5.2 features for each module. See Update Module for additional details.

- 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.
- You must update the Suite Admin module before you update any other CloudCenter Suite module.
- **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.**
- You may see one or more error messages during the update process. Be aware that these messages will not affect the update itself.

See SaaS Access for FAQs on updating SaaS environments.

The 30-day trial is a limited program that ends on September 30, 2020. Contact a Cisco sales representative for additional details.

Cisco supports the corresponding Kubernetes engine (or managed services) for the following public clouds for the CloudCenter Suite:

- Amazon Elastic Container Service for Kubernetes (Amazon EKS)
- Google Kubernetes Engine (GKE)
- Azure Kubernetes Service (AKS)

Cisco supports the following private clouds for the CloudCenter Suite:

- VMware vSphere 6.5
- OpenStack Queens

See the Installer Overview for additional details.

Effective CloudCenter 5.2.2, two additional, optional fields are available to provide the From email address and and the From alias details to enable SMTP authentication in the Email Setup page. See Email Settings for additional details.

As part of our Security Hardening process, the Suite Admin software now uses the versions listed in the Open Source Matrix (see https://www.cisco.com/c/en/us/about/legal/open-source-documentation-responsive.html#~documentation) for the following applications: Alpine, Curator, Elasticsearch, Grafana, and FluentD.

The following documentation changes were implemented in CloudCenter Suite 5.2.2:

- SaaS Access (added the limited trial program note for the 30-day trial)
- Private Cloud (updated scripts for technical accuracy and added a note to Step 10)
- OpenStack Upgrade (updated the first screenshot and removed steps for technical accuracy)
- VMware vSphere Upgrade (updated the first screenshot and removed steps for technical accuracy)
- Upgrade Approach (updated the first screenshot)
- Updated the following pages to reflect the Action Orchestrator backup/restore additions:
  - Private Cloud (added the Action Orchestrator-Specific Post-Restore Procedure section)
  - Backup Approach (updated the What Data Is Backed Up? section)
- Backup (emphasized backup only being available for new CloudCenter Suite clusters)

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

Suite Admin 5.2.1

Suite Admin 5.2.1 Release Notes

First Published: June 8, 2020

Updated:

- June 17, 2020: Added the *Documentation* section to include a list of pages that were updated.
- June 23, 2020: Added details about the Personal Information banner in the CloudCenter Suite UI section.
- July 21, 2020: Updated the *Documentation* section to include a list of pages that were updated.
- August 4, 2020: Removed references to SaaS EU from the entire site.
- August 26, 2020: Added the *Limited Trial Program* section.

CloudCenter Suite 5.2.1 is available as installers for ALL components for all supported clouds. Contact the CloudCenter Suite Support team for additional details**.**

No updates

No updates

While you can update just the modules without upgrading the Kubernetes cluster, you will continue to see the new CloudCenter Suite 5.2 features for each module. See Update Module for additional details.

- 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.
- You must update the Suite Admin module before you update any other CloudCenter Suite module.
- **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.**
- You may see one or more error messages during the update process. Be aware that these messages will not affect the update itself.

See SaaS Access for FAQs on updating SaaS environments.

The 30-day trial is a limited program that ends on September 30, 2020. Contact a Cisco sales representative for additional details.

SA 5.2.1 includes enhancements to address Personally Identifiable Information (PII) requirements in SaaS environments.

Effective CloudCenter 5.2.1, the following Personal Information banner is visible in the CloudCenter Suite 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.

You can acknowledge and dismiss this banner by clicking the **Acknowledge** button. See Suite Admin Dashboard for additional details.

The following documentation changes were implemented in CloudCenter Suite 5.2.1:

- Private Cloud (updated for technical accuracy in the scripts and added use case to use Minio for backup/restore to new cluster when CloudCenter Suite cluster is online)
- Restore without Proxy (updated the Cloud Remote procedure to include the Scenario 4)
- Restore with Proxy (updated the Cloud Remote procedure to include the Scenario 4)
- Monitor Modules (setup email alerts in Grafana)
- SaaS Access (removed references to SaaS EU)

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

Suite Admin 5.2.0

Suite Admin 5.2.0 Release Notes

First Published: July 13, 2020

Updated:

- September 23, 2020: Updated the *Documentation* section to include a list of pages that were updated.
- September 24, 2020: Updated the *Installation* section to include the sub-folder configuration and allowed URL changes.

CloudCenter Suite 5.2.0 is available as installers for ALL components for all supported clouds. Contact the CloudCenter Suite Support team for additional details**.**

VMware Sub-folder Behavior

While the following behavior applies to VMware environments using CloudCenter Suite 5.2.1 and earlier versions:

- You **MUST** select an installation folder, however do **NOT** select a sub-folder.
- Select the same Datacenter Cluster or Host as the Suite Installer.
- The Suite Installer does **NOT** support Datastore Clusters.

Effective %5.2.2, CloudCenter Suite supports the following changes for VMware environments:

- VMware environments can configure Clusters, DataStores, and/or Networks under a sub-folder. For example, sub-folder/Cluster , sub-folder /Datastore , sub-folder/Network
- You can install a CloudCenter Suite cluster under any sub-folder
- See VMware vSphere Installation for additional details.

This is a change!

Allowed URLs

In CloudCenter Suite 5.1 and earlier, if your environment has strict URL rules that redirects (for example, using a shorter URL that redirects to https://storage.googleapis.com) the configured URL, you may not be able to complete the installation as these kind of redirects may not be allowed if you have installed the repository in an offline cluster. As the offline solution is not completely air gapped in CloudCenter Suite 5.0 and 5.1, you must added these URLs to your allowed lists behind the firewall so you can access these sites.

While CloudCenter Suite 5.2 offers a completely air gapped environment, your CCS cluster will require access to the URLs in the above table if your internet access is via a proxy environment. However, as the offline solution is a completely air gapped environment and you do not need to adds URLs to your acceptable list of URLs when using the Air Gap Installation approach. *This is a change!*

See VMware vSphere Installation for additional details.

CloudCenter Suite 5.2.0 supports installation of the CloudCenter Suite in environments that do not have an internet connection (equivalent of an isolated network). While ***Air Gap Installation*** *r*efers to the feature*,* ***Offline Repository*** refers to the delivery mechanism for the Air Gap Installation feature.

Effective CloudCenter Suite 5.2, the CloudCenter Suite installer exchanges certificates and host information with the offline repository as soon as the installer in launched, it connects to the offline repository VM (equivalent of an isolated network). After the cluster is launched, you can update the offline appliance at any point and then install modules through the CloudCenter Suite cluster

See Air Gap Installation for additional details.

No updates

While you can update just the modules without upgrading the Kubernetes cluster, you will continue to see the new CloudCenter Suite 5.2 features for each module. See Update Module for additional details.

> ⚠
>
> - 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.
> - You must update the Suite Admin module before you update any other CloudCenter Suite module.
> - **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.**
> - You may see one or more error messages during the update process. Be aware that these messages will not affect the update itself.

See SaaS Access for FAQs on updating SaaS environments.

No updates

The following cloud details were changed for each cloud:

- **Amazon EKS:**
  - Maximum Supported Version: EKS Version 1.15.10 and earlier
  - Additional Permissions Required: add permission AmazonSSMFullAccess
  - See Amazon EKS Installation and Amazon EKS Upgrade for additional details
- **Azure AKS:**
  - Maximum Supported Version: AKS Version 1.15.10 and earlier
  - See Azure AKS Installation and Azure AKS Upgrade for additional details
- **Google GKE:**
  - Maximum Supported Version: GKE Version 1.15.10 and earlier
  - See Google GKE Installation and Google GKE Upgrade for additional details
- **Existing Clusters**:
  - Kubernetes Version: The existing Kubernetes cluster must be of Version v1.13.0 and later
  - See Existing Cluster Installation for additional details

No updates

No updates

No updates

No updates

No updates

No updates

No updates

No updates.

No updates

This section summarizes the new and updated API calls and parameters.

New API Calls

The following new APIs were introduced in CloudCenter Suite 5.2.0:

- **Verify the SMTP Connection**
  - GET /api/v1/smtpConfig/current
  - Verifies if the current SMTP config is effective, and also performs an optional connection check.
  - See Email Service API Calls 5.2.0 for additional details.
- **Verify the Validity of the Tenant Login ID**
  - PUT /api/v1/tenants/validity/tenantLoginId
  - Checks the validity of a new tenantLoginId
  - See IDM Service API Calls 5.2.0 for additional details.

Updated API Calls

The following API calls were updated in CloudCenter Suite 5.2.0:

- **New smtpConfigured Parameter:**
    - POST /api/v1/smtpConfig/testConnection
    - When testing the SMTP connection, a new **smtpConfigured** parameter is displayed if SMTP is configured.
    - See Email Service API Calls 5.2.0 for additional details.
- **The tenantName parameter is modified to be a unique, alphanumeric Tenant ID:**
    - View the tenant hierarchy – GET /api/v1/admin/tenant_hierarchy
    - Get current user information – GET /api/v1/currentUser/userInfo
    - Create a tenant – POST /api/v1/tenants
    - Create a tenant with a tenantAdmin user – POST /api/v1/tenantWithAdmin
    - Return the requested tenant – GET /api/v1/tenants/{tenantId}
    - Update a tenant – PUT /api/v1/tenants/{tenantId}
    - Get information for an user – GET` /api/v1/users/{userId}/userInfo
    - See IDM Service API Calls 5.2.0 for additional details.

The following documentation changes were implemented in CloudCenter Suite 5.2.0:

- Prepare Infrastructure (updated to include Action Orchestrator 5.2 infrastructure resource requirements)
- VMware vSphere Installation (added details to ensure communication to cluster from datastore)
- Air Gap Installation (added a note relating to admin password change)
- Upgrade Offline Repository (added this section)
- Install Module (added a note on the Action Orchestrator installation and added a procedure for offline upgrade for Action Orchestrator)
- Restore without Proxy (updated the Cloud Remote procedure to include the Scenario 4)
- Restore with Proxy (updated the Cloud Remote procedure to include the Scenario 4)
- Monitor Modules (setup email alerts in Grafana)
- Private Cloud (added use case to use Minio for backup/restore to new cluster when CloudCenter Suite cluster is online, updated scripts to be technically accurate)
- VMware vSphere Appliance Setup (clarified the need to use a unique ID in Step 10 by adding a note)

CloudCenter Suite 5.2.0 has the following known issue:

- When deploying CloudCenter Suite, the installer and the target cluster must reside in the main datacenter folder, and not in any sub-folder within the main folder as the installation will not complete. This issue does not have a workaround and you will need to restart the installation if you encounter this issue.

CloudCenter Suite 5.2.0 has the following resolved issue:

- **CSCvs33223**: When CloudCenter Suite is installed using Static IP allocation, 2 services are not coming up in Workload Manager.
  Resolution: When CloudCenter Suite 5.2.0 is installed using Static IP allocation, the two services are coming up fine, you do not need an additional workaround in either Workload Manager or Cost Optimizer when you add a Workload Manager cloud and cloud account.

UI Language Availability

UI Language Availability

Cisco provides *English* as the only language option for CloudCenter Suite documentation.

You have multiple language options when you view the CloudCenter Suite UI.

> In CloudCenter Suite 5.1.0, the UI for the installation 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.

Cisco provides the following language choices to view the CloudCenter Suite UI:

- English
- French
- Japanese
- Simplified Chinese

The CloudCenter Suite detects your browser's language of choice and automatically displays the CloudCenter Suite 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 CloudCenter Suite installation, each end user can change the language at any time from the module to which each user has access.

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.

Suite Admin Dashboard

Suite Admin Dashboard

The Suite Admin Dashboard displays the following information:

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

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

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 *navigate to the Suite Admin Dashboard*. This step implies that the suite administrator must access this home page to perform the remaining procedure!

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

Effective CloudCenter 5.2.1, the following Personal Information banner is visible in the CloudCenter Suite 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.

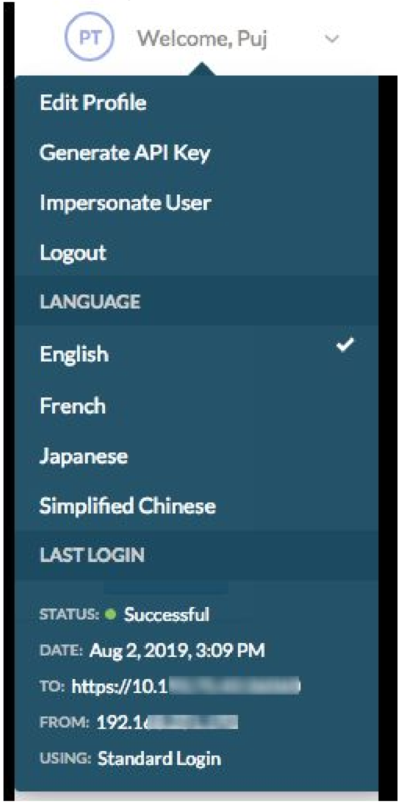
While you can acknowledge and dismiss this banner by clicking the **Acknowledge** button, be aware of the following nuances:

- This banner is only visible in the CloudCenter 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 CloudCenter Suite 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.



STATUS: ● Successful

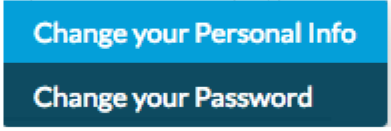
DATE: Aug 2, 2019, 3:09 PM

TO: https://10.1[redacted]

FROM: 192.1[redacted]

USING: Standard Login

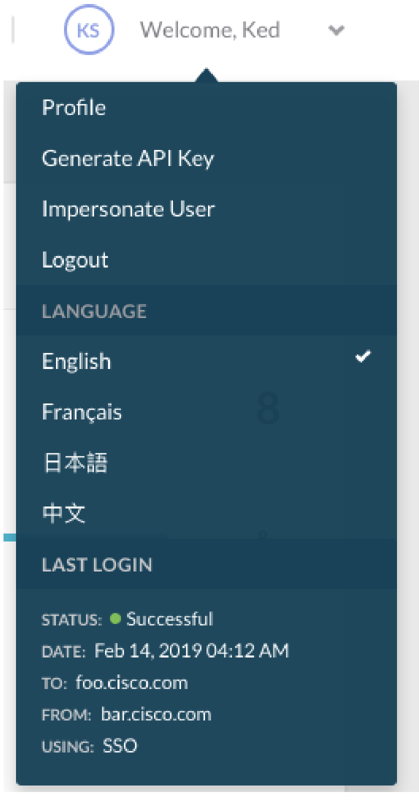
- When you click the **Profile** link, you see the profile settings based on your user level and user configuration:
  - If a user was created in the Suite Admin, then that user can edit profile details available in the Actions dropdown as displayed in the following screenshot.
  - If a user was created using SSO setup, then this SSO user cannot reset password after logging into the CloudCenter Suite.
    - SSO users 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 key* to use CloudCenter Suite APIs, click **Generate API Key**. The suite administrator can generate/regenerate the API management key for any user within their tenant). See API Key for details.
- Besides, **English**, you have multiple language options to view the CloudCenter Suite UI. See UI 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:



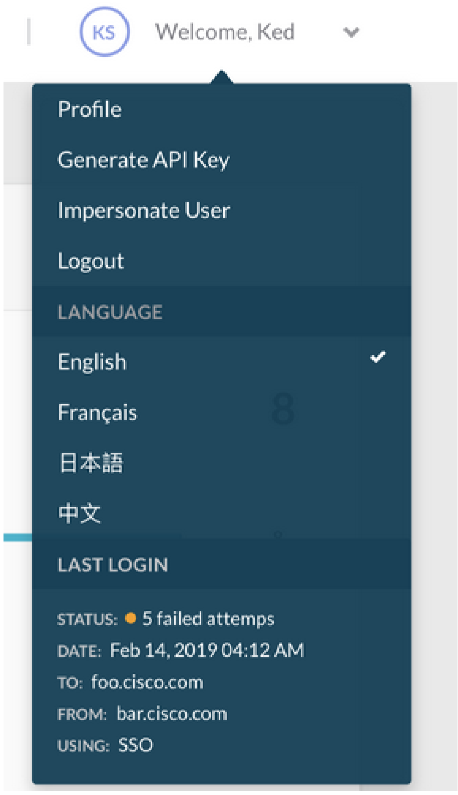
    - Personal profile information by clicking **Actions** > **Change your Personal Info**
    - User Password by clicking **Actions** > **Change your Password**

Last Login Indicator

The log session history information for each CloudCenter 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.



STATUS: ● Successful
DATE: Feb 14, 2019 04:12 AM
TO: foo.cisco.com
FROM: bar.cisco.com
USING: SSO



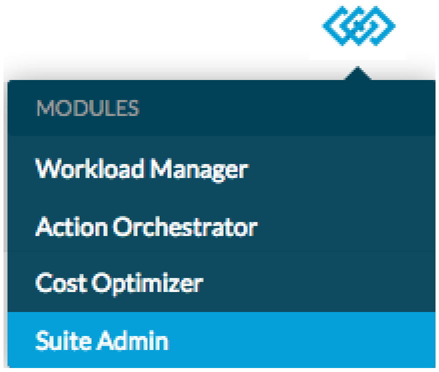
STATUS: ● 5 failed attemps
DATE: Feb 14, 2019 04:12 AM
TO: foo.cisco.com
FROM: bar.cisco.com
USING: SSO

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 CloudCenter Suite 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 CloudCenter Suite 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.

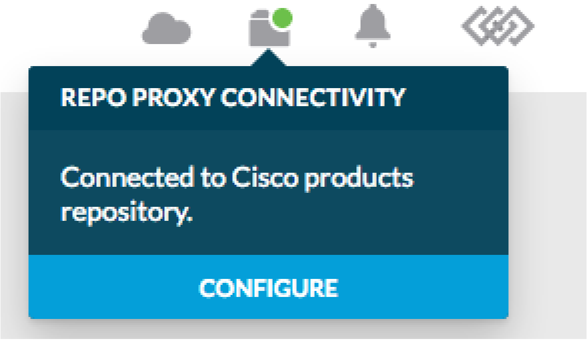
Module Navigation

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



Offline Repo

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



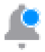
Connected to Cisco products repository.

Notifications

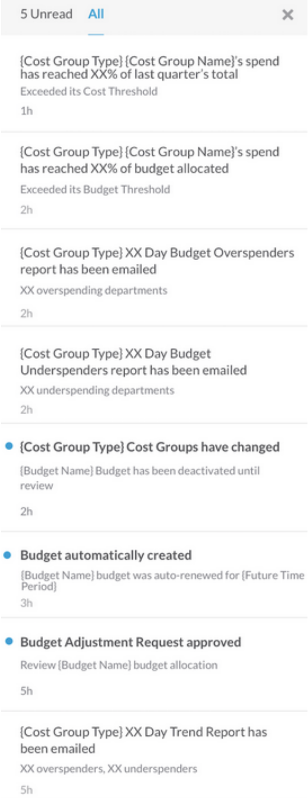
> This feature is available for all modules, however, the notification content feed is only triggered by the Action Orchestrator and Cost Optimizer modules.

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 relative time (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 CloudCenter Suite.
- 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.



{Cost Group Type} {Cost Group Name}'s spend has reached XX% of last quarter's total
Exceeded its Cost Threshold
1h

{Cost Group Type} {Cost Group Name}'s spend has reached XX% of budget allocated
Exceeded its Budget Threshold
2h

{Cost Group Type} XX Day Budget Overspenders report has been emailed
XX overspending departments
2h

{Cost Group Type} XX Day Budget Underspenders report has been emailed
XX underspending departments
2h

● {Cost Group Type} Cost Groups have changed
{Budget Name} Budget has been deactivated until review
2h

● Budget automatically created
{Budget Name} budget was auto-renewed for {Future Time Period}
3h

● Budget Adjustment Request approved
Review {Budget Name} budget allocation
5h

{Cost Group Type} XX Day Trend Report has been emailed
XX overspenders, XX underspenders
5h

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

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

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

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 5.1for 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 suite administrator to additional configuration capabilities.

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.*

- CloudCenter Suite Documentation
- Terms of Service
- Online Privacy Policy
- Trademark information
- The CloudCenter Suite being used

See the following release notes for version-specific information:

- The CloudCenter Suite release notes
- The Suite Admin Release Notes

User Tenant Management

User Tenant Management

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

Create and Manage Users

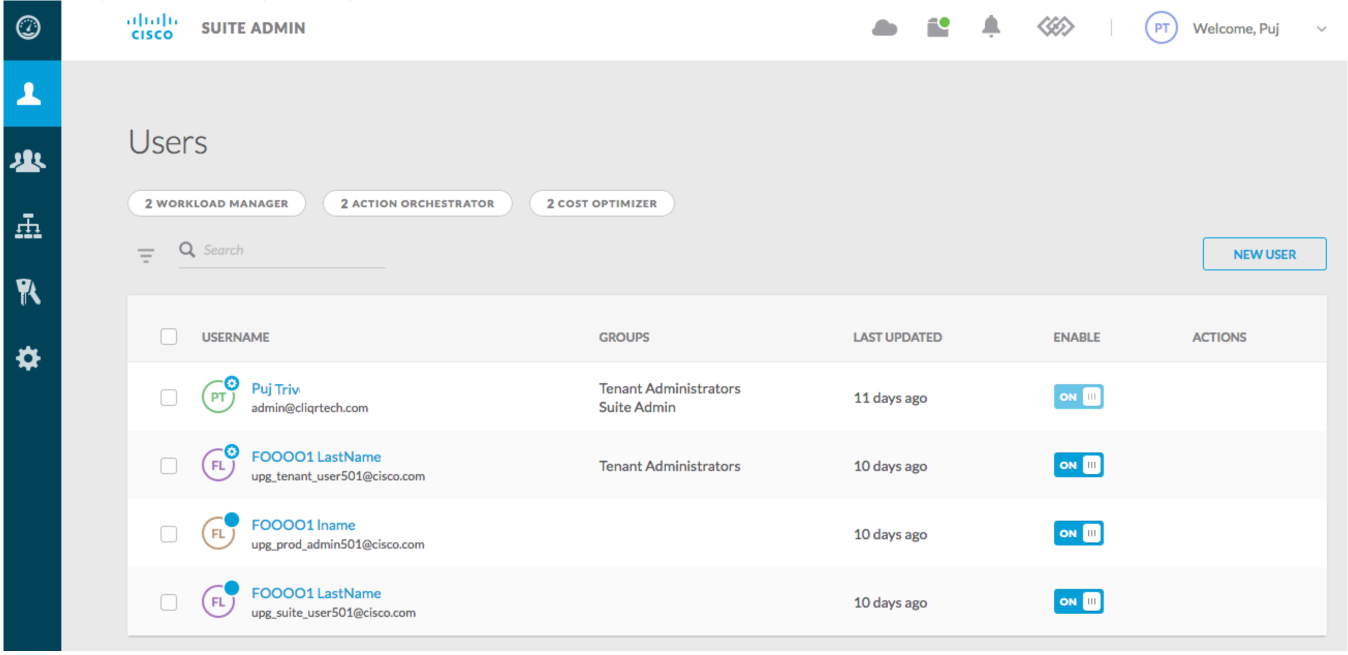
Create and Manage Users

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

When you navigate to the Users page from the Suite 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
- The total number of cross-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.

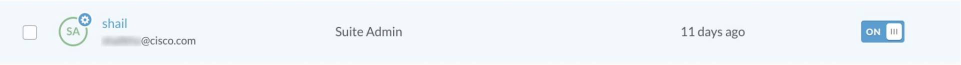
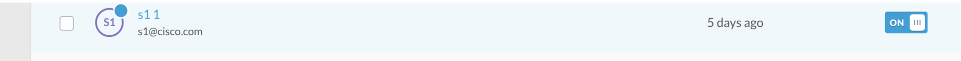


USERNAME	GROUPS	LAST UPDATED	ENABLE	ACTIONS
Puj Triv admin@cliqrtech.com	Tenant Administrators Suite Admin	11 days ago	ON	
FOOOO1 LastName upg_tenant_user501@cisco.com	Tenant Administrators	10 days ago	ON	
FOOOO1 lname upg_prod_admin501@cisco.com		10 days ago	ON	
FOOOO1 LastName upg_suite_user501@cisco.com		10 days ago	ON	

The **Groups** column 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 CloudCenter Suite User	Icon in the Suite Admin UI

Suite Administrator	 □ SA shail [redacted]@cisco.com Suite Admin 11 days ago ON
Suite User	 □ S1 s1 1 s1@cisco.com 5 days ago ON
SSO User	

The suite administrator:

- Is configured as part of the Initial Administrator Setup process.
- Is responsible for all user roles for all modules. As such, all CloudCenter Suite of modules share the same user base.
- Can add other suite administrators.

> Suite Administrator must exercise control over the number of suite administrator configured for the CloudCenter Suite as they have the highest level of permissions and privileges in the CloudCenter Suite!

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

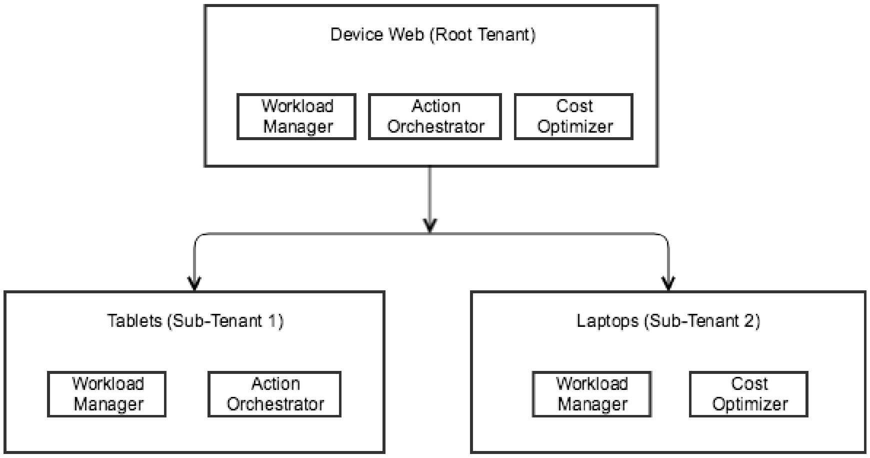
A user created with administrative permission at the tenant level is referred to as a *Tenant Admin*. A tenant admin does not have visibility into the Suite Admin Dashboard.

- 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 suite administrator 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 suite administrator or their parent tenant.

The following image identifies a sample multi-tenant environment.



Each (sub)tenant does not have any default **suite admin** group and cannot execute Module Lifecycle Management or Kubernetes Cluster Management functions – they can only execute User Tenant Management functions at their tenant level.

To create a CloudCenter Suite user, follow this procedure.

1. Navigate to the Suite 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 be Designation, 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.

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 suite administrator group to which you want to add this user.
4. Assign the newly added user to the suite administrator group.

This newly-assigned suite administrator now has all administrative abilities associated with the suite administrator group.

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.

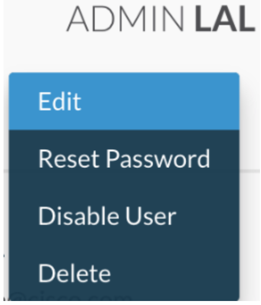
This newly-assigned tenant admin now has all administrative abilities associated with the tenant admin group.

A module administrator refers to a user who can administer any of the CloudCenter Suite modules. The suite administrator can add a user to a module-specific role to make this user a module administrator. See Understand Roles for details.

To import Active Directory data, you must follow a manual process to import user data. See SSO Setup for additional details.

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

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.

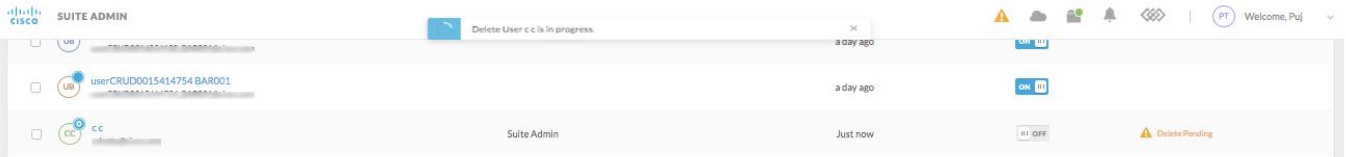
Suite-Level Actions	Multi-Select Action?	Description
Edit User	No	Users with suite administrator permissions and/or tenant administrator permissions for this tenant can edit any user's profile by changing the first/middle/last name and email, Configure metadata details, Configure groups, Reset password, 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 tenant administrator can temporarily sign into the CloudCenter Suite as a different user. See the *Impersonate User* section below for additional details.
Manage Groups	No	Users with suite administrator 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.	

The Enable column allows administrators to individually enable or disable CloudCenter Suite 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.

When you, as the administrator, attempt to delete a CloudCenter Suite 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.



Delete User c c is in progress.

□	UB [redacted]		a day ago	ON	
□	UB userCRUD0015414754 BAR001 [redacted]		a day ago	ON	
□	CC c c [redacted]	Suite Admin	Just now	OFF	⚠ Delete Pending

User impersonation allows you to temporarily sign into any CloudCenter Suite 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 CloudCenter Suite 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.

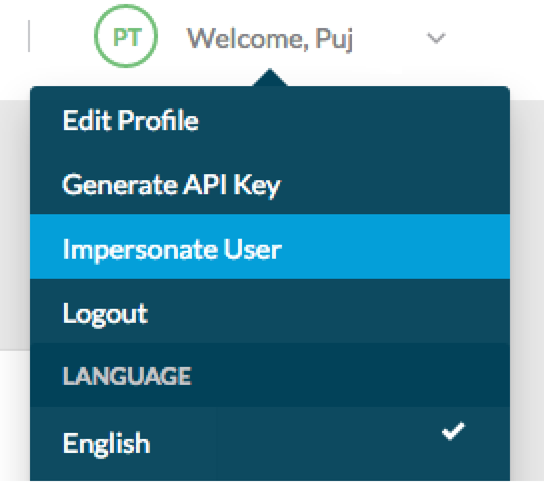
When an administrator impersonates another user and performs any operation, the log files will display the original User ID, the impersonated User ID, and the impersonated user's Tenant ID in the POD details for the corresponding service as visible in the following DEBUG snippet:

```
./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]
```

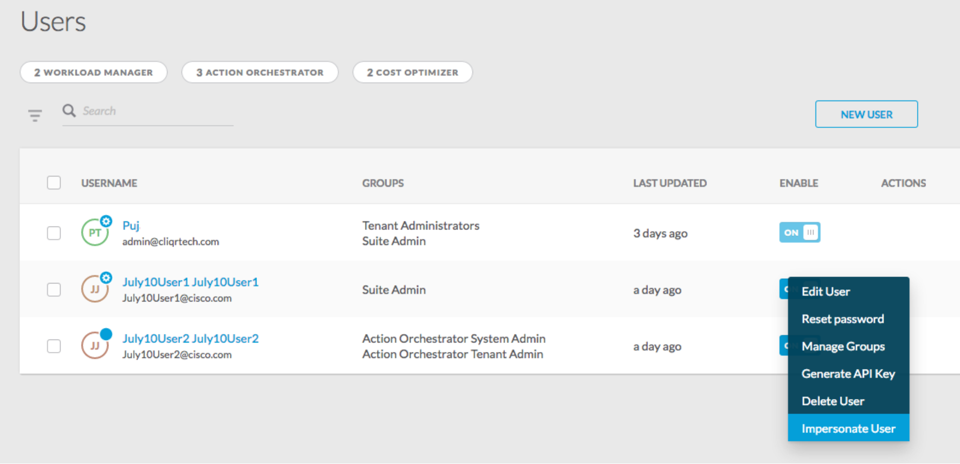
Process

To create a CloudCenter Suite user, follow this procedure.

1. Navigate to the Suite Admin Dashboard and click your account profile dropdown and click the **Impersonate User** link (displayed in the following screenshot) to initiate the process.

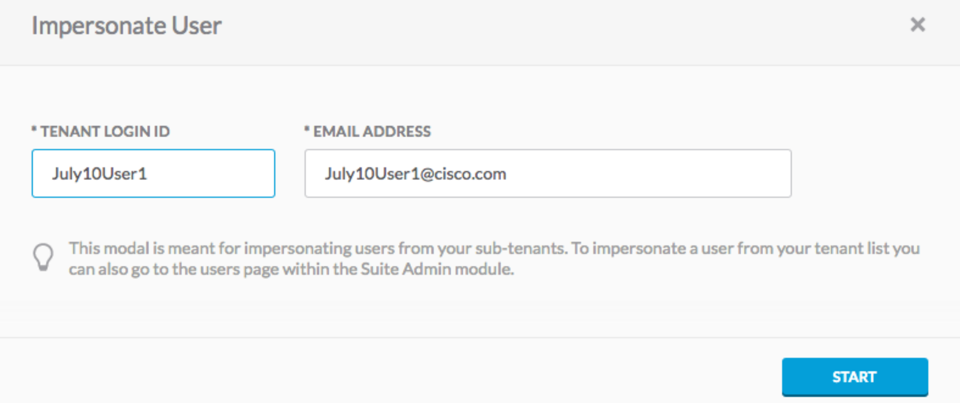


Alternately, you can navigate to the **Users** page and click the Actions dropdown (displayed in the following screenshot) for the required user.



□	USERNAME	GROUPS	LAST UPDATED	ENABLE	ACTIONS
□	Puj admin@cliqrtech.com	Tenant Administrators Suite Admin	3 days ago	ON	
□	July10User1 July10User1 July10User1@cisco.com	Suite Admin	a day ago		
□	July10User2 July10User2 July10User2@cisco.com	Action Orchestrator System Admin Action Orchestrator Tenant Admin	a day ago		

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.



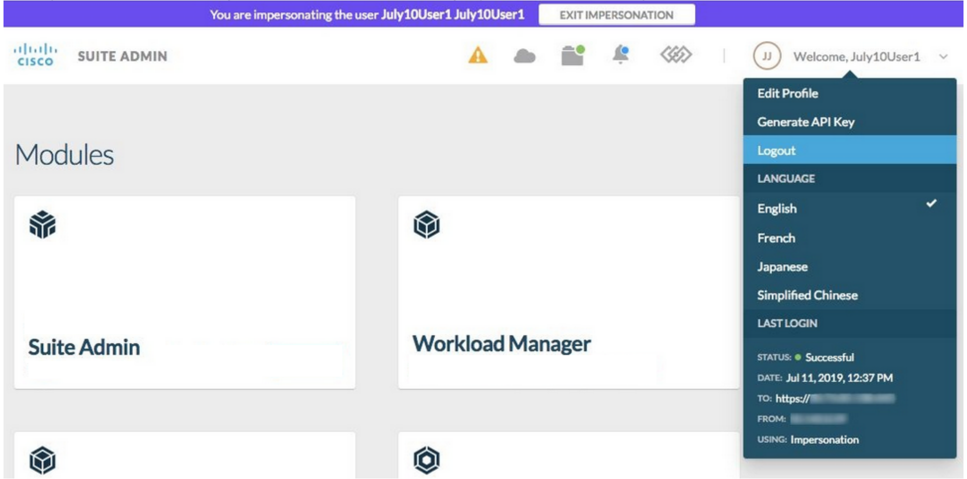
Impersonate User

* TENANT LOGIN ID: July10User1

* EMAIL ADDRESS: July10User1@cisco.com

This modal is meant for impersonating users from your sub-tenants. To impersonate a user from your tenant list you can also go to the users page within the Suite Admin module.

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 are impersonating the user July10User1 July10User1

Welcome, July10User1

LAST LOGIN

STATUS: ● Successful

DATE: Jul 11, 2019, 12:37 PM

TO: https://[redacted]

FROM: [redacted]

USING: Impersonation

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

- Click **Logout** in your account 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.

Create and Assign Groups

Create and Assign Groups

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!

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.

Two default groups are available to the suite administrator out-of-box:

- The **suite administrator** group
- The **tenant admin** group

When the suite administrator installs 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 and leverage the functionality of these module-level, default groups.

By installing the module, the suite administrator:

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

A module administrator role allows the module admin to monitor and manage the module.

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 the Suite 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 suite administrator 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.

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.

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.

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 suite administrator 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 suite administrator 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.

OOB Suite Admin Groups

OOB Suite Admin Groups

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 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 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 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.

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

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.

Custom Groups by Admin

Custom Groups by Admin

- Overview
- Create a Custom Group
- Deleting Custom Groups

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

A suite administrator **cannot** be added to *any* custom group!

To create a custom group, follow this procedure.

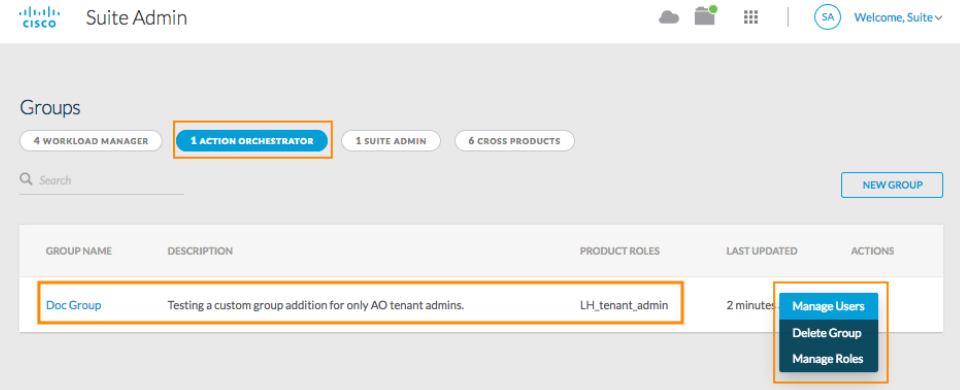
1. Navigate to the Suite Admin Dashboard > **Groups** page.
2. Click **New Group**.
3. Provide a **Group Name** and **Description**.
4. Select the roles to be assigned to this group from the **Assign Roles** dropdown.

   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 actions displayed in the following screenshot for this custom group.



GROUP NAME	DESCRIPTION	PRODUCT ROLES	LAST UPDATED	ACTIONS
Doc Group	Testing a custom group addition for only AO tenant admins.	LH_tenant_admin	2 minutes	

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

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.

Understand Roles

Understand Roles

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 actions permitted 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 on tenant association, module restriction, and user level (see Understand User Levels).

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 with user groups. Coupled with permissions and Access 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. Only the Action Orchestrator allows custom role creation.

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

See Action Orchestrator Roles for content specific to the Action Orchestrator at the tenant level.

Predefined, default roles are 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 module is a fluid list that is created and made available for each tenant or user within the module.

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.

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

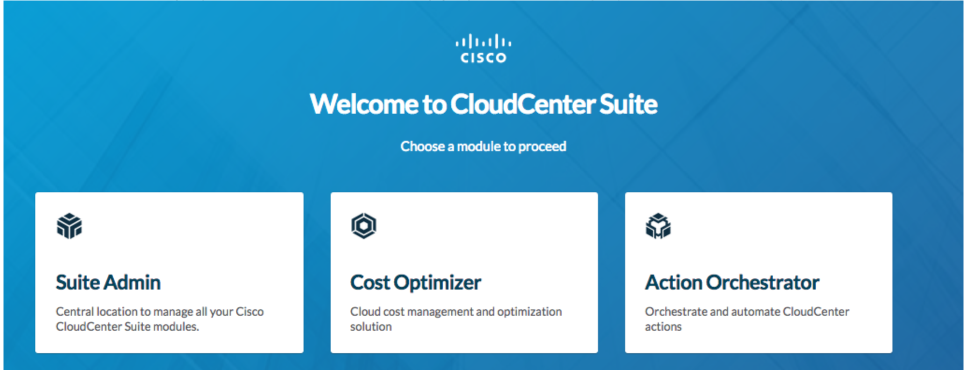
Understand User Levels

Understand User Levels

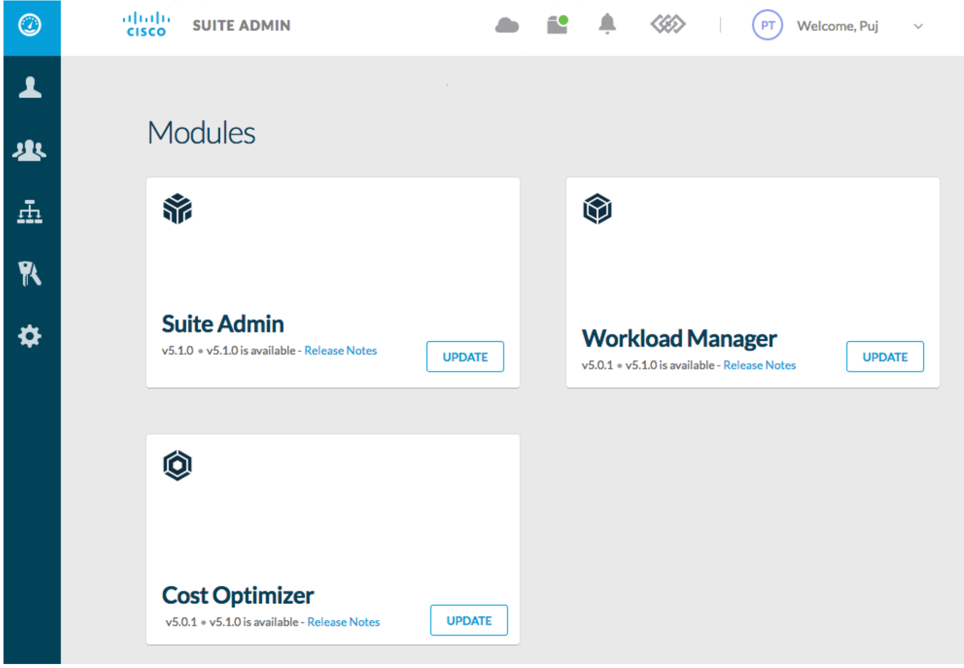
The term *user level* refers to the user's permission level. Each user level requires explicit permissions to perform specific tasks at the suite level, the cluster level, the module level, the tenant level, or the sub-tenant level.

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:

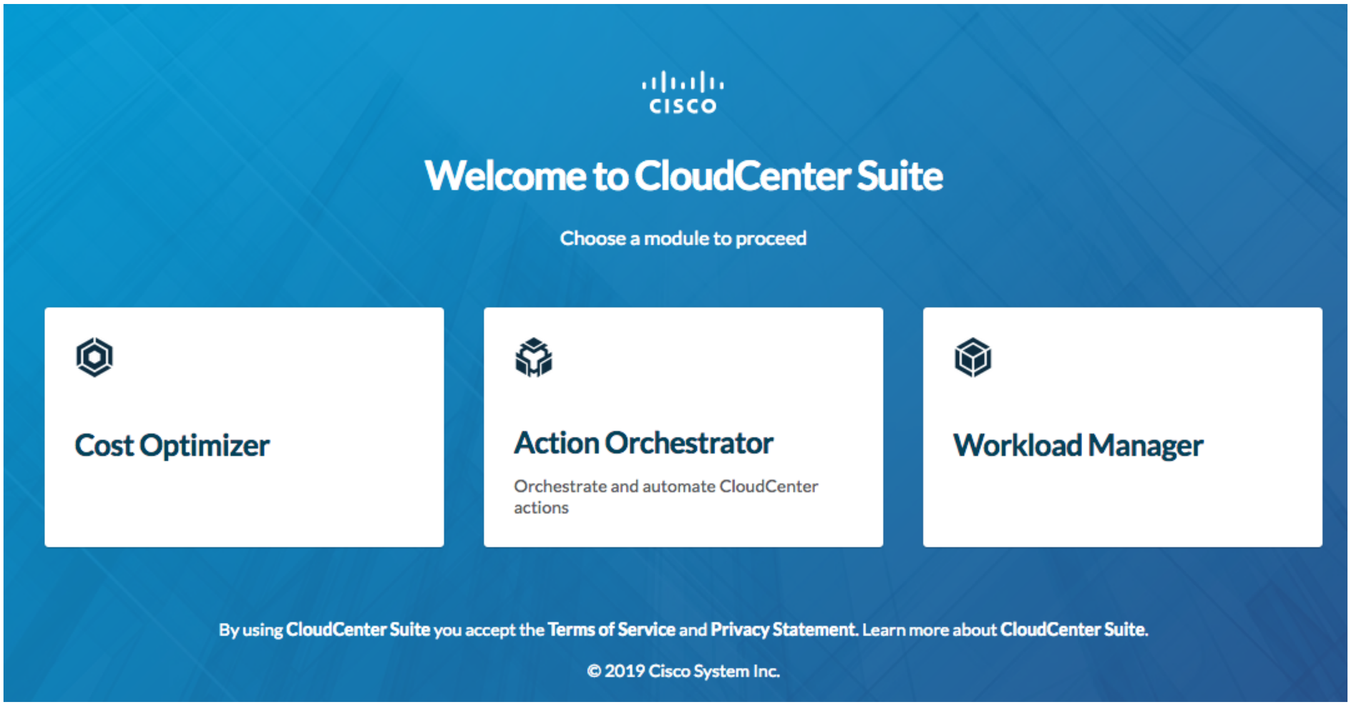

cisco
Welcome to CloudCenter Suite
Choose a module to proceed
Suite Admin
Central location to manage all your Cisco CloudCenter Suite modules.
Cost Optimizer
Cloud cost management and optimization solution
Action Orchestrator
Orchestrate and automate CloudCenter actions

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


cisco SUITE ADMIN
PT Welcome, Puj
Modules
Suite Admin
v5.1.0 • v5.1.0 is available - Release Notes
UPDATE
Workload Manager
v5.0.1 • v5.1.0 is available - Release Notes
UPDATE
Cost Optimizer
v5.0.1 • v5.1.0 is available - Release Notes
UPDATE

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.

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



Welcome to CloudCenter Suite

Choose a module to proceed

Cost Optimizer

Action Orchestrator

Orchestrate and automate CloudCenter actions

Workload Manager

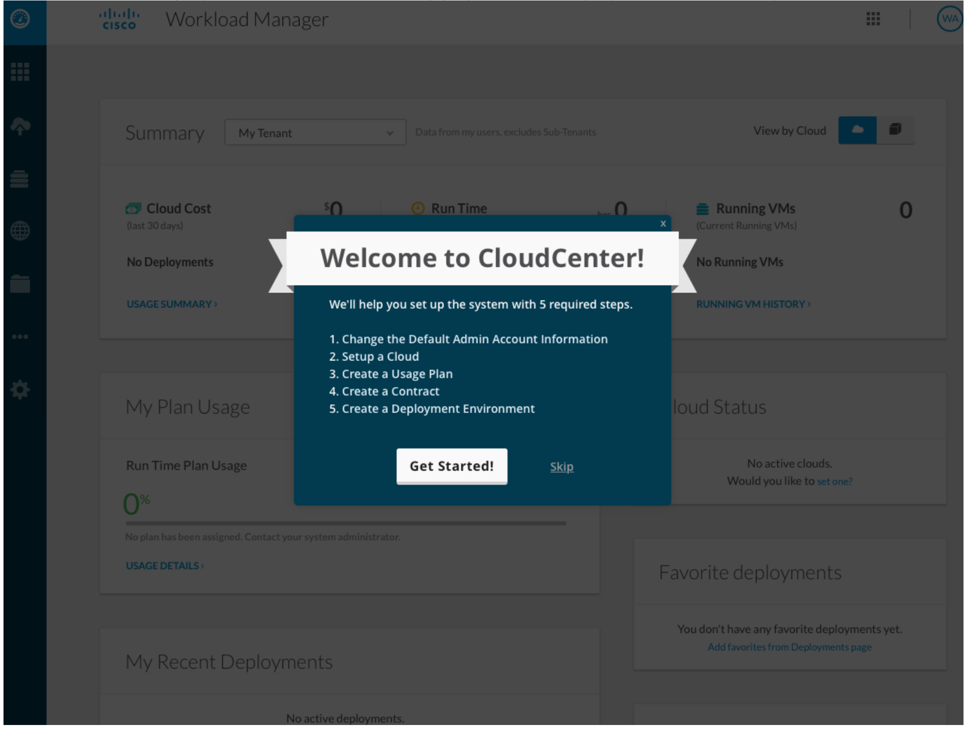
By using CloudCenter Suite you accept the Terms of Service and Privacy Statement. Learn more about CloudCenter Suite.

© 2019 Cisco System Inc.

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.

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

- The Information displayed at the browser landing page level is displayed in the following screenshot:

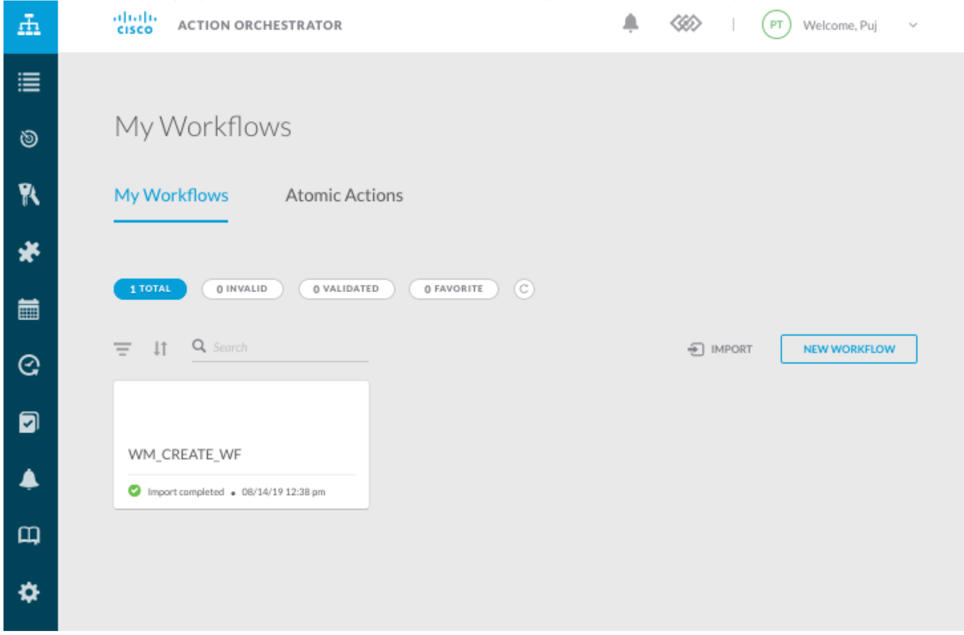


Welcome to CloudCenter!

We'll help you set up the system with 5 required steps.

1. Change the Default Admin Account Information
2. Setup a Cloud
3. Create a Usage Plan
4. Create a Contract
5. Create a Deployment Environment

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



My Workflows

WM_CREATE_WF

Import completed • 08/14/19 12:38 pm

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.

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	Suite A dministrator	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	✓	★	★	✓

Manage Tenants

Manage Tenants

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.

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.

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

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**.

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.

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.

Manage Module-Specific Content

Manage Module-Specific Content

- Overview
- Associate Modules
- Characteristics
- Process

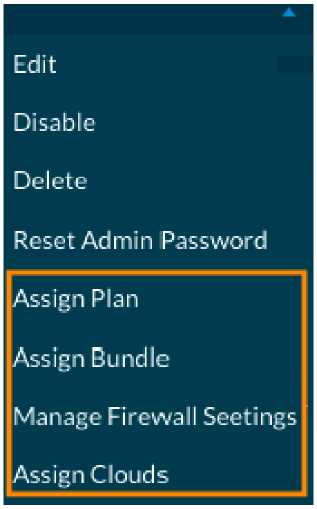
Each module in the CloudCenter Suite may have content that is specific to just that module. The suite administrator can manage these settings at the tenant level and the user level.

Currently, the Workload Manager is the only module that uses this feature. See Tenant Management in the Workload Manager documentation for an example.

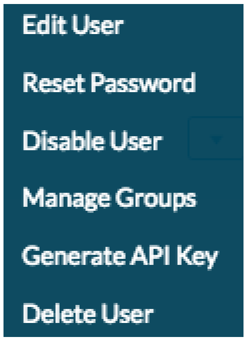
The actions displayed for each module is a fluid list based on which module-specific actions were created and made available for each tenant or user within the module – **this information is configured from the module**.

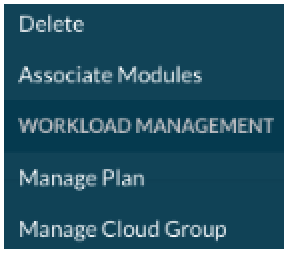
The configured content is **visible** from the Suite Admin's **Tenants** list page or the **Users** list page, which displays the configured action for each tenant or user within the Actions dropdown list.

The following screenshot displays content that is specific to the Workload Manager 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.

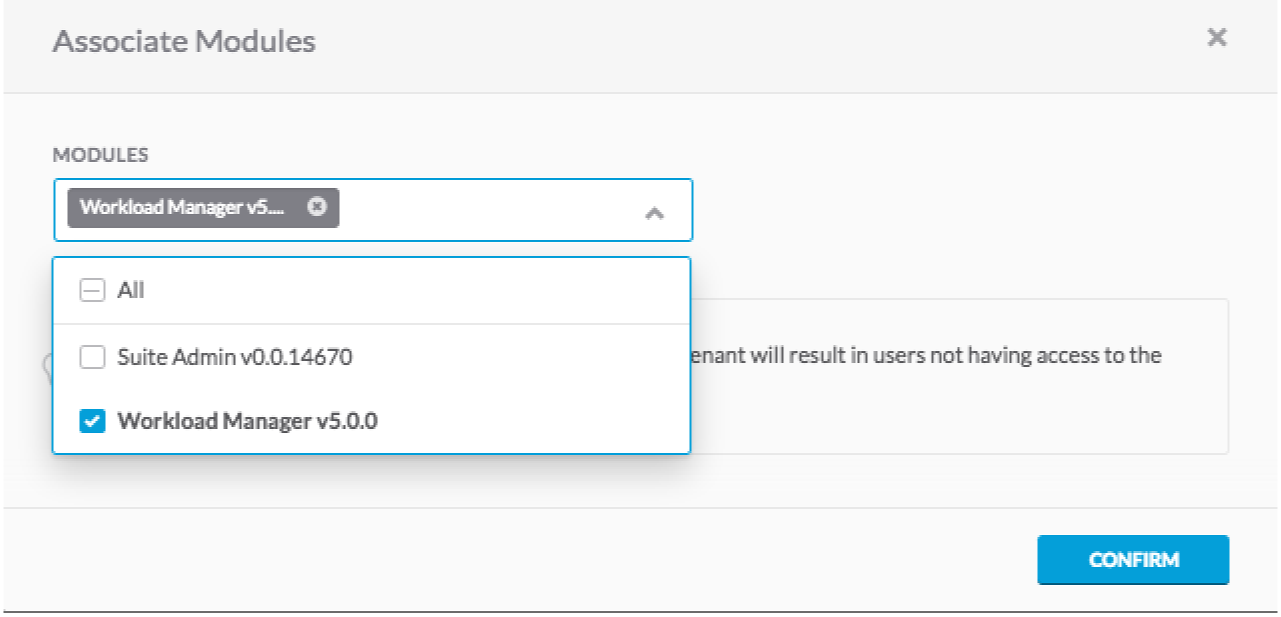


The following screenshots display content that is generally available to different users. This screenshot does not include any module-specific actions as they have not been configured.





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.



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.

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.

Admin Menu

Admin Menu

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

Backup

Backup Approach

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.

> 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 the CloudCenter 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.

> 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 **A dmin** > **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), the Arangodump should occur *before* you install the new Action Orchestrator version. See for additional details on Private Cloud > *Action Orchestrator-Specific Post-Restore Procedure* for additional details.
- Action Orchestrator Backup Requirements:

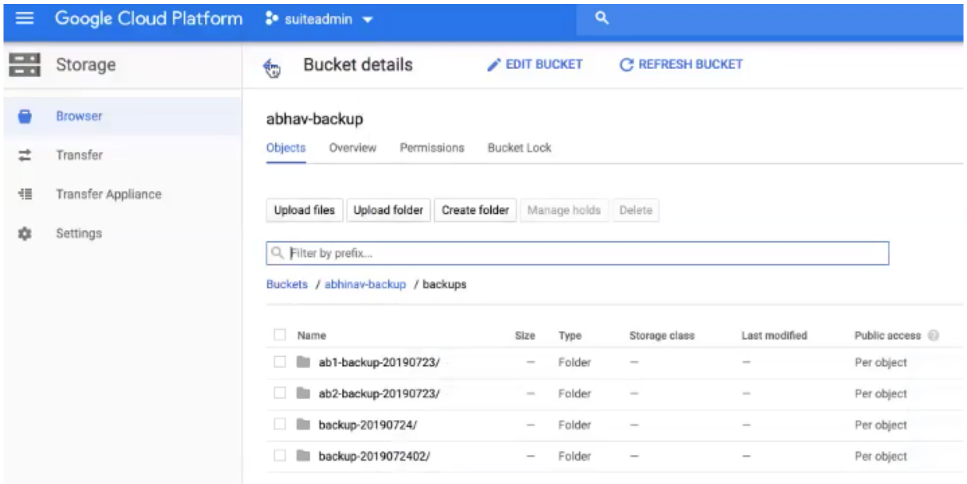
    1. Backup the Action Orchestrator database using the arangodump tool.
    2. Uninstall Action Orchestrator from the CCS cluster.
    3. Backup Suite Admin, Workload Manager, and Cost Optimizer using Velero.
- Action Orchestrator Restore Requirements:

    1. Restore Suite Admin, Workload Manager, and Cost Optimizer using Velero
    2. Reinstall Action Orchestrator.
    3. Restore the Action Orchestrator database using arangorestore tool

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:



Name	Size	Type	Storage class	Last modified	Public access
ab1-backup-20190723/	–	Folder	–	–	Per object
ab2-backup-20190723/	–	Folder	–	–	Per object
backup-20190724/	–	Folder	–	–	Per object
backup-2019072402/	–	Folder	–	–	Per object

    - 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:**

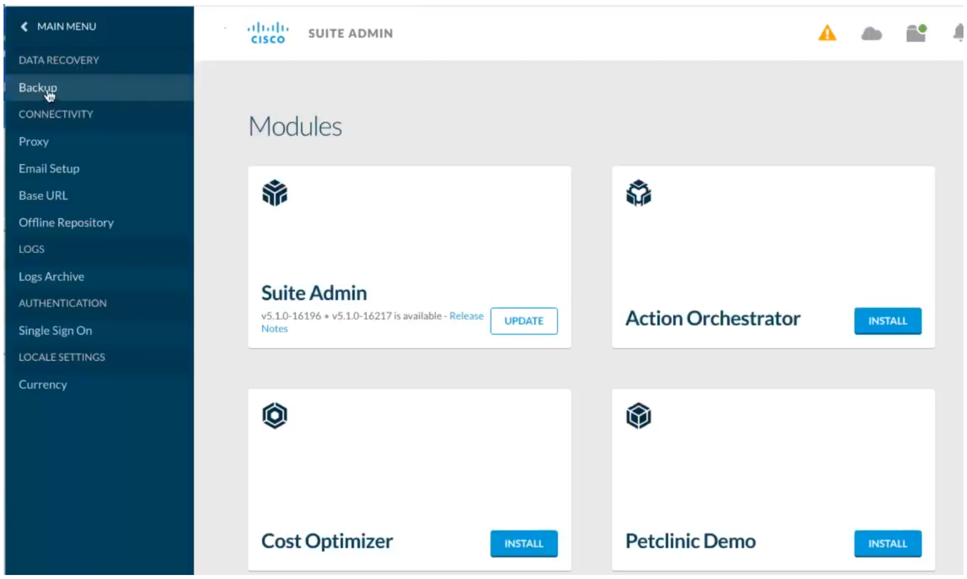
    - The storage bucket in your AWS S3 environment must be empty with the applicable ACL permission.
    - The IAM user permissions define the user privilege on the S3 bucket as listed in the following screenshot:

> 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!

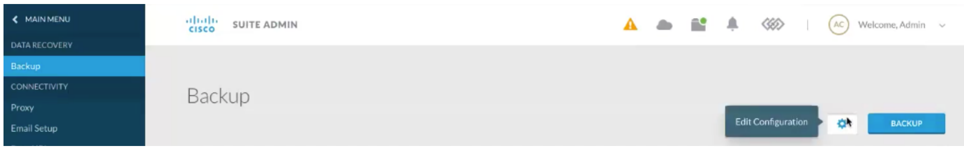
```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "ec2:DescribeRegions",
            "ec2:DescribeVolumes",
            "ec2:DescribeSnapshots",
            "ec2:CreateTags",
            "ec2:CreateVolume",
            "ec2:CreateSnapshot",
            "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:::*"
         ]
      }
   ]
}
```

To backup the CloudCenter Suite data, follow this procedure.

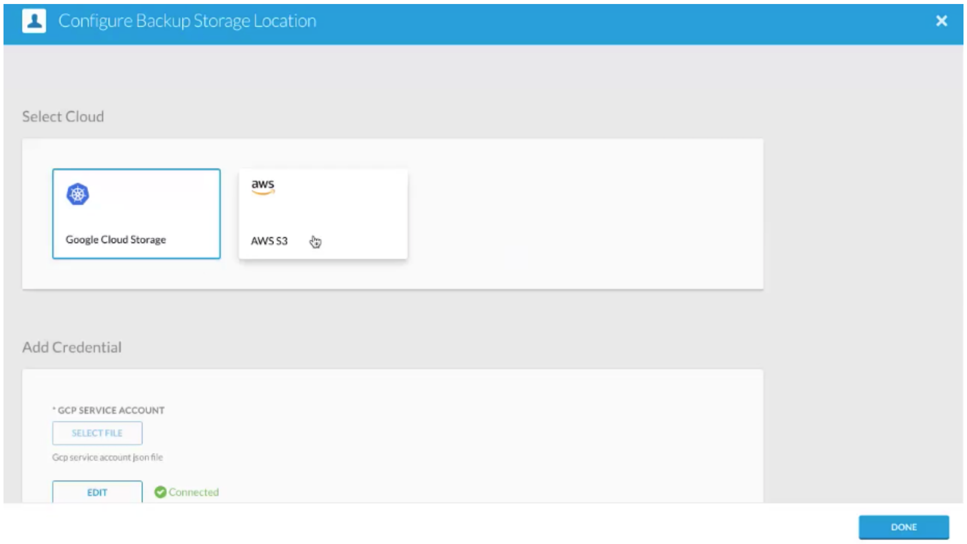
1. Navigate to the Suite Admin Dashboard.
2. Click **Admin** > **Backup** (under the Data Recovery section) to access the Backup page as displayed in the following screenshot.



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



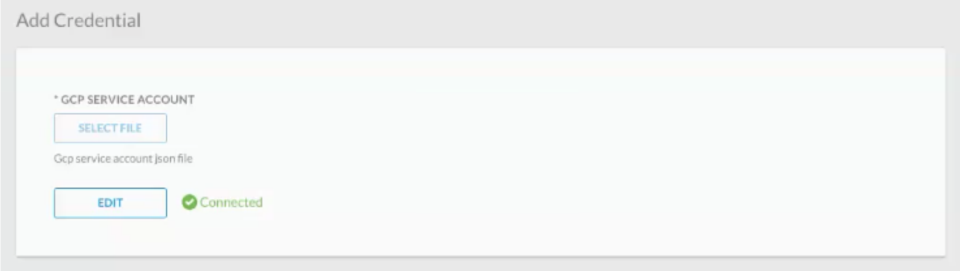
4. Select the required cloud in the Configure a Backup Storage Location page as displayed in the following screenshot.



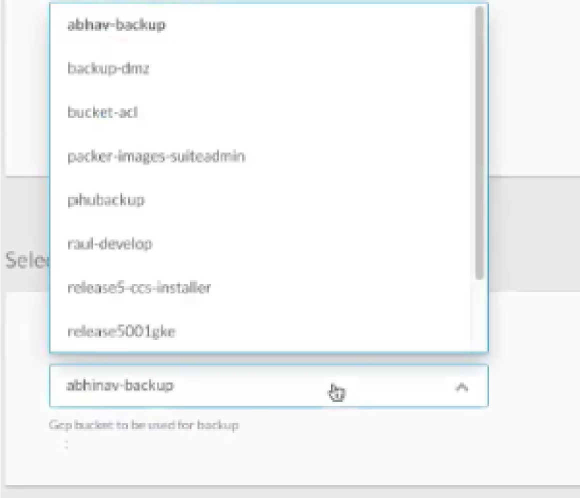
5. Depending on the selected cloud, the Add Credential section differs:

   - GCP:

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



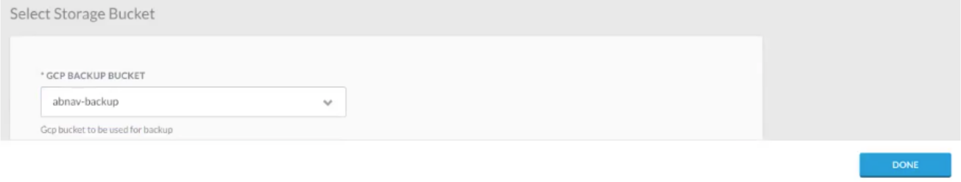
     b. Select the Storage bucket as displayed in the following screenshot.



abhinav-backup

Gcp bucket to be used for backup

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


Select Storage Bucket

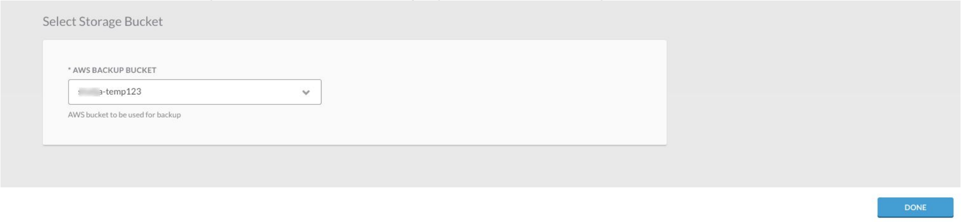
* GCP BACKUP BUCKET

abnav-backup

Gcp bucket to be used for backup

- AWS S3:

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

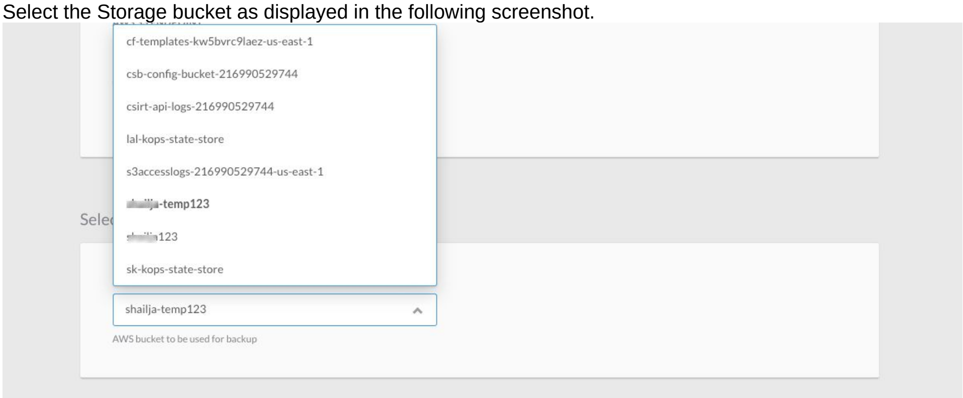

Select Storage Bucket

* AWS BACKUP BUCKET

[redacted]-temp123

AWS bucket to be used for backup

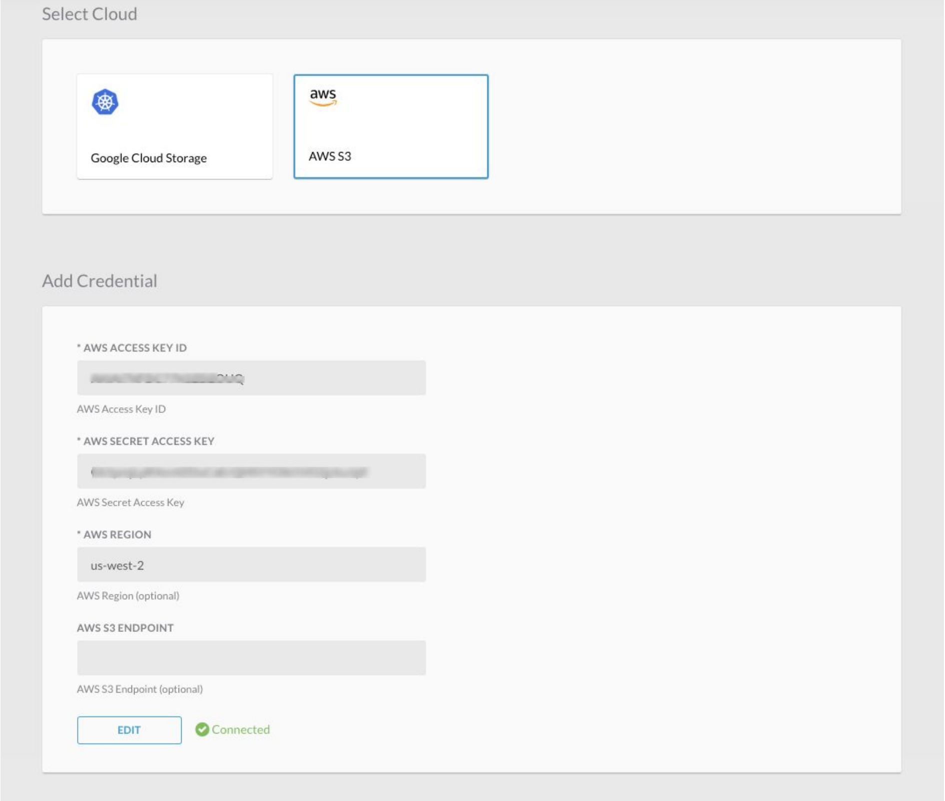
b. Select the Storage bucket as displayed in the following screenshot.


cf-templates-kw5bvrc9laez-us-east-1
csb-config-bucket-216990529744
csirt-api-logs-216990529744
lal-kops-state-store
s3accesslogs-216990529744-us-east-1
[redacted]-temp123
[redacted]123
sk-kops-state-store
Selec

shailja-temp123

AWS bucket to be used for backup

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



Select Cloud

Add Credential

* AWS ACCESS KEY ID

[redacted]

AWS Access Key ID

* AWS SECRET ACCESS KEY

[redacted]

AWS Secret Access Key

* AWS REGION

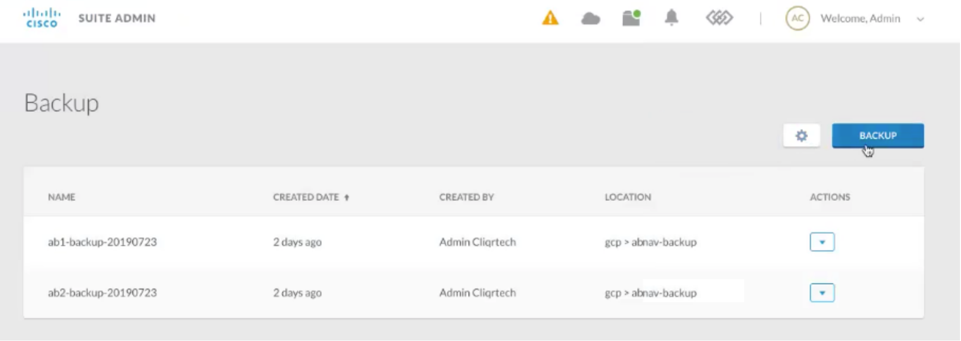
us-west-2

AWS Region (optional)

AWS S3 ENDPOINT

AWS S3 Endpoint (optional)

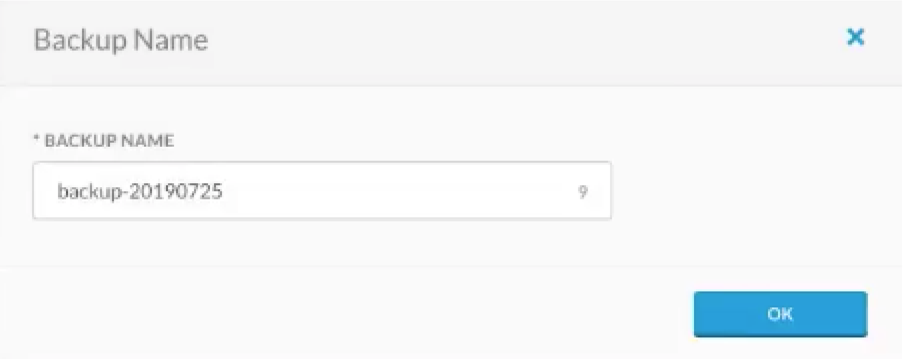
6. Once configured, click **Backup** in the Backup page to initiate the data backup. Until you initiate the first backup, this page will be empty. Once you have initiated one or more backups, they are automatically listed in this page as visible in the following screenshot.



Backup

NAME	CREATED DATE ↑	CREATED BY	LOCATION	ACTIONS
ab1-backup-20190723	2 days ago	Admin Cliqrtech	gcp > abnav-backup	▾
ab2-backup-20190723	2 days ago	Admin Cliqrtech	gcp > abnav-backup	▾

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.



Backup Name

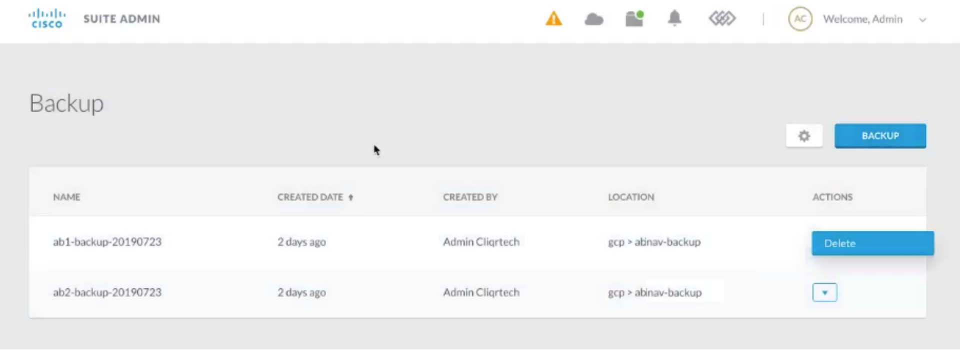
* BACKUP NAME

backup-20190725

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

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:



NAME	CREATED DATE	CREATED BY	LOCATION	ACTIONS
ab1-backup-20190723	2 days ago	Admin Cliqrtech	gcp > abinav-backup	Delete
ab2-backup-20190723	2 days ago	Admin Cliqrtech	gcp > abinav-backup	▾

- **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

Proxy Settings

Proxy Settings

- Overview
- Guidelines
- Suite Administrator Proxy Configuration

The Suite Admin uses proxy settings for licensing and module configuration purposes. Proxy settings are disabled by default. If not provided, then no proxy configuration is set!

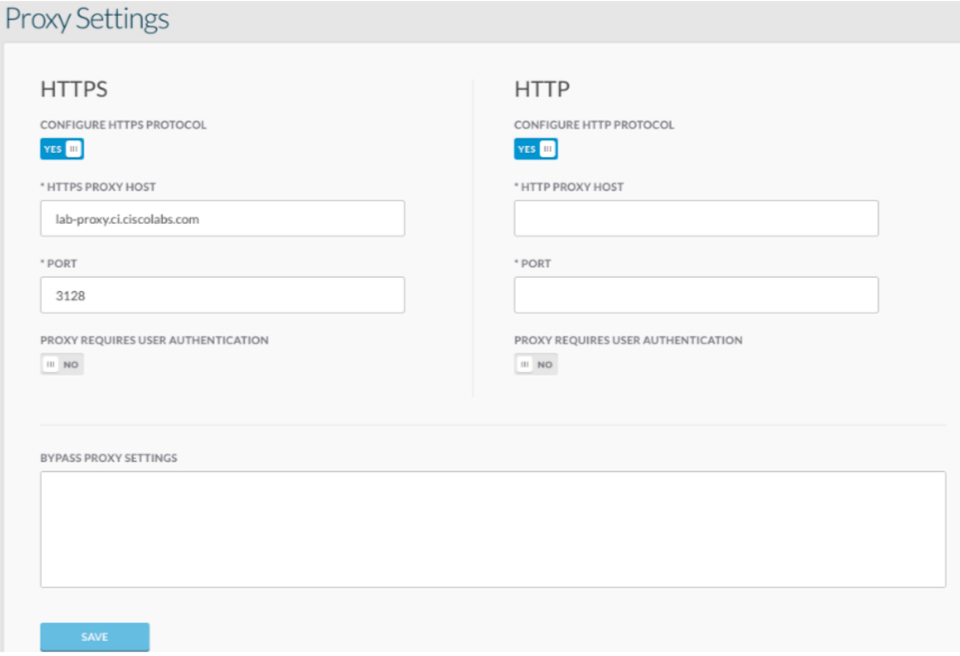
> Web service calls are routed through the proxy. When proxy settings are modified on the Suite Admin, the CloudCenter Suite management pod is rebooted to apply the configuration.

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.

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 the Suite 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.



Proxy Settings

HTTPS

CONFIGURE HTTPS PROTOCOL: YES

* HTTPS PROXY HOST: lab-proxy.ci.ciscolabs.com

* PORT: 3128

PROXY REQUIRES USER AUTHENTICATION: NO

HTTP

CONFIGURE HTTP PROTOCOL: YES

* HTTP PROXY HOST:

* PORT:

PROXY REQUIRES USER AUTHENTICATION: NO

BYPASS PROXY SETTINGS

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 code example:

> Depending on the environment where you have installed the CloudCenter Suite, 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 CloudCenter Suite, the connection to this IP/FQDN will bypass the Proxy value – when CloudCenter Suite 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.

Email Settings

Email Settings

Email settings are required to communicate with CloudCenter Suite users when triggering the reset password function or the password auto-generation function – the email settings are used to construct the links when resetting a password for new or existing users.

✓ The Suite Admin does not support TLS ports – it only supports SSL ports to configure SMTP mail servers.

You can enable the *SMTPS* protocol to 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.

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 the https://myaccount.google.com/?utm_source=OGB&utm_medium=act page, 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 Configuration and completed the Email Settings to ensure that the URL is accessible and that an email can be sent to the user.

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

1. Navigate to the Suite 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 switch to 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.

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

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

   ⓘ When you save the SMTP settings, be aware that you are only saving the configuration parameters to the CloudCenter Suite database and that the connection is still pending connection verification. As soon as the connection is verified by the CloudCenter Suite, 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.

Base URL Configuration

Base URL

- Overview
- Requirements
- Process

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

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

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

Effective CloudCenter Suite 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.

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.

Offline Repository Configuration

Offline Repository Configuration

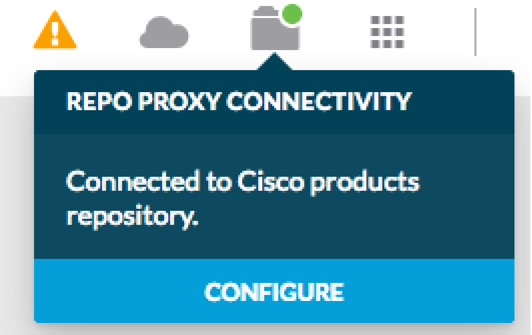
- Overview
- Connectivity Icon
- Process

A repository connection enables access from one of the CloudCenter Suite VMs to a local **Cisco Products Repository**. This default repository is only accessible if you have internet access. See Offline Repository for details.

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

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

- If the CloudCenter Suite is able to connect to the Cisco Products Repository, then you'll see a green circle displayed in the Suite Admin Dashboard header.
- 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).



Connected to Cisco products repository.

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.

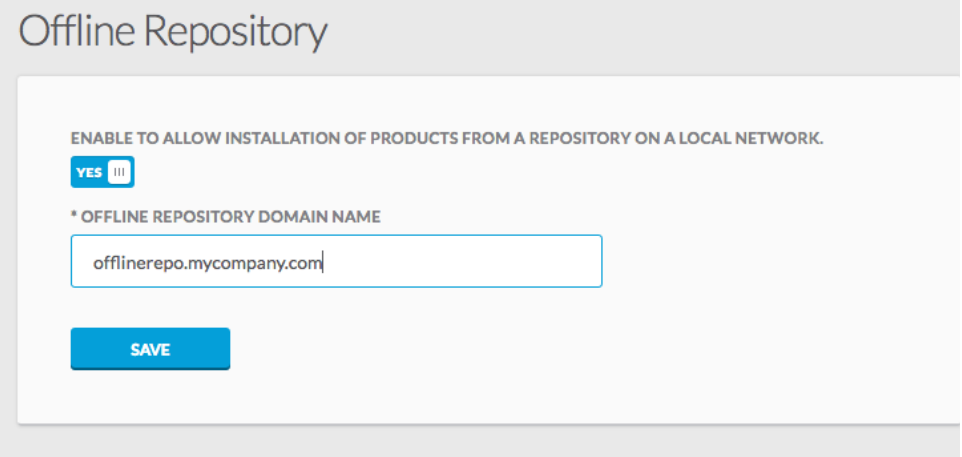
The color of the circle on the folder icon identifies the status of the repository (even if it is the default Cisco repository) connected to the CloudCenter Suite as identified in the following table.

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.

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

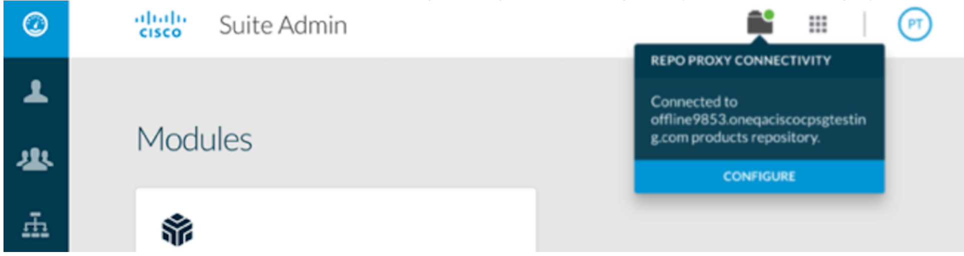
1. Click the folder icon to re-configure the proxy settings.
   Optional. Navigate to the Suite Admin Dashboard > **Admin** and click **Offline Repository**.
2. Toggle the switch (disabled by default) to enable access to the CloudCenter Suite via a local repository (displayed in the following screenshot).



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

* OFFLINE REPOSITORY DOMAIN NAME
offlinerepo.mycompany.com

3. Provide the DNS of the offline repository server 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:



REPO PROXY CONNECTIVITY

Connected to offline9853.oneqaciscocpsgtesting.com products repository.

Log Archive

Log Archive

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.

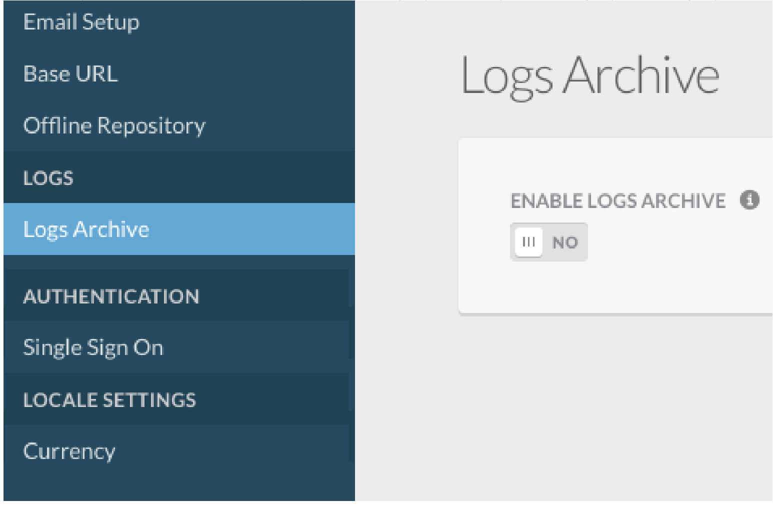
To store logs for a longer period, you can configure an archive location for your AWS S3 region – if you configure an archive location for your AWS S3 region, the CloudCenter Suite logs can also be saved to the AWS S3 region besides the temporary location on the CloudCenter Suite server. If so, you can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

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.

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.



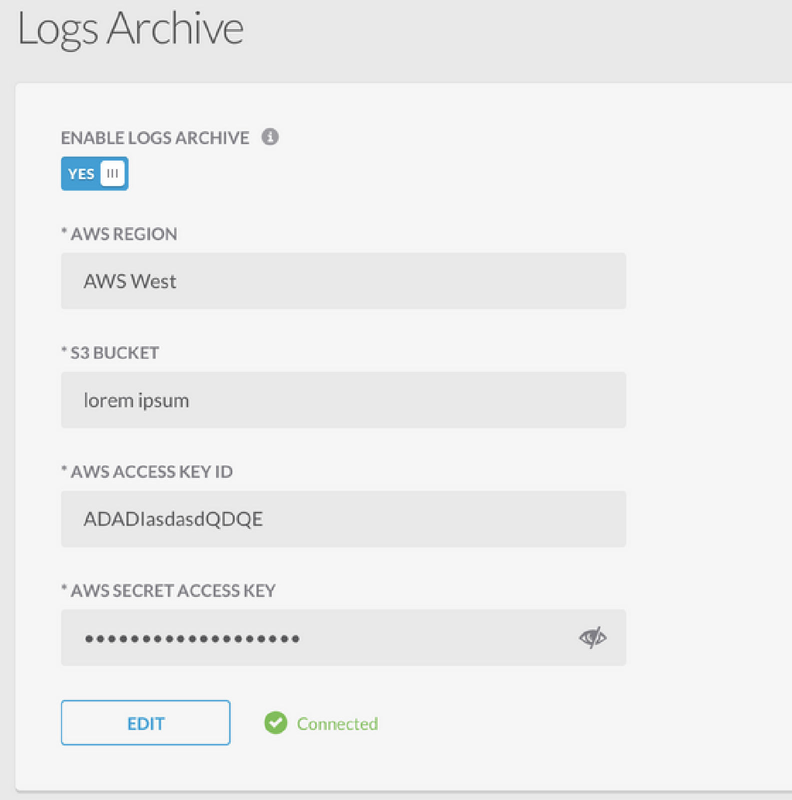
Logs Archive

ENABLE LOGS ARCHIVE

NO

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.



Logs Archive

ENABLE LOGS ARCHIVE

YES

* AWS REGION

AWS West

* S3 BUCKET

lorem ipsum

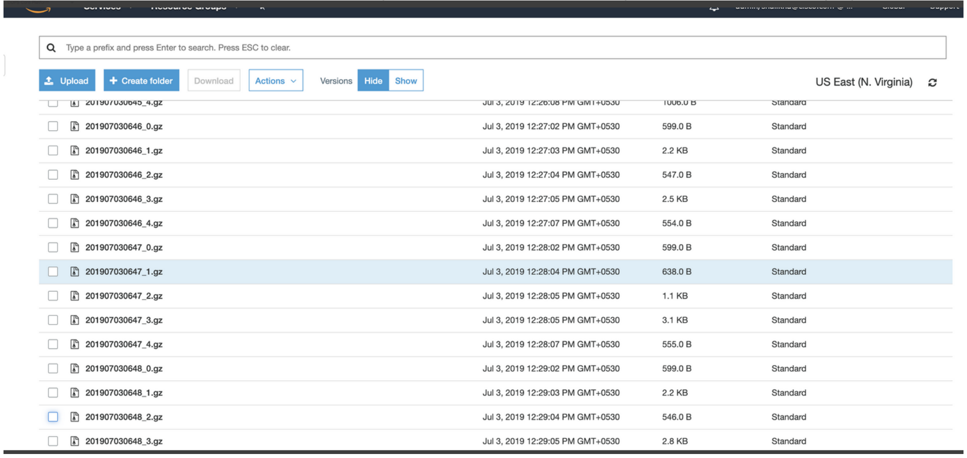
* AWS ACCESS KEY ID

ADADIasdasdQDQE

* AWS SECRET ACCESS KEY

•••••••••••••••••••

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



□	201907030645_4.gz	Jul 3, 2019 12:26:08 PM GMT+0530	1006.0 B	Standard
□	201907030646_0.gz	Jul 3, 2019 12:27:02 PM GMT+0530	599.0 B	Standard
□	201907030646_1.gz	Jul 3, 2019 12:27:03 PM GMT+0530	2.2 KB	Standard
□	201907030646_2.gz	Jul 3, 2019 12:27:04 PM GMT+0530	547.0 B	Standard
□	201907030646_3.gz	Jul 3, 2019 12:27:05 PM GMT+0530	2.5 KB	Standard
□	201907030646_4.gz	Jul 3, 2019 12:27:07 PM GMT+0530	554.0 B	Standard
□	201907030647_0.gz	Jul 3, 2019 12:28:02 PM GMT+0530	599.0 B	Standard
□	201907030647_1.gz	Jul 3, 2019 12:28:04 PM GMT+0530	638.0 B	Standard
□	201907030647_2.gz	Jul 3, 2019 12:28:05 PM GMT+0530	1.1 KB	Standard
□	201907030647_3.gz	Jul 3, 2019 12:28:05 PM GMT+0530	3.1 KB	Standard
□	201907030647_4.gz	Jul 3, 2019 12:28:07 PM GMT+0530	555.0 B	Standard
□	201907030648_0.gz	Jul 3, 2019 12:29:02 PM GMT+0530	599.0 B	Standard
□	201907030648_1.gz	Jul 3, 2019 12:29:03 PM GMT+0530	2.2 KB	Standard
□	201907030648_2.gz	Jul 3, 2019 12:29:04 PM GMT+0530	546.0 B	Standard
□	201907030648_3.gz	Jul 3, 2019 12:29:05 PM GMT+0530	2.8 KB	Standard

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.

SSO Setup

Single Sign On (SSO) Setup

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 CloudCenter 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 CloudCenter 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.

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

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.

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

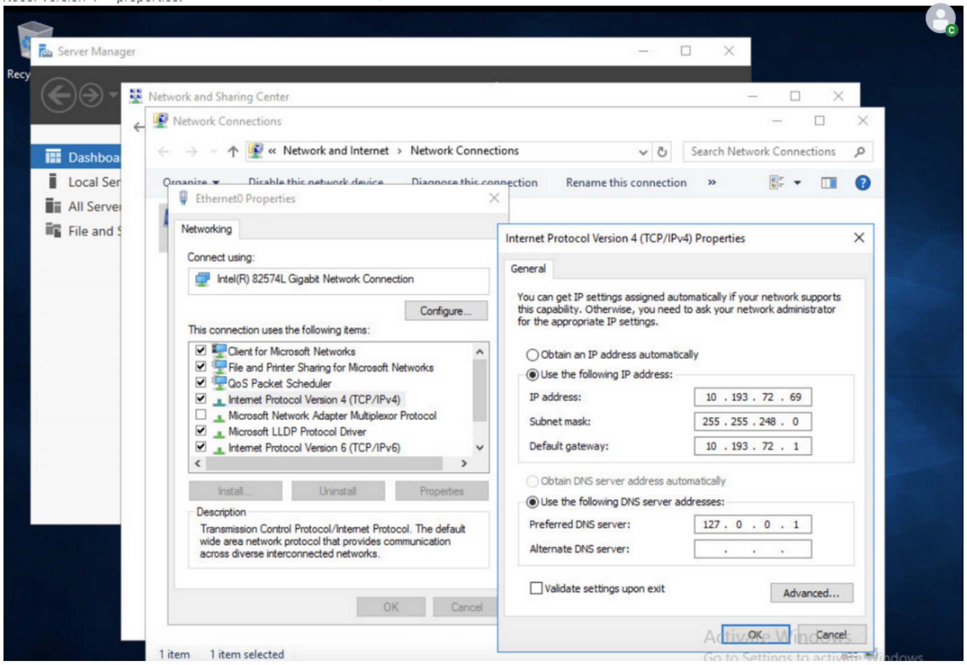
To setup ADFS in *Windows* 2016 for a vSphere environment, follow these steps.

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.



Ethernet0 Properties

Networking

Connect using:

Intel(R) 82574L Gigabit Network Connection

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☐ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Internet Protocol Version 6 (TCP/IPv6)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address:	10 . 193 . 72 . 69
Subnet mask:	255 . 255 . 248 . 0
Default gateway:	10 . 193 . 72 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

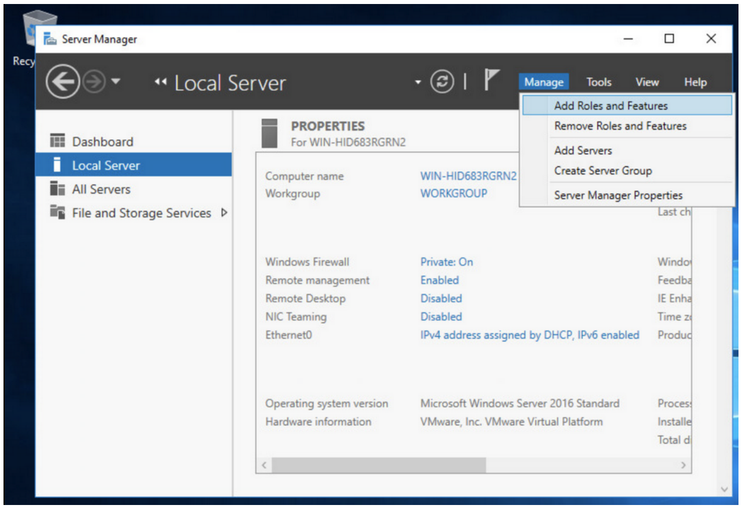
Preferred DNS server:	127 . 0 . 0 . 1
Alternate DNS server:	. . .

☐ Validate settings upon exit

    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.

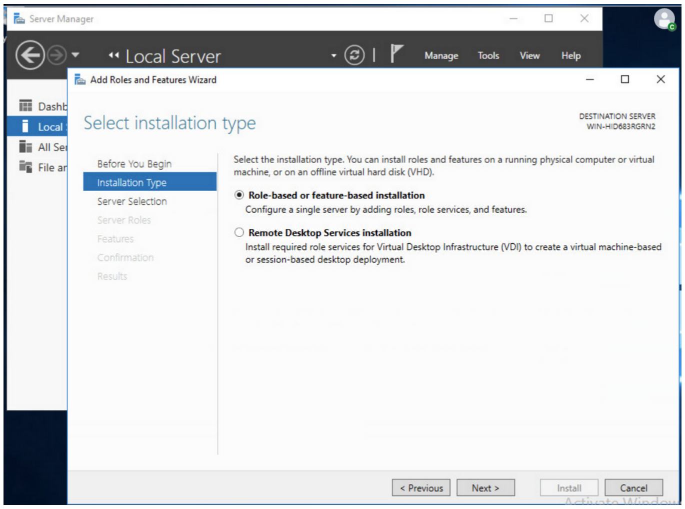
    a. Access **Server Manager** > **Manage** > **Add Roles and Features** as reflected in the following screenshot.



PROPERTIES
For WIN-HID683RGRN2

Computer name	WIN-HID683RGRN2
Workgroup	WORKGROUP
Windows Firewall	Private: On
Remote management	Enabled
Remote Desktop	Disabled
NIC Teaming	Disabled
Ethernet0	IPv4 address assigned by DHCP, IPv6 enabled
Operating system version	Microsoft Windows Server 2016 Standard
Hardware information	VMware, Inc. VMware Virtual Platform

    b. Select the type of Installation as reflected in the following screenshot.



Select installation type

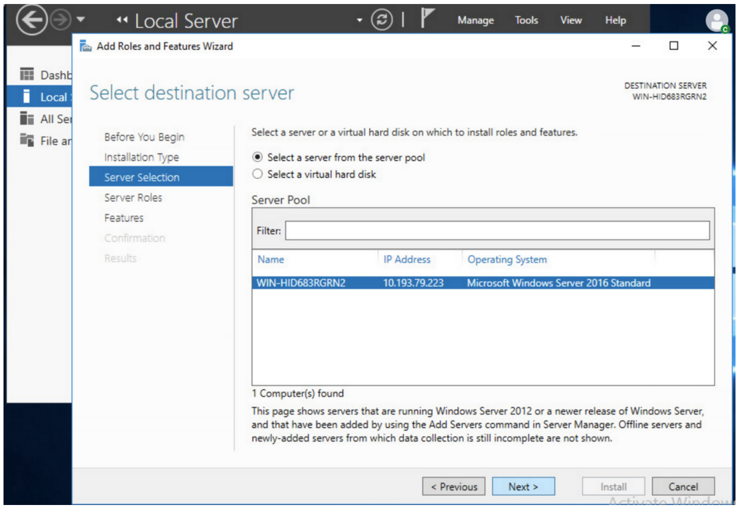
DESTINATION SERVER
WIN-HID683RGRN2

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

c. Select the destination server as reflected in the following screenshot.



Select destination server

DESTINATION SERVER
WIN-HID683RGRN2

Select a server or a virtual hard disk on which to install roles and features.

● Select a server from the server pool
○ Select a virtual hard disk

Server Pool

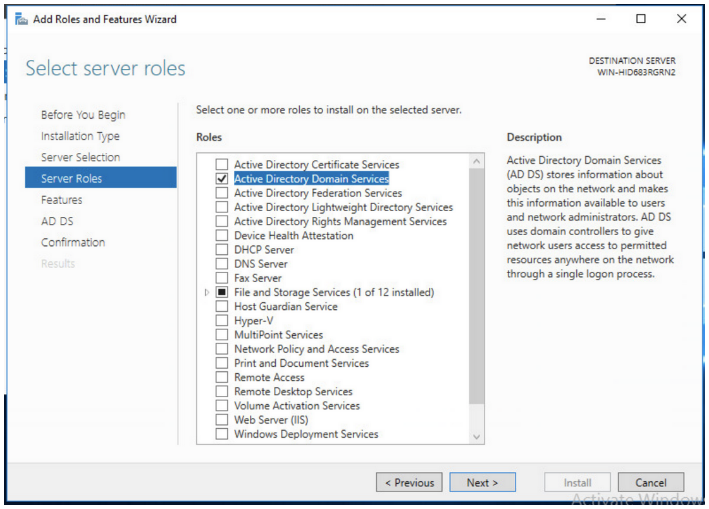
Filter:

Name	IP Address	Operating System
WIN-HID683RGRN2	10.193.79.223	Microsoft Windows Server 2016 Standard

1 Computer(s) found

This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

d. Select **Active Directory Domain Services** as reflected in the following screenshot.



Select server roles

DESTINATION SERVER
WIN-HID683RGRN2

Select one or more roles to install on the selected server.

Roles

- □ Active Directory Certificate Services
- ☑ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Device Health Attestation
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- ■ File and Storage Services (1 of 12 installed)
- □ Host Guardian Service
- □ Hyper-V
- □ MultiPoint Services
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services
- □ Volume Activation Services
- □ Web Server (IIS)
- □ Windows Deployment Services

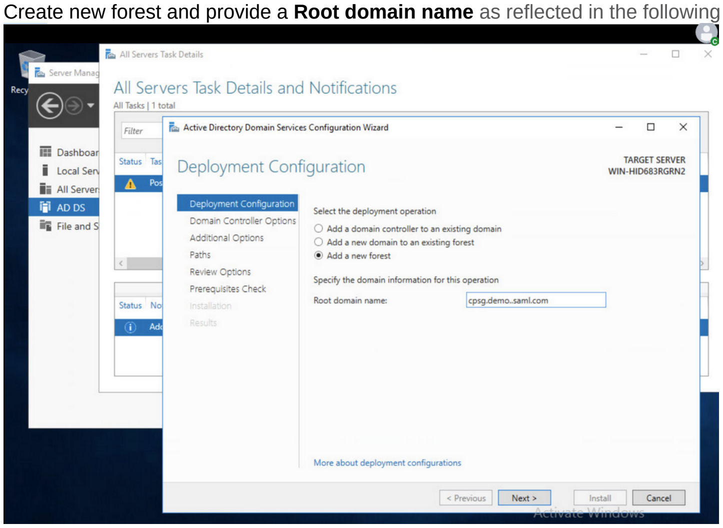
Description

Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.

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.



Active Directory Domain Services Configuration Wizard

Deployment Configuration

TARGET SERVER
WIN-HID683RGRN2

Select the deployment operation

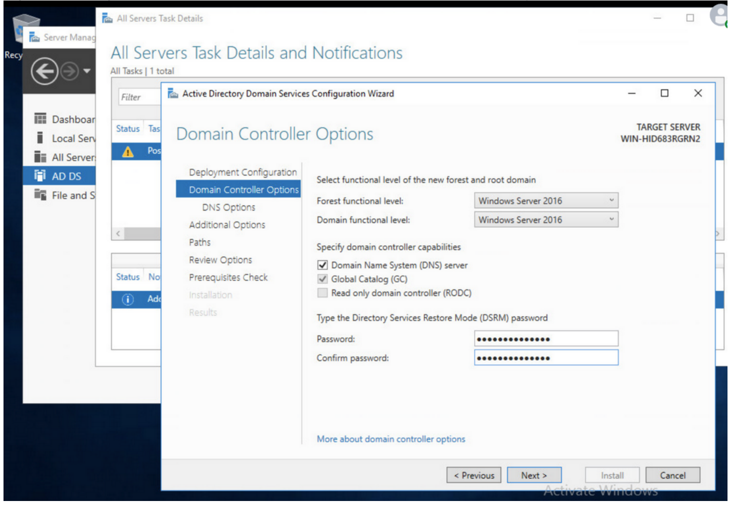
○ Add a domain controller to an existing domain
○ Add a new domain to an existing forest
● Add a new forest

Specify the domain information for this operation

Root domain name: cpsg.demo..saml.com

More about deployment configurations

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



Active Directory Domain Services Configuration Wizard

Domain Controller Options

TARGET SERVER
WIN-HID683RGRN2

Select functional level of the new forest and root domain

Forest functional level: Windows Server 2016

Domain functional level: Windows Server 2016

Specify domain controller capabilities

☑ Domain Name System (DNS) server
☑ Global Catalog (GC)
☐ Read only domain controller (RODC)

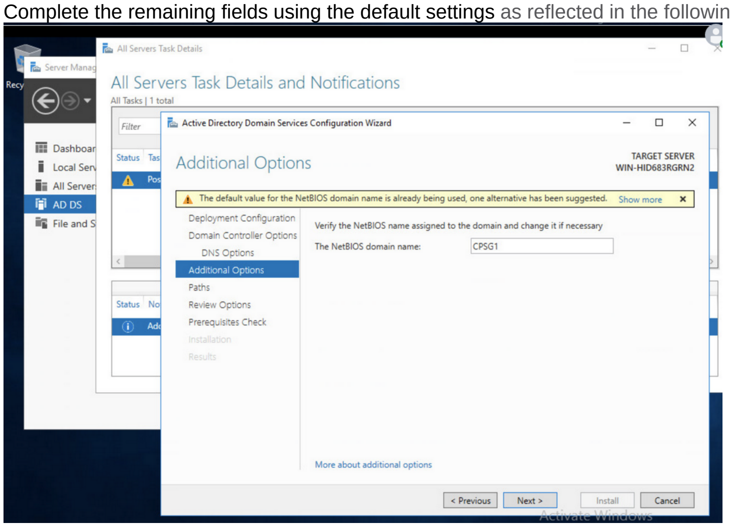
Type the Directory Services Restore Mode (DSRM) password

Password: ••••••••••••••

Confirm password: ••••••••••••••

More about domain controller options

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



Active Directory Domain Services Configuration Wizard

Additional Options

TARGET SERVER
WIN-HID683RGRN2

The default value for the NetBIOS domain name is already being used, one alternative has been suggested. Show more

Verify the NetBIOS name assigned to the domain and change it if necessary

The NetBIOS domain name: CPSG1

More about additional options

d. Save your configuration and restart the VM.

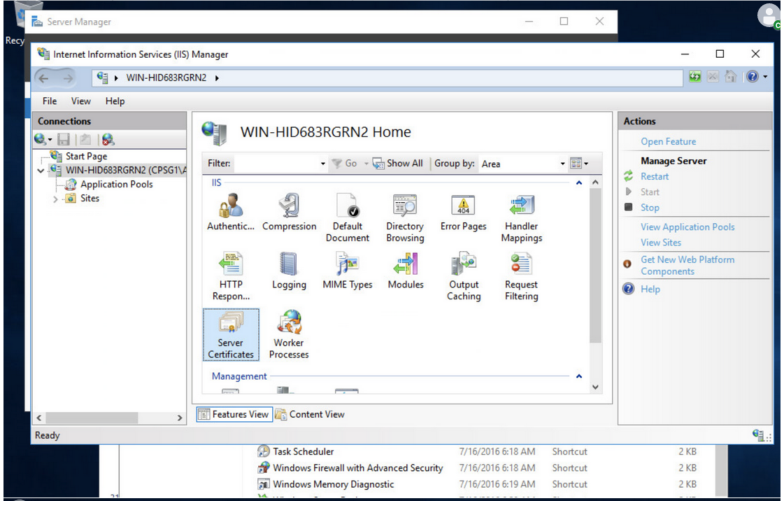
8. Install a DNS Server.

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

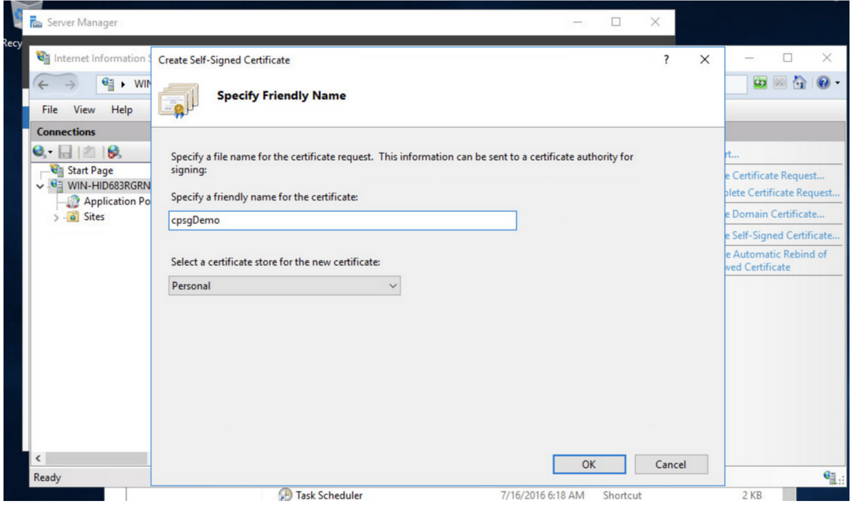
9. Install the Web Server (IIS Manager)

   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 as reflected in the following screenshot.



e. Click the **IIS server name** (below the **Start Page** option in the left pane) as reflected in the following screenshot.


Create Self-Signed Certificate

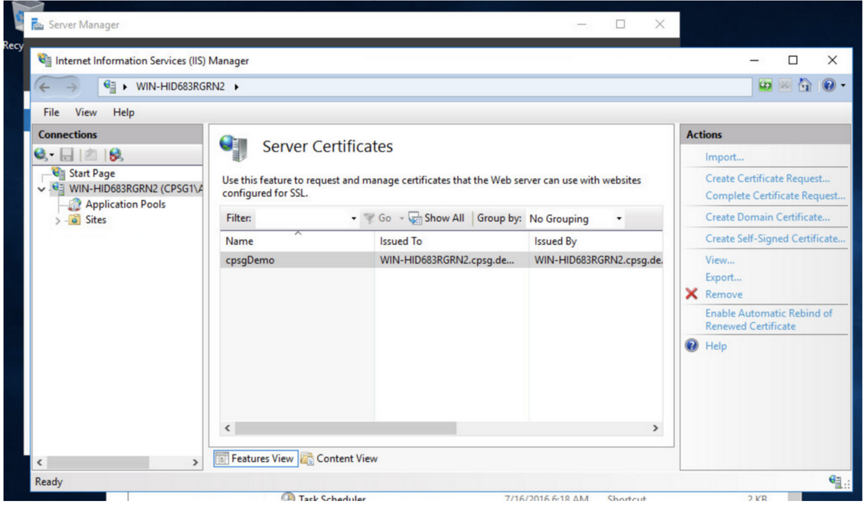
Specify Friendly Name

Specify a file name for the certificate request. This information can be sent to a certificate authority for signing:

Specify a friendly name for the certificate: cpsgDemo

Select a certificate store for the new certificate: Personal

f. Create Self signed certificate by accessing **Create server certificates** > **New self-signed** as reflected in the following screenshot.


Server Certificates

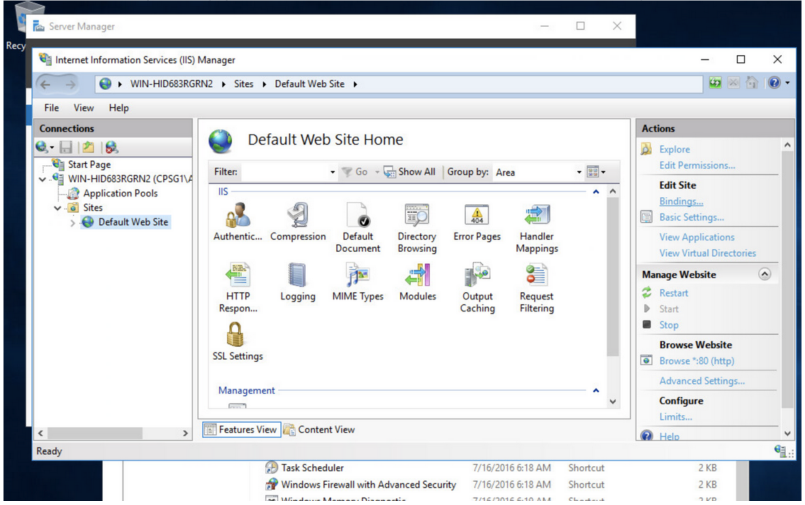
Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

Filter: Go Show All Group by: No Grouping

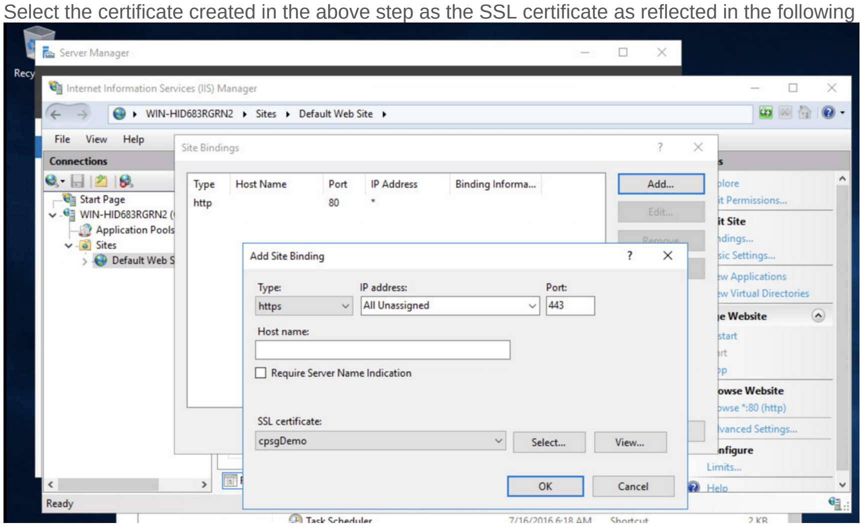
Name	Issued To	Issued By
cpsgDemo	WIN-HID683RGRN2.cpsg.de...	WIN-HID683RGRN2.cpsg.de.

Server Manager
Internet Information Services (IIS) Manager
WIN-HID683RGRN2
File View Help
Connections
Start Page
WIN-HID683RGRN2 (CPSG1\A
Application Pools
Sites
Features View
Content View
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
View...
Export...
Remove
Enable Automatic Rebind of Renewed Certificate
Help
Ready

g. Enable HTTPS (Bindings) and select HTTPS as reflected in the following screenshot.


Server Manager
Internet Information Services (IIS) Manager
WIN-HID683RGRN2 ▸ Sites ▸ Default Web Site ▸
File View Help
Connections
Start Page
WIN-HID683RGRN2 (CPSG1\A
Application Pools
Sites
Default Web Site
Default Web Site Home
Filter: Go Show All Group by: Area
IIS
Authentic... Compression Default Document Directory Browsing Error Pages Handler Mappings
HTTP Respon... Logging MIME Types Modules Output Caching Request Filtering
SSL Settings
Management
Features View Content View
Ready
Actions
Explore
Edit Permissions...
Edit Site
Bindings...
Basic Settings...
View Applications
View Virtual Directories
Manage Website
Restart
Start
Stop
Browse Website
Browse *:80 (http)
Advanced Settings...
Configure
Limits...
Help
Task Scheduler 7/16/2016 6:18 AM Shortcut 2 KB
Windows Firewall with Advanced Security 7/16/2016 6:18 AM Shortcut 2 KB

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



Type	Host Name	Port	IP Address	Binding Informa...
http		80	*	

Type: https

IP address: All Unassigned

Port: 443

Host name:

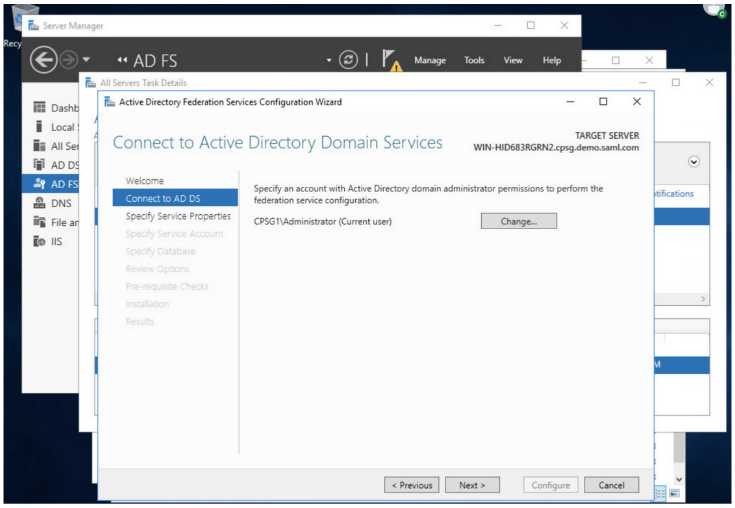
☐ Require Server Name Indication

SSL certificate: cpsgDemo

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** as reflected in the following screenshot.



Connect to Active Directory Domain Services

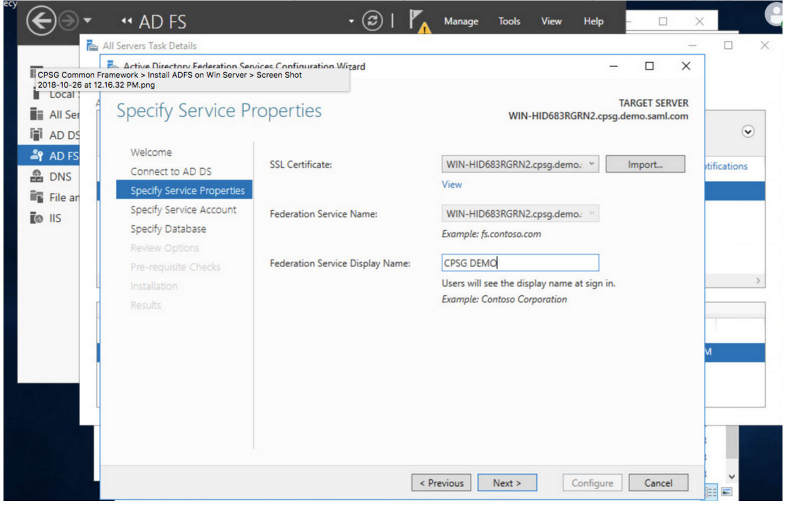
TARGET SERVER
WIN-HID683RGRN2.cpsg.demo.saml.com

Specify an account with Active Directory domain administrator permissions to perform the federation service configuration.

CPSG1\Administrator (Current user)

b. Select Create the first federation server.

i. Select the SSL Cert from the drop down and provide the ADFS display name (any) as reflected in the following screenshot.



Specify Service Properties

TARGET SERVER
WIN-HID683RGRN2.cpsg.demo.saml.com

SSL Certificate: WIN-HID683RGRN2.cpsg.demo.

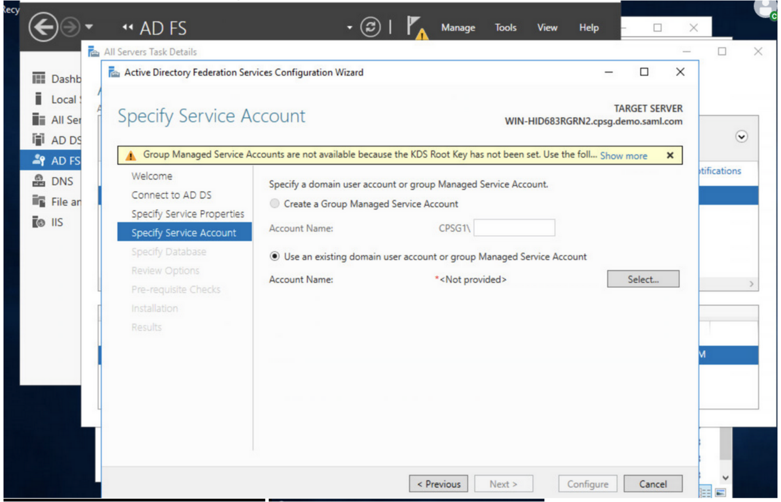
Federation Service Name: WIN-HID683RGRN2.cpsg.demo.

Example: fs.contoso.com

Federation Service Display Name: CPSG DEMO

Users will see the display name at sign in.
Example: Contoso Corporation

ii. Select the **Use an existing domain user account...** button as reflected in the following screenshot.



Specify Service Account

TARGET SERVER
WIN-HID683RGRN2.cpsg.demo.saml.com

Group Managed Service Accounts are not available because the KDS Root Key has not been set. Use the foll...

Specify a domain user account or group Managed Service Account.

○ Create a Group Managed Service Account

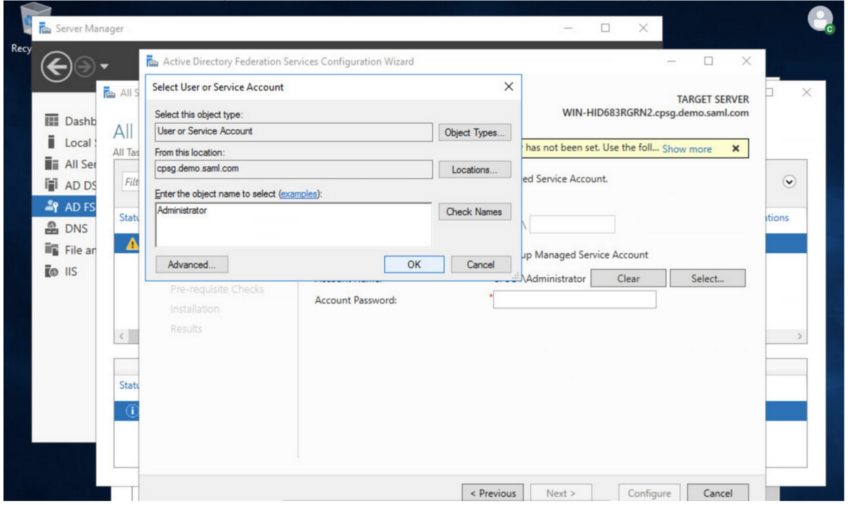
Account Name: CPSG1\

● Use an existing domain user account or group Managed Service Account

Account Name: *<Not provided>

iii. Complete the installation using the default values for the remaining fields.

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



Select User or Service Account

Select this object type: User or Service Account

From this location: cpsg.demo.saml.com

Enter the object name to select (examples): Administrator

TARGET SERVER
WIN-HID683RGRN2.cpsg.demo.saml.com

has not been set. Use the foll...

ed Service Account.

up Managed Service Account

\Administrator

Account Password: *

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 can access the Single Sign On (SSO) page using the following URL format.

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

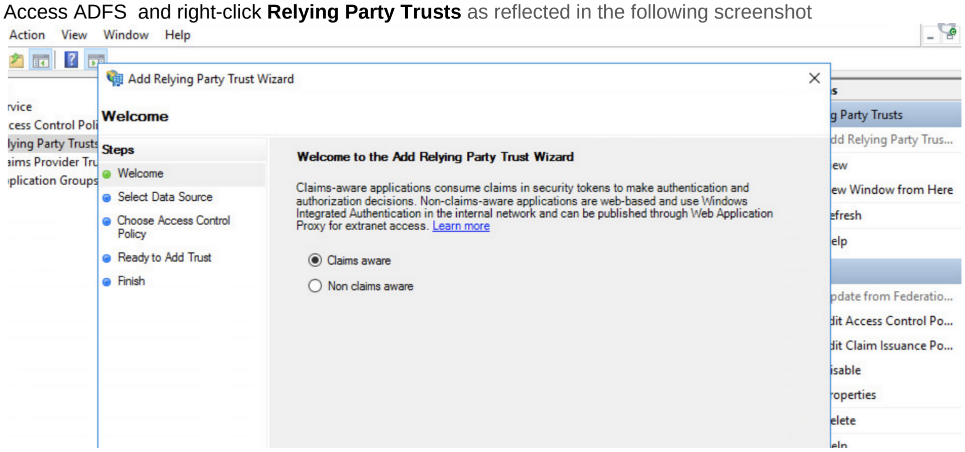
You have now setup ADFS in *Windows* 2016 for a vSphere environment.

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



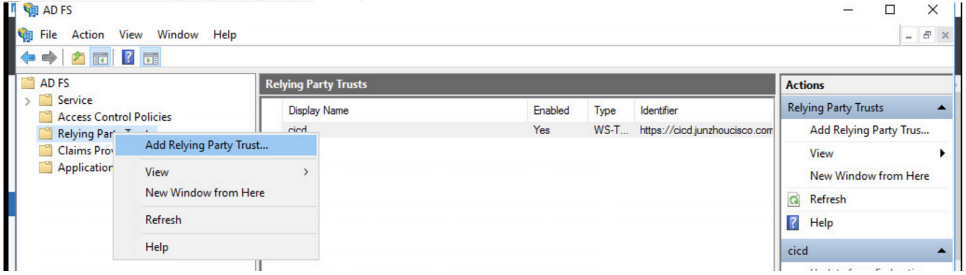
Welcome to the Add Relying Party Trust Wizard

Claims-aware applications consume claims in security tokens to make authentication and authorization decisions. Non-claims-aware applications are web-based and use Windows Integrated Authentication in the internal network and can be published through Web Application Proxy for extranet access. Learn more

● Claims aware

○ Non claims aware

2. Select the **Add Relying Party Trust...** option as reflected in the following screenshot.



Display Name	Enabled	Type	Identifier
cicd	Yes	WS-T...	https://cicd.junzhoucisco.com

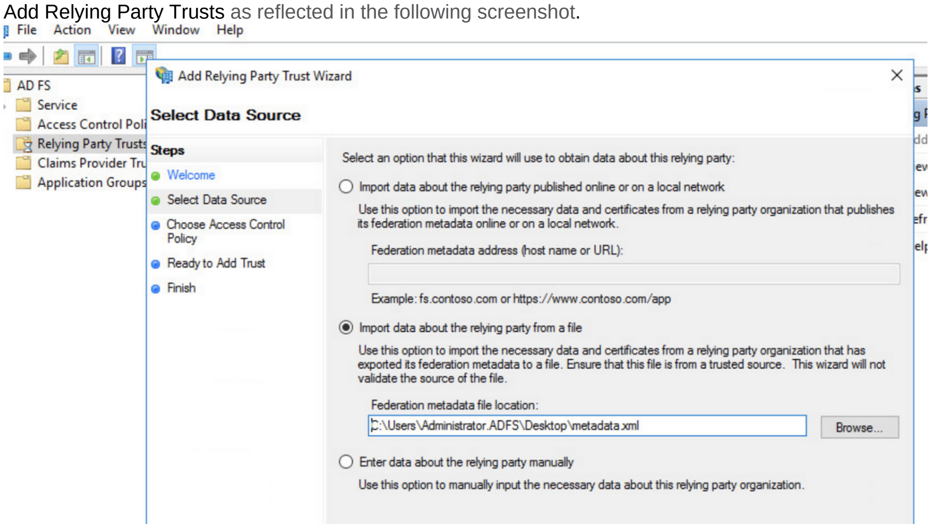
3. Download the Suite Admin's metadata file using the following URL and save it on the local disk of your Windows server.

> ✓ 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.



Select Data Source

Select an option that this wizard will use to obtain data about this relying party:

○ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

● Import data about the relying party from a file

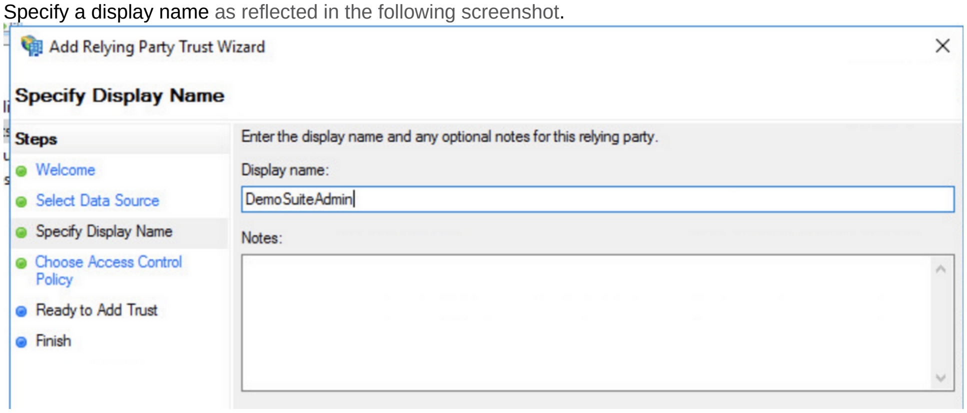
Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

Federation metadata file location: C:\Users\Administrator.ADFS\Desktop\metadata.xml

○ Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

b. Specify a display name as reflected in the following screenshot.



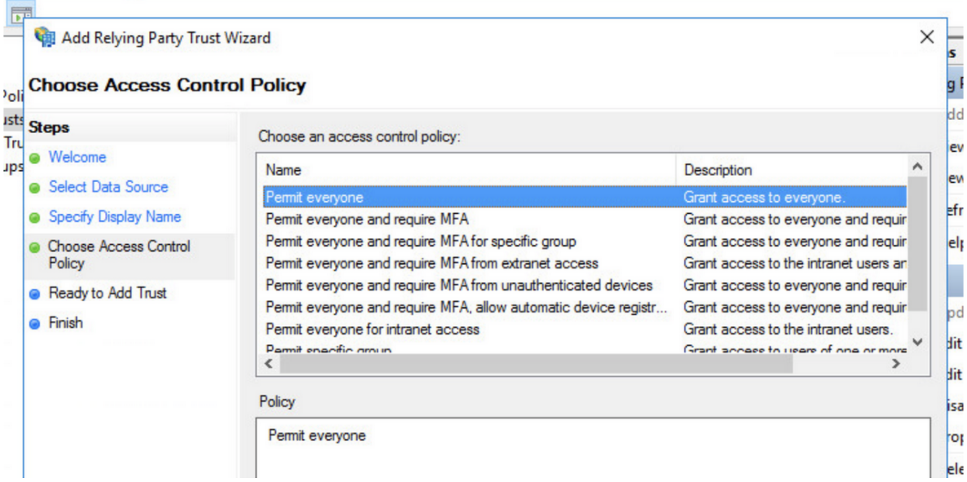
Specify Display Name

Enter the display name and any optional notes for this relying party.

Display name: DemoSuiteAdmin

Notes:

c. Select an access control policy as reflected in the following screenshot.



Choose Access Control Policy

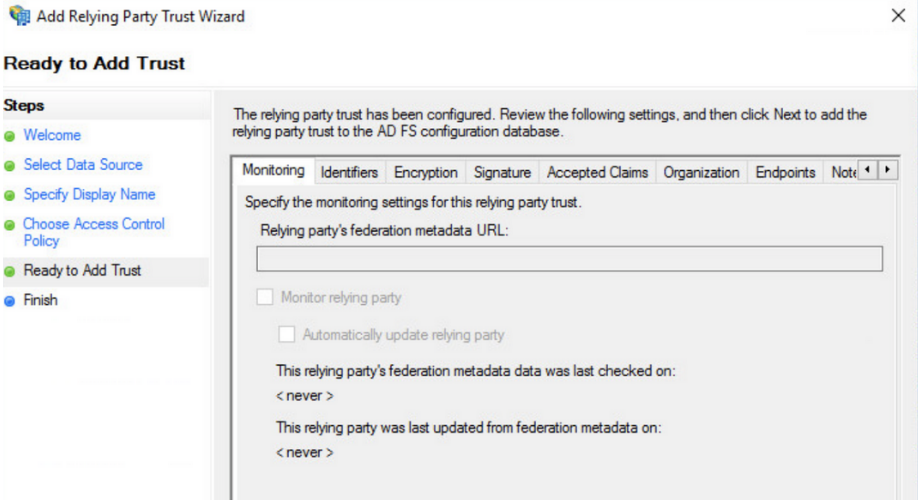
Choose an access control policy:

Name	Description
Permit everyone	Grant access to everyone.
Permit everyone and require MFA	Grant access to everyone and requir
Permit everyone and require MFA for specific group	Grant access to everyone and requir
Permit everyone and require MFA from extranet access	Grant access to the intranet users ar
Permit everyone and require MFA from unauthenticated devices	Grant access to everyone and requir
Permit everyone and require MFA, allow automatic device registr...	Grant access to everyone and requir
Permit everyone for intranet access	Grant access to the intranet users.
Permit specific group	Grant access to users of one or more

Policy

Permit everyone

d. Review the configuration and add the trust as reflected in the following screenshot.



Add Relying Party Trust Wizard

Ready to Add Trust

The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.

Specify the monitoring settings for this relying party trust.

Relying party's federation metadata URL:

□ Monitor relying party

□ Automatically update relying party

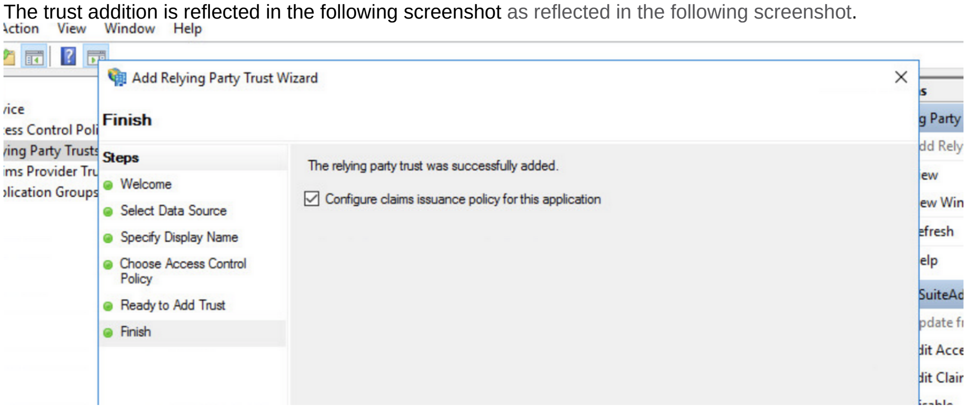
This relying party's federation metadata data was last checked on:

< never >

This relying party was last updated from federation metadata on:

< never >

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



Add Relying Party Trust Wizard

Finish

The relying party trust was successfully added.

☑ Configure claims issuance policy for this application

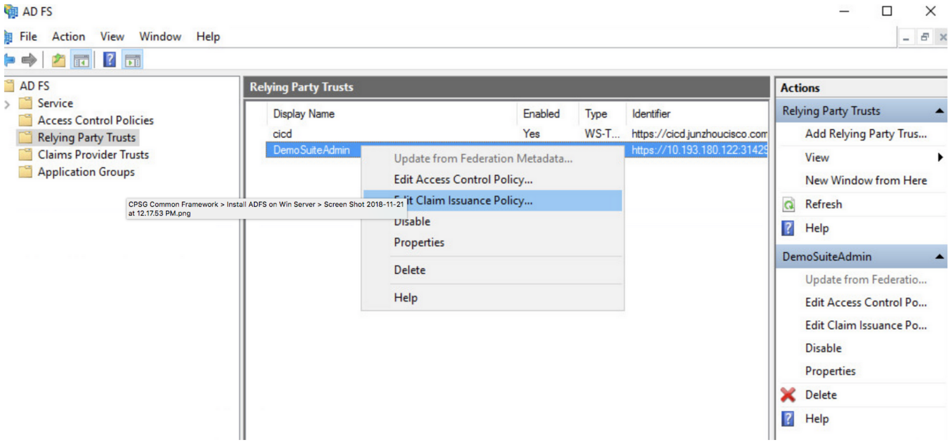
You have now established a trust between the service provider and ADFS.

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).



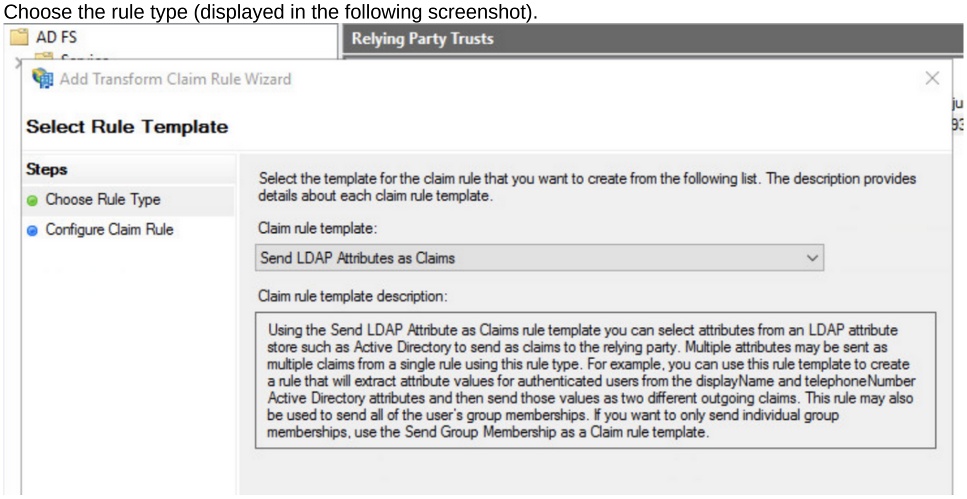
AD FS

Relying Party Trusts

Display Name	Enabled	Type	Identifier
cicd	Yes	WS-T...	https://cicd.junzhoucisco.com
DemoSuiteAdmin			https://10.193.180.122:31429

CPSG Common Framework > Install ADFS on Win Server > Screen Shot 2018-11-21 at 12.17.53 PM.png

b. Choose the rule type (displayed in the following screenshot).



Add Transform Claim Rule Wizard

Select Rule Template

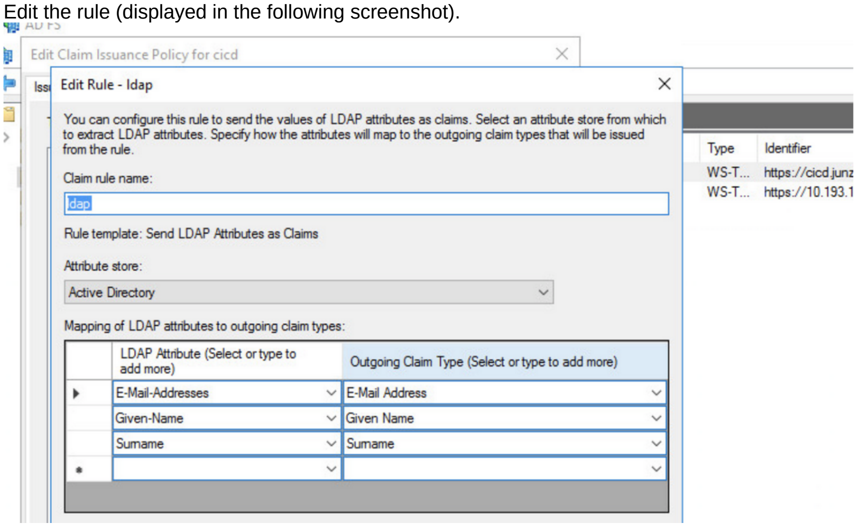
Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template: Send LDAP Attributes as Claims

Claim rule template description:

Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

c. Edit the rule (displayed in the following screenshot).



Edit Claim Issuance Policy for cicd

Edit Rule - ldap

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: ldap

Rule template: Send LDAP Attributes as Claims

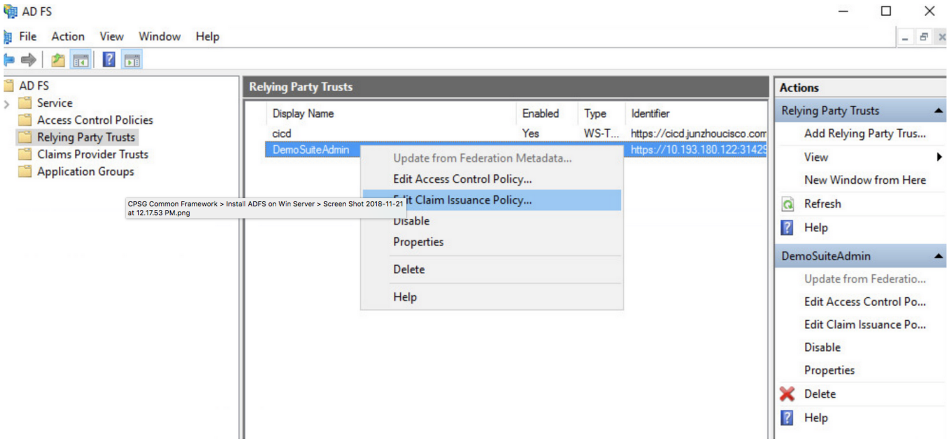
Attribute store: Active Directory

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

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.

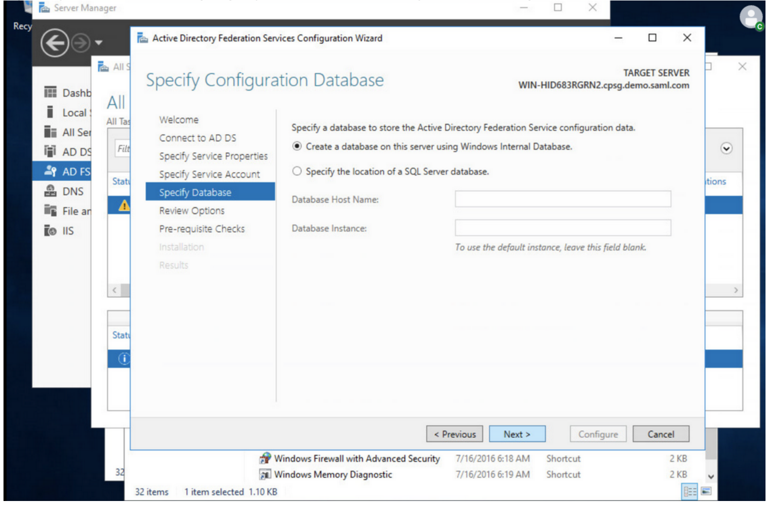
a. Edit the claim issuance policy (displayed in the following screenshot).



Display Name	Enabled	Type	Identifier
cicd	Yes	WS-T...	https://cicd.junzhoucisco.com
DemoSuiteAdmin			https://10.193.180.122:31429

CPSG Common Framework > Install ADFS on Win Server > Screen Shot 2018-11-21 at 12.17.53 PM.png

b. Specify the database (displayed in the following screenshot).



Active Directory Federation Services Configuration Wizard

Specify Configuration Database

TARGET SERVER
WIN-HID683RGRN2.cpsg.demo.saml.com

Specify a database to store the Active Directory Federation Service configuration data.

● Create a database on this server using Windows Internal Database.

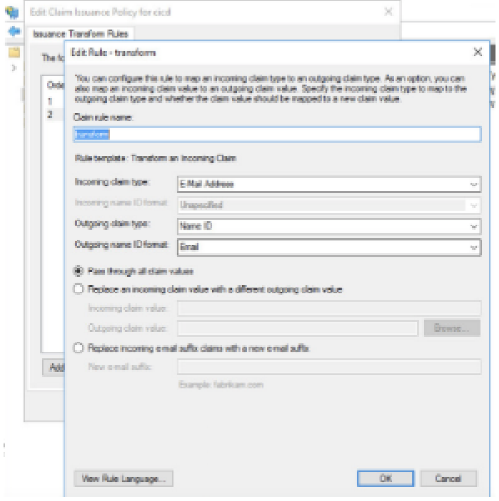
○ Specify the location of a SQL Server database.

Database Host Name:

Database Instance:

To use the default instance, leave this field blank.

c. Edit the rule (displayed in the following screenshot).



Edit Rule - transform

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name:
transform

Rule template: Transform an Incoming Claim

Incoming claim type: E-Mail Address

Incoming name ID format: Unspecified

Outgoing claim type: Name ID

Outgoing name ID format: Email

● Pass through all claim values

○ Replace an incoming claim value with a different outgoing claim value

Incoming claim value:

Outgoing claim value:

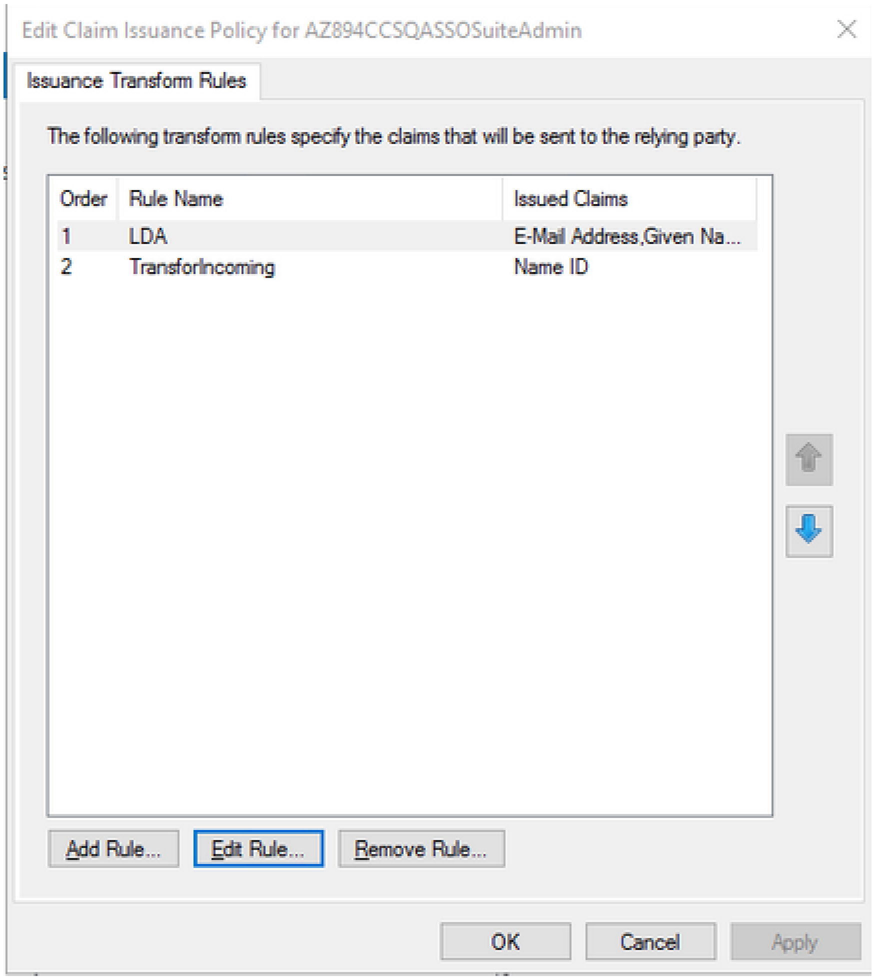
○ Replace incoming e-mail suffix claims with a new e-mail suffix

New e-mail suffix:

Example: fabrikam.com

d. Make note of the following items so you can use the same information in the Suite Admin SSO Configuration page.

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



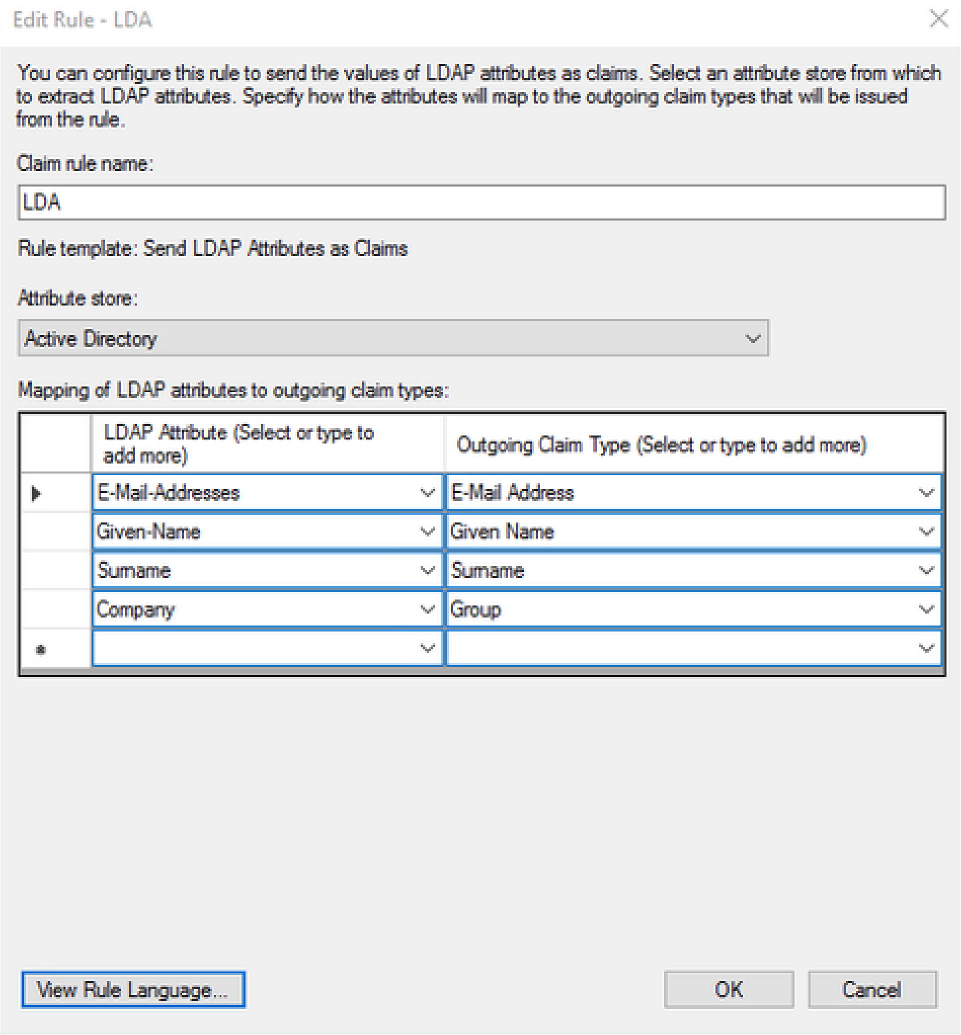
Edit Claim Issuance Policy for AZ894CCSQASSOSuiteAdmin

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

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

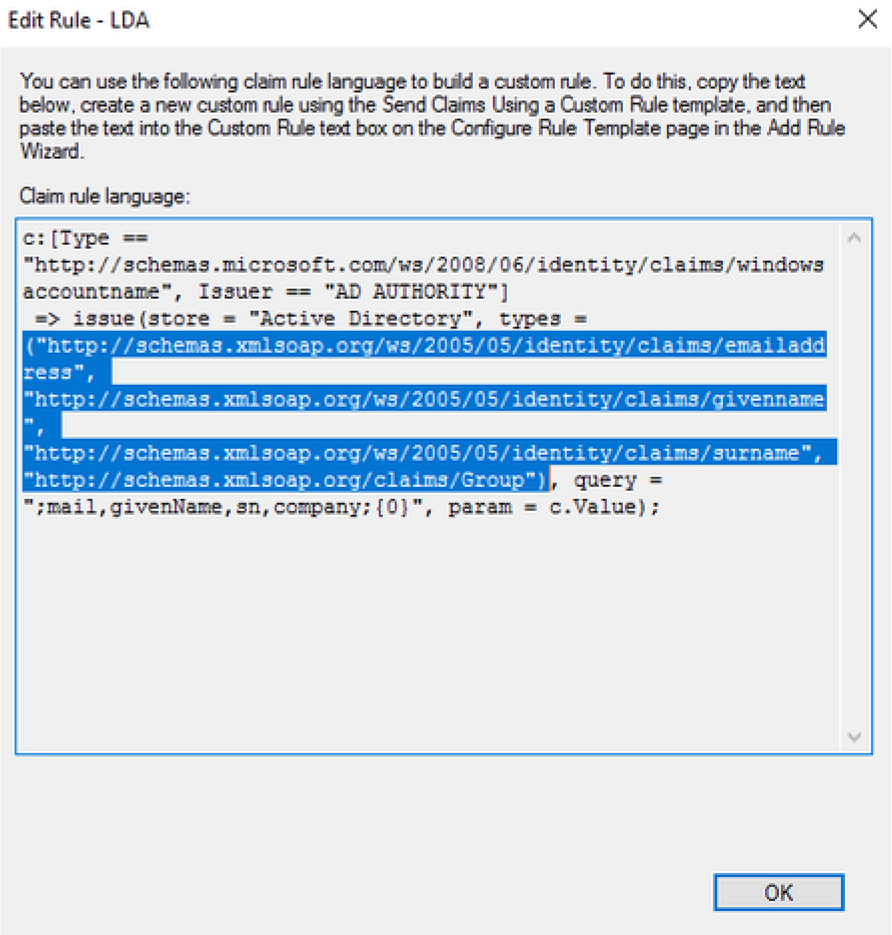
Attribute store:

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
*		

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);
```

You have now setup claim rules to transform 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>
```

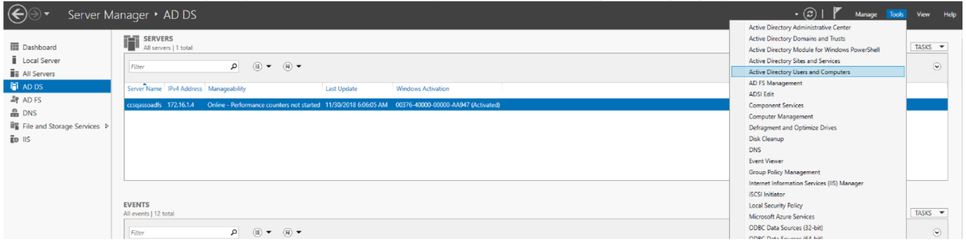
Creating a New User in ADDS

The system time for the ADFS server and the Suite Admin 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.

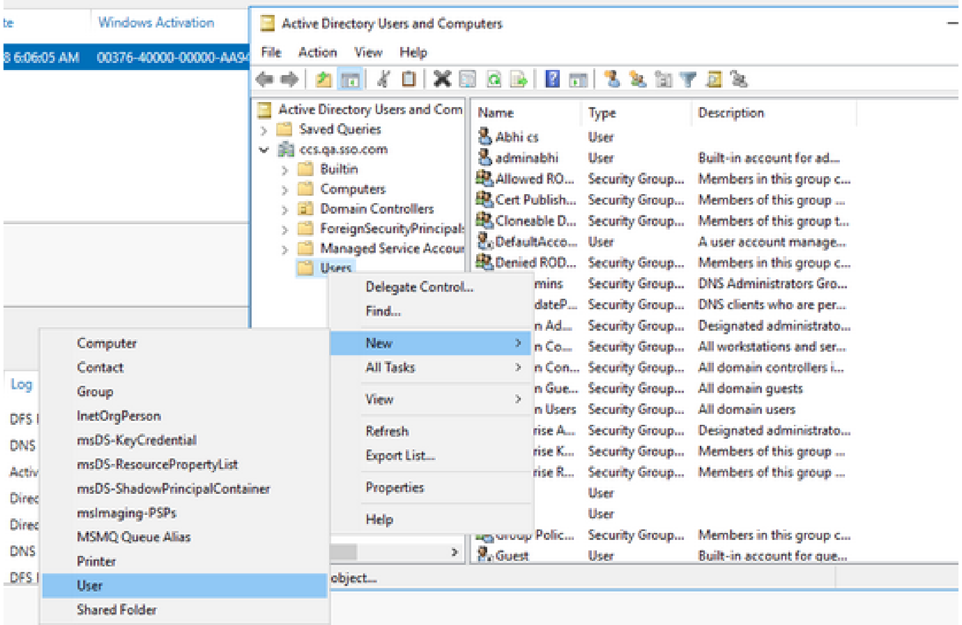
1. From the Server Manager, go to **Active Directory Users and Computers** (displayed in the following screenshot).



Server Manager ▸ AD DS
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
AD FS
DNS
File and Storage Services
IIS
SERVERS
All servers | 1 total
Filter
EVENTS
All events | 12 total
Filter
TASKS
TASKS
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
AD FS Management
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
Disk Cleanup
DNS
Event Viewer
Group Policy Management
Internet Information Services (IIS) Manager
iSCSI Initiator
Local Security Policy
Microsoft Azure Services
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)

Server Name	IPv4 Address	Manageability	Last Update	Windows Activation
ccsqassoadfs	172.16.1.4	Online - Performance counters not started	11/30/2018 6:06:05 AM	00376-40000-00000-AA947 (Activated)

2. Create a new user (displayed in the following screenshot).

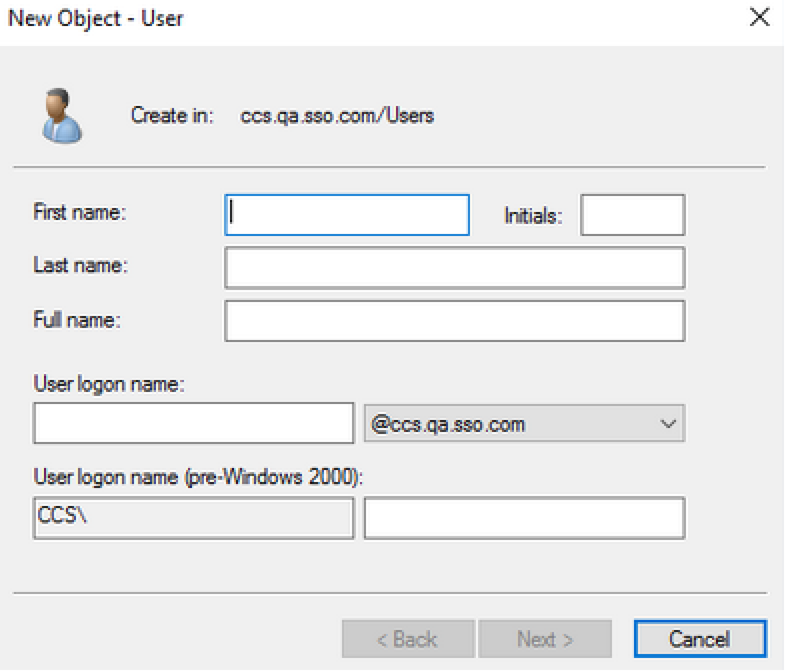


Name	Type	Description
Abhi cs	User	
adminabhi	User	Built-in account for ad...
Allowed RO...	Security Group...	Members in this group c...
Cert Publish...	Security Group...	Members of this group ...
Cloneable D...	Security Group...	Members of this group t...
DefaultAcco...	User	A user account manage...
Denied ROD...	Security Group...	Members in this group c...
mins	Security Group...	DNS Administrators Gro...
dateP...	Security Group...	DNS clients who are per...
n Ad...	Security Group...	Designated administrato...
n Co...	Security Group...	All workstations and ser...
n Con...	Security Group...	All domain controllers i...
n Gue...	Security Group...	All domain guests
n Users	Security Group...	All domain users
rise A...	Security Group...	Designated administrato...
rise K...	Security Group...	Members of this group ...
rise R...	Security Group...	Members of this group ...
	User	
	User	
Group Polic...	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...

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.



Create in: ccs.qa.sso.com/Users

First name:

Initials:

Last name:

Full name:

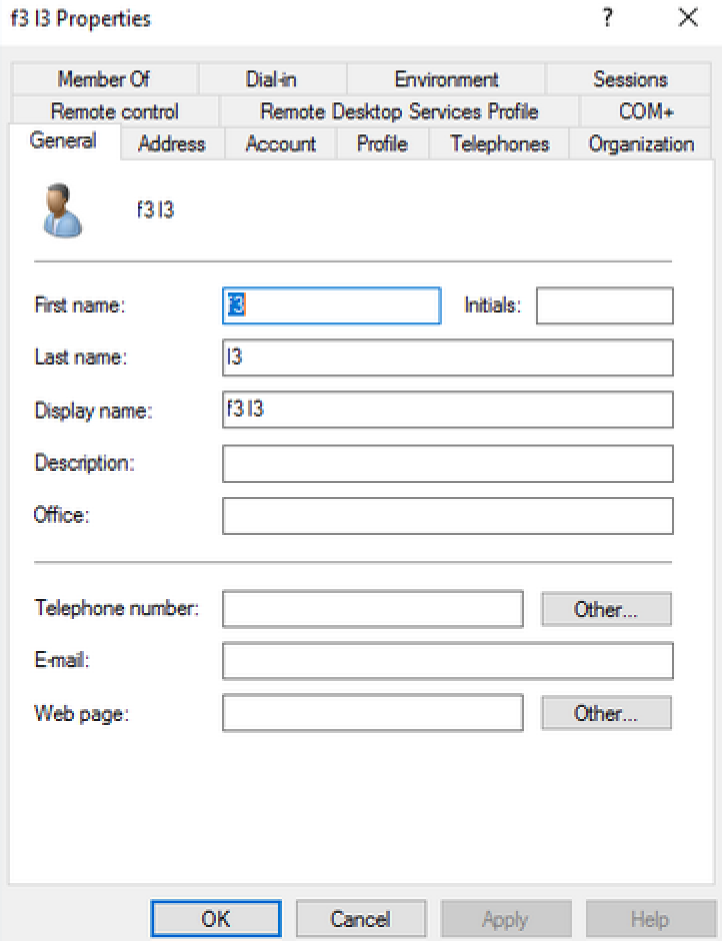
User logon name:

@ccs.qa.sso.com

User logon name (pre-Windows 2000):

CCS\

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



f3 l3

First name: f3

Initials:

Last name: l3

Display name: f3 l3

Description:

Office:

Telephone number:

E-mail:

Web page:

6. Enter the email – this information is used for authentication when this user tries login from the ADFS

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 URL page 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 the Suite Admin as listed in the previous sections.
8. Create one user in ADFS as listed in the previous sections.
9. Login into Suite Admin as 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.xml link.
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 the actual 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 the user can login to the Suite Admin and view the Product Dashboard page base on this user's permission level (see Understand 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 information again 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.

Currency Conversion

Currency Conversion

- Overview
- Process

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.

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.

Troubleshoot Suite Admin

Troubleshoot Suite Admin

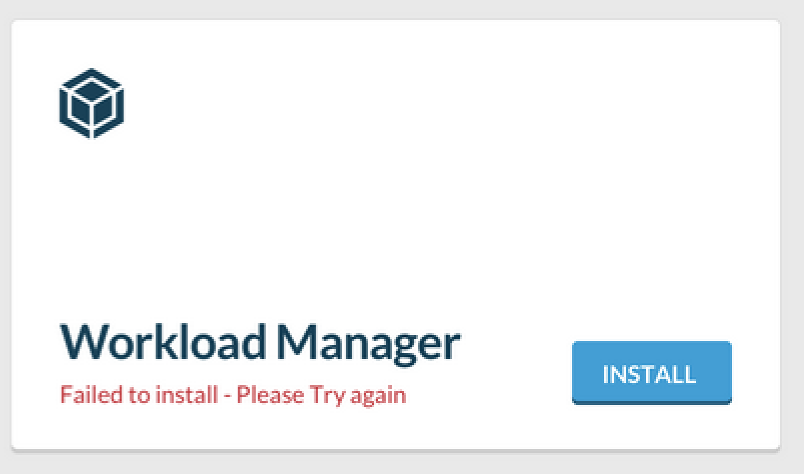
This section lists some of the issues that you may encounter and suggests workarounds.

See Monitor Modules > *Download Logs*.

See Monitor Modules > *View Logs in Kibana*.

See Monitor Modules > *Configure Grafana Dashboard Alert*.

When installing the CloudCenter Suite for a OpenStack Installation or a VMware vSphere Installation, you have the option to configure NTP 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.

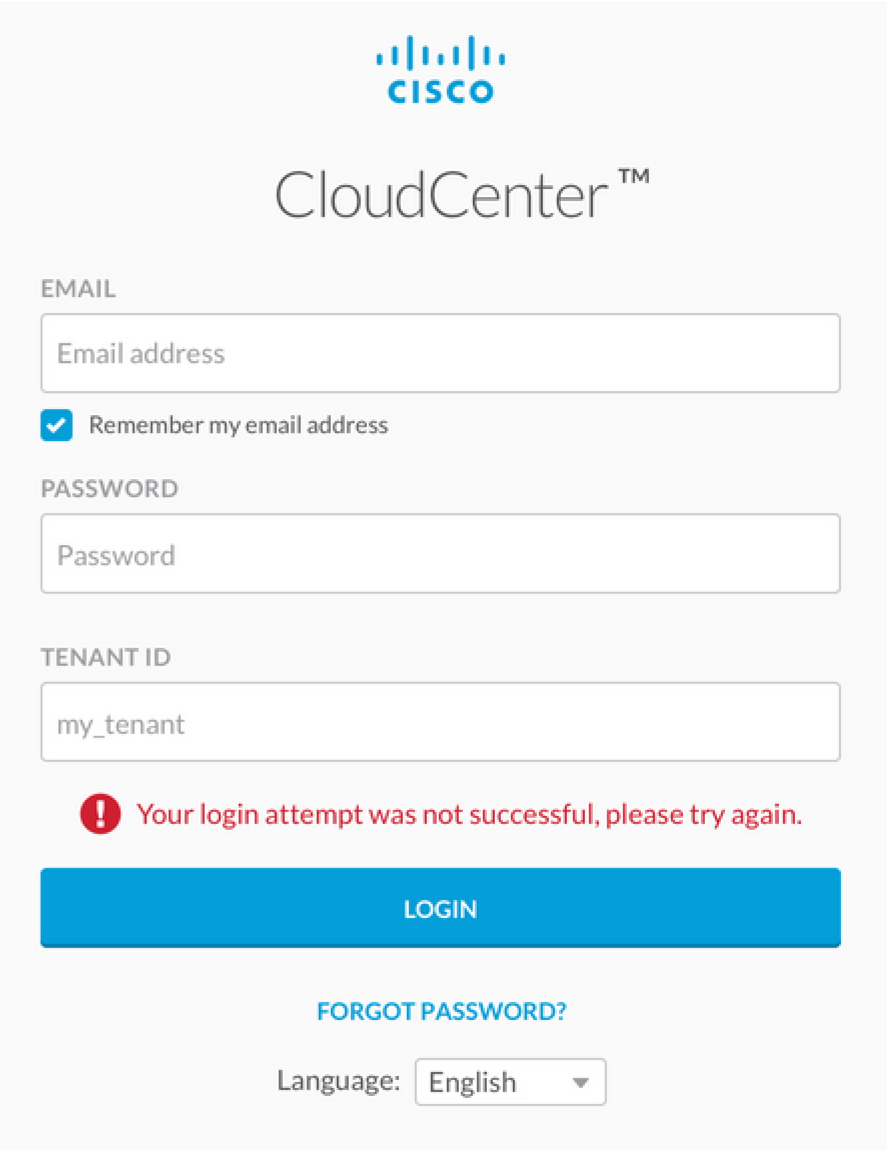


Workload Manager

Failed to install - Please Try again

To workaround this issue, be sure to synchronize the server time for all instances running the CloudCenter Suite.

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.


CloudCenter ™

EMAIL

Email address

☑ Remember my email address

PASSWORD

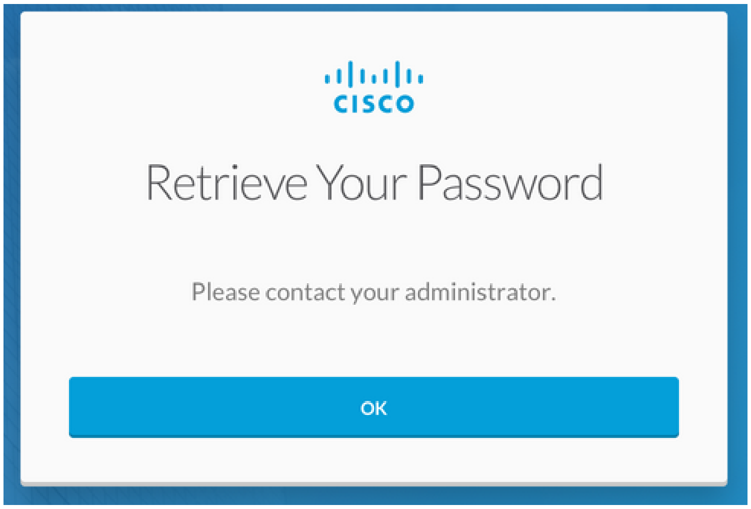
Password

TENANT ID

my_tenant

Your login attempt was not successful, please try 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).


Retrieve Your Password

Please contact your administrator.

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 Suite administrators based on their enterprise policies. If a user does not have any active roles, this user may see a blank screen on log in.

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 to login by using the direct URL (ui/auth/login).

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

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.

When you uninstall the Workload Manager or Cost Optimizer modules in the Suite Admin, the Kubernetes Persistent Volume Claims (PVCs) are not deleted – they are retained as is for the Suite Administrator to take appropriate steps to backup or manually delete the PVC. The secrets for the Workload Manager and the Cost Optimizer are 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>
  ```

Suite Admin API

Suite Admin API

API Overview

CloudCenter Suite API Overview

The payloads for the CloudCenter Suite APIs are visible in the API documentation section for each module.

CloudCenter Suite APIs provide support for the CloudCenter Suite modules: Suite Admin API, Workload Manager API, Action Orchestrator API, and Cost Optimizer API.

The User, Groups, and Tenant APIs are part of the Suite Admin and each API using these services have an additional prefix in the URI. The payloads for the CloudCenter Suite APIs are visible 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.

The CloudCenter Suite API date and time values are formatted in Unix time to the millisecond level. The APIs are agnostic to dates and time zones.

CloudCenter Suite APIs support the following request methods:

- **GET**: To query or view the server information based on a CloudCenter Suite deployment
- **PUT**: To replace the entire object for update operations
- **POST**: To perform a CloudCenter Suite task or creating the resource
- **DELETE**: To remove specific aspects of the CloudCenter Suite deployment

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

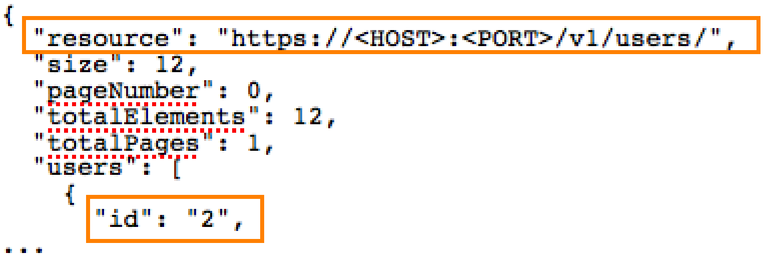
  ```
  Content-Type: application/xml Accept: application/xml
  ```

- CSV (Only for Reports)

  ✓ The CSV format only applies to report-based APIs

  ```
  Content-Type: application/csv Accept: text/csv
  ```

For each API request, you see two common attributes displayed in the API response:

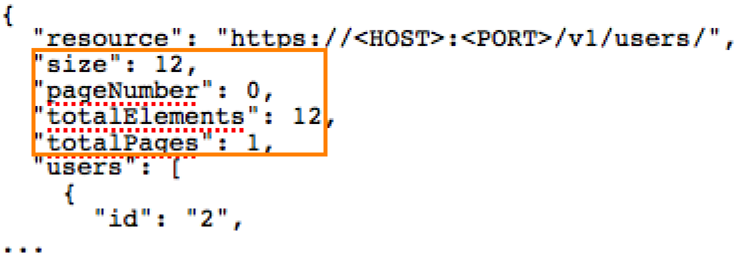


```
{
  "resource": "https://<HOST>:<PORT>/v1/users/",
  "size": 12,
  "pageNumber": 0,
  "totalElements": 12,
  "totalPages": 1,
  "users": [
    {
      "id": "2",
...
```

- The **resource** URL: A unique URL that provides access to the requested *CloudCenter Suite Resource.*
- The POST and PUT API calls additionally provide an **id** attribute for each new *CloudCenter Suite Resource*.

The pagination information differs based on the API version:

- **v1 APIs**: The GET (view or list) APIs support pagination by default. CloudCenter Suite APIs use the following attributes to provide paginated results:



```
{
  "resource": "https://<HOST>:<PORT>/v1/users/",
  "size": 12,
  "pageNumber": 0,
  "totalElements": 12,
  "totalPages": 1,
  "users": [
    {
      "id": "2",
...
```

- **v2 APIs**: Requires the *page* and *size* attributes for any request. The default size for v2 APIs now list 50 records by default.

Pagination Request Attributes

page

- **Description:** The total number of pages in for the API listing.
  - Default = 0
  - If **size=0**, then the *page* value is ignored.
  - If not specified (**page=0&size=20**), the default size (default = 20) value displays the first 20 elements, which is equal to one page
  - If you specify both the page and the size values, the following applies:

If you specify...	...then
size=21	Elements numbered 21 - 40 entities are displayed, which is equal to 2 pages
page=0 (or not specified)	The first set of 20 elements in the list, elements 1 to 20 are displayed
page=1	The second set of 20 elements in the list, elements 21 to 40 are displayed
page=2	The third set of 20 elements in the list (the third page). ✓ 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 = 20 records
  - v2 APIs = 50 records
- **Type**: Integer

Pagination Response Attributes

- v1 APIs:
  pageResource
  - **Description**: Identifies the pagination information for each resource
  - **Type**: Sequence of attributes for v1 APIs

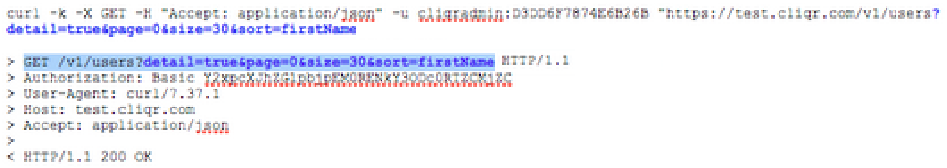
size (see above)
pageNumber • **Description**: The page number that the client wants to fetch. Page numbers start with 0 (default). • **Type**: Integer
totalElements • **Description**: The number resources that an API call returns • **Type**: Long
totalPages • **Description**: The number of pages in 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

- **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/End time for this resource. Unix epoch time in milliseconds.
- **Type**:
  - v1 APIs = Long
  - v2 APIs = Epoch time as a String

totalCost

- **Description**: Identifies the total cost per hour of the job for billing purposes. See the Cost Optimizer APIs section to view additional details.
- **Type**: Float

nodeHours

- **Description**: The number of VM hours for this resource. See the Cost Optimizer APIs section to view additional details.
- **Type**: Float

name

- **Description**: The name assigned for this *CloudCenter Suite Resource*. Valid characters are letters, numbers, underscores, and spaces.
- **Type**: String

deploymentEntity.name

- **Description**: Identifies evolving resource details about the deployment. The deploymentEntity attribute uses the *deploymentEntity.name* format, where **.name** is a search value for deploymentEntity and deploymentEntity itself is a JSON object.

  > ✓ Instead of placing the deployment name at the top level search and adding numerous query parameters, this format allows for nested search results. The top level **name** is the job name and deploymentEntity.**name** is the deployment name.

- **Type**: JSON objects

favoriteCreationTime

- **Description**: If the job was configured as a favorite job, then this attribute identifies the time when this configuration took place. See the *Favorite Deployments* section for the relevant release for additional context.
- **Type**: Epoch time as a String

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

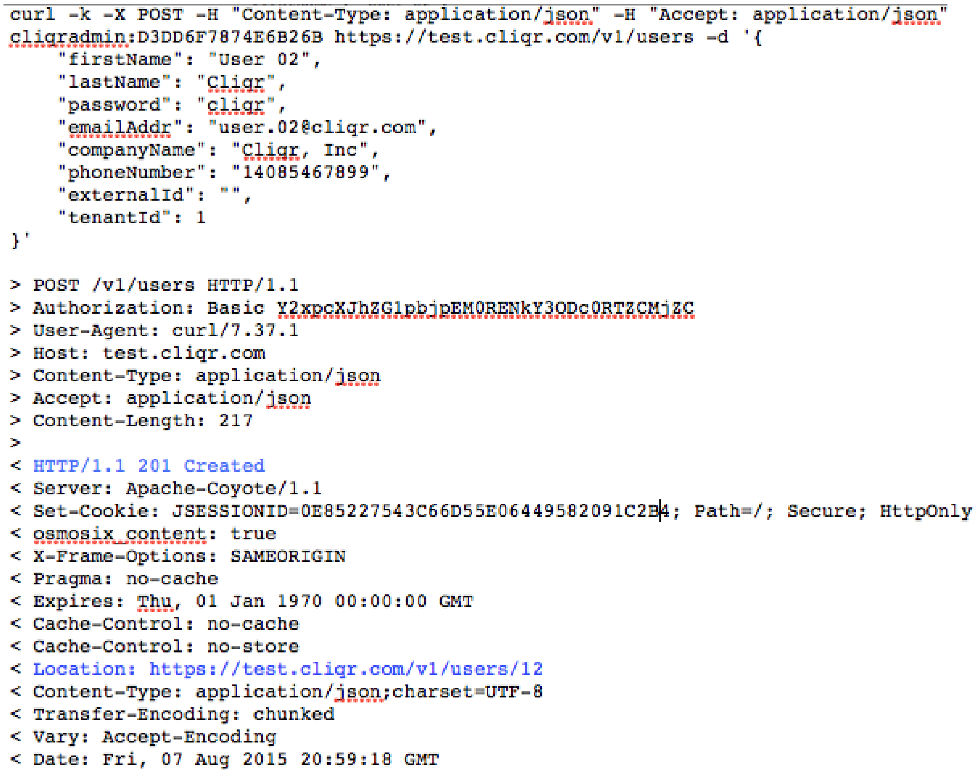
searchType	Format
eq	==
ne	!=
el	LIKE *pattern*%
fl	LIKE %*pattern*
eln	NOT LIKE *pattern*%
fln	NOT LIKE %*pattern*
fle	LIKE %*pattern*%"
gt	> *searchValue*
lt	< *searchValue*
ge	>= *searchValue*
le	<= *searchValue*
gtlt	*> searchValue && searchValue*
gtelt	*>= searchValue && < searchValue*
gtlte	*> 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

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 Y2xpcXJhZG1pbjpEM0RENkY3ODc0RTZCMjZC
> 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
```

Both admins and users can use CloudCenter Suite REST APIs.

Your login credentials determine if you are an admin (platform (root), tenant admin, or co-admin) or a user. If you do not have the required Permission Control level to access any *resource*, you receive the HTTP 403 status error mentioned in the HTTP Status Codes section.

Back to:

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

API Authentication

API Authentication

CloudCenter Suite APIs require the following authentication details for each API call:

- Username
- API access key

> The authentication HTTP header is not required when making standalone REST API calls using the username/API Key credentials.

Standalone CURL Request Example:

```
curl -H "Accept:application/json" -H "Content-Type:application/json" -u writer:BED74F4D9BFE0DA0 -X GET
https://<HOST>:<PORT>/v1/users/27
```

In this CURL request example:

- **writer1** is the username
- **BED74F4D9BFE0DA0** is the API accessKey

Your tenant administrator can retrieve the username and API access key from the UI. See API Key for additional details.

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.

The CloudCenter Suite authentication session times out after 15 minutes. If you use a REST client to make API calls by authenticating through the UI's, this session timeout applies to the REST client as well.

However, if you add and save the REST client authentication headers or if you issue CURL commands with the authentication details, you can circumvent the session timeout restriction.

Back to:

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

API Key

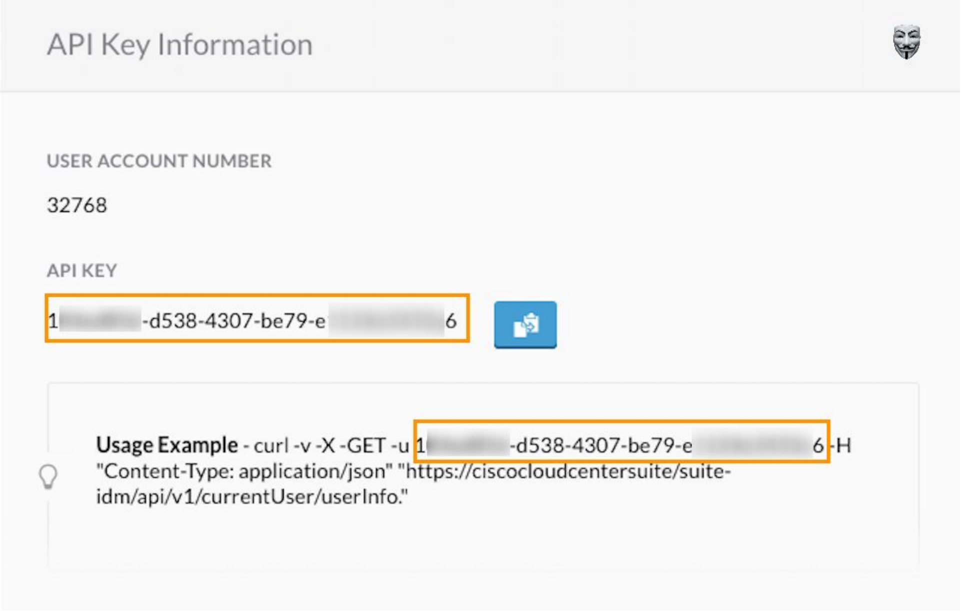
Generate API Key

- Overview
- UI Process to Generate Your Own API Key
- UI Process to Generate API Key for Another User
- API Process to Generate a New API Key

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.

To generate the API key from the UI for yourself, follow this procedure:

1. Navigate to the Suite Admin Dashboard and click your account profile dropdown.
2. Click the **Generate API Key** link to generate a new API key.
3. Click **Yes** to replace the API key. You can now use this key to make REST API calls as listed in the Usage Example in the following screenshot.



API Key Information

USER ACCOUNT NUMBER

32768

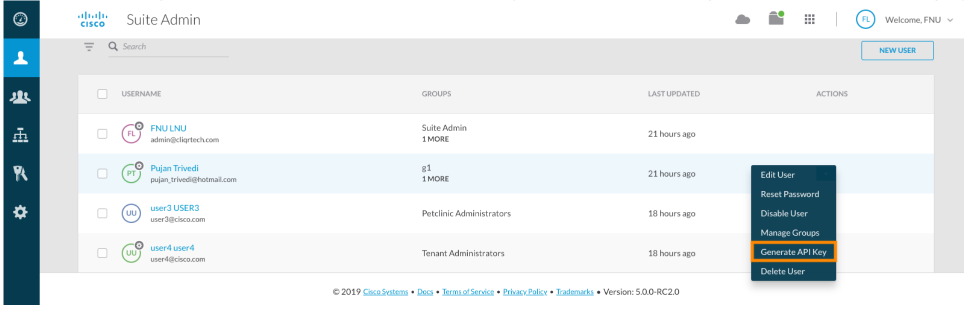
API KEY

1[redacted]-d538-4307-be79-e[redacted]6

Usage Example - curl -v -X -GET -u 1[redacted]-d538-4307-be79-e[redacted]6 -H "Content-Type: application/json" "https://ciscocloudcentersuite/suite-idm/api/v1/currentUser/userInfo."

To generate the API key from the UI for another user, follow this procedure:

1. Navigate to the Suite Admin Dashboard > **Users**.
2. Search for the required user and select **Generate API Key** from the Actions dropdown for this user as displayed in the following screenshot.



USERNAME	GROUPS	LAST UPDATED	ACTIONS
FNU LNU admin@cliqrtech.com	Suite Admin 1 MORE	21 hours ago	
Pujan Trivedi pujan_trivedi@hotmail.com	g1 1 MORE	21 hours ago	
user3 USER3 user3@cisco.com	Petclinic Administrators	18 hours ago	
user4 user4 user4@cisco.com	Tenant Administrators	18 hours ago	

Edit User
Reset Password
Disable User
Manage Groups
Generate API Key
Delete User
© 2019 Cisco Systems • Docs • Terms of Service • Privacy Policy • Trademarks • Version: 5.0.0-RC2.0

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.

To generate the API key using the Suite Admin API call, follow this procedure:

1. Issue the Password Service API Calls > **/api/v1/users/{userId}/user_api_key** API POST call to generate/regenerate the API key for yourself or for any other user.

```
POST https://host-port/suite-password/api/v1/users/1/user_api_key
```

2. Retrieve the *apiKey* from the response for this API.

```
{
   "userId":1,
   "apiKey":"1.......-d538-4307-be79-e..........6",
   "accountNumber":"32768"
}
```

3. Use this *apiKey* to make REST API calls.

Back to:

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

Base URI Format

Base URI Format

The base URI format is **https:// <host>:<port>/*...***

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.

The port is generally represented at <PORT> in all CloudCenter APIs. It represents the port used to connect to the CCO 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.

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 used to make the API call are displayed after the APIs and are called out after the description.

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 name–value pair where each element is an attribute–value 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

90

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

CSRF Token Protection

CSRF Token Protection

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

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.

To set a CSRF token, add **X-CSRF-TOKEN** to the header name (case sensitive, all uppercase).

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)

See the following request for examples of using a CSRF Token.

Java Rest Client Example

```
WebResource.Builder builder = webResource.type(MediaType.APPLICATION_JSON).header("X-CSRF-TOKEN", "<TOKEN>");
```

Python Example

```
headers = {'content-type': 'application/json', 'X-CSRF-TOKEN': '<TOKEN>'}

requests.delete(url, headers = headers, verify=False)

requests.post(url, json=jobJson, headers = headers, verify=False)
```

Where **<TOKEN>** is retrieved as specified in the *Retrieving the CSRF Token* section above.

Back to:

- Suite Admin API

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

API Permissions

API Permissions – Allowed Roles

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.

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.

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_ADMIN	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 Suite Administrator 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_PASSWORD	Users with SUITE_ADMIN permissions and/or SUITE_TENANT_ADMIN for this tenant as described in Create and Manage Users > *User Actions.* This user can perform the following tasks: • Edit any user's profile by changing the first/middle/last name and email • Configure metadata details • Configure groups • Reset password • Disable a user

See OOB Groups, Roles, and Permissions for details.

See Action Orchestrator Roles for details.

See Access and Roles for details.

Back to:

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

95

Synchronous and Asynchronous Calls

Synchronous and Asynchronous Calls

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 **Status 204 No Content** after deleting the *resource* in the background.

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 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.

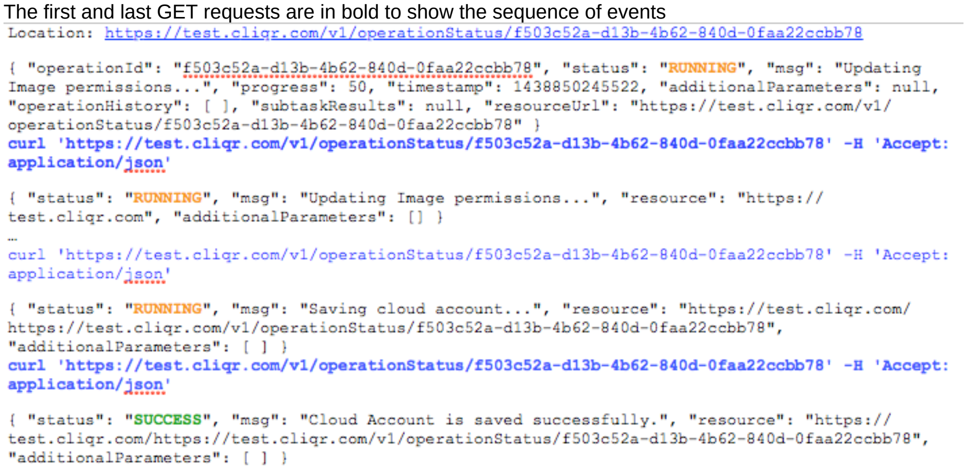
After submitting an asynchronous API call:

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

Suite Admin 5.2.0 API Calls

Suite Admin 5.2.0 API Calls

Refer to the Suite Admin 5.2 JSON files.