Dell EMC CloudLink

Version 6.8

Administration Guide for Enterprise

302-002-056

REV 12

Published February 2019

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS-IS." DELL MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. USE, COPYING, AND DISTRIBUTION OF ANY DELL SOFTWARE DESCRIBED IN THIS PUBLICATION REQUIRES AN APPLICABLE SOFTWARE LICENSE.

Published in the USA.

Dell EMC
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.DellEMC.com

CONTENTS

CHAPTER 1

Introduction

This chapter presents the following topics:

About this guide

This guide describes how to administer Dell EMC CloudLink. It is intended for CloudLink Center administrators who use the CloudLink Center administration interface to manage the security of machines registered with CloudLink Center. This guide is also intended for IT administrators who are responsible for the deployment and maintenance of machines in the CloudLink Center environment, but not necessarily for the security of data on those machines.

Related documents

The following Dell EMC publications provide additional information:

- *CloudLink Deployment Guide for Microsoft Azure*
- *CloudLink Deployment Guide for Enterprise*
- *CloudLink Release Notes*

REST documentation

CloudLink includes a comprehensive set of REST APIs. For documentation about these APIs, see **About** > **REST Documentation** in the CloudLink Center **Contents** panel.

CloudLink overview

Cloud computing offers significant benefits for deployment flexibility, infrastructure scalability, and cost-effective use of IT resources. You can take advantage of these benefits by deploying enterprise workloads in the cloud. However, because cloud computing is based on a shared, multitenant compute, network, and storage architecture, traditional security controls are not sufficient. Data owners must secure sensitive data that resides in the cloud to address privacy and regulatory compliance requirements, and satisfy requirements related to data that might remain in the cloud after it is no longer being used.

CloudLink secures sensitive information within machines across both public and private clouds. It provides encryption for the boot volume and additional data volumes with pre-startup authorization for cloud-hosted machines. CloudLink provides this encryption by using the following native operating system encryption features: Microsoft BitLocker for Windows or dm-crypt for Linux.

BitLocker and dm-crypt are proven high-performance volume encryption solutions that are widely implemented for physical machines. However, customers have not been able to use these solutions in the cloud, where you cannot use the native operating system encryption features alone to encrypt the boot volume. CloudLink solves this problem.

CloudLink's virtual machine encryption functionality enables you use native operating system encryption features to encrypt a machine's boot and data volumes in a multitenant cloud environment. This encryption helps protect the integrity of the machine itself against unauthorized modifications. CloudLink encrypts the machine boot and data volumes with unique keys that enterprise security administrators control. Neither cloud administrators nor other tenants in the cloud have access to the keys. Securing the machine lets you define the security policy that it must meet before passing pre-startup authorization, including verifying the integrity of the machine's boot chain. This offers protection against tampering.

CloudLink ensures that only trusted and verified machines can run and access sensitive data stored in the cloud. As part of the CloudLink solution, CloudLink Center defines the key release policy, performs pre-startup authorization, and monitors all CloudLink Agents, events, and logs.

Getting started

Before you can use CloudLink Center, you must deploy CloudLink into your enterprise infrastructure or into the public cloud. For deployment information, see *CloudLink Deployment Guide for Microsoft Azure* or *CloudLink Deployment Guide for Enterprise*, depending on your environment.

Use a web browser to access the CloudLink Center management interface. For more information, see Accessing CloudLink Center on page 11.

Note

CloudLink Center uses a self-signed certificate by default. You can import a certificate issued by a certification authority.

Accessing CloudLink Center

Most management tasks are performed from CloudLink Center. Access CloudLink Center from an HTTPS session by using a web browser with JavaScript enabled.

Procedure

1. In your web browser, type the CloudLink Center URL in the following format:

   ```
   https://clc_address
   ```

   where *clc_address* is the CloudLink Center address. The *clc_address* must be in either FQDN, IPv4, or IPv6 format. For more information, see CloudLink Center server address on page 11.

2. On the CloudLink Center home page, do one of the following:

   - Type a username and password.
     For information about the first-time login to CloudLink Center or about the username or password, see *CloudLink Deployment Guide for Enterprise*.
   - Click **Log in with my Windows credentials**.
     This option is available only for domain users if CloudLink Center has been joined to the Microsoft Windows domain. For more information, see Microsoft Windows domain for user accounts on page 126.

CloudLink Center server address

You use the CloudLink Center server address frequently. For example, you provide the address in the URL used to access the CloudLink Center user interface (UI), and in commands used to download installation files.

The CloudLink Center address can be configured as an IPv4 address, IPv6 address, or hostname. The address is set to IPv4 by default, but it can be changed to an IPv6 address or hostname in the Initial Configuration wizard. If the Domain Name System (DNS) has an entry for CloudLink Center, Dell EMC recommends that you specify the CloudLink Center server address as a hostname in fully qualified domain name (FQDN) format, such as clc.example.com. For more information, see Domain Name System servers on page 133. If you choose to use an IP address, use a static one.

Note

In a CloudLink Center cluster, cluster node servers and CloudLink Agents use this server address for communication. Before creating the cluster, you must specify the server address in the format you prefer for each server. You can use a mix of FQDNs and IP addresses in a cluster, but you cannot change the format after creating a cluster.

For more information about prerequisites and requirements for server addresses in clusters, see *CloudLink Deployment Guide for Microsoft Azure* or *CloudLink Deployment Guide for Enterprise*, depending on your environment.

CHAPTER 2

CloudLink Center Interface

This chapter presents the following topics:

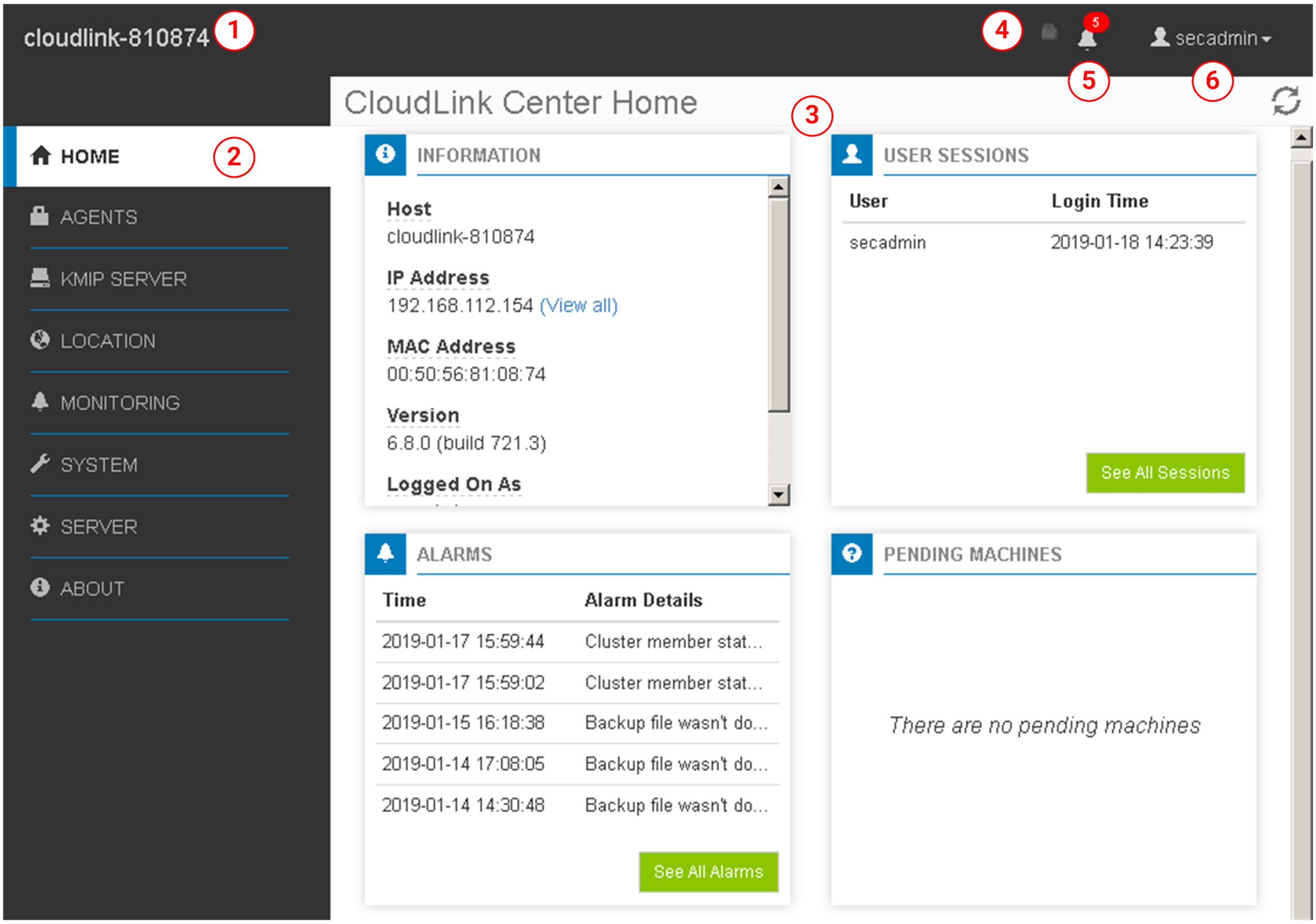
Overview

CloudLink Center provides an easy-to-use interface with many features to help you manage registered machines, and to configure and monitor the environment.

Navigating CloudLink Center

The following figure shows CloudLink Center and identifies the primary navigation features.

Figure 1 CloudLink Center Home



Host
cloudlink-810874

IP Address
192.168.112.154 (View all)

MAC Address
00:50:56:81:08:74

Version
6.8.0 (build 721.3)

Logged On As

User	Login Time
secadmin	2019-01-18 14:23:39

Time	Alarm Details
2019-01-17 15:59:44	Cluster member stat...
2019-01-17 15:59:02	Cluster member stat...
2019-01-15 16:18:38	Backup file wasn't do...
2019-01-14 17:08:05	Backup file wasn't do...
2019-01-14 14:30:48	Backup file wasn't do...

There are no pending machines

1—CloudLink Center server

Identifies the CloudLink Center server that you are logged in to.

2—Contents panel

Lists the pages that you can select in the **Edit** panel. The preceding figure shows that the **Home** page is selected.

3—Edit panel

Shows the page that is selected in the **Contents** panel.

4—Manual lock

Indicates that CloudLink Vault is locked. The Manual lock icon disappears when the CloudLink Vault is unlocked. For more information, see CloudLink Vault on page 124.

5—Alarms notification

Displays a badge with the number of current alarms, if any. An alarm represents a state or condition that you should be aware of. Click the Alarms notification icon to view alarms. For more information, see Viewing alarms on page 20.

6—User Name menu

Displays your user name. You can log out of CloudLink Center from this menu.

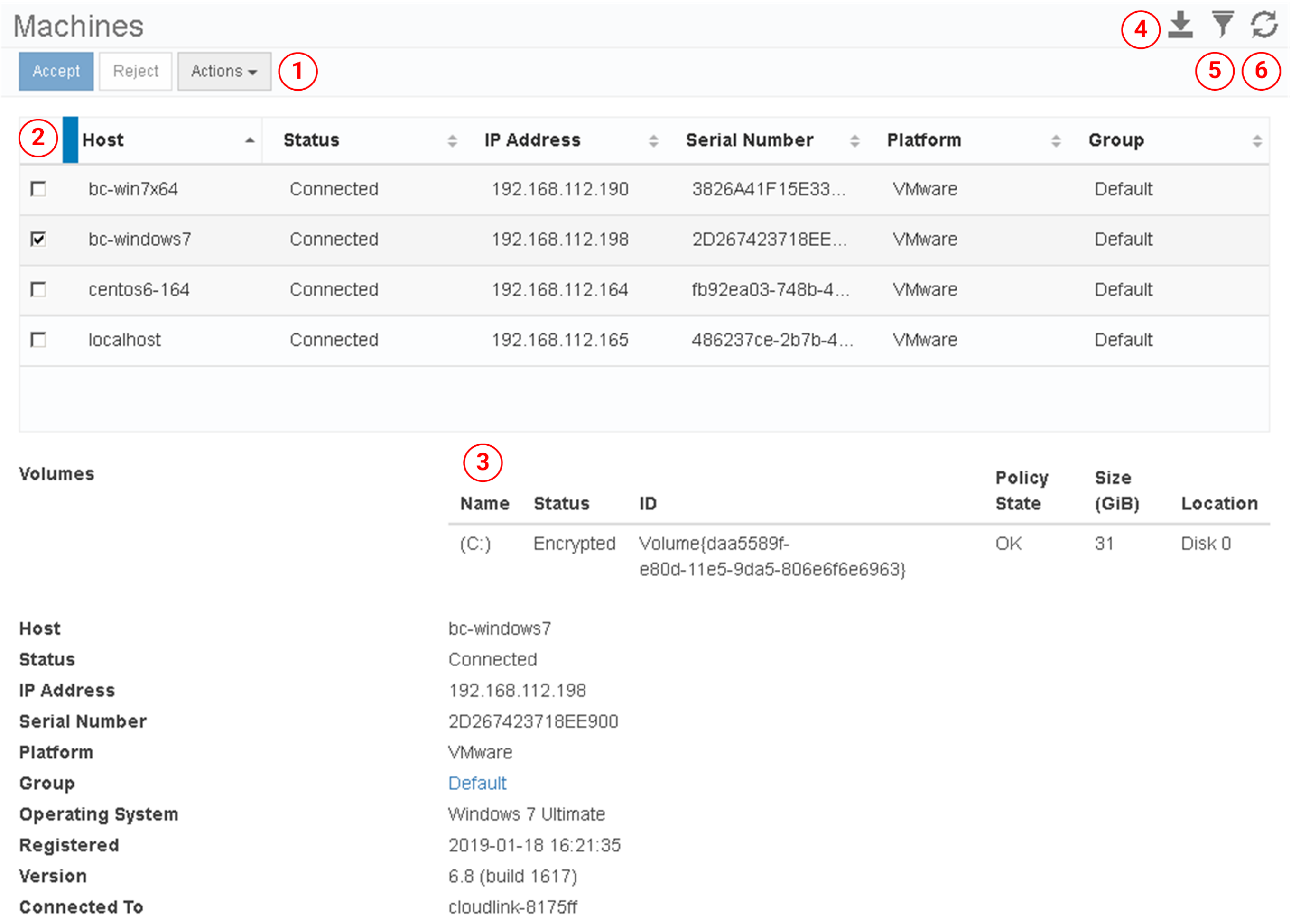
Note

Every CloudLink user is assigned a role that determines the user's permissions. If you find that some CloudLink Center features are not available to you, contact your secadmin user.

Working in the Edit panel

The Edit panel displays the CloudLink Center page that is selected in the Contents panel. The following figure shows the **Machines** page, with the primary navigation features identified.

Figure 2 CloudLink Center Edit panel



	Host	Status	IP Address	Serial Number	Platform	Group
☐	bc-win7x64	Connected	192.168.112.190	3826A41F15E33...	VMware	Default
☑	bc-windows7	Connected	192.168.112.198	2D267423718EE...	VMware	Default
☐	centos6-164	Connected	192.168.112.164	fb92ea03-748b-4...	VMware	Default
☐	localhost	Connected	192.168.112.165	486237ce-2b7b-4...	VMware	Default

Volumes

Name	Status	ID	Policy State	Size (GiB)	Location
(C:)	Encrypted	Volume{daa5589f-e80d-11e5-9da5-806e6f6e6963}	OK	31	Disk 0

Host	bc-windows7
Status	Connected
IP Address	192.168.112.198
Serial Number	2D267423718EE900
Platform	VMware
Group	Default
Operating System	Windows 7 Ultimate
Registered	2019-01-18 16:21:35
Version	6.8 (build 1617)
Connected To	cloudlink-8175ff

1—Command bar
2—Table
3—Table details
4—Export
5—Filter
6—Refresh

1—Performing actions using the command bar

The command bar includes one or more buttons for tasks you can perform on the current page, such as **Add** or **Change** and **Accept** or **Reject**. This bar might also include buttons for tasks you can perform for a selected table row.

For example, on the **Users** page, the Add button creates a new user that is then displayed in a new row in the table.

On the **Machines** page, the Actions menu provides a list of actions that you can perform on the selected table row. Based on the state of a selected machine, the actions you can perform include: encrypt, manage self-encrypting drives (SEDs), decrypt, release SEDs, remove, shred, update keys, show key history, show pending volumes/disks, move to a machine group, upgrade CloudLink Agent, and show event history.

Note

Some pages display commands in the **Edit** panel.

2—Viewing table entries

Most CloudLink Center pages include a table of relevant entries for the page. For example, the table on the **Machines** page lists the machines registered with CloudLink Center or pending registration. Similarly, the **Users** page lists all the CloudLink Center users.

The table includes a header that identifies the information provided for each entity (machines, users, and so on) in that table. Click a column name in the table header to sort the table based on that column.

For tables with more than ten rows, choose the number of rows to be displayed per page using the numbered buttons that appear below the table. When a table spans more than one page, CloudLink Center also displays pagination buttons that you can use to scroll table pages.

3—Viewing details for a table row entry

You can view details about a table row entry by selecting the table row or the checkbox in the first column of the row. Table row details are displayed below the table. For example, on the **Machines** page, select the row for a specific machine to view its details, such as its IP address, serial number, volumes and their encryption state, and so on.

To perform most tasks in the Edit panel, you must first select the table row that you want to work with.

4—Exporting table entries

You can use data available in tables in other applications. For example, from the **Machines** page, you can export the list of machines that are registered with CloudLink Center, and then include the list in a distribution report. CloudLink Center exports data to a standard comma-separated value (CSV) file in your Downloads folder.

Click the **Export** icon to export data in a table.

5—Filtering table rows

For tables with many rows, it might be difficult to quickly find a particular row or subset of rows. For example, if hundreds of machines are registered or pending registration with CloudLink Center, the Machines table spans many pages.

For convenience, use the **Filter** icon to quickly search for table rows that match criteria that you specify. When you select the Filter icon, a set of search boxes appears above the table header. Type search criteria into any of the search boxes.

To help you define criteria, keep the following in mind:

- Type text in the filter box to see all table rows that contain the text. For example, type `Connect` in the **Status** box to see all table rows where the status is Connected or Disconnected. Both these words contain the criteria Connect.
- Type an exclamation mark as the first symbol in a filter box to see all table rows that do not match the criteria. For example, type `!102` in the IP address box to see all table rows that do not contain 102 in the IP address.
- Type text enclosed in double or single quotation marks to see all table rows with an exact match for the criteria. For example, type `"Connected"` in the Status box to see only table rows where the status is Connected.
  Similarly, type `!"vmware"` in the Platform box to see all table rows where the platform is not VMware.

- Search criteria are case-insensitive. For example, `vmware` and `VMware` are considered to be the same text.

6. Refreshing the page
Generally, CloudLink Center pages show information in real time. However, to ensure that you are viewing the most current information, click the **Refresh** icon to refresh a page.

Documentation conventions for performing tasks

In this guide, topics that provide procedures include a task summary that lists:

- Permissions required to perform the procedure
- CloudLink Center panel on which the procedure is performed
- Commands used to perform the procedure

The following example of the task summary for adding a user indicates that you must:

- Have the Add User permission before you can add a user.
- Select **Configuration** > **Users** in the **Contents** panel to access the page to perform the procedure.
- Click **Add** to perform the procedure.

Task summary

Permissions	Add User
Contents panel	**Configuration** > **Users**
Commands	**Add**

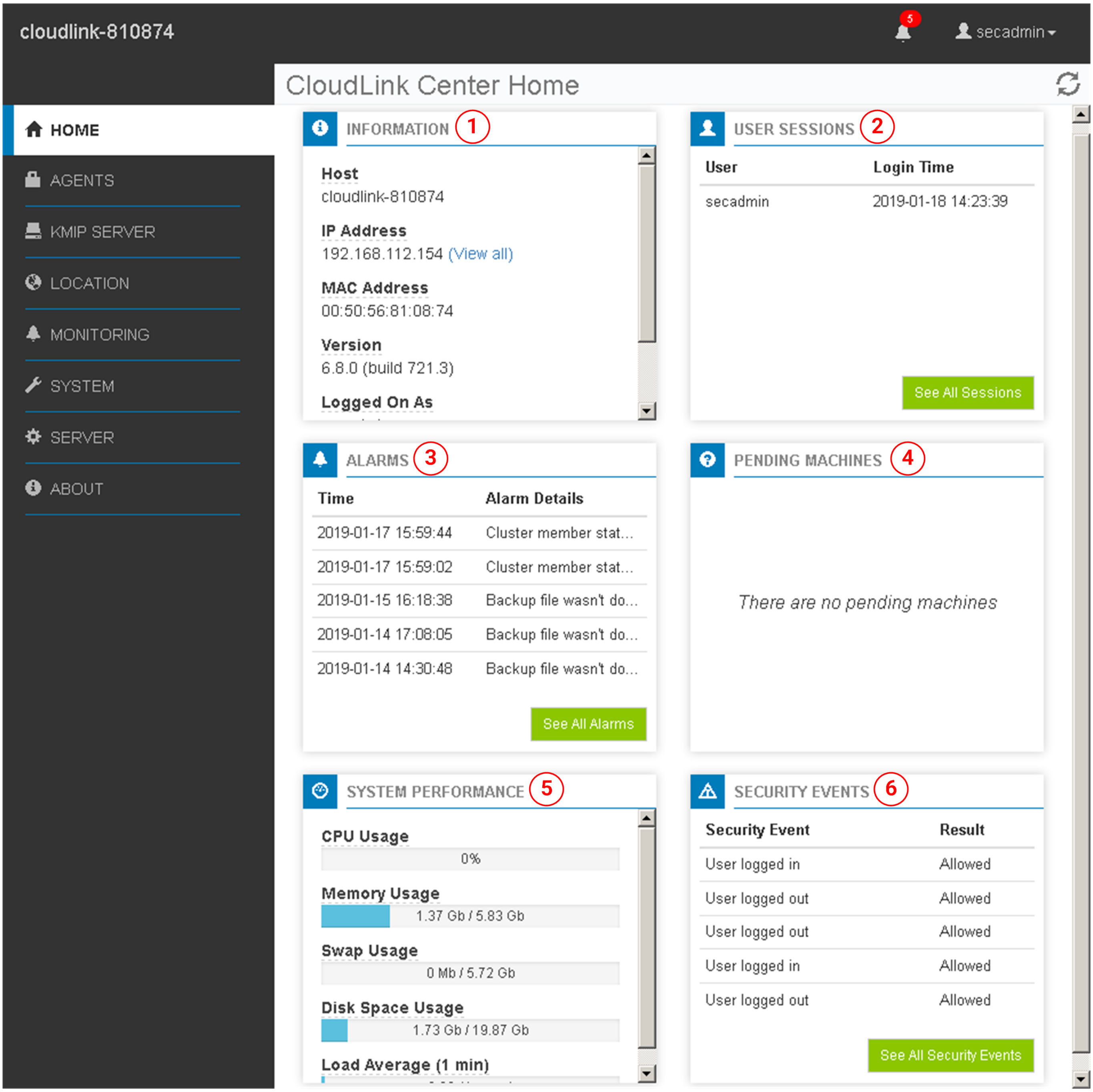
Step-by-step instructions, instead of the task summary, are provided for:

- Procedures that involve more than one task
- Procedures initiated from, or performed outside of, CloudLink Center that involve specifying URLs in a web browser or commands from the command line

CloudLink Center Home

The CloudLink Center **Home** page, shown in the following figure, provides a dashboard view of CloudLink Center.

Figure 3 CloudLink Center Home page



CloudLink Center Home

INFORMATION

Host
cloudlink-810874

IP Address
192.168.112.154 (View all)

MAC Address
00:50:56:81:08:74

Version
6.8.0 (build 721.3)

Logged On As

USER SESSIONS

User	Login Time
secadmin	2019-01-18 14:23:39

See All Sessions

ALARMS

Time	Alarm Details
2019-01-17 15:59:44	Cluster member stat...
2019-01-17 15:59:02	Cluster member stat...
2019-01-15 16:18:38	Backup file wasn't do...
2019-01-14 17:08:05	Backup file wasn't do...
2019-01-14 14:30:48	Backup file wasn't do...

See All Alarms

PENDING MACHINES

There are no pending machines

SYSTEM PERFORMANCE

CPU Usage
0%

Memory Usage
1.37 Gb / 5.83 Gb

Swap Usage
0 Mb / 5.72 Gb

Disk Space Usage
1.73 Gb / 19.87 Gb

Load Average (1 min)

SECURITY EVENTS

Security Event	Result
User logged in	Allowed
User logged out	Allowed
User logged out	Allowed
User logged in	Allowed
User logged out	Allowed

See All Security Events

The **Home** page includes the following panels:

1—Information

Provides connection information about the server on which CloudLink Center is running.

2—User Sessions

Lists the users who are currently logged in to CloudLink Center, including the time of the user's login and last action. For more information, see User sessions on page 101.

3—Alarms

Lists the alarms that are currently in effect. An alarm represents a state or condition of which you must be aware. For more information, see Viewing alarms on page 20.

4—Pending Machines

Lists the machines that are waiting for you to accept or reject startup. For more information, see Accepting or rejecting a pending machine on page 75.

5—System Performance

Provides information about the server that is hosting CloudLink Center, including CPU and memory usage, available disk space, and so on.

6—Security Events

Provides information about user logins, failed vault unlock attempts, machine registration, changes to the CloudLink Vault, secure user actions, and encryption key activities. For more information, see Monitoring CloudLink Center on page 93.

Viewing alarms

An alarm represents a state or condition of which you must be aware. When one or more alarm conditions exist, CloudLink Center displays a badge on the Alarms icon in the **Home** page. The badge shows the number of alarms.

Click the Alarms icon to view the list of alarms. CloudLink Center removes alarms from this table only when the condition or state that raised the alarm is resolved. For example, CloudLink Center raises an alarm if a backup file is generated but not downloaded. When you download the backup file, the alarm disappears.

An alarm generates at least one event. For more information, see Viewing events on page 95.

Task summary

Permissions	View Alarms
Contents panel	n/a
Commands	n/a

Alarms table information

The Alarms table includes the following information for each alarm:

Name

A summary of the condition that triggered the alarm.

Timestamp

The date and time that the alarm occurred.

Host

The CloudLink Center server on which the alarm was raised.

Target

The object that generated the alarm.

Severity

An indicator of how quickly your attention is required. The severity is either High or Low.

For example, if the keystore is inaccessible, **Host** shows the CloudLink Center server hosting the keystore and **Target** shows the name of the keystore.

Alarms details

For some alarms, details are provided in addition to information provided in the Alarms table. For example, when a machine is put in the pending state, alarm details provide the reason.

CHAPTER 3

Managing Roles

This chapter presents the following topics:

Overview

A role determines the permissions in CloudLink Center of users who are assigned that role. For example, you may assign one or more users the Admin role, which lets them perform many administrative functions in CloudLink Center. However, this role does not permit its users to perform functions that require the higher level of security available in the SecAdmin role, such as keystore configuration.

Built-in roles

CloudLink Center provides three built-in roles: SecAdmin, Admin, and Observer. You can define additional roles to customize the permissions allowed for users assigned to that role, as required.

- SecAdmin has full access to all CloudLink Center functionality, including managing user accounts, configuring keystores, and accessing events log.
  The SecAdmin role has permission to view and manage all objects (such as a role, user, keystore, or machine group). For example, a user assigned the SecAdmin role can see all machine groups, regardless of the managing role assigned to individual machine groups.
- Admin has limited access to CloudLink Center functionality, primarily for managing user accounts and backups, and viewing event logs.
- Observer can view configuration options and event logs.

CloudLink Center provides one built-in user account that is assigned the SecAdmin role. For more information, see Built-in secadmin user on page 30. CloudLink Center does not provide built-in user accounts for Admin or Observer roles. If built-in roles do not meet your requirements, you can create custom roles. For more information, see Creating roles on page 26.

Implicit permissions

For a given object (such as a role, user, keystore, or machine group), a role with permissions that allow changes to that object automatically includes any view permissions. For example, if a role includes the Add User or Delete User permission, the role automatically includes the View Users permission, even if it is not explicitly assigned.

Managing custom roles

Every custom role has a role that administers it (referred to as the managing role). Only users belonging to a managing role for a role can administer it and administer users belonging to that role.

For example, to delete a role named TestRole, you must be a user assigned to a role that is identified as a managing role for TestRole and that managing role must contain the Delete Role permission. To add a user in TestRole, you must be a user assigned to a role that is identified as a managing role for TestRole and that managing role must contain the Add User permission.

You can assign one or more managing roles to a role. For example, an IT – East Coast role might be managed by both the IT – North America role and the IT – US role.

You assign managing roles when creating a custom role. For more information, see Creating roles on page 26. Managing roles for a custom role can be changed by users belonging to one of those managing roles. For more information, see Changing managing roles on page 27. For information about permissions available for custom roles, see Permissions and Roles on page 157.

Note

This guide assumes that you belong to the appropriate managing roles to perform tasks.

Role administration example

To understand custom role management, let’s look at a few examples. For these examples, a user named John has three roles:

- Role Creator with only the Add Role permission
- East Coast User Management with the Add User and Change User Password permissions
- Role Deleter with Delete Role permission

To create a new role, a user must have the Add Role permission. They can acquire this permission from any role they belong to. For example, if John belongs to three roles and any of those roles contains Add Role, he is allowed to create a new role and set any role as the managing role. John has the Add Role permission from his membership in Role Creator.

To delete a role, the user must have the Delete Role permission and that permission must come from one of the role's managing roles. For example, if John wants to delete TestRole, then Role Deleter must be one of the managing roles. If only East Coast Management was one of the managing roles, John can manage users with this role but John cannot delete it.

To change a user's password, the user must have the Change User Password permission for all of the roles that a user belongs to. For example, to change John's password, another user requires the Change User Password permission via a managing role for Role Creator, East Coast User Management, and Role Deleter.

Viewing roles

You can view existing roles, which include the built-in roles and any custom roles that you have defined.

Task summary

Permissions	View Roles
Contents panel	**System** > **Roles**
Commands	n/a

Roles table information

The Roles table includes the following information for each role:

Name

The name of the role.

Description

A description that meaningfully identifies the purpose or scope of the role.

Built In

A flag that identifies whether the role is provided with CloudLink Center.

Managed By

The names of the roles that administer this role. For information, see Managing custom roles on page 24.

Role details

In addition to the information provided in the Roles table, details for a selected role include:

Permissions

A list of permissions assigned to this role. For information, see Permissions and Roles on page 157.

Creating roles

If built-in roles do not meet your requirements, you can create roles to customize the permissions for users assigned to that role, as required. For more information about built-in roles, see Built-in roles on page 24.

A custom role can include any combination of permissions. For example, you might create a custom role named AdminDelegate that allows only a subset of Admin permissions, such as unlocking accounts. In the event that an Admin user is not available, the AdminDelegate is available to help users who are locked out of their accounts. This AdminDelegate role cannot perform more sensitive activities, such as changing passwords.

A user can be assigned multiple roles, which gives them a combined set of permissions. For more information, see Adding users on page 32.

Task summary

Permissions	Add Role
Contents panel	**System** > **Roles**
Commands	**Add**

Role values

When creating a role, provide the following values:

Name

The name of the role.

Description

A description that meaningfully identifies the purpose or scope of the role.

Use Permissions From

An existing role from which you want to copy permissions.

Permissions

A list of permissions assigned to this role. The initial permissions are the same as those for the role selected in Use Permissions From. Customize the permissions for the role you are creating. For information about permissions, see Permissions and Roles on page 157.

Managed By

The names of the roles that administer this role. For information, see Managing custom roles on page 24.

Modifying roles

You can modify any role, except built-in roles.

Task summary

Permissions	Modify Role
Contents panel	**System** > **Roles**
Commands	**Modify**

Role values

When modifying a role, change the following values:

Description

A description that meaningfully identifies the purpose or scope of the role.

Permissions

A list of permissions assigned to this role. Customize the permissions as required. For information about permissions, see Permissions and Roles on page 157.

Changing managing roles

You can change the managing role for a role. For example, a change to your organization’s structure may mean that a particular managing role no longer has the authority to manage one of its current roles. For more information, see Managing custom roles on page 24.

Prerequisites

You must be a user who is assigned to a role that manages the role you want to change.

Task summary

Permissions	Change Role Administration
Contents panel	**System** > **Roles**
Commands	**Change Managing Roles**

Role values

When changing a managing role, you provide the following value:

Managed By

The names of the roles that administer this role. For information about custom role administration, see Managing custom roles on page 24.

Deleting custom roles

You can delete custom roles.

Prerequisites
You must be a user who is assigned to a role that manages the role you want to delete.

Task summary

Permissions	Delete Role
Contents panel	**System** > **Roles**
Commands	**Delete**

CHAPTER 4

Managing Users

This chapter presents the following topics:

Overview

Each person who needs to work with CloudLink must be defined as a user in CloudLink Center. Each user is assigned a role that determines their permissions in CloudLink Center.

You can also use existing user accounts in your organization's Microsoft Windows domain and assign those accounts the appropriate CloudLink Center role.

A user can be assigned multiple roles, giving them a combined set of permissions.

Built-in secadmin user

CloudLink Center provides one built-in user with the user name secadmin, and assigned the SecAdmin role. For more information, see Built-in roles on page 24.

First-time access to CloudLink Center after deployment requires logging in as this secadmin user, providing a default password. The default password is changed by the secadmin user immediately after first-time login to CloudLink Center. For information about first-time login to CloudLink Center, including the default password used, see *CloudLink Deployment Guide* for your environment.

After deployment, you can continue using this built-in secadmin user. You cannot delete this user, change its user name (secadmin), or change its role. These restrictions mean that no administrative activity can result in you being completely locked out from CloudLink Center. Dell EMC recommends that you store the built-in secadmin account credentials safely in a location with access only by trusted security officers. You can create other user accounts for daily operations.

User account types

You can create the following types of CloudLink Center user accounts:

Local

These user accounts existing only in CloudLink.

Domain

These user accounts represent existing user accounts in your organization's Microsoft Windows domain.

Domain Group

These user accounts represent existing group accounts in your organization's Microsoft Windows domain. CloudLink supports only Active Directory universal groups.

Client

These user accounts are intended only for use with the REST APIs. You must provide a name and secret for authenticating to the REST APIs from a client application. For more information, see the REST API documentation.

For more information, see Adding users on page 32.

Local accounts

Local user accounts exist only within CloudLink. To log in to CloudLink Center, local users provide a password that you define when setting up the account.

Domain and domain group accounts

Rather than creating users specifically for your CloudLink needs, you can use existing accounts in your organization’s Microsoft Windows domain and assign those accounts to the appropriate CloudLink Center role.

Domain accounts are convenient because:

- If CloudLink Center has been configured to use Integrated Windows Authentication (IWA), domain users and groups can use their Windows login credentials to log in to CloudLink Center.
- If you use Windows domain groups, you can create a user in CloudLink Center that corresponds to it. You do not need to create a domain account in CloudLink Center for every user in the Windows domain group.

  This practice is useful if you have a Windows domain group for administrators and you want all administrators to have access to CloudLink Center. For security, CloudLink Center uniquely records audits for actions taken by each administrator. If an administrator belongs to more than one Windows domain group, and two or more of these groups have corresponding user accounts in CloudLink Center, the administrator has all the privileges of all their user accounts.

Before you can add domain accounts, you must configure a Microsoft Windows domain. For more information, see Configuring a Microsoft Windows domain on page 127.

Note

You must set the domain group's scope to Universal so CloudLink can correctly check users' group membership.

Two-factor authentication

To access CloudLink Center, a user must provide both a user name and password. For increased security, you may require a user to log in using two-factor authentication. After providing the CloudLink Center credentials, the user must provide additional credentials generated by a third-party provider.

CloudLink supports two-factor authentication using these third-party providers:

- Google Authenticator—This application is typically installed on the user’s mobile device and generates a token that the user provides as the additional credentials when logging in to CloudLink Center.
- RSA SecurID—A hardware or software token generates a tokencode that the user provides as the additional credentials when logging in to CloudLink Center.

Two-factor authentication is available for individual local and domain users, but not for domain group users. For more information, see User account types on page 30.

Note

If you configure CloudLink Center to use Integrated Windows Authentication (IWA) and two-factor authentication, CloudLink Center uses only the IWA credentials for domain users.

Before you can set up users for two-factor authentication using RSA SecurID, you must configure the RSA Authentication Manager. For more information, see RSA Authentication Manager on page 128.

Viewing users

You can view existing users.

Task summary

Permissions	View Users
Contents panel	**System** > **Users**
Commands	n/a

User Accounts table information

The User Accounts table includes the following information for each user account:

User Name

Identifies the user in the system. If the user type is domain, this value is the exact username from the domain user account.

Access Roles

Identifies the role for the user that determines the user's access permissions. For more information, see Managing Roles on page 23.

User Type

Identifies whether the user is a local, domain, domain group, or client user. For more information, see Adding users on page 32.

Built-in

Displays Yes for built-in users and No for users you have created.

Locked

Indicates whether the user has been locked out of CloudLink Center because of too many incorrect login attempts. For more information, see Unlocking accounts on page 35.

2fa

Indicates whether the user is required to log in to CloudLink Center using two-factor authentication. For more information, see Local accounts on page 31. Values include: None, RSA SecurID, or Google.

Adding users

Every CloudLink Center user must have an account. The account information uniquely identifies the user and determines their access permissions in CloudLink Center.

Prerequisites

If you are adding a user that represents a Windows domain group, the user must already exist in the Windows domain. CloudLink does not validate user presence in a Windows domain.

Task summary

Permissions	Add User
Contents panel	**System** > **Users**
Commands	**Add**

User values

When creating a user, provide the following values:

User Name

Identifies the user in the system. If the user type is Domain or Domain Group, type the exact account name as defined in the Windows domain.

Access Roles

Identifies the role for the user that determines the user's access permissions. For more information, see Managing Roles on page 23.

User Type

Identifies whether the user is a local or domain user.

2fa Type

Indicates whether the user is required to log in to CloudLink Center using two-factor authentication. For more information, see Two-factor authentication on page 31. Values include: None, RSA SecurID, or Google.

Domain Name

Name of the Windows domain to which the user belongs.

Password/Confirm Password (local users only)

Defines the user's initial password.

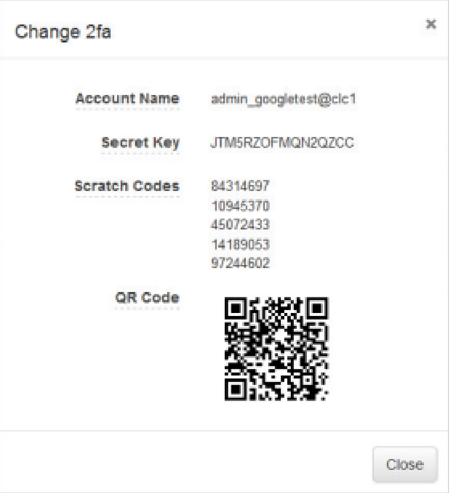
Change Password (local users only)

Determines whether the user must change the initial password on first login (**On the first login**) or when they choose to (**On demand**).

Additional account set up for Google two-factor authentication

For users with **2fa Type** set to Google, a dialog box similar to the following is displayed after you create a user:

Figure 4 Change 2fa page



Change 2fa

Account Name: admin_googletest@clc1

Secret Key: JTM5RZOFMQN2QZCC

Scratch Codes:
84314697
10945370
45072433
14189053
97244602

QR Code

You must ask the user to scan the QR code using the Google Authenticator application on the user’s mobile device. Alternatively, you can provide the user with the Account Name and Secret Key value, which the user can enter manually into the Google Authenticator application. For manual entry, ensure the time-based option is selected in Google Authenticator.

Note

You may also want to provide the user with the Scratch Codes. Each of these codes can be used once instead of the randomly generated token to log in to CloudLink Center. These codes are intended only for exceptional circumstances, where the user may not have access to Google Authenticator and must log in to CloudLink Center.

Changing user roles

You can change the role of users to another existing role.

Task summary

Permissions	Change User Roles
Contents panel	**System** > **Users**
Commands	**Actions** > **Change Roles**

User Role values

When changing user roles, provide the following value:

Roles

The roles for the user, which determines the user’s access permissions. You can assign more than one role to a user. For more information, see Built-in roles on page 24.

Changing user passwords

You can change the CloudLink Center password for users. You must provide the new password and confirm it.

Note

Users can change their own password, regardless of whether they have the Change User Password permission. Users can change their own passwords using the Change Password option in the **User Name** menu.

Task summary

Permissions	Change User Password
Contents panel	**System** > **Users**
Commands	**Actions** > **Change Password**

Change Password values

When changing another user's password, provide the following values:

New Password/Confirm Password

Defines the user's initial password

Change Password

Determines whether the user must change the initial password on first login (**On the first login**) or when they choose to (**On demand**)

Changing two-factor authentication

You can change whether a user is required to log in to CloudLink Center using two-factor authentication. For more information, see Two-factor authentication on page 31.

If you change a user to require Google two-factor authentication, a new account must be created in Google Authenticator using the credentials that CloudLink Center displays after you change the two-factor authentication type. For information, see Additional account set up for Google two-factor authentication on page 33.

Task summary

Permissions	Change User Second Factor
Contents panel	**System** > **Users**
Commands	**Actions** > **Change 2fa**

Unlocking accounts

For security, local users, including the built-in secadmin user, have a limited number of attempts to provide the correct password when logging in to CloudLink Center. After the specified number of login attempts, the user is locked out of the account.

When a user is locked out of their account, CloudLink Center displays a message below the Password box indicating that the account is locked. The account is automatically unlocked after fifteen minutes. If the user requires immediate access, the account must be manually unlocked.

For more information about setting the number of login attempts, see Changing the number of login attempts before lockout on page 133.

You can identify users who have been locked out on the Users page. For these users, the table displays **Yes** in the **Locked** column.

Manually unlocking local users

With the exception of the built-in secadmin user, users are manually unlocked from CloudLink Center.

Task summary

Permissions	Unlock User
Contents panel	**System** > **Users**
Commands	**Actions** > **Unlock**

Manually unlocking the built-in secadmin user

Before you begin

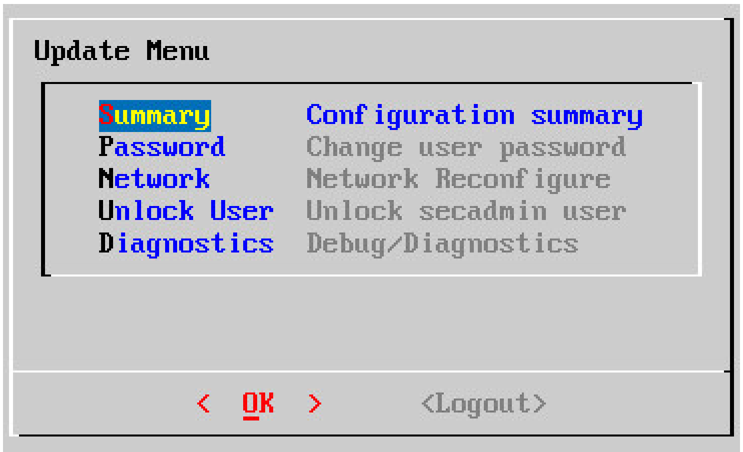
You must have access to the CloudLink Center console interface, which is used to configure underlying network- or system-level connections. You used the console interface for the first time when deploying CloudLink Center. For more information, see *CloudLink Deployment Guide for Microsoft Azure* or *CloudLink Deployment Guide for Enterprise*, depending on your environment.

The built-in secadmin user is unlocked from the CloudLink Center console interface. This interface is the only way to unlock this user if there are no other users assigned the SecAdmin role or they have also been locked out. For more information, see Built-in secadmin user on page 30.

Procedure

1. Access the CloudLink Center console interface.
2. From the **Update** menu, select **Unlock User** as shown in the following figure.

Figure 5 Update menu



```
Update Menu

   Summary        Configuration summary
   Password       Change user password
   Network        Network Reconfigure
   Unlock User    Unlock secadmin user
   Diagnostics    Debug/Diagnostics


          <  OK  >        <Logout>
```

3. Click **OK**.

Deleting users

You can delete any user except the built-in secadmin user.

Prerequisites
You must have the Delete User permission in a managing role for all the users' roles.

Task summary

Permissions	Delete User
Contents panel	**System** > **Users**
Commands	**Actions** > **Delete**

CHAPTER 5

Managing Encryption Keystores and Keys

This chapter presents the following topics:

Overview

CloudLink uses the following types of encryption keys to secure machines:

- A volume key encryption key (VKEK) that is generated by CloudLink. CloudLink generates a VKEK for each volume.
- A volume encryption key that is used by native technologies in the machine's operating system. A unique volume encryption key is generated for each encrypted volume.

These keys can be stored in the CloudLink Center keystore or an external keystore. A keystore is a combination of a key location and a key protector. For more information, see Key location access control and backup recommendations on page 42.

For a machine, volume encryption keys secure the boot or data volumes, as determined by the key release policy. For more information, see Key release policies on page 57. The VKEK protects the volume encryption keys:

- When CloudLink Center receives a request from CloudLink Agent to encrypt a volume on its machine, CloudLink Center generates a new VKEK in a keystore and uses it to encrypt the volume encryption key.
- When a volume requires decryption, CloudLink Center decrypts the volume encryption key using the VKEK and sends it to CloudLink Agent.

You must understand the difference between the types of encryption keys used to secure machines. However, because volume encryption keys are created and managed by native technologies in machines' operating systems, they are not discussed in detail in CloudLink documentation. Unless specified otherwise, the terms encryption keys and keys in this guide refer to the VKEK.

During deployment, CloudLink Center creates an initial keystore for encryption keys called CloudLink Vault. For more information on using CloudLink Vault, see CloudLink Vault on page 124. If you do not want to use the initial, or default, keystore to store encryption keys, external options are available, including Microsoft Active Directory, Amazon S3, or an S3-compatible bucket.

Encryption keys are also encrypted, or protected, by one or more key protectors, including CloudLink Vault, SafeNet LunaSA, Microsoft Azure Key Vault, a KMIP key manager, or a password.

If you add keystores, only one can be active for each machine group, but multiple keystores can be used in each CloudLink Center or CloudLink Center cluster deployment. Keys generated by CloudLink Center are stored in a keystore. You can modify and delete keystores.

If you have more than one keystore, you can move keys from a source keystore to a destination keystore. However, you cannot move keys from a keystore that is assigned to a machine group. This approach is useful for keeping as many keys as possible in a keystore. If you prefer, you can leave keys in the keystores where CloudLink Center created them. When CloudLink Center requires a key, it checks each accessible keystore.

You can change the frequency that CloudLink Center automatically updates keys, referred to as the key lifetime. See Key Lifetime on page 61 for more information. You can also manually update keys.

You can view keys in a keystore and the key history for a machine.

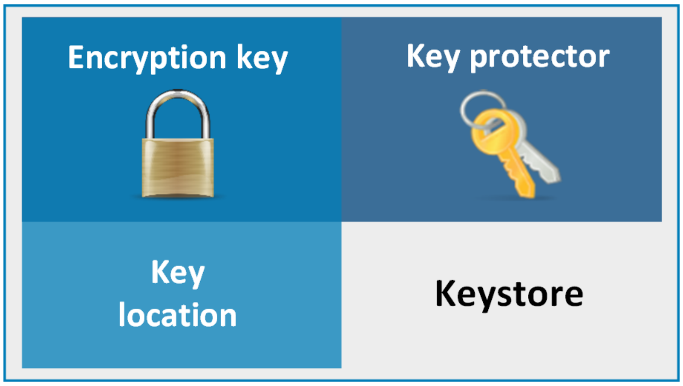
Encryption key location and protector options

CloudLink supports a variety of encryption key location and protection options.

Keystores

The term keystore refers to the combination of a key location and a key protector. Encryption keys are stored in a key location and are encrypted, or protected, by a key protector. The following figure shows the relationship between encryption keys, key locations, and key protectors.

Figure 6 Keystore diagram



Key locations

CloudLink Center supports several options for the key location used to store encryption keys:

Local Database

An internal key location.

Microsoft Active Directory

An external key location.

Amazon S3

An external key location. You must have an Amazon Web Services (AWS) account to use this location.

S3-compatible bucket

An external S3-compatible key location.

Key protectors

CloudLink Center supports several options for encryption key protectors.

Note

The type of available key protector depends on the selected key location.

CloudLink Vault

An internal key protector.

SafeNet LunaSA

An external key protector using a hardware security module (HSM) for protection.

Microsoft Azure or Azure Stack Key Vault

An external key protector using an Azure or Azure Stack Key Vault for protection.

KMIP server

An external key protector using a Key Management Interoperability Protocol (KMIP) server for protection.

Password

The encryption key is protected with a password.

Key location access control and backup recommendations

You are responsible for your encryption keys and for ensuring that the appropriate access control and backup policies and procedures are in place to protect the keys against loss or theft. If your keys become unavailable, you cannot access any data that was encrypted using those keys.

Backups are critical for restoring CloudLink Center. It is important to have a CloudLink Center backup so that you can deploy a new server and restore CloudLink Center. If you are using the local database, volume encryption keys are stored in CloudLink Center. Backups are the only method of restoring keys so that you can access encrypted data.

Ensure that you have met all prerequisites for restoring CloudLink Center from backup. If all prerequisites are not met, you cannot access encrypted data after restoring from a backup file. For more information about CloudLink Center backups and restoring from a backup file, see Backing Up and Restoring CloudLink Center on page 107.

The following table identifies which key protectors are available for each type of key location.

Table 1 Key location and key protector options

Key protectors	Local Database key location	Microsoft Active Directory key location	Amazon S3 key location	S3-compatible bucket key location
CloudLink Vault	Yes	Not allowed	Not allowed	Not allowed
SafeNet LunaSA	Yes			
Microsoft Azure Key Vault	Yes			
KMIP key manager	Yes	Yes	Yes	Yes
Password	Yes	Yes	Yes	Yes

Key locations

Local Database

CloudLink Center includes a secure local database protected by CloudLink Vault. This initial key location encrypts credentials used to access remote resources. For example, CloudLink Vault stores credentials required to access the Microsoft Windows domain, FTP or SFTP servers, and external key locations.

You can continue to use this initial key location or configure a different key location. When used as the key location, the CloudLink Vault local database encrypts and stores VKEKs. If you delete a CloudLink Vault key location, all keys are destroyed.

For CloudLink Center clusters, CloudLink Vault is replicated to each server in a cluster. The key location is automatically available on each cluster server.

CloudLink Center backups must be configured when using CloudLink Vault as the key location. For more information, see Key location access control and backup recommendations on page 42.

Note

If you do not use the initial CloudLink Vault as the key location, CloudLink Center still requires it to store credentials used to access remote resources. For more information about working with CloudLink Vault, see Configuring the CloudLink Center Environment on page 123.

Microsoft Active Directory organizational unit
The authentication credentials for Active Directory are stored in the CloudLink Vault. Ensure key safety by backing up the Active Directory server.

If you delete an Active Directory keystore, the keys remain in the Active Directory base container. You can add this container to CloudLink Center with the same key protector to regain access.

Amazon S3 bucket
The authentication credentials for Amazon S3 are stored in the CloudLink Vault. Ensure key safety by protecting your S3 bucket from accidental deletion.

If you delete an Amazon S3 keystore, the keys remain in the S3 bucket. You can add this bucket to CloudLink Center with the same key encryption password to regain access.

S3-compatible bucket
The authentication credentials for an S3-compatible bucket are stored in the CloudLink Vault. Ensure key safety by protecting your S3-compatible bucket from accidental deletion.

If you delete an S3-compatible keystore, the keys remain in the S3-compatible bucket. You can add this bucket to CloudLink Center with the same key encryption password to regain access.

Key protectors

A key protector is the protection mechanism used to encrypt and protect the volume encryption keys. Key protectors include:

CloudLink Vault
See CloudLink Vault on page 124.

SafeNet LunaSA
A SafeNet LunaSA key protector uses a hardware security module (HSM) to protect encryption keys.

The main authorization credentials to LunaSA HSM are configured on each server in a cluster. These credentials are not stored in the CloudLink Vault.

Microsoft Azure Key Vault
A Microsoft Azure Key Vault is a service provided by Microsoft Azure to protect your encryption keys.

KMIP server
A KMIP server can be used to protect your encryption keys. A KMIP server key protector protects all encryption keys stored in a location.

Password
Encryption keys can be password protected.

Viewing keystores

A keystore is a combination of a key location and a key protector. You can view the keystores that you have added.

Task summary

Permissions	View Keystores
Contents panel	**System** > **Keystores**
Commands	n/a

Keystores table information
The Keystores table includes the following information for each keystore:

Name

The name of the keystore

Description

The description of the keystore

Key Location Type

The encryption key location type. For more information, see Encryption key location and protector options on page 41.

Protector Type

The encryption key protector

Status

The keystore status, which is one of the following:

- Accessible—indicates that CloudLink Center can work with the keystore.
- Inaccessible—(shown in red text) indicates a problem working with the keystore. For example, CloudLink Center cannot reach the keystore host.

Keystore details
In addition to the information provided in the Keystores table, details show:

Date Created

The date and time that the keystore was added

Used in Groups

The machine groups that use the keystore

Key Location Status

The encryption key location accessibility

Protector Status

The key protector accessibility

Amazon S3 details include:

Bucket Name

The name of the bucket resource for the keystore

Access Key ID

The Access Key ID associated with your AWS account

Region

The Secret Access Key associated with your AWS account

S3-compatible bucket details include:

EndPoint

The S3-compatible bucket endpoint

Bucket Name

The name of the bucket resource for the keystore

Access Key ID

The Access Key ID associated with your S3-compatible storage account

URL Style

Either a virtual-hosted-style URL where the bucket name is a subdomain, or path-style URL where the bucket name is appended to the domain name and is a part of URL path.

Active Directory details include:

Domain

The domain name of one or more Active Directory hosts

AD Hosts

The Active Directory hostname or hostnames

Base DN

The name of the container configured on one or more Active Directory hosts

Username

The login name for the bind user

Configuring a keystore

The initial CloudLink Vault keystore is configured during server setup. You can configure one or more additional keystores.

Note

You can have only one current, or active, keystore for each machine group, but multiple keystores can be used in each CloudLink Center or CloudLink Center cluster deployment.

Adding a keystore

You can add a new keystore, in addition to the initial CloudLink Vault keystore. When you add a keystore, you must define the key location and the key protector.

Task summary

Permissions	Add Keystore
Contents panel	**System** > **Keystores**
Commands	**Add**

Keystore values

When creating a keystore, provide the following values:

Name

The name of the keystore

Description

The description of the keystore

Key Location Type

The location of the key, either Local Database, Active Directory, or Amazon S3 Bucket

Protector Type

The encryption key protector

For encrypted key location options, see Adding an encryption key location on page 46.

Adding an encryption key location

You can use the Local Database, Active Directory, an Amazon S3 bucket, or an S3-compatible bucket to store encrypted keys.

Local Database

You can use the local CloudLink Vault database to store encryption keys.

Active Directory

To use Microsoft Active Directory for the CloudLink keystore, you must have a Microsoft Windows domain controller that is reachable by CloudLink Center. For information on configuring an Active Directory on a Windows server, see Configuring Active Directory for Use as the Keystore on page 163.

Verify that CloudLink Center has a DNS configured. For more information, see Domain Name System servers on page 133.

When creating an Active Directory keystore, provide the following values:

Domain

The domain name configured on the Active Directory host, such as example.com.

Base DN

The name of the container configured on the Active Directory host. For example: CN=MyKeys,OU=MyOU,DC=cloudlink,DC=com.

Hosts (comma separated)

The Active Directory hostname, such as clc.example.com. The Active Directory host is a Windows Server where Active Directory is configured. You can add additional Active Directory hostnames for redundancy. Do not use an IP address.

Username

The login name for the bind user.

Password

The password configured for the bind user.

Amazon S3 Bucket

When creating an Amazon S3 Bucket keystore, provide the following values:

Bucket Name

The name of the bucket resource for the keystore. If the bucket does not exist, CloudLink Center creates it. If the bucket exists, CloudLink Center tries to connect to it. If CloudLink Center cannot connect to the bucket, CloudLink Center displays an Access Denied error.

Region

The region where your bucket is expected to be located.

Access Key ID

The Access Key ID associated with your AWS account.

Access Key

The Secret Access Key associated with your AWS account.

S3 Compatible Bucket

When creating an S3-compatible bucket keystore, provide the following values:

S3 Endpoint

The endpoint for your S3-compatible bucket.

Bucket Name

The name of the bucket resource for the keystore. If the bucket does not exist, CloudLink Center creates it. If the bucket exists, CloudLink Center tries to connect to it. If CloudLink Center cannot connect to the bucket, CloudLink Center displays an Access Denied error.

URL Style

Either a virtual-hosted-style URL where the bucket name is a subdomain, or path-style URL where the bucket name is appended to the domain name and is a part of URL path.

Access Key

The access key associated with your S3-compatible storage account.

Secret Key

The secret key associated with your S3-compatible storage account.

Note

You can test the configuration values using the **Test** button.

For encrypted key protector options, see Adding an encrypted key protector on page 48.

Adding an encrypted key protector

You add an encrypted key protector to protect encryption keys. CloudLink supports CloudLink Vault, SafeNet LunaSA, Azure KeyVault, and VMware KMIP servers as encryption key protectors.

CloudLink Vault
You can choose CloudLink Vault as the key protector.

SafeNet LunaSA
You add a SafeNet LunaSA key protector with the assistance of Dell EMC Support. Contact your Dell EMC representative for more information.

Azure KeyVault
When adding an Azure Key Vault as the key protector, provide the following values:

Key ID

The identifier for the key used to protect the keystore

Client ID

A character string assigned by Microsoft during registration

Client Secret

A security key provided by Microsoft

KMIP
You can configure a KMIP server as a key protector. For more on KMIP servers, see KMIP Servers on page 147.

You must meet the following additional requirements when using a KMIP server as a key protector:

- You must have a KMIP server.
- The KMIP server must be reachable by CloudLink Center.
- CloudLink Center must have a DNS configured. For more information, see Domain Name System servers on page 133.

When adding a KMIP server, provide the following values:

KMIP Server Address

KMIP server hostname

Port

Optional parameter that defines the TCP port number to use with KMIP. KMIP standard TCP port 5696 is used if the port is not specified.

Credential Type

Username and Password, Device, or No Credentials

Username/Serial Number

Username for client authentication to a KMIP server

Password

Password for client authentication to a KMIP server (optional)

Key

Private key for client authentication when authenticating a TLS connection

Certificate

Certificate for client authentication when authenticating a TLS connection

Trusted certificate

KMIP server certificate used as a trust anchor when authenticating a TLS connection

Note

You can test the configuration values using the **Test** button.

Password
You can protect encryption keys with a password.

Setting the current keystore

CloudLink Center stores new encryption keys in the current keystore for the machine group. Only one keystore can be current at a time for a machine group. You might want to change the current keystore after adding a new keystore in which you want CloudLink Center to store new encryption keys.

When you switch the current keystore for a machine group, encryption keys are not automatically moved to the new keystore. You can move keys to the new keystore, except for keys stored in SafeNet LunaSA.

You set the current keystore for a machine group by modifying the machine group. For more information, see Modifying a machine group on page 63.

Modifying a keystore

You can modify some key location and key protector properties after adding a keystore.

Note

Only one keystore can be active at a time for each Machine Group.

Task summary

Permissions	Modify Keystore
Contents panel	**System** > **Keystores**
Commands	**Actions** > **Change Description** **Actions** > **Modify Key Location** **Actions** > **Modify Protector**

Key location properties

For a CloudLink Vault keystore, you can change the Description property.

For an Active Directory keystore, you can change the following properties:

- Description
- Hosts (comma separated)
- User
- Password

For an Amazon S3 keystore, you can change the following properties:

- Description
- Region
- Access Key ID
- Access Key

For an S3-compatible keystore, you can change the following properties:

- Description
- URL Style
- Access Key
- Secret Key

Key protector properties

For a Microsoft Azure Key Vault keystore, you can change the following properties:

- Description
- Client ID
- Client Secret

For a KMIP server keystore, you can change the following properties:

- Description
- Key
- Certificate
- Trusted certificate
- Port

Note

For a SafeNet LunaSA keystore, do not change properties without the assistance of Dell EMC Support.

Deleting a keystore

You can delete any keystore that is not actively used in a machine group. A keystore in use by a machine group must be removed from the machine group before it can be deleted. The results and behavior following deletion depend on the keystore type. For information, see Encryption key location and protector options on page 41.

When you delete a keystore, you must retype the keystore name. This practice is intended to minimize the risk of deleting the wrong keystore.

If you delete a keystore and later determine that it contained keys required to access encrypted volumes, you may be able to restore the keystore from a backup. For more information, see Restoring keystores from a backup file on page 114.

Task summary

Permissions	Delete Keystore
Contents panel	**System** > **Keystores**
Commands	**Actions** > **Delete**

Resolving the Missing Key alarm

Each day, CloudLink Center checks if it can access volume keys for connected and registered machines. If CloudLink Center detects that it cannot access one or more volume keys, it generates the Missing Key alarm for each key. After raising this alarm, CloudLink Center checks hourly to see whether the key has become available. CloudLink Center lowers the alarm only when the key is available during the check. The alarm is also lowered when a machine is disconnected.

This alarm occurs if a keystore containing the required key becomes inaccessible because CloudLink Center cannot access the volume keys stored in the keystore. This alarm also occurs if an administrator deletes a keystore that contains required volume keys, or deletes a key from a keystore during a shred operation or by using external tools.

This alarm is intended to notify you in a timely manner that volume keys are missing. Actions that you might need to take to resolve this alarm may include checking network connectivity for the keystore or restoring a keystore from a backup file. For more information, see Restoring keystores from a backup file on page 114.

Showing keys in a keystore

You can view the keys stored in a selected keystore.

Task summary

Permissions	View Key Policy
Contents panel	**System** > **Keystores**
Commands	**Actions** > **Show Keys**

Moving keys to another keystore

You can move keys from one keystore to another. For example, you may want to use an external keystore such as Microsoft Active Directory instead of the initial keystore. After configuring the external keystore, move keys to it from the initial keystore.

Note

Keys cannot be moved from a keystore assigned to a machine group.

Prerequisites

The source and destination keystores must both be accessible by CloudLink Center.

Task summary

Permissions	Move Keys
Contents panel	**System** > **Keystores**
Commands	**Actions** > **Move Keys**

Showing the key history for a machine

You can view the history of the encryption keys for a machine.

Task summary

Permissions	View VMs
Contents panel	**Agents** > **Machines**
Commands	**Actions** > **Show Key History**

Key History table information

The Key History table includes the following information for each key:

Key ID

The unique identifier of the key.

Creation Time

The date and time that CloudLink Center created the key across multiple keystores, if applicable.

Expiration Time

The date and time that the key expires.

Archived Time

The date and time that the key was archived. When a key is updated, it is archived. Keys are archived so that any older versions of volumes encrypted with an older key can still be decrypted.

Volume Name/ID

The name and unique identifier of the volume for which this key was used for encryption or decryption. For example: `(E:) Volume{c41ec234-9542-4c91-a0c7-17d25f00ca87}`.

Key history details

No additional details are displayed.

Updating keys

You can update keys to re-encrypt all of a machine's volume encryption keys with new volume key encryption keys (VKEK).

Prerequisites

The machine must be in the connected state.

Task summary

Permissions	Change VM Volume Keys
Contents panel	**Agents** > **Machines**
Commands	**Actions** > **Update Keys**

CHAPTER 6

Managing Secure Machines

This chapter presents the following topics:

Overview

From CloudLink Center, manage the secure machines to which CloudLink Agent has been deployed. To help you administer and manage these machines, organize them using machine groups. For all machines in a group, the machine group policies determine the role that administers the machines, the conditions under which machines may start up automatically, the encryption that must be in effect for the machine, and so on.

For individual machines in a group, you can encrypt and decrypt volumes, and choose whether to allow a particular volume to be exempt from the policy for the machine group. You can perform other management operations such as accepting, rejecting, or removing a machine.

Self-encrypting drives

CloudLink Center can manage encryption keys for self-encrypting drives (SEDs). When CloudLink Agent is installed on machines with SEDs, you can lock and unlock SEDs in CloudLink Center.

When CloudLink Center takes ownership of an SED, it releases SED encryption keys when the physical machine containing the SEDs is powered on or rebooted. If the SED cannot retrieve the key from CloudLink Center, the SED remains locked.

When managed by CloudLink Center, SED encryption keys are stored in the current keystore for the machine group they are in. SED functionality requires a separate SED license.

Pre-startup authorization

Pre-startup authorization enables a machine to start up automatically when:

- The machine has been previously registered with CloudLink Center and is able to connect to it
- The machine’s boot volume is encrypted and the machine meets key release policies for boot volume encryption. For more information, see Key release policies on page 57.

Note

If a machine’s boot volume is not encrypted, but one or more data volumes are encrypted, the machine can start. After the machine starts up, CloudLink Center determines whether encryption keys for encrypted data volumes can be released automatically based on key release policies. If key release policies are not met for the data volume, CloudLink Center puts the machine in the pending state.

If a machine does not pass pre-startup authorization, CloudLink Center puts the machine in the pending state and you must explicitly accept the machine’s startup before it is allowed to continue.

Machine groups

You can organize machines into groups for administrative or operational purposes. For example, you might group machines for your Finance department where the volume encryption policy requires encryption of all boot and data volumes. You might also group machines for your DevOps department where the volume encryption policy requires encryption of only boot volumes. Each machine group might have a different administrator.

Each machine must belong to a machine group. A machine is assigned to a machine group during deployment. If you do not specify a group during deployment, the machine is assigned to the built-in machine group named **Default**. You can change the machine group that a machine belongs to after deployment.

All machines in a group use the same:

- Key release policies that determine when a machine in the group can start up automatically. For more information, see Key release policies on page 57.
- Volume encryption policy that determines the types of volumes that must be encrypted (boot, data, or both boot and data). Volume encryption policy applies to virtual machines (boot and data volumes) or physical machines (data volume only). Volume encryption policy does not apply to a physical machine's boot volume. For more information, see Volume encryption policy on page 59.
- Keystore where encryption keys are stored. For more information, see Managing Encryption Keystores and Keys on page 39.
- Managing roles that determine the roles that administer it. Only users belonging to a managing role for a machine group can view and make changes to it.
- Approved networks from which machines in the machine group can start up automatically. For more information, see Approved networks for machine groups on page 67.
- Approved location that is used to verify that a machine is in the correct place. For more information, see Approved locations for machine groups on page 69.
- Key lifetime that determines the frequency that CloudLink Center updates encryption keys for machines in the group. Once a key is updated, the previous key is expired. By default, keys never expire, which is referred to as an infinite lifetime. You can change the key lifetime.

Key release policies

Before CloudLink Center automatically releases keys, a machine must:

- Meet key release policies.
- Use an IP address that belongs to an approved network. For more information, see Approved networks for machine groups on page 67.
- Belong to an approved location. For more information, see Approved locations for machine groups on page 69
- Not have been previously removed. For more information, see Removing a machine on page 77.

Key release policies may be required to enable:

- A machine to boot as part of the pre-startup authorization process
- Access to encrypted data volumes

If a machine does not meet the policies, CloudLink Center puts the machine in the pending state and you must manually choose whether to allow the key release. For more information about manually allowing key release, see Accepting or rejecting a pending machine on page 75.

Key release policies are set for a machine group. For more information, see Machine groups on page 56.

Types of key release policies

The following key release policies are available:

IP Change

Determines whether CloudLink Center allows a machine to boot automatically when it starts up with an IP address that is different from the one recorded in the CloudLink Center database.

For virtual machines, this policy applies to boot or data volumes on machines with IP addresses that belong to an approved network. For more information, see Approved networks for machine groups on page 67.

Moved Volume

Determines whether CloudLink Center allows keys to be released (if any) when it detects that a volume is now attached to a different machine than the one recorded in the CloudLink Center database.

For more information about moved volumes, see Moving an Encrypted Disk to Another Machine on page 175.

Platform Change

Determines whether CloudLink Center allows a machine to boot automatically when it starts up with a different platform than the one recorded in the CloudLink Center database.

This policy applies to boot or data volumes on virtual machines.

Integrity Change

Determines whether CloudLink Center allows a machine to boot automatically when it starts up with an integrity value that is different than the one recorded in the CloudLink Center database.

This policy applies only to boot volumes on virtual machines.

Machine Clone

Determines whether CloudLink Center allows a cloned machine to boot automatically.

This policy applies to boot or data volumes on virtual machines.

For more information about cloned machines, see Working with cloned machines on page 79.

You can change these key release policies. For more information, see Changing key release policies for a machine group on page 64.

Pending machine policy

The pending machine policy determines whether or not a machine is placed in the pending state when it connects to CloudLink Center for the first time, or when it connects from a network or location not previously associated with the machine. You can choose to allow the machine to automatically register with CloudLink Center, or remain in the pending state and require manual approval.

The following pending machine policy is available:

New Machine

If a new machine that has an approved IP address is added to CloudLink Center, you can choose to allow it to automatically (default) connect to CloudLink Center or require manual approval to connect to CloudLink Center.

This policy applies to virtual machines.

Change the pending machine policy the same way you change a key release policy. For more information, see Changing key release policies for a machine group on page 64.

Volume encryption policy

Volume encryption policy determines which volumes must be encrypted for virtual or physical machines. For example, the All Data volume encryption policy requires that all existing data volumes on a machine must be encrypted.

Volume encryption policy applies to boot or data volumes for virtual machines.

Volume encryption policy is set for a machine group and can be changed at any time. For more information, see Machine groups on page 56.

For an individual machine in a machine group, you can allow a particular volume to be exempt from the group policy. For more information, see Viewing volume encryption policy compliance on page 89.

Types of volume encryption policies

CloudLink Center provides the following volume encryption policies:

Boot and Manual Data

The boot volume must be encrypted. Data volumes are not required to be encrypted.

All Data

Data volumes must be encrypted. The boot volume is not required to be encrypted.

On Windows machines, data volumes added are automatically encrypted.

On Linux machines, data volumes (mounted devices) must be manually encrypted.

Boot and All Data

The boot and all data volumes must be encrypted.

On Windows machines, data volumes added to the machine are automatically encrypted.

On Linux machines, data volumes (mounted devices) must be manually encrypted.

Manual

The boot and data volumes are not required to be encrypted.

Note

Key release requires that the boot volume is encrypted. For more information, see Key release policies on page 57.

Handling of existing encrypted Windows volumes

You can deploy CloudLink Agent to Windows machines with volumes that are already encrypted by BitLocker. During deployment, these volumes remain encrypted, and are put under CloudLink Center management.

Machine group properties

A machine group is composed of several properties. You define many of these properties when creating a machine group. You can modify these properties at a later time. Other properties are for informational purposes only and cannot be changed.

Machine group properties include:

Name

The unique name of the machine group.

Description (optional)

A brief description of the machine group.

Keystore

The keystore used by all machines in the group. For information, see Setting the current keystore on page 49.

Managed By

The names of the roles that administer this machine group.

Approved Networks (optional)

The networks to which machines in this group belong. The networks must be defined as an approved network. For more information, see Approved networks for machine groups on page 67.

Approved Locations (optional)

An approved location is used to verify that a machine is in the correct place when the machine starts. For more information, see Approved locations for machine groups on page 69.

Shutdown on Locations Failure

Whether or not to automatically shutdown a machine that starts up outside of an approved location.

Registration Code

The code used when deploying CloudLink Agent to a machine to assign it to this machine group.

During deployment of CloudLink Agent to a machine, it is assigned to the Default machine group if no group registration code is provided. As a deployment option, you can assign the machine to another, existing group by specifying the machine group’s registration code in the deployment command. For more information, see the *CloudLink Deployment Guide* for your environment.

Volume Encryption Policy

The volume encryption policy that applies to all machines in this group. For more information, see Volume encryption policy on page 59.

Manage SED Drives

Select **Enabled** to have CloudLink manage SED encryption keys. When a machine with SEDs is registered with this machine group, CloudLink Center controls releasing keys to all SEDs in that machine.

If you select **Disabled**, a CloudLink administrator must manually select each SED in the machine to control encryption key release.

This property is only available if you have an SED license and select either the **All Data** or **Boot and All Data** encryption policy.

Machine Agent Upgrade

Whether or not to automatically upgrade a machine's CloudLink Agent when you upgrade CloudLink Center.

Max Usage Since Last Reset

The maximum number of encrypted machine instances (instance or socket license) or encrypted capacity used in this group since the last reset. This information might be useful if you are assessing your peak license usage over a specific time frame.

Current Usage

The number of machine instances currently encrypted (instance or socket license) or encrypted capacity used in a group.

Key Lifetime

The frequency that CloudLink Center updates for machines in the group. Once a key is updated, the previous key is expired. By default, keys never expire, which is referred to as an infinite lifetime.

You can trigger automatic encryption key changes based on a time interval of days. For example, if you specify an interval of one day, new encryption keys are generated every day.

When modifying a key lifetime, you can change the following values:

- Infinite—The encryption key never expires
- <Number> days—A list of preset values for the number of days before expiry
- Custom—A number of days before expiry that you specify

Policies

The current setting of the key release policies that control automatic startup of machines in the group. For more information, see Key release policies on page 57.

Viewing a machine group

You can view a list of machine groups that you have permission to view on the Groups panel.

Task summary

Permissions	View Group

Contents panel	**Agents** > **Machine Groups**
Commands	n/a

Groups table information

The Groups table includes the following information for each machine group:

- Name
- Description (optional)
- Keystore
- Managed By
- Approved Networks (optional)
- Approved Locations (optional)

For more information about these properties, see Machine group properties on page 60.

Groups details

In addition to the information provided in the Groups table, details include:

- Shutdown on Locations Failure
- Registration Code
- Volume Encryption Policy
- Manage SED Drives

  Note

  This property is only available if you have an SED license and select either the All Data or Boot and All Data encryption policy.

- Machine Agent Upgrade
- Max Usage Since Last Reset
- Current Usage
- Key Lifetime
- Policies

For more information about these properties, see Machine group properties on page 60.

Creating a machine group

A machine group must exist before you can assign a machine to it.

Task summary

Permissions	Add Group
Contents panel	**Agents** > **Machine Groups**
Commands	**Add**

Group values

When creating a machine group, provide the following values:

- Name

- Description
- Volume Encryption Policy
- Manage SED Drives

  Note

  This property is only available if you have an SED license and select either the All Data or Boot and All Data encryption policy.

- Keystore
- Managed By
- Approved Networks (optional)
- Key Lifetime
- Machine Agent Upgrade

For more information about these properties, see Machine group properties on page 60.

Modifying a machine group

You can modify all properties for a machine group, except the name.

Task summary

Permissions	Modify Group
Contents panel	**Agents** > **Machine Groups**
Commands	**Actions** > **Modify**

Machine group values

When modifying a machine group, provide the following values:

- Description (optional)
- Volume Encryption Policy
- Manage SED Drives

  Note

  This property is only available if you have an SED license and select either the All Data or Boot and All Data encryption policy.

- Keystore
- Managed By (not available for the Default machine group)
- Approved Networks (optional)
- Key Lifetime
- Machine Agent Upgrade

For more information about these properties, see Machine group properties on page 60.

Changing the volume encryption policy

You can change the volume encryption policy for a machine group.

For example, a particular machine group may use the Boot and Manual Data policy. This policy requires that only the boot volume is encrypted for machines in this group.

No data volumes must be encrypted. You may want to change to the All Data policy so that data volumes added to Windows machine are automatically encrypted.

Changing the volume encryption policy does not affect the boot volume or any existing data volumes. The new policy is applied when data volumes are added to the machine.

Task summary

Permissions	Modify Group
Contents panel	**Agents** > **Machine Groups**
Commands	**Actions** > **Modify**

Changing a machine group's location

You can add an approved location to a machine group. You must create an approved location before you add it to a machine group. See Approved locations for machine groups on page 69 for more information.

If you set **Shutdown on Locations Failure** to **Yes**, you must specify the amount of time CloudLink waits before it shuts down the machine.

Task summary

Permissions	Modify Group
Contents panel	**Agents** > **Machine Groups**
Commands	**Actions** > **Change Locations**

Machine group location values

When changing a machine group's location, provide the following values:

- Name
- Approved Locations
- Shutdown on Locations Failure
- Waiting Time if Location Unknown (optional)

Changing key release policies for a machine group

For a machine group, you can modify the key release policies that must be met for a machine in that group to start automatically.

Here are two examples where default policy settings cause CloudLink Center to prevent a machine from starting up automatically:

- A machine attempts to start up with a different IP address than the one recorded for that machine in the CloudLink Center database. CloudLink Center puts this machine in the pending state.
- A machine registered with CloudLink Center cannot boot, so you move its encrypted data volume to another registered machine. When this machine attempts to start, CloudLink Center detects that the data volume is associated with a different machine than the one recorded in the CloudLink Center database. CloudLink Center allows the machine to start up, but puts it in the pending state and locks the moved data volume to make it inaccessible.

When machines are in the pending state, you can manually accept or reject the startup. For more information, see Accepting or rejecting a pending machine on page 75.

To avoid having to manually accept each startup, you can change the default key release policy to allow CloudLink Center to release keys for machine's volumes when machines start up. For example, you can allow CloudLink Center to release the key for moved data volumes on startup. CloudLink Center also updates its database to associate the moved data volume with the current machine and automatically unlocks data volumes.

Note

For information about unlocking a moved volume, see Unlocking a moved volume on page 90. For information about the procedure for moving a data volume, see Moving an Encrypted Disk to Another Machine on page 175.

Task summary

Permissions	Change VM Policy
Contents panel	**Agents** > **Machine Groups**
Commands	**Actions** > **Change Pending Policies**

Policy values

When changing a policy setting, provide the following values:

Require Manual Approval (default)

If the key release policy is not met, you must manually accept the startup.

Allow Automatically

If the key release policy is not met, the startup is allowed to continue.

Allow if Address is on the Same Subnet (available only for IP Change)

If the IP address of the machine is different from the address stored in the CloudLink Center database, but remains in the same subnet (/24 mask), the startup is allowed to continue. The new IP address is recorded for this machine in the database.

This option is useful when you know that the IP address of a machine may change. For example, in some cloud environments (such as Microsoft Azure), the public IP address of a machine may change when it is shut down and restarted. A new IP address is assigned from the same subnet as the previous address.

Generating a registration code for a machine group

The registration code is used to assign a machine to a machine group during deployment. For more information, see Machine group properties on page 60.

When you create a machine group, CloudLink Center generates a registration code. You may want to generate a new registration code for a machine group. For example, you might suspect that the existing machine code has been compromised.

Task summary

Permissions	Modify Group
Contents panel	**Agents** > **Machine Groups**

Commands	**Actions** > **Generate New Code**

Resetting usage for a machine group

If you are assessing your peak license usage over a specific time frame, you can reset the license usage for a machine group.

CloudLink Center keeps track of the:

- Maximum number of encrypted machine instances or maximum amount of encrypted capacity used in each machine group. CloudLink Center displays the value using the Max Usage Since Last Reset machine group property.
- Number of encrypted machine instances or amount of encrypted capacity used. CloudLink Center displays this value using the Current Usage machine group property.

These values work in combination to help you understand your license usage, as described in the following example.

- You encrypt three machines in the Production machine group. Both the Max Usage Since Last Reset and Current Usage values are 3.
- At a later time, you move one machine to another machine group. The Max Usage Since Last Reset value is 3 and the Current Usage value is 2.
- You reset the usage for the Production machine group. The Max Usage Since Last Reset value is 2 and the Current Usage value is 2.

If you reset the usage for a machine group at regular intervals (for example, on the first day of each month), you can monitor your license usage over time.

Task summary

Permissions	Modify Group
Contents panel	**Agents** > **Machine Groups**
Commands	**Actions** > **Reset Usage**

Deleting a machine group

You can delete any machine group except the built-in Default machine group.

Prerequisites
You must be a user who is assigned to a role that manages the machine group you want to delete.

The machine group must not have any machines assigned to it.

Task summary

Permissions	Modify Group
Contents panel	**Agents** > **Machine Groups**
Commands	**Actions** > **Delete**

Approved networks for machine groups

When a machine starts up, its IP address is checked against a list of approved networks (or approved IP addresses) for its machine group. If the IP address of the machine belongs to an approved network for the group and all key release policies are met, the machine is allowed to start. For more information, see Key release policies on page 57.

Each approved network is assigned a unique name, which allows approved networks to be reused across machine groups. For example, you might create an approved network named CloudLink Lab and select that name to easily specify it as an approved network for machine groups.

If a machine starts up and its IP address does not belong to an approved network for the group, the machine is put in the pending state.

There is one circumstance in which a machine can automatically start if its IP address does not belong to an approved network. On initial startup following deployment of CloudLink Agent, CloudLink Center allows the machine to go directly to the connected state. However, if the machine is restarted, CloudLink Center puts it in the pending state.

CloudLink Center supports IPv4 and IPv6 addresses for specifying IP addresses for approved networks.

Viewing approved networks

You can view the list of approved networks that have been defined in CloudLink Center on the Approved Networks panel.

Task summary

Permissions	View Approved Networks
Contents panel	**Agents** > **Approved Networks**
Commands	n/a

Approved Networks table information

The Approved Networks table includes the following information for each approved network:

Name

The unique name of the approved network

Description

A brief description of the approved network

IP Addresses

One or more IP addresses of the following types:

- Individual IP addresses
- Range of consecutive IP addresses
- Network of IP addresses (CIDR)
  If more than one type of IP address is defined, each is separated by a comma.

Approved Networks details

For a selected approved network, you can edit or delete IP address specifications.

Adding an approved network

You add approved networks that you want to assign to machine groups. Adding an approved network involves defining its name and, optionally, description. After adding an approved network, you specify its IP addresses. For more information, see Adding IP addresses for an approved network on page 68.

Task summary

Permissions	Add Approved Network
Contents panel	**Agents** > **Approved Networks**
Commands	**Add**

Approved Network values

When adding an approved network, provide the following values:

Name

The unique name of the approved network. This name makes it easier to assign to a machine group. For more information, see Creating a machine group on page 62.

Description (optional)

A brief description of the approved network.

Adding IP addresses for an approved network

You add the IP address that you want automatically approved to each approved network. CloudLink Center supports IPv4 and IPv6 addresses for specifying IP addresses for approved networks.

Prerequisites

Before you can add IP addresses, the approved network must exist. For information, see Adding an approved network on page 68.

Task summary

Permissions	Add Approved Network
Contents panel	**Agents** > **Approved Networks**
Commands	**Actions** > **Add IP to Network**

Adding an IP address to network values

When adding an IP address specification to an approved network, provide the following values:

Type

One of:

- IP Addresses—A single IP address
- IP Addresses Range—A range of consecutive IP addresses, from a start IP address to an end IP address

- CIDR—A network of IP addresses using Classless Inter-Domain Routing

IP (for Type with the value IP Addresses)
Specify an individual IP address

Start IP (for Type with the value IP Addresses Range)
Specify the first IP address in the range of consecutive IP addresses

End IP (for Type with the value IP Addresses Range)
Specify the last IP address in the range of consecutive IP addresses

CIDR (for Type with the value CIDR)
Specify a network of IP addresses using CIDR

Editing or deleting IP addresses for an approved network

You can edit or delete an IP address for an approved network.

You can edit the approved network type and its associated IP addresses. For more information, see Adding IP addresses for an approved network on page 68.

Task summary

Permissions	Add Approved Network
Contents panel	**Agents** > **Approved Networks**
Commands (in the Approved Networks table IP Addresses row)	**Edit** **Delete**

Modifying or deleting an approved network

You can modify or delete an approved network.

You can modify an approved network to change its description.

You can delete an approved network, as long as it has not been assigned to a machine group.

Task summary

Permissions	Modify Approved Network Delete Approved Network
Contents panel	**Agents** > **Approved Networks**
Commands	**Actions** > **Modify** **Actions** > **Delete**

Approved locations for machine groups

It is sometimes necessary to limit data access by location. Data sovereignty regulations might mandate that machines containing specific data only reside and run in specific locations or data centers.

CloudLink can validate that a machine is running in an approved VMware vCenter, Microsoft Azure subscription, Microsoft Azure Stack subscription, or Amazon Web Services location. Each approved location is given a unique name, which allows approved locations to be reused across machine groups. For example, you can create an approved location named “US Datacenter” and select it as an approved location for multiple machine groups. An approved location is created using specific locations from a cloud provider. For example, the VMware vCenter provider allows data centers, clusters, ESXi hosts, or vCenter folders to be specified as an approved location.

When a machine starts up, its location is checked against a list of approved locations for its machine group. No check is performed if a machine group has no assigned approved locations. A machine is allowed to start if it belongs to an approved location for its machine group and all key release policies are met. See Key release policies on page 57 for more information.

If a machine starts up and it is not located in an approved location for the machine group, CloudLink Center can automatically shut down the machine after a specified amount of time, or leave the machine running.

A machine’s location is periodically checked while it is running to ensure it has not been moved. A machine is shut down if its location has changed and it is no longer running in an approved location. Machines may also shut down if you change the approved locations in CloudLink Center. This shutdown limits data exposure in an unapproved location. All shutdown requests are recorded as a security event that includes information about how long the machine may have been running in the unapproved location.

Approved locations are also checked when a machine registers with CloudLink Center. Registration is unsuccessful if a machine’s location is not approved for use within the machine group.

Adding Cloud Providers for approved locations

A Cloud Provider is a server or host that provides information about the location of a machine. CloudLink Center supports VMware vCenter, Microsoft Azure, and Amazon Web Services as Cloud Providers. The VMware vCenter provider allows for an entire vCenter, a datacenter, a cluster, a folder, or an ESXi host to be specified as a location.

Prerequisites
You need a Cloud Provider host, such as VMware vCenter.

Task summary

Permissions	Add Provider
Contents panel	**Location** > **Cloud Providers**
Commands	**Add Provider**

Add Cloud Provider
Provide the following values when adding any type of Cloud Provider:

Provider Name

The Cloud Provider hostname

Description

A descriptive name for the Cloud Provider

Type

Select the type of Cloud Provider

VMware vCenter

Provide the following values when adding a vCenter Cloud Provider:

Address

Cloud Provider address, in FQDN format or an IPv4 or IPv6 address

Username

Domain and username for the Cloud Provider account

Password

Password for the Cloud Provider account

Microsoft Azure Subscription

Note

Use only with machines deployed in the new portal at portal.azure.com.

Provide the following values when adding an Azure Cloud Provider:

Subscription ID

Azure subscription ID

Client ID

Azure client ID

Client Key

Azure client key

Microsoft Azure Stack Subscription

Provide the following values when adding an Azure Stack subscription:

Server

The server hostname or IP address

Subscription ID

Azure subscription ID

Client ID

Azure client ID

Client Key

Azure client key

Amazon Web Services

Provide the following values when adding an Amazon Web Services (AWS) Cloud Provider:

Region

Physical location of the AWS Cloud Provider.

Access Key ID

Access key for your AWS account. This access key must have permission to check for running instances associated with your AWS account. At a minimum, the AWS account must have the Identity and Access Management (IAM) policy Amazon EC2 Read Only Access.

Secret Access Key

Secret access key for your AWS account.

Adding an approved location

You can add approved locations and assign them to machine groups. Adding an approved location involves defining its name and, optionally, description. After adding an approved location, you add a Cloud Provider instance to the location.

Task summary

Permissions	Add Approved Location
Contents panel	**Location** > **Approved Locations**
Commands	**Add**

Approved Location values

When adding an approved location, provide the following values:

Name

The unique name of the approved location. This enables you to assign it to a machine group. For more information, see Creating a machine group on page 62.

Description (optional)

A brief description of the approved location.

Adding a Cloud Provider instance to an approved location

A Cloud Provider instance is a location in a Cloud Provider, such as a datacenter or cluster. The instance can be defined as all of a Cloud Provider or a subset of a Cloud Provider.

Prerequisites

You need a Cloud Provider host, such as VMware vCenter. For information, see Adding Cloud Providers for approved locations on page 70.

Task summary

Permissions	Modify Approved Location
Contents panel	**Location** > **Approved Locations**
Commands	**Actions** > **Add Instance To Location**

Add Instance to Location

Provide the following values when adding a Cloud Provider instance to a location:

Location

The approved location name, cannot be changed

Provider

A previously added Cloud Provider

Type

A location in the Cloud Provider, such as

- Provider
- Datacenter
- Cluster
- Folder
- Host

Name

The name of the location type in the Cloud Provider

Viewing approved locations

You can view the list of approved locations that have been defined in CloudLink Center on the Approved Locations panel.

Task summary

Permissions	View Approved Locations
Contents panel	**Location** > **Approved Locations**
Commands	n/a

Approved Locations table information

The Approved Networks table includes the following information for each approved location:

Name

The unique name of the approved location

Description

The approved location's description

Instances

The Cloud Provider and the location within the Cloud Provider

Modifying or deleting a Cloud Provider

You can modify or delete a Cloud Provider.

You can modify the Cloud Provider description, username, or password. For more information, see Adding Cloud Providers for approved locations on page 70.

Task summary

Permissions	Modify Provider Delete Provider
Contents panel	**Location** > **Cloud Providers**
Commands	**Actions** > **Modify** **Actions** > **Delete**

Modifying or deleting an approved location

You can modify or delete an approved location. You can modify an approved location to change its description. You can delete an approved location, as long as it has not been assigned to a machine group.

Task summary

Permissions	Modify Approved Location Delete Approved Location
Contents panel	**Location** > **Approved Locations**
Commands	**Actions** > **Modify Location** **Actions** > **Add Instance To Location** **Actions** > **Delete**

Registered machines

From CloudLink Center, you manage individual machines on which CloudLink Agent has been deployed. For example, you can view a list of machines and their current states, and accept or reject machine startup.

Each machine registered with CloudLink Center is assigned a unique serial number that is stored in the CloudLink Center database. If a machine has more than one volume, CloudLink Center management operations can be performed on individual volumes. For example, you can encrypt or decrypt volumes on an individual basis.

Machine startup

You can allow machines to start up automatically using key release policies set for the machine group. For more information, see Key release policies on page 57.

On startup, if a machine does not meet all key release policies, CloudLink Center puts the machine in the pending state. In this state, an administrator must explicitly accept the machine's startup. For example, you can set a key release policy so that CloudLink Center does not allow a machine to start up automatically if its IP address does not belong to an approved network for the machine group. For more information about the pending state and manually accepting a machine's startup, see Accepting or rejecting a pending machine on page 75.

Machine states

Each registered machine is assigned a state that you can view in CloudLink Center. For more information, see Viewing registered machines on page 76. The state of a machine determines the actions that you can perform, including encrypting volumes, decrypting volumes, accepting or rejecting startup, or removing a machine. Available actions depend on whether the machine is running Windows or Linux.

States include:

Connected

The machine is registered and running.

Disconnected

The machine is registered, but is either not running or not reachable by CloudLink Center.

Pending

The machine is registered and running, but conditions exists that require manual intervention before it is allowed to complete its startup process. For more information, see Accepting or rejecting a pending machine on page 75.

Rejected

An administrator has manually chosen to disallow this machine's startup.

Accepting or rejecting a pending machine

When a registered machine with an encrypted boot volume attempts to start up, CloudLink Center may suspend the startup process and put the machine in the pending state. This state means that key release policies are not met, and CloudLink Center cannot release encryption keys for the machine's boot volume. For more information, see Key release policies on page 57.

You can view the reason for the pending state in the Details column of the Machines panel. As a one-time option, you can then choose to manually:

- Accept the machine's startup. CloudLink Center releases encryption keys for the boot volume, and the machine continues its startup process. CloudLink Center shows the machine with the connected state.
- Reject the machine's startup. CloudLink Agent disconnects from CloudLink Center and stops requesting encryption keys. CloudLink Center shows the machine with the disconnected state.

For example, by default, CloudLink Center checks that the machine's IP address belongs to an approved network for the machine's group. For more information, see Approved networks for machine groups on page 67. If the IP address is not in this list, CloudLink Center puts the machine in the pending state. After determining whether you want to allow this machine to start up, you choose to accept or reject the startup process.

Accepting or rejecting a machine applies to the current startup process only. The next time a previously accepted or rejected machine starts, it is put in the pending state again if any reason for this state is detected. You must once again choose whether to accept or reject the machine. If no conditions exist for the pending state (for example, the previous issue has been resolved), the machine's state is connected.

Prerequisites

You can accept or reject a machine only if it is in the pending state.

Task summary

Permissions	Control VM Boot
Contents panel	**Agents** > **Machines**
Commands	**Accept** **Reject**

Viewing registered machines

You can view a list of machines registered with CloudLink Center.

Task summary

Permissions	View VMs
Contents panel	**Agents** > **Machines**
Commands	n/a

Machines table information

The Machines table includes the following information for each machine:

Host

The name of this machine.

Status

The status of the machine (for example, disconnected or connected). For servers in a cluster, the status is not provided.

IP Address

The IP address of this machine.

Serial Number

The unique identifier for the machine in the CloudLink Center database.

Platform

The platform hosting the machine.

Group

The machine group that this machine belongs to.

Machine details

In addition to the information provided in the Machines table, details include:

Volumes

A list of the volumes for this machine, identifying the volume name, encryption status, unique identifier in the CloudLink Center database, the SED the volume is on if SEDs are used, and compliance with the machine group’s volume encryption policy.

SED

A list of self-encrypting drives for this machine, identifying the drive name, lock status, model name, whether or not it is supported by CloudLink, and the size.

Operating System

The operating system running on this machine.

Registered

The date and time that CloudLink Agent registered with CloudLink Center.

Version

The version of CloudLink Agent.

Connected To

The CloudLink Center host the machine is connected to.

Moving a machine to a different machine group

Every machine registered with CloudLink Center belongs to a machine group. You can change the machine group to which a machine belongs.

Task summary

Permissions	Control VM Boot
Contents panel	**Agents** > **Machines**
Commands	**Actions** > **Move To Group**

Removing a machine

Remove a machine when you no longer want it registered with CloudLink Center. Typically, you remove a machine because:

- You no longer want to make use of the machine in the CloudLink environment. In this case, you want to decrypt any encrypted volumes and remove CloudLink Agent from the machine. The machine must be in the disconnected state.
- You want to release a machine instance license. In this case, you want to de-register the machine from CloudLink Center. At some time in the future, you may re-register the machine. The machine must be in the disconnected state.

Note

An encrypted capacity license's capacity is increased when a device is decrypted.

Removing a machine from the CloudLink environment

If you no longer want to use a machine in the CloudLink environment, you can remove it so that the machine is unregistered from CloudLink Center and CloudLink Agent is automatically uninstalled.

Prerequisites

The machine must be in the disconnected state.

We recommend that you decrypt the boot volume and any additional data volumes (Windows) or mounted devices (Linux) that you want to use after the machine has been de-registered from CloudLink Center, as they will be inaccessible otherwise. For more information, see Machine volumes on page 81.

Task summary

Permissions	Remove VM
Contents panel	**Agents** > **Machines**
Commands	**Actions** > **Remove**

Releasing a license

If you want to temporarily remove a machine instance, encrypted capacity, or a KMIP client from CloudLink Center to release a license, ensure it is in the disconnected state. Once removed, the machine does not appear in the **Machines** panel. However, if the machine is restarted, it is listed in this panel in the pending state. For more information, see Accepting or rejecting a pending machine on page 75.

Prerequisites
The machine must be in the disconnected state.

Task summary

Permissions	Remove VM
Contents panel	**Agents** > **Machines**
Commands	**Actions** > **Remove**

Shredding a machine

Shred encrypted machines to make the machines and their volumes completely inaccessible by destroying their keys in the keystore.

If you attempt to shred a machine and a keystore that contains keys for the machine is not accessible, CloudLink Center does not shred the machine. CloudLink Center deletes keys in all accessible keystores. You can try to shred the machine again after the inaccessible keystore is accessible.

With one exception, shredding a machine prevents that machine, including all backups, from being started again. The exception is when the keys are in the CloudLink Vault keystore and a backup of CloudLink Center exists that might have those keys.

When you shred a machine, you must retype the machine name. This practice is intended to minimize the risk of deleting the wrong machine.

If you shred a machine that has older shared keys from cloning or upgrading, the shared keys are not deleted and an error message stating “Some keys have not been deleted” is displayed. The current keys for the machine are deleted, however, and if the machine boot drive was encrypted, it no longer boots.

Prerequisites
The machine must be in the disconnected state.

To completely remove a machine from CloudLink Center, you must also:

- Decrypt the machine's disks.
- Uninstall CloudLink Agent on the machine.

Task summary

Permissions	Shred VM
Contents panel	**Agents** > **Machines**
Commands	**Actions** > **Shred**

Viewing the event history for a machine

You view only the events for a selected machine. For information about choosing the timeframe in which events occurred and the information provided on the Events page, see Viewing events on page 95.

Task summary

Permissions	View Events

Contents panel	**Agents** > **Machines**
Commands	**Actions** > **Show Event History**

Refreshing a Linux machine’s mounted devices

If you add a new mounted device for a Linux machine, you must refresh the machine, so that the new device is added to the **Machines** panel.

To refresh a Linux machine’s mounted devices, from the Linux machine command line, type the following: `svm reload [-v ]`

For information about optional `svm` parameters, see Commands for CloudLink Agent on page 167.

Working with cloned machines

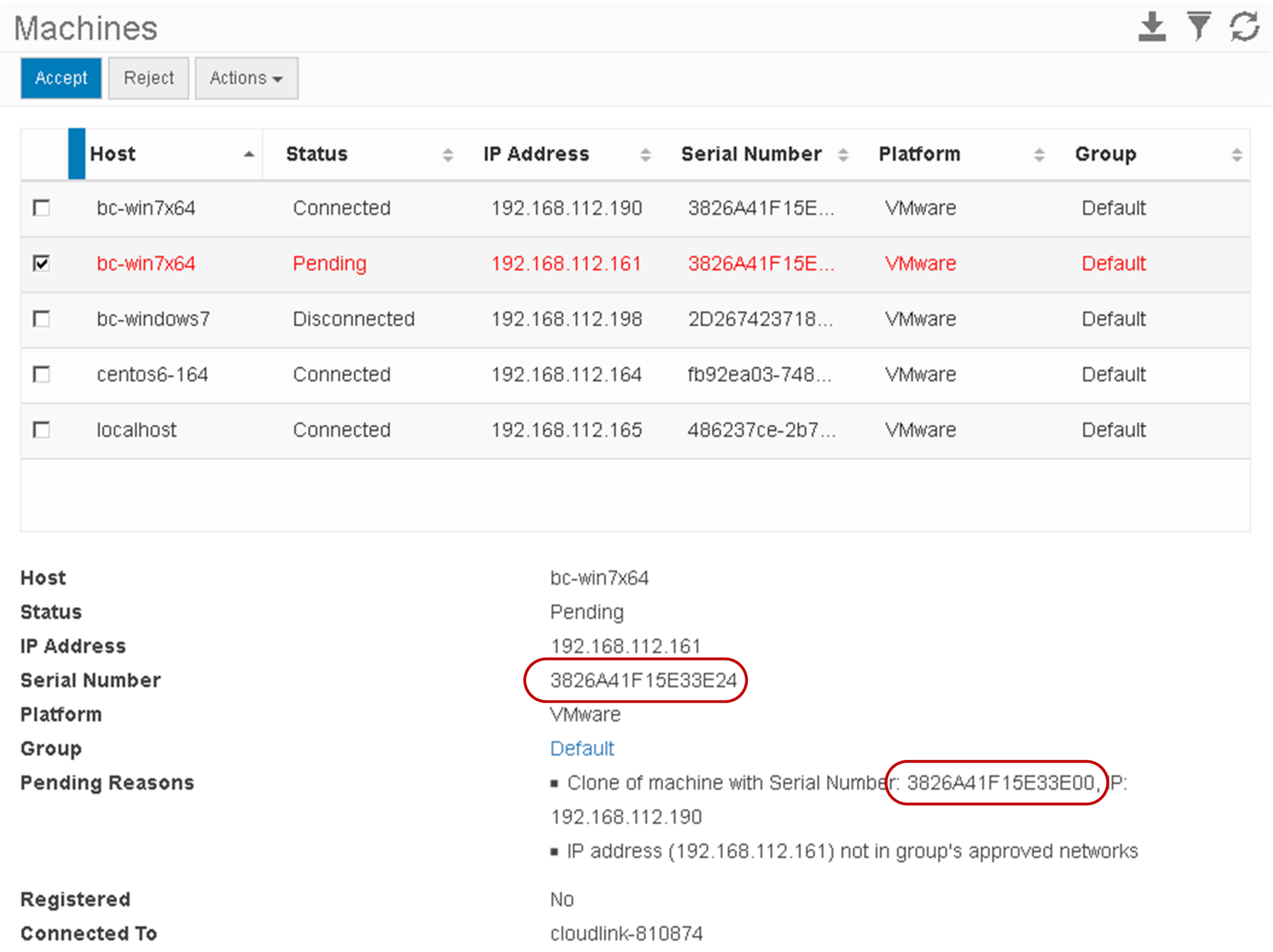
Each machine registered with CloudLink Center is assigned a unique serial number that is stored in the CloudLink Center database. By default, if you clone a registered machine in the connected state, and then start the clone, CloudLink Center puts the clone in the pending state. For more information, see Machine states on page 74.

CloudLink Center puts the clone in the pending state because the default key release policy does not allow CloudLink Center to release keys to a clone of a previously registered machine. You can change this key release policy, allowing automatic release of keys to clones of machines belonging to the group. For more information, see Key release policies on page 57.

To show the relationship with the machine in the pending state to the machine from which it was cloned, the serial number for the machine clone is the same as the original machine, with the exception of the last two digits.

As shown in the figure below, details for the selected machine show that it is in the Pending state. The serial number for the pending machine ends with the digit 60 and the serial number for the machine from which it was cloned ends with the digit 00.

Figure 7 Cloned machine serial numbers



	Host	Status	IP Address	Serial Number	Platform	Group
□	bc-win7x64	Connected	192.168.112.190	3826A41F15E...	VMware	Default
☑	bc-win7x64	Pending	192.168.112.161	3826A41F15E...	VMware	Default
□	bc-windows7	Disconnected	192.168.112.198	2D267423718...	VMware	Default
□	centos6-164	Connected	192.168.112.164	fb92ea03-748...	VMware	Default
□	localhost	Connected	192.168.112.165	486237ce-2b7...	VMware	Default

Host	bc-win7x64
Status	Pending
IP Address	192.168.112.161
Serial Number	3826A41F15E33E24
Platform	VMware
Group	Default
Pending Reasons	▪ Clone of machine with Serial Number: 3826A41F15E33E00, IP: 192.168.112.190 ▪ IP address (192.168.112.161) not in group's approved networks
Registered	No
Connected To	cloudlink-810874

To allow the startup process for the cloned machine to continue, you must accept the machine. For more information, see Accepting or rejecting a pending machine on page 75. Once a cloned machine has been accepted, it is restarted and assigned a new serial number.

Subsequent startups of the machine are enabled automatically, as long as the machine passes pre-startup authorization. For more information, see Pre-startup authorization on page 56.

Changing encryption keys on Linux machines

If boot or data volumes on the original machine were encrypted when the clone was created, the data on both machines is encrypted with the same key. If you want data on each machine encrypted with different keys, you must decrypt and then encrypt any encrypted volumes on one of the machines. For more information, see Machine volumes on page 81.

Changing encryption keys on Windows machines

New keys are generated for the cloned machine when it is accepted.

Changing hostnames

The hostname for a cloned machine is the same as the machine from which it was cloned. To help distinguish machines from their clones, you may want to change the hostname for clones. See the documentation provided for the clone's operating system.

Restarting the CloudLink Agent service on Linux machines

For Linux machines, you must restart the CloudLink Agent service if the networking configuration is changed after CloudLink Agent deployment.

To restart the CloudLink Agent service on a Linux machine, from the machine's command line, type this command: `service svmd restart`

Machine volumes

Each machine registered with CloudLink Center is assigned a unique serial number that is stored in the CloudLink Center database. If a machine has more than one volume, CloudLink Center management operations (such as encrypting or decrypting a machine's boot or data volumes) can be performed on individual volumes.

Before removing a machine that you no longer want under CloudLink Agent control, you should decrypt the volumes if you want to continue using the machine. Otherwise, its volumes remain encrypted and therefore inaccessible.

For information about monitoring encryption or decryption processes on a machine, see Monitoring the real-time progress of encryption and decryption processes on page 88.

Encrypting a volume

In CloudLink Center, you can encrypt system partitions or data volumes.

The following Linux system partitions are automatically encrypted or decrypted with the `/` partition:

`/`	`/bin`	`/sbin`	`/root`	`/lib`	`/var`
`/usr`	`/usr/local`	`/initrd`	`/tmp`	`/home`	`/opt`

⚠ WARNING

If at least one system partition is encrypted by CloudLink 6.7 or earlier, you cannot encrypt an individual system partition. You must first decrypt all system partitions, then encrypt `/` to encrypt all system partitions at once.

If more than one volume on the machine is unencrypted, choose the one that you want to encrypt. You can encrypt only one volume at a time.

For Linux machines, CloudLink encrypts using dm-crypt. The device must be mounted. CloudLink Center first unmounts the mount point. If files are open, an error occurs and the encryption does not occur.

When encryption completes, CloudLink Center reboots the machine.

Encrypting a data volume on a self-encrypting drive

You can encrypt a data volume on a self-encrypting drive (SED) by selecting **Encrypt**, as long as SED encryption is not being managed by CloudLink. If SED encryption is being managed by CloudLink, then volume encryption is blocked. You do not need an SED license to encrypt data volumes on an SED.

Note

CloudLink does not support boot volume encryption on physical machines.

Task summary

Permissions	Change VM Encryption
Contents panel	**Agents** > **Machines**
Commands	**Actions** > **Encrypt**

Managing a self-encrypting drive from CloudLink Center

You can take ownership of an SED by selecting **Manage SED**. This option is only available if an SED license is uploaded and an SED is detected in the physical machine managed by CloudLink Center.

When CloudLink Center manages an SED, the SED is locked and the encryption key must be released by CloudLink Center to unlock the SED. When a machine with SEDs is powered on, or when an SED is removed from a machine, the SED must be unlocked by CloudLink Center.

Note

The **Manage SED** option does not change any data on an SED. It only takes ownership of the encryption key.

Task summary

Permissions	Change VM Encryption
Contents panel	**Agents** > **Machines**
Commands	**Actions** > **Manage SED**

Managing a self-encrypting drive from the command line

As an alternative to managing an SED from CloudLink Center, you can manage it from the command line.

Procedure

- Type this command to manage an SED from the command line:

```
svm manage [device_name]
```

For example:

```
svm manage /dev/sdb
```

Encrypting a Linux machine's devices from the command line

As an alternative to encrypting a Linux machine's mounted device from CloudLink Center, you can encrypt it from the command line.

Before you begin

The device must already be mounted.

The following Linux system partitions are automatically encrypted or decrypted with the / partition:

/	/bin	/sbin	/root	/lib	/var
/usr	/usr/local	/initrd	/tmp	/home	/opt

⚠WARNING

If at least one system partition is encrypted by CloudLink 6.7 or earlier, you cannot encrypt an individual system partition. You must first decrypt all system partitions, then encrypt / to encrypt all system partitions at once.

You can encrypt the data volume for a Linux machine from the command line. If more than one volume on the machine is unencrypted, you choose the one that you want to encrypt. You can encrypt only one volume at a time.

The process used to encrypt the data volume is the same as when encrypting from CloudLink Center. For more information, see Encrypting a volume on page 81.

Procedure

- To encrypt a Linux machine's devices, encrypt the new data disk using this command:

  ```
  svm encrypt [mount_point]
  ```

  For example:

  ```
  svm encrypt /MyData/MyMountPoint
  ```

- You can also force encryption from the command line using this command:

  ```
  svm encrypt -f [mount_point]
  ```

  For example:

  ```
  svm encrypt -f /MyData/MyMountPoint
  ```

Note

The `-f` option restarts a Linux machine and encrypts the data partition. The `-f` option is for users who want to encrypt a Linux data partition that is in use.

For information about `svm` parameters, see Commands for CloudLink Agent on page 167.

Decrypting a volume

In CloudLink Center, you can decrypt boot or data volumes in the connected state on Windows or Linux machines.

If more than one volume is encrypted, choose the one that you want to decrypt.

If decrypting a volume means that it no longer complies with the volume encryption policy for the machine group, CloudLink Center prompts you to confirm that you want to decrypt the volume. For information, see Volume encryption policy on page 59. If you choose to decrypt the volume, CloudLink Center generates an alarm and you can choose to allow its non-compliance through an exemption. For more information, see Viewing volume encryption policy compliance on page 89.

Decrypting a data volume on a self-encrypting drive
You can decrypt data volumes on a self-encrypting drive (SED) by selecting **Decrypt**.

Note

CloudLink does not support boot volume encryption or decryption on physical machines.

Prerequisites
The machine must be in the connected state.

Task summary

Permissions	Change VM Encryption
Contents panel	**Agents** > **Machines**
Commands	**Actions** > **Decrypt**

Releasing a self-encrypting drive

You can release ownership of an SED by selecting **Release SED**. This option is only available if an SED license is uploaded and an SED is detected in the physical machine managed by CloudLink Center.

When CloudLink releases an SED, the SED is unlocked and the encryption key is released by CloudLink Center.

Note

The **Release SED** option does not change any data on an SED. It only releases ownership of the encryption key.

Task summary

Permissions	Change VM Encryption
Contents panel	**Agents** > **Machines**
Commands	**Actions** > **Release SED**

Releasing management of a self-encrypting drive from the command line

You can release management of an SED from the command line.

Procedure

- Type this command to release management of an SED:

  ```
  svm release [device_name]
  ```

  For example:

  ```
  svm release /dev/sdb
  ```

Decrypt a Linux machine's boot volume from the command line

As an alternative to decrypting a Linux machine's boot volume from CloudLink Center, you can decrypt it from the command line.

If you decrypt a volume and it no longer complies with the group's volume encryption policy, CloudLink Center generates an alarm and you can choose to allow its non-compliance through an exemption. For more information, see Viewing volume encryption policy compliance on page 89.

The procedure used to decrypt the boot volume depends on the version of CloudLink that was used to encrypt the boot volume. CloudLink version 5.0 and earlier uses eCryptfs for encryption. CloudLink version 6.8 uses dm-crypt.

Decrypting a boot volume encrypted using CloudLink 6.8

Procedure

1. Back up all data.
2. From the command line, type the following:

   ```
   svm decrypt / [-v ]
   ```

   For information about this command, see Commands for CloudLink Agent on page 167.

3. When prompted to restart the machine, select **Yes**.
4. Wait until the machine is displayed in the **Agents** > **Machines** panel showing the state as connected.

Note

The time required to complete this operation depends on the size of the boot disk and the environment type.

Decrypting a boot volume encrypted using CloudLink 5.0 or earlier

Procedure

1. Back up all data.
2. Attach a second disk that is at least as large as the root disk.

   This disk should not contain any data as it will be overwritten with contents from the encrypted disk. Do not mount this disk.

3. From the command line, type the following:

   ```
   svm decrypt /[target_disk] [-v ]
   ```

   where target_disk is the disk attached in Step 2.

   For example:

   ```
   svm decrypt /dev/sdb
   ```

   For information about this command, see Commands for CloudLink Agent on page 167.

4. When prompted to restart the machine, select **Yes**.
5. Wait until the machine is displayed in the **Agents** > **Machines** panel with the connected state.

   Note

   The time required to complete this operation depends on the size of the boot disk and the environment type.

6. When CloudLink Center shows the boot volume is connected and decrypted, you can safely detach the second disk.

Decrypt a Linux machine’s mounted volumes from the command line

As an alternative to decrypting a Linux machine’s mounted volumes from CloudLink Center, you can decrypt them from the command line. This process decrypts the data to a new volume that is mounted with the same name as the encrypted mount point. In addition to decrypting the data, this process unregisters the mount point from CloudLink Center.

If you decrypt a volume and it no longer complies with the group’s volume encryption policy, CloudLink Center generates an alarm and you can choose to allow its non-compliance through an exemption. For more information, see Viewing volume encryption policy compliance on page 89.

The procedure used to decrypt a volume depends on the version of CloudLink that was used to encrypt the volume. CloudLink version 5.0 and earlier uses eCryptfs to encrypt volumes. CloudLink version 6.8 uses dm-crypt.

Decrypting a volume encrypted using CloudLink 6.8

Use this command to decrypt the encrypted data disk for a volume encrypted using CloudLink 6.8.

```
svm decrypt [mount_point]
```

For example:

```
svm decrypt /MyData/MyMP
```

You can also force decryption from the command line using this command:

```
svm decrypt -f [mount_point]
```

For example:

```
svm decrypt -f /MyData/MyMountPoint
```

Note

The `-f` option restarts a Linux machine and decrypts the data partition. The `-f` option is for users who want to decrypt a Linux data partition that is in use.

For information about `svm` parameters, see Commands for CloudLink Agent on page 167.

Decrypting a volume encrypted using CloudLink 5.0

Procedure

1. Add a new data disk that is at least as large as the encrypted disk.
   For example:

   ```
   /dev/sdc
   ```

   This disk should not contain any data as it will be overwritten with contents from the encrypted disk.

2. Mount the new disk.
   For example, mount it to the following directory:

   ```
   /MyData/AdditionalMP
   ```

3. Decrypt the encrypted data disk:

   ```
   svm decrypt [encrypted_mount_point] [additional_mp]
   ```

   For example:

   ```
   svm decrypt /MyData/MyMP /MyData/AdditionalMP
   ```

   All the decrypted data is now on an additional disk /dev/sdc, which is mounted to /MyData/AdditionalMP.

   If you want to keep your decrypted data mounted to the original location (for example, /MyData/MyMP), complete Steps 4 to 7.

   If you want to keep your decrypted data on the new mount point (for example, /MyData/AdditionalMP), go to Step 8.

4. Copy your data from the new mount point to the original mount point:

   ```
   mv /MyData/AdditionalMP /MyData/MyMP
   ```

5. Unmount the new disk:

   ```
   umount /MyData/AdditionalMP
   ```

6. Edit the /etc/fstab file:

   For example, you need to update any lines that refer to the original mount point:

   ```
   /dev/sdc1 /MyData/MyMP ext4 defaults 1 2
   ```

7. Mount the original mount point (/MyData/MyMP).
8. Reload the configuration into CloudLink:

   ```
   svm reload
   ```

Monitoring the real-time progress of encryption and decryption processes

After initiating an encryption or decryption process on a Windows machine, you can monitor progress. On a Linux machine, you can monitor progress of encryption processes.

Windows machines

On a Windows machine, you can monitor progress of encryption or decryption processes in real-time on the machine. You can also monitor the progress in the Machines panel. For more information, see Viewing registered machines on page 76.

To monitor progress on a Windows machine:

Procedure

1. Click the **CloudLink Agent** icon in the Windows taskbar.
2. Click the **Encryption Status** option to display the percentage of encryption or decryption that is complete.

Linux machines

After initiating an encryption process on Linux machine, the current encryption progress is shown in the machine console. You can also monitor progress in the Machines panel. For more information, see Viewing registered machines on page 76.

The progress of decryption processes is not available for Linux machines.

Viewing volume encryption policy compliance

For each machine volume, CloudLink Center indicates its state relative to the machine group's volume encryption policy.

For a selected machine, you can view the policy states for each volume on the Machines panel. For more information, see Viewing registered machines on page 76.

Volume policy states include:

OK

The volume complies with the volume encryption policy for the machine group. Any policy exemptions have been allowed.

Violated

The volume does not comply with the volume encryption policy for the machine group

Allowing an exemption

The volume encryption policy for a machine group applies to all volumes for all machines belonging to the group. You may want to exempt a particular volume from the policy. For example, you might have assigned the Boot and All Data volume encryption policy to a machine group. However, you want one volume on an individual machine in that group to be decrypted. When you manually decrypt this volume, it no longer complies with the volume encryption policy for the machine group.

To indicate that a volume does not comply with the machine group's volume encryption policy, CloudLink Center:

- Generates an alarm
- Displays an exempt link beside the volume name on the Machines panel

You can specify that you want to allow the non-compliance by allowing an exemption for the volume.

Only decryption of a volume that does not comply with the existing volume encryption policy generates an alarm. Encryption of a volume will not make a volume non-compliant.

Task summary

Permissions	Change VM Encryption Policy

Contents panel	**Agents** > **Machines**
Commands (in the Machines table Volumes row)	**Exempt**

Unlocking a moved volume

A key release policy determines the conditions under which CloudLink Center allows keys to be released (if any) when it detects that a volume is associated with a different machine than the one recorded in the CloudLink Center database. For information, see Key release policies on page 57.

The policy may require that you manually unlock the volume. For information about the procedure for moving a volume and manually unlocking the volume, see Moving an Encrypted Disk to Another Machine on page 175.

Task summary

Permissions	Control VM Boot
Contents panel	**Agents** > **Machines**
Commands	**Actions** > **Pending Volumes/Disks** **Accept**

Changing the CloudLink Center IP address

If you needed to change the static IP of CloudLink Center and you deployed CloudLink Agent using the static IP, you may need to change the CloudLink Center IP address.

You must update each CloudLink Agent with the new CloudLink Center IP address, which is used by CloudLink Agent to communicate with CloudLink Center.

Windows machine

Procedure

1. Type the following command in PowerShell:

   ```
   svm  /S clc_address
   ```

   For information about this command, see Command actions for Windows PowerShell on page 170.

Linux machine

Procedure

1. Type the following command from the Linux machine's command line:

   ```
   svm -S clc_address [-v ]
   ```

For information about this command, see Command actions for Linux on page 168.

Moving a machine to a different CloudLink Center

You may want a machine put under management of a different CloudLink Center. You must decrypt volumes before moving the machine. Encrypted volumes moved to another machine will not be accessible.

Procedure

1. Decrypt any encrypted volumes on the machine.
2. Uninstall CloudLink Agent.
3. Deploy CloudLink Agent to the machine from the new CloudLink Center.

   For information about deploying CloudLink Agent, see *CloudLink Deployment Guide for Enterprise*.

CHAPTER 7

Monitoring CloudLink Center

This chapter presents the following topics:

Overview

CloudLink Center provides comprehensive monitoring of the CloudLink environment and its machines.

Monitoring information is organized using several categories:

- Actions
- Events
- Security Events
- Alarms
- Diagnostics
- Users Sessions
- Usage

Actions, events, security events, and alarms

When an action, event, or security event occurs, CloudLink Center displays a notification header and all notifications in the lower, right-hand corner of the window. You can show or hide notifications using the icons in the notification header. The notification header and notifications automatically disappear after a few seconds.

Each hour, CloudLink Center checks to determine if more than 10,000 actions, events, and security events exist. If so, CloudLink Center deletes entries older than four days, starting with the oldest entry, until the total number of entries is less than 10,000.

In addition to action and event notifications, CloudLink Center raises alarms to make you aware of critical states or conditions. For more information, see Viewing alarms on page 20.

Viewing actions

The Actions page shows the actions initiated by users, such as uploading or assigning licenses, accepting a pending machine, or setting the CloudLink Vault mode.

An action generates at least one event. For more information, see Viewing events on page 95.

Actions table information
The Actions table includes the following information for each action:

Action
A description of the action

Started
The date and time that the user initiated the action

Completed
The date and time that the user completed the action

User
The user who performed the action

Target
The object that generated the action (for example, Host:clc1)

Status

The current status of the action

Note

You can filter the table to show a subset of actions that occurred in the last 10, 30, or 60 minutes.

Action details

In addition to the information in the Action table, details include:

Host

The CloudLink Center server on which the user performed the action

Details

A brief description of the action

Task summary

Permissions	View Actions
Contents panel	**Monitoring** > **Actions**
Commands	**Last 10 minutes** **Last 30 minutes** **Last Hour** **All**

Viewing events

The Events page shows internal activity in the system, as well as activity related to actions and alarms.

CloudLink assigns one of six levels to each event to indicate its importance. These levels map to syslog levels 1 to 6. For example, Alert is level 1, Critical is level 2 and so on.

Event level name	Syslog level number
Alert	1
Critical	2
Error	3
Warning	4
Notice	5
Information	6

For alarms, CloudLink Center creates an event when an alarm is raised, assigning it a level of Error if the severity is high or Warn if the severity is low. CloudLink Center creates another event if the condition or state that caused the alarm is resolved, assigning this event the Information level.

For actions, CloudLink Center creates an event when the user initiates the action, assigning it to the Notice level. On completion of the action, CloudLink Center may create additional events based on the internal processing of an action (if needed). CloudLink Center always creates an event that indicates when an action completed.

CloudLink writes events to the configured syslog server. Details about when events were initiated and completed are available only in the syslog server. These details are not provided in the Events table.

Events table information

The Events table includes the following information for each event:

Event

A description of the event

Level

The importance level of the event

Target

The object that generated the event (for example, User:secadmin)

Timestamp

The date and time that the event occurred

Note

You can filter the table to show a subset of actions that occurred in the last 10, 30, or 60 minutes.

Events details

In addition to the information in the Events table, details include:

Host

The CloudLink Center server on which the event occurred

Task summary

Permissions	View Events
Contents panel	**Monitoring** > **Events**
Commands	**Last 10 minutes** **Last 30 minutes** **Last Hour** **All**

Viewing security events

The Security Events page shows all CloudLink security events, such as:

- Logins by users
- Failed attempts to unlock the CloudLink Vault using a passcode
- Registrations for machines
- Changes to the CloudLink Vault mode
- Successful or failed attempts to execute a secure user action
- Key activities such as requests, updates, or moves

CloudLink Center assigns each security event a level to indicate its importance. The level types are the same as those for events. For information, see Viewing events on page 95.

CloudLink writes security events to the configured syslog server.

Task summary

Permissions	View Security Events
Contents panel	**Monitoring** > **Security Events**
Commands	**Last 10 minutes** **Last 30 minutes** **Last Hour** **All**

Security Events table information

The Security Events table includes the following information for each security event:

Event

A description of the event

Level

The importance level of the event

Target

The object that generated the event (for example, User:secadmin)

Timestamp

The date and time that the security event occurred

Result

The outcome of the security event (for example, Allowed)

Note

You can filter the table to show a subset of actions that occurred in the last 10, 30, or 60 minutes.

Security Event details

In addition to the information in the Security Events table, details include:

Host

The hostname of the CloudLink Center server on which the security event occurred

In addition to the information in the Security Events table, for security events generated for an action, details include:

Action Status

The status of the action that generated the security event

Action Details

A brief description of the action that generated the security event

In addition to the information in the Security Events table, for security events that are not related to actions, details include:

Details

A brief description of the security event

Viewing alarms

For more information, see Viewing alarms on page 20.

Alarms configuration

Users can choose whether CloudLink Center continues to report alarms or ignores them. In the Alarms Configuration panel, you can select an alarm and choose whether that alarm is watched or ignored. You can also choose whether or not email notifications are sent for selected alarms.

Configuring alarms and notifications

You can change alarm notification states and email notification status by selecting an alarm in the **Alarms Configuration** panel.

Task summary

Permissions	n/a
Contents panel	**System** > **Alarms Configuration**
Commands	**Change**

Configure an alarm state

When configuring an alarm state, choose one of these options:

Watched

Future notifications for this alarm type are reported.

Ignored

Future notifications for this alarm type are ignored.

Configure email notifications

When configuring an alarm state, choose one of these options:

Send

Send email notifications for this alarm.

Do not send

Do not send email notifications for this alarm.

Email notifications

Email notifications can be sent when a CloudLink Center alarm is raised or updated. You can configure the CloudLink Center server that generates an alarm to send an email notification whenever an alarm is generated or updated.

Adding an email server and account

You can add an email server and account to use to send notifications.

Task summary

Permissions	n/a
Contents panel	**System** > **Email Notifications**
Commands	**Change Configuration**

Configure an email server

Provide the following values when configuring an email server:

Server Type
: The type of Simple Mail Transfer Protocol (SMTP) server

Server Address
: The SMTP server address

Port
: The SMTP server port

Sender Address
: The originating email address

User Name
: The email account username

Password
: The email account password

Email subject and recipient settings

You send a test email, change the subject line, add recipients, and delete selected recipients.

Task summary

Permissions	n/a
Contents panel	**System** > **Email Notifications**
Commands	**Send Test Email** **Change Subject Format** **Add Recipient** **Delete Recipient**

Recipient Address panel

Lists the alert email recipients. The list can be sorted by address.

Log files

You can view individual CloudLink Center log files or download all log files in a compressed ZIP file.

Viewing individual log files

You can view the tail of an individual log file and specify the frequency that it automatically refreshes.

Task summary

Permissions	View Server Logs
Contents panel	**Monitoring** > **Diagnostics**
Commands	**View Logs**

View Log values

When selecting a log file to view, provide the following values:

Log File

The name of the log file to view

Lines To Show

The number of lines from the tail of the log file to view

Update Interval (sec)

The frequency (seconds) to update the view with the current file content

Downloading log files

You can download all the CloudLink Center log files in a compressed ZIP file. For example, when reporting an issue to Dell EMC Customer Support, this file is required.

Task summary

Permissions	View Server Logs
Contents panel	**Monitoring** > **Diagnostics**
Commands	**Actions** > **Download Logs**

Creating a diagnostics log file

The Generate Diagnostics command creates a diagnostics log file that is used by Dell EMC Customer Support in case of a support issue. It is downloaded with the log files.

Task summary

Permissions	View Server Logs
Contents panel	**Monitoring** > **Diagnostics**
Commands	**Actions** > **Generate Diagnostics**

Enabling debug mode

Dell EMC Customer Support uses debug mode when investigating support issues.

Task summary

Permissions	View Server Logs
Contents panel	**Monitoring** > **Diagnostics**
Commands	**Actions** > **Enable Debug**

User sessions

You can view information about each user's session. You can also terminate user sessions.

Viewing user sessions

You can view information about each user's current session. For users who are not currently logged in, you can view information about their last session.

Task summary

Permissions	View User Sessions
Contents panel	**Monitoring** > **User Sessions**
Commands	n/a

User Sessions table information

The User Sessions table includes the following information for each user session:

User

The user name

User Roles

The roles assigned to the user

Login Time

The date and time that the user last logged in

Originated From

The IP address of the host from which the user logged in to CloudLink Center server

User Session details

In addition to the information in the User Session table, details for a selected user session include:

Current

A flag that indicates the current web application session

Terminating user sessions

You can terminate a user session to immediately log out a user. The next time the user performs a task in the web browser, CloudLink Center displays its login screen.

Task summary

Permissions	Terminate User Session
Contents panel	**Monitoring** > **User Sessions**
Commands	**Terminate**

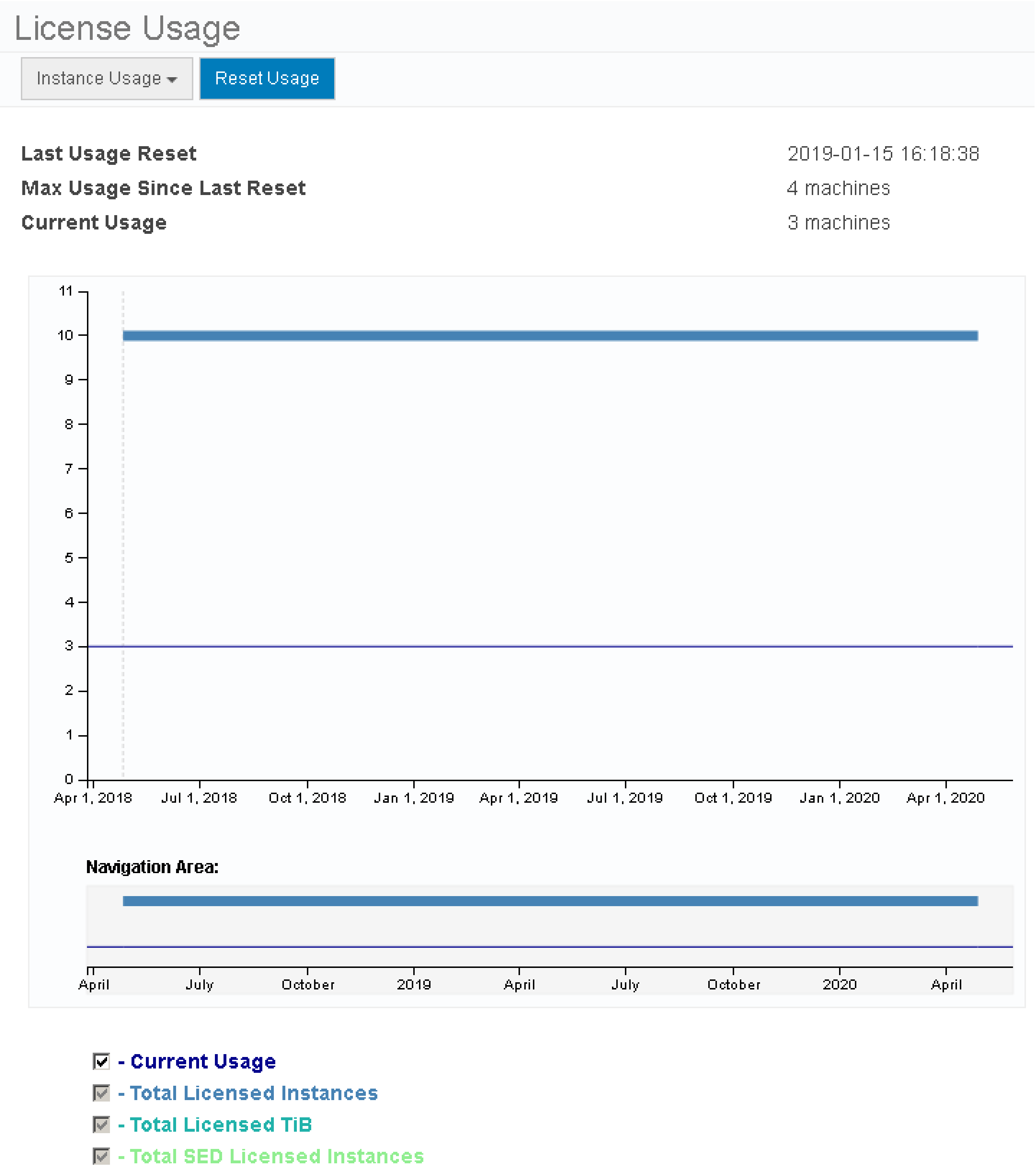
Usage

You can view usage statistics for machine instance, physical machines with SEDs, or encrypted capacity. There are no usage statistics for KMIP client or VMware ESXi socket licenses.

Viewing usage

You can view a chart, as shown in the following figures, of machine instance, physical machines with SEDs, or encrypted storage capacity, and summary information about registered instances, registered physical machines with SEDs, and used encrypted storage capacity.

Figure 8 License usage panel for instances



License Usage

Last Usage Reset	2019-01-15 16:18:38
Max Usage Since Last Reset	4 machines
Current Usage	3 machines

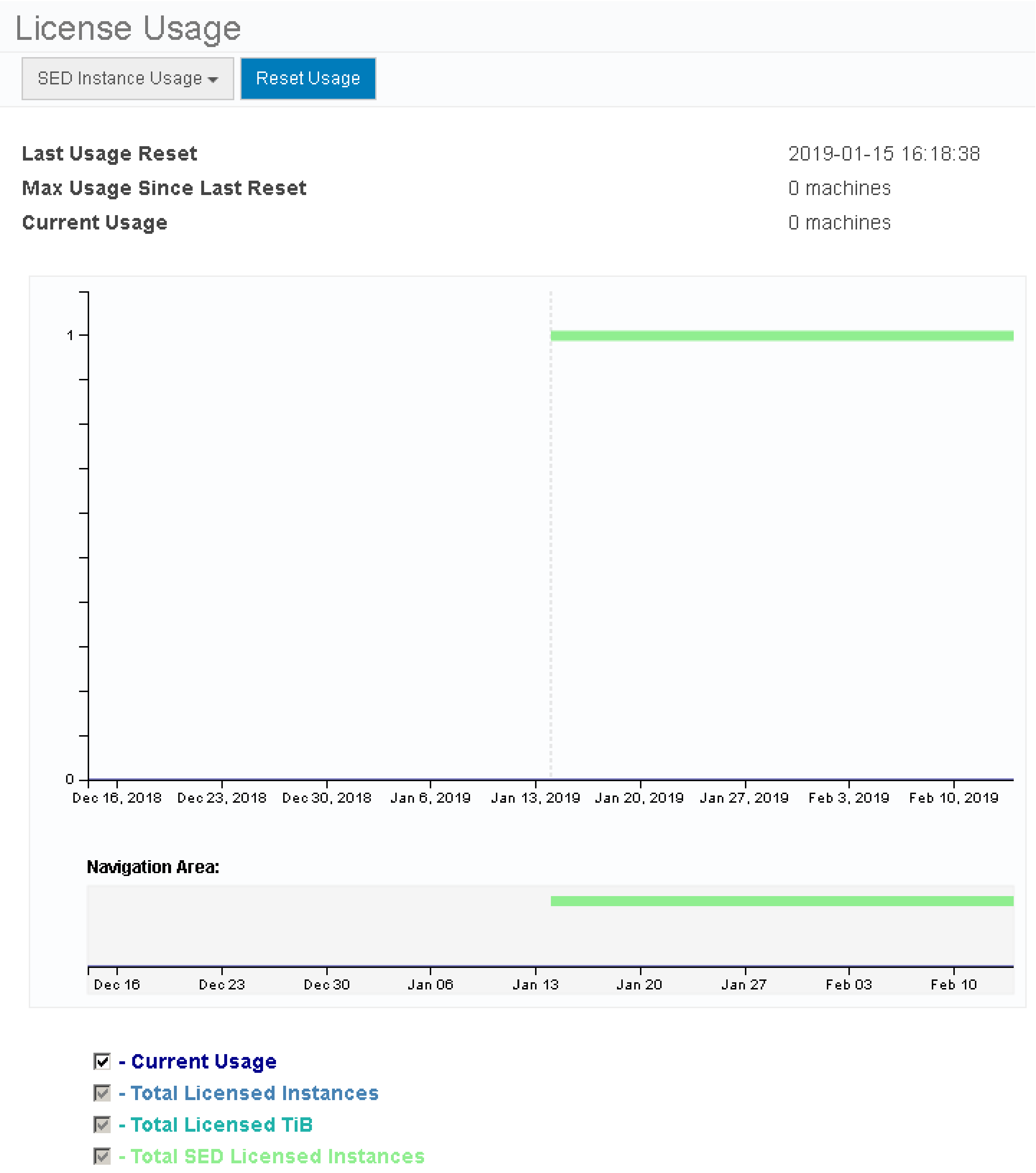
☑ - Current Usage

☑ - Total Licensed Instances

☑ - Total Licensed TiB

☑ - Total SED Licensed Instances

Figure 9 License Usage panel for SEDs



License Usage

SED Instance Usage ▾ | Reset Usage

Last Usage Reset	2019-01-15 16:18:38
Max Usage Since Last Reset	0 machines
Current Usage	0 machines

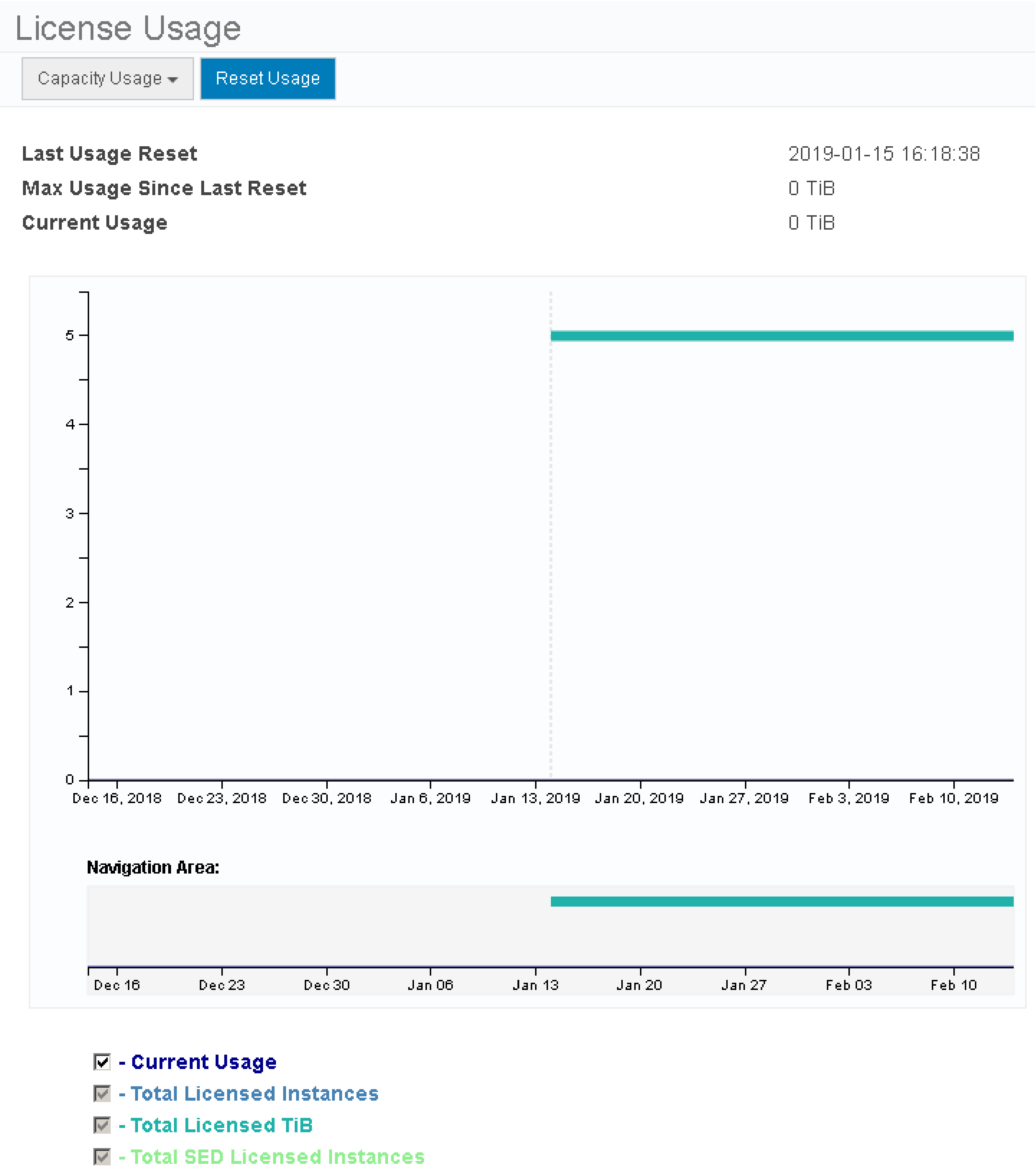
☑ - Current Usage

☑ - Total Licensed Instances

☑ - Total Licensed TiB

☑ - Total SED Licensed Instances

Figure 10 License Usage panel for capacity



License Usage

Last Usage Reset 2019-01-15 16:18:38

Max Usage Since Last Reset 0 TiB

Current Usage 0 TiB

Above the graph, CloudLink Center displays several statistics:

Last Usage Reset

The date and time that license usage statistics were reset. This statistic is provided for machine instance, physical machines with SEDs, or encrypted storage capacity. For information, see Resetting usage on page 106.

Max Usage Since Last Reset

The maximum number of machine instances registered, physical machines with SEDs registered, or encrypted capacity used since the last reset. This information might be useful if you are assessing your peak license usage over a specific time frame.

Current Usage

The number of machine instances currently registered, physical machines with SEDs registered, or encrypted capacity currently used.

The vertical axis of the graph represents the number of instances or amount of encrypted capacity registered or used. The horizontal line represents dates.

The graph displays a horizontal blue or green line that shows the total assigned licenses. Hover your mouse over the blue line to view information about that license.

The graph shows a blue or green line representing the number of registered machine instances, registered physical machines with SEDs, or used encrypted capacity. The amount of machine instances, physical machines with SEDs, or encrypted capacity that can be registered with CloudLink Center on any given date equals the sum of the machine instances, physical machines with SEDs, or encrypted capacity for all licenses valid on that date.

Task summary

Permissions	View Usage
Contents panel	**Monitoring** > **Usage**
Commands	**Instance Usage** **Capacity Usage** **SED Instance Usage**

Resetting usage

You can reset the value for the maximum number of registered machine instances, registered physcial machines with SEDs, or used encrypted capacity. For example, if you are monitoring the maximum number of machine instances registered, physical machines with SEDs registered, or encrypted capacity used each month, reset the usage on the first day of each month.

Task summary

Permissions	Reset Usage
Contents panel	**Monitoring** > **Usage**
Commands	**Reset Usage**

CHAPTER 8

Backing Up and Restoring CloudLink Center

This chapter presents the following topics:

Overview

System issues such as power interruptions or hardware failures may cause problems in CloudLink Center, such as data loss or database corruption. If problems occur, it is important to have a backup of CloudLink Center so that you can deploy a new server and restore CloudLink Center from the backup.

CloudLink Center backup

A backup file includes all critical information to get CloudLink Center up and running, including keystore configuration, user accounts, machine registrations and policies, and events. You can create backup files manually or automatically. You can create a backup store where CloudLink Center stores automatic backups.

Note

A backup file does not include CloudLink Center cluster information or licenses.

Backup key pairs and backup files

A backup is stored in a file that is encrypted using an AES-256 key protected by an RSA-2048 key pair.

You generate the RSA-2048 key pair. The public key is stored in CloudLink Center. Download and save the private key when the key pair is generated. To restore CloudLink Center from a backup file, both the backup file and its private key must be available to you.

The key pair is assigned a sixteen-digit ID. This ID is included in filenames for the private key required to use the backup and for the backup file. The filename for the private key uses the prefix cckey. The filename for the backup file uses the prefix `ccbackup`, by default. For more information about changing the prefix for the filename for the backup file, see Changing the filename prefix for the backup file on page 108.

The following are example file names for a private key and a backup file that requires the private key:

Private Key File Name

```
cckey-189a6361dc9772060730b654d9422b5f.pem
```

Backup File Name

```
ccbackup-189a6361dc9772060730b654d9422b5f-2015-03-23_09-15-
01.bak
```

Changing the filename prefix for the backup file

By default, the filename for the backup file uses the prefix `ccbackup`. You can change this prefix. For example, if you have multiple CloudLink Centers, you can use a prefix that uniquely identifies their backups. Using a different prefix for each CloudLink Center can help you to better identify the required backup if you need to restore a CloudLink Center.

Task summary

Permissions	Change Backup Configuration
Contents panel	**System** > **Backup**
Commands	**Actions** > **Change Backup File Prefix**

Viewing backup information

You can view the backup information.

Task summary

Permissions	View Backup Configuration
Contents panel	**System** > **Backup**
Commands	n/a

Backup page information

The Backup page includes the following information:

Backup File Prefix

Prefix used for the backup files

Current Key ID

The identifier for the current RSA-2048 key pair

Current Backup File

The name of the current backup file

Current Backup Time

The date and time that the current backup file was generated

Last Downloaded File

The name of the backup file that was last downloaded

Last Downloaded Time

The date and time of the last backup file download

Backup Schedule

The schedule for generating automatic backups

Next Backup In

The time remaining before the next automatic back is generated

The Backup page includes the following additional information when a backup file has been downloaded:

Backup Store

The backup store configuration type. If you have not configured a backup store, the value is Local. If Amazon S3 is used, the value is AMAZONS3.

The Backup page includes the following additional information when a FTP/SFTP/FTPS or S3-compatible backup store has been configured:

Host

The remote FTP/SFTP/FTPS host where a user is intended to save the CloudLink Center backups. You can set this value to the host IP address or hostname (if DNS is configured). This field also lists the endpoint if an S3-compatible backup store is used.

Port

The port used to access the backup store

User

The user with permission to access the backup store

Directory

The directory in the backup store where backup files are available
The Backup page includes the following additional information when a backup file has been generated.

Generating a backup key pair

You can generate a new backup key pair. For example, if the private key for the backup key pair is lost, you can generate a new key pair. You cannot access your backup files without the associated private key. When you generate a new key pair, CloudLink Center automatically generates a new backup file to ensure that the current backup can be opened with the private key of the current key pair.

Dell EMC recommends the following practices when you generate a new backup key pair to ensure that you have both a private key and backup file that it can open:

- Download the private key to the Downloads folder for the current user account (for example, `C:\Users\Admnistrator\Downloads`).The previously generated backup key will not open a backup file created after a new key is generated.
- Create a backup of the private key. Move both the backup and the private key to secure locations that are different from CloudLink Center. Store the private and public key in different locations.

Task summary

Permissions	Generate Backup Key
Contents panel	**System** > **Backup**
Commands	**Actions** > **Generate and Download New Key**

Changing the backup store for automatic backups

CloudLink Center automatically generates a backup file. You can use local storage or configure a remote backup store where CloudLink Center stores the backup file.

Regardless of whether you have configured a backup store, you can manually download the backup file. See Downloading the current backup file on page 112 for more information.

Task summary

Permissions	Change Backup Configuration

Contents panel	**System** > **Backup**
Commands	**Actions** > **Change Backup Store**

Backup Store values

When changing the backup store, provide the following values:

Store Type

Options are: Local, FTP, SFTP, FTPS, Amazon S3, or S3-compatible storage

Host

The remote FTP/SFTP/FTPS host where a user is intended to save the CloudLink Center backups. You can set this value to the host IP address or hostname (if DNS is configured).

Port

The port used to access the backup store

User

The user with permission to access the backup store

Password

The password used to access the backup store

Directory

The directory in the backup store where backup files are available

Endpoint

The endpoint for an S3-compatible backup store

URL Style

Either a virtual-hosted-style URL where the bucket name is a subdomain, or path-style URL where the bucket name is appended to the domain name and is a part of URL path.

Access Key ID

The Access Key ID associated with your Amazon Web Services (AWS) account or S3-compatible storage

Access Key

The Secret Access Key associated with your AWS account or S3-compatible storage

Bucket Name

The name of the bucket resource for the AWS or S3-compatible backup store

Region

The region where your AWS bucket is located

Note

You can test the backup store values using the **Test** button.

Changing the schedule for automatic backups

CloudLink Center automatically generates a backup file each day at midnight (UTC time). You can change the schedule for generating automatic backups.

Task summary (Manual Generation)

Permissions	Change Backup Configuration
Contents panel	**System** > **Backup**
Commands	**Actions** > **Change Backup Schedule**

Generating a backup file manually

You can generate a backup manually if you want to preserve CloudLink Center before the next automatic back up. When you generate a backup file manually, Dell EMC recommends that you download the backup file. For more information, see Downloading the current backup file on page 112.

An alarm occurs under these conditions:

- A backup has never been created (either manually or automatically)
- A backup has not been generated (manually or automatically) in the last seven days

For example, this alarm may be triggered if CloudLink Center cannot write the automatically created backup file to disk. The alarm may also be triggered if you are not using a backup store and have not manually downloaded the backup file in the last seven days.

Task summary (Manual Generation)

Permissions	Generate Backup
Contents panel	**System** > **Backup**
Commands	**Generate New Backup**

Downloading the current backup file

You can download the current backup file at any time. The current backup file is either:

- The last backup file that CloudLink Center automatically created
- The last backup file that you manually generated after the last automatic backup

When you download the current backup file, CloudLink Center displays the age of the backup file. For example, the message might indicate that the current backup was generated 14 hours and 23 minutes ago. CloudLink Center also displays the identifier of the private key needed to access the backup file.

The backup file is saved to your Downloads folder (for example, `C:\Users\Administrator\Downloads`). For information about backup file names, see Backup key pairs and backup files on page 108.

After downloading the file, we recommend that you move it to a location that is different from the CloudLink Center server. If CloudLink Center fails, you can access the backup file and its private key.

Prerequisites

You must have access to the last backup file that CloudLink Center generated automatically or you must manually generate a backup file.

Task summary

Permissions	Download Backup
Contents panel	**System** > **Backup**
Commands	**Actions** > **Download Backup**

Restoring CloudLink Center from a backup file

Before you begin

You must be a secadmin user to restore CloudLink Center from a backup file.

You need a CloudLink license. Licenses are not included in backups. You must upload a license when restoring from the backup.

You also need the:

- Backup file representing CloudLink Center at the time you want to restore to
- Private key for that backup file
- Passcodes for unlocking CloudLink Vault
- If using an external keystore, access to the keystore that contains the keys used at the time the backup file was generated

If problems occur with CloudLink Center, you can deploy a new server and restore CloudLink Center from the backup file.

Procedure

1. Deploy a new CloudLink Center server. For information, see *CloudLink Deployment Guide for Enterprise*.
2. From the **Initial Configuration** dialog box, in the **Deployment Type** list, click **Restore from Backup**, and click **Next**.
3. Select the backup file that you want to restore from and its backup key, and click **Restore**.
4. If the CloudLink Center server deployed in Step 1 has a different IP address than the original server, for each machine that was under the control of the previous CloudLink Center, configure the server address of the new CloudLink Center. For information, see Changing the CloudLink Center IP address on page 90.

Restoring a CloudLink Center cluster

Do not restore a CloudLink Center server in a cluster from a backup file. It is not restored as part of the cluster. It is restored as a standalone CloudLink Center.

CloudLink Center backups do not contain CloudLink Center cluster information. To restore a CloudLink Center that was part of a cluster, you must delete the CloudLink Center you want to restore from the cluster. See Removing a cluster server on page 122 for more information. Next, deploy a new CloudLink Center and join it to the cluster. See Joining a server to the cluster on page 119 for more information.

Restoring keystores from a backup file

If you delete a keystore and later determine that it contained keys required to access encrypted volumes, you might be able to restore the keystore from a backup. For more information about deleting keystores, see Deleting a keystore on page 50. You can modify some keystore properties after restoring a keystore.

Prerequisites

To restore CloudLink Center from a backup file, you must be a secadmin user.

You also need the:

- Backup file that contains the keystore before it was deleted
- Private key for that backup file
- If manual unlock was used for CloudLink Vault when the backup was created, passcodes for unlocking CloudLink Vault at that time

Task summary

Permissions	secadmin
Contents panel	**System** > **Backup**
Commands	**Actions** > **Restore Keystores**

Restore Keystore values

When restoring keystores, provide the following values:

Key

The private key for the backup file you are restoring from

Backup

The backup file that contains the keystore you want to restore

Unlock Passcode

The passcode for CloudLink Vault

When you restore keystores from a backup file, all keystores included in the backup are restored. On the Keystores page, CloudLink Center lists both existing and restored keystores. The names of restored keystore begin with the prefix restored_. For information about the Keystore page and its list of keystores, see Viewing keystores on page 44.

You can show the keys for each restored keystore to find the ones that are missing. For more information, see Showing keys in a keystore on page 51. You can then move all keys from a restored keystore to the keystore for the appropriate machine group. For information, see Moving keys to another keystore on page 51.

Dell EMC recommends that you delete restored keystores after obtaining the keys from a restored keystore. See Deleting a keystore on page 50 for more information.

Backup and restore guidelines

Keep the following information in mind when working with backup keys and files.

- During initial server configuration, you downloaded the private key for the RSA-2048 key pair. Ensure that you create a backup of this key.
- After you have completed configuration following deployment (such as assigning licenses, creating user accounts, and setting machine boot policy), create a backup.
- Ensure that you store the private key and backup files in separate, secure locations that are different from CloudLink Center. To restore CloudLink Center from a backup file, both the backup file and its private key must be available to you.
- If you need to regenerate the private key (for example, the original key was lost), generate both the private key and a backup file. Previous backup files are not accessible using the new private key.
- A backup includes the CloudLink Vault, Microsoft Azure Key Vault, and SafeNet LunaSA keystores. If you are using a different keystore type, you must back up your encryption keys. For information, see Managing Encryption Keystores and Keys on page 39.
- If you are using RSA SecurID for two-factor authentication, you must clear the shared node secret after restoring a keystore and before the first authentication attempt. For more information, see Clearing the shared node secret on page 129.
- A CloudLink Center cluster server that is restored from backup is not restored as part of a cluster. It is restored as a stand-alone server. Cluster configuration is not part of the backup file. You must delete the server from the cluster and redeploy it as a new CloudLink Center server, then join it to the cluster.

CHAPTER 9

Creating and Managing a CloudLink Center Cluster

This chapter presents the following topics:

Overview

A CloudLink Center cluster provides high availability if one CloudLink Center server in the cluster becomes unavailable. For example, a server may become unavailable unexpectedly due to a connection issue. A server may also become unavailable during periods of planned maintenance, when a server is taken offline.

A CloudLink Center cluster is comprised of up to four CloudLink Center servers, where each is active at all times. There is no master server. The agents can be actively connected to any server in the cluster.

CloudLink Center replicates configuration information between all servers in a cluster. This replication means that all servers contain the same critical configuration information: CloudLink licenses, volume encryption policy, user accounts, manual passcodes for unlocking CloudLink Vault, actions, alarms, and security events.

A CloudLink Center cluster only replicates CloudLink Center server data. Data from external resources, such as key locations, key protectors, and key management servers, are not replicated.

You can remove a server from a CloudLink Center cluster at any time. See Removing a cluster server on page 122 for more information.

For information about upgrading a CloudLink Center cluster, see the *CloudLink Upgrade Guide*.

Creating a CloudLink Center cluster

This section assumes that you have already deployed and configured a CloudLink Center server that will act as the initial server in the cluster.

Creating a CloudLink Center cluster involves the following tasks:

1. Deploy and configure one or more CloudLink Center servers.
   Each server must be deployed as a clean installation of CloudLink Center. For information about deploying and configuring CloudLink Center servers, see *CloudLink Deployment Guide for Enterprise*.
2. Join each additional server to the existing server using the Initial Configuration wizard. For information, see Joining a server to the cluster on page 119.

CloudLink Center server addresses in clusters

In a CloudLink Center cluster, servers and CloudLink Agents use the CloudLink Center server address for communication. You can specify this server address as a static IP address or a hostname in fully qualified domain name (FQDN) format, such as clc.example.com. You must specify the server address in the format you prefer before creating the cluster. You can use a mix of static IPv4 addresses, static IPv6 addresses, and FQDNs to create a CloudLink Center cluster. You cannot change the format after creating the cluster. For more information about pre-requisites and requirements for server addresses in clusters, see the *CloudLink Deployment Guide* for your environment.

Joining a server to the cluster

To create a CloudLink Center cluster, you join servers to the existing server. You can join one server at a time.

During the join process, a server uses the same CloudLink Vault mode (automatic or manual) as the existing server. You can change the CloudLink Vault mode for a new server after the join is complete. For information, see Changing the CloudLink Vault mode on page 125.

Note

Passcodes for unlocking CloudLink Vault operating in manual mode are global across the cluster.

Prerequisites

Before you can join a server to the cluster, you must have deployed and configured a clean installation of a CloudLink Center server (see *CloudLink Deployment Guide* for your environment).

To perform the join, you need the following information:

- Server address for the CloudLink Center server that will be the initial server. You can use the hostname if you have configured the DNS server first. For information, see Domain Name System servers on page 133.
- For the initial server, CloudLink Center login credentials (user name and password) for a user with Join To Cluster permissions.
- Public server address for the new server, referred to as the Cluster Server Name/ Address.

Procedure

1. From the **Initial Configuration** wizard, in the **Deployment Type** list, select **Add as a Cluster Member**.
2. Click **Next**.
3. In the **Server Name or IP Address** box, type the DNS name or IP address used to connect to this server. Click **Next**.
4. Type the following information:
   - In the **Server** box, type the IP address for the existing server.
   - In the **User Name** and **Password** boxes, type the login credentials for a user that has the *Join to Cluster* permission.
5. Click **Join Cluster**.

   After joining the server to the cluster, it is a good idea to verify the status of both servers. For information, see Viewing CloudLink Center cluster servers on page 120.

Administering a cluster

When accessing CloudLink Center to perform administration tasks, you can use any server in the cluster. The web application shows the server that the agent is connected to, but operations can be initiated from any server.

Guidelines for working with a cluster

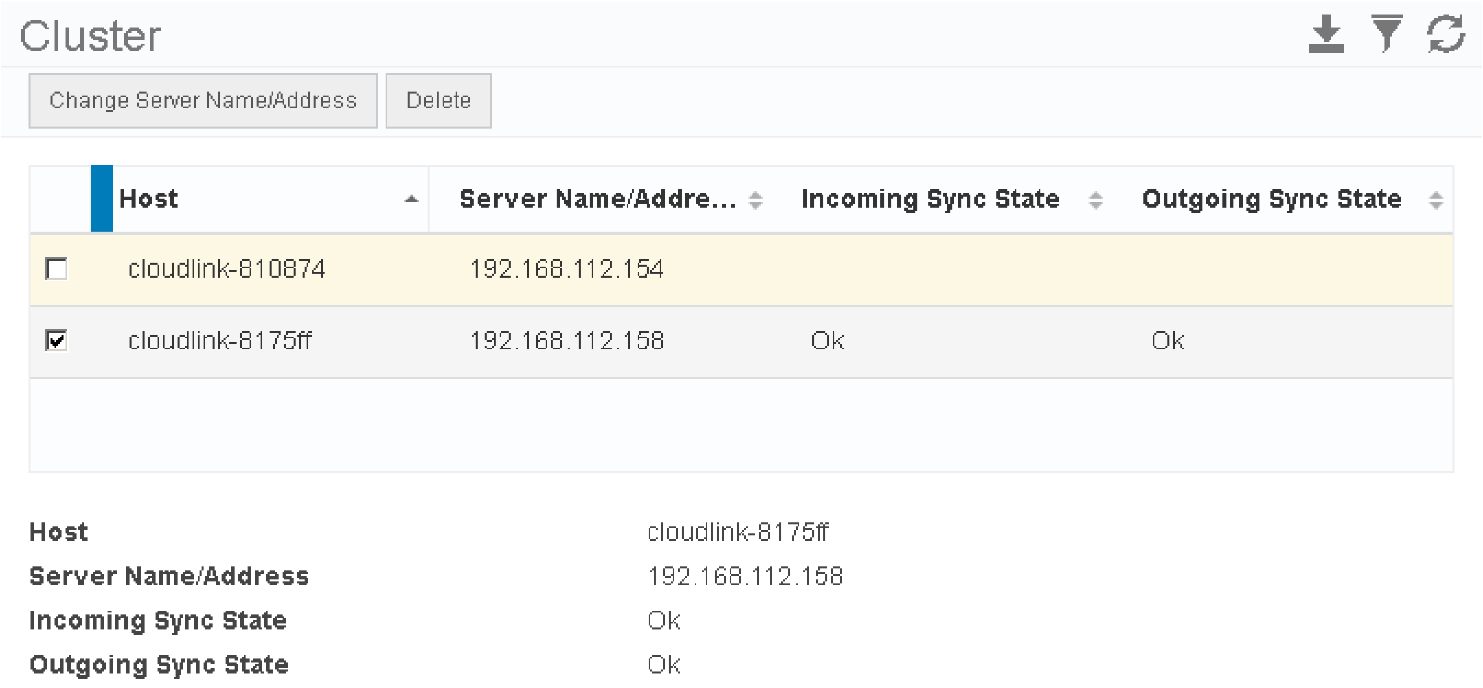
When working with CloudLink Center clusters, keep the following in mind:

- Each server in a cluster has its own CloudLink Vault. For a CloudLink Vault in automatic mode, unlocking the CloudLink Vault unlocks it only for the current server. CloudLink Vault for other servers in the cluster remain locked.
- If you want to use a keystore other than CloudLink Vault, for all servers in the cluster, configure DNS as described in Domain Name System servers on page 133.
- For user accounts, configure the Microsoft Windows domain as described in Domain Name System servers on page 133.
- If a CloudLink Agent is disconnected from a cluster when waiting for a pending key release, it reconnects to a cluster server if it is accepted.
- If you use a vSphere key management server (KMS), separately join each CloudLink Center in the cluster to the KMS.

Viewing CloudLink Center cluster servers

You can view the servers belonging to a CloudLink Center cluster. The Cluster Server Name/Address identifies the server on which you are using CloudLink Center. The figure below shows the Cluster panel viewed from a server.

Figure 11 Cluster panel viewed from a server



	Host	Server Name/Addre...	Incoming Sync State	Outgoing Sync State
□	cloudlink-810874	192.168.112.154		
☑	cloudlink-8175ff	192.168.112.158	Ok	Ok

Host	cloudlink-8175ff
Server Name/Address	192.168.112.158
Incoming Sync State	Ok
Outgoing Sync State	Ok

Task summary

Permissions	View Cluster Member

Contents panel	**System** > **Cluster**
Commands	n/a

Cluster table information

The Cluster table includes the following information:

Host

The common name of the server

Server Name/Address

The hostname or IP address of the server

Incoming Sync State

See below for sync state values

Outgoing Sync State

Indicates whether information is being replicated across cluster servers. One of:

- INITIALIZING—status check initialization, show after restart or during the join process while sync is establishing.
- OK—The server has recorded a heartbeat within the last 15 minutes
- ERROR—Database synchronization error
- OFF—sync isn’t working at all, most likely due to network connectivity
- TIME_DIFFERENCE—time difference between two nodes is more than one minute

Awaiting Outgoing Monitoring Batches

The number of monitoring batches waiting to be sent to the selected cluster server.

Awaiting Outgoing Config Batches

The number of configuration batches waiting to be sent to the selected cluster server.

Awaiting Outgoing Heartbeat Batches

The number of heartbeat batches waiting to be sent to the selected cluster server.

Cluster details

None

Changing a cluster server name or address

You can change a cluster server name or address after it is joined to a cluster.

Task summary

Permissions	Change Server Specific Configuration
Contents panel	**System** > **Cluster**
Commands	**Change Server Name/Address**

Removing a cluster server

You can remove a server from a CloudLink Center cluster.

Prerequisites
Before removing a server, stop the server.

Task summary

Permissions	Delete Cluster Member
Contents panel	**System** > **Cluster**
Commands	**Delete**

CHAPTER 10

Configuring the CloudLink Center Environment

This chapter presents the following topics:

Overview

Configuration of the CloudLink Center environment generally occurs during your initial set up. You can change the configuration, as needed. For example, you may want to change passcodes used to unlock CloudLink Vault if you suspect that an administrator has compromised existing passcodes.

CloudLink Vault

CloudLink Center includes an encrypted container, referred to as the CloudLink Vault that encrypts and protects:

- Credentials used to access remote resources

  For example, CloudLink Vault stores credentials required to access the Microsoft Windows domain, FTP or SFTP servers, and external keystores.
- Volume key encryption key (VKEK), if CloudLink Vault is used as the keystore

  For more information about using CloudLink Vault as the keystore, see Encryption key location and protector options on page 41.

When a CloudLink Center server restarts, it must unlock CloudLink Vault before CloudLink Center can authorize machine operations, ensuring that a stolen copy of CloudLink Vault or the disk on which it is stored does not contain any unprotected secrets or encryption keys.

CloudLink Vault was configured during initial server setup. For more information, see *CloudLink Deployment Guide for Enterprise*. You can view and change the configuration at any time to:

- Change the mode for opening the CloudLink Vault (automatic or manual)
- Change passcodes used to unlock the CloudLink Vault in manual mode

For information about CloudLink Vault and CloudLink Center clusters, see Creating and Managing a CloudLink Center Cluster on page 117.

Viewing the CloudLink Vault configuration

You can view the current CloudLink Vault configuration.

Task summary

Permissions	View Vault Mode
Contents panel	**System** > **Vault**
Commands	n/a

Vault page information

The Vault page includes the following information:

State

Identifies whether the CloudLink Vault is currently locked or unlocked. When locked, CloudLink Center displays a Manual lock on the Home page. For information, see Navigating CloudLink Center on page 14.

Unlock Mode

Indicates whether the CloudLink Vault is set to automatic or manual mode

Vault details

None

Changing the CloudLink Vault mode

Two modes are available for unlocking the CloudLink Vault when CloudLink Center starts:

- Manual Unlock requires a passcode. For information, see Setting CloudLink Vault passcodes on page 125. Because the available operations are limited when the CloudLink Vault is locked, CloudLink Center raises an alarm when the CloudLink Vault is locked.
- Auto Unlock opens the CloudLink Vault automatically using a unique key. This key is generated during each startup using server-specific values. The key is not stored.

Task summary

Permissions	Change Vault Mode
Contents panel	**System** > **Vault**
Commands	**Actions** > **Change Mode**

Setting CloudLink Vault passcodes

In manual mode, when CloudLink Center starts, an administrator must provide a passcode to unlock the CloudLink Vault.

One to three passcodes were defined during the initial server configuration. You can change passcodes at any time.

Task summary

Permissions	Set Vault Unlock Passcodes
Contents panel	**System** > **Vault**
Commands	**Actions** > **Set Passcodes**

Unlocking the CloudLink Vault

If CloudLink Center cannot unlock the CloudLink Vault on startup, CloudLink Center triggers an alarm. You must manually unlock the CloudLink Vault by providing a CloudLink Vault passcode. For more information, see Setting CloudLink Vault passcodes on page 125.

Task summary

Permissions	Unlock Vault
Contents panel	**System** > **Vault**
Commands	**Unlock**

CloudLink Vault guidelines

Guidelines for working with CloudLink Vault:

- When you restore a stand-alone CloudLink Center from a CloudLink backup file (see Restoring CloudLink Center from a backup file on page 113), and the CloudLink Vault is configured in Manual Unlock mode, you must use one of the defined passcodes to unlock the CloudLink vault.
- When you restore a stand-alone CloudLink Center from a CloudLink backup file (see Restoring CloudLink Center from a backup file on page 113), and the CloudLink Vault is configured in Auto unlock mode, the vault is automatically unlocked.
- When you restore a stand-alone CloudLink Center from a VMware backup or a clone, you must use one of the defined passcodes to unlock the CloudLink vault for either Manual or Auto Unlock modes.
- When you upgrade to a new version of CloudLink, CloudLink Vault must be set to Auto Unlock mode. If CloudLink Vault is set to Manual Unlock mode before the upgrade, it remains in Manual Unlock mode after the upgrade and the vault is locked. For more information, see the *CloudLink Upgrade Guide*.

Microsoft Windows domain for user accounts

Rather than creating users specifically for your CloudLink needs, you can use existing user accounts in your organization’s Microsoft Windows domain and assign those accounts the appropriate CloudLink Center roles.

Before you can add Domain accounts, you must configure a Microsoft Windows domain. For information, see User account types on page 30.

After joining the domain, domain users can log in to CloudLink Center using their Windows credentials.

Viewing the Microsoft Windows domain

You can view the current Microsoft Windows domain configuration.

Task summary

Permissions	View System Configuration
Contents panel	**System** > **Windows Domain**
Commands	n/a

Windows Domain table information

The Windows Domain table includes the following information:

Host Name

The Windows Domain Controller host name

Address

The domain controller host address

Global Catalog Port Status

Either:

- Accessible—CloudLink Center can reach the Global Catalog port
- Inaccessible—The Global Catalog port cannot be reached. While the Global Catalog port is inaccessible, all domain login attempts fail.

LDAP Port Status

Either:

- Accessible—CloudLink Center can reach the LDAP port
- Inaccessible—The LDAP port cannot be reached. While the LDAP port is inaccessible, all domain login attempts fail.

Configuring a Microsoft Windows domain

Prerequisites

You must meet the following prerequisites before joining CloudLink Center to a Microsoft Windows domain:

- You must configure a Microsoft Windows domain. For more information, see User account types on page 30.
- Verify that CloudLink Center has a DNS server configured. For more information, see Domain Name System servers on page 133.
- On the DNS server, create a reverse lookup zone for the Microsoft Windows domain controller subnet
- On the DNS reverse lookup zone, configure a pointer to the Microsoft Windows domain controller

Task summary

Permissions	Change System Configuration
Contents panel	**System** > **Windows Domain**
Commands	**Configure**

Configure Microsoft Windows domain values

CloudLink Center can dynamically find the Microsoft Windows domain controller. When specifying the Windows domain parameters, omit the **Primary Host** and **Secondary Host** values.

The provided username and password are used to:

- Join this server to an Active Directory domain and join any future servers added to a CloudLink Center cluster
- Validate a domain user's domain group membership and determine the user's roles

Note

Dell EMC recommends that the username and password used to join the Windows domain is a dedicated user whose password does not expire, because these credentials are saved and used as described above.

Domain

The domain name configured on the Microsoft Windows domain host. For example: example.com

Create computer account

If you choose to create a computer account, CloudLink creates the computer account and its principal in the domain's Active Directory (AD) and Key

Distribution Center (KDC). This option is required only for Integrated Windows Authentication (IWA).

If you chose not to create a computer account, no changes are made in AD. All domain user and domain group features (except IWA) work normally without creating a computer account.

Primary Host (optional)

The Microsoft Windows domain controller hostname, which is a Windows server where the Microsoft Windows domain is configured. For example: clc.example.com

Secondary Host (optional)

The Microsoft Windows domain hostname available for redundancy

User

A user in a Microsoft Windows domain who has permission to add a new server to that Microsoft Windows domain

Password

The password configured for the user

RSA Authentication Manager

For increased security, you may require a user to log in using RSA SecurID two-factor authentication, where the user provides a passcode, in addition to CloudLink Center credentials. For more information, see Two-factor authentication on page 31.

Before you can set up users for this type of two-factor authentication, you must configure RSA Authentication Manager.

Viewing RSA Authentication Manager

You can view whether RSA Authentication Manager is configured.

Task summary

Permissions	View System Configuration
Contents panel	**System** > **RSA Authentication Manager**
Commands	n/a

Uploading the RSA Authentication Manager configuration file

Before you can configure users for two-factor authentication using RSA SecurID, you must upload a configuration file to CloudLink Center.

You generate the configuration file (`REC`) using RSA Security Console, which puts the file in a compressed file (`ZIP`). You download the `ZIP` file and extract the `REC` file from it. For more information, see the RSA Security Console documentation.

You can replace the current configuration file with a new one. Ensure that you clear the shared node secret using RSA Security Console. For more information, see Clearing the shared node secret on page 129.

Prerequisites

The configuration file generated from RSA Security Console, available in a location where it is accessible for uploading to CloudLink Center.

Task summary

Permissions	Change System Configuration
Contents panel	**System** > **RSA Authentication Manager**
Commands	**Config**

Deleting the RSA Authentication Manager configuration

If you no longer require two-factor authentication using RSA SecurID, you can delete its configuration. If any users are set up to use RSA SecurID two-factor authentication, CloudLink Center displays a message and does not delete the configuration.

Ensure that you clear the shared node secret using RSA Security Console. For more information, see Clearing the shared node secret on page 129.

Task summary

Permissions	Change System Configuration
Contents panel	**System** > **RSA Authentication Manager**
Commands	**Delete**

Clearing the shared node secret

RSA Authentication Manager requires a unique node secret for each Authentication Agent. RSA Authentication Manager automatically creates the node secret it shares with CloudLink Center (an Authentication Agent) during its first successful authentication.

If you delete or replace the configuration files (`REC`), the secret is deleted in CloudLink Center. CloudLink Center cannot present this node secret when requesting authentication, and RSA Authentication Manager will not perform the authentication.

You must clear this shared node secret in RSA Security Console so that a new shared secret can be generated. For more information, see the RSA documentation.

Syslog

The actions, events, and security events visible in CloudLink Center can be automatically exported to a syslog server. Dell EMC recommends that you configure CloudLink to forward this information to a centralized log server or SIEM via syslog. All existing and new information is forwarded via syslog.

Viewing syslog configuration

You can view the Syslog status and configuration on the Syslog panel.

Task summary

Permissions	View Syslog Configuration

Contents panel	**Server** > **Syslog**
Commands	n/a

Syslog page information

The Syslog page includes the following information for each role:

Status

The service status is one of:

- Postponed—Logs are not sent out until the syslog status is explicitly set to Resume
- Active—Messages are sent to the configured syslog server until the Postpone command is selected.

Host

The host where system logs are sent

Facility

The facility on which the syslog messages are to be logged

Syslog details

None

Configuring a syslog logger

If your organization requires the long-term retention of system events, Dell EMC recommends that you configure CloudLink to forward its events to a centralized log server or SIEM via syslog. By default, CloudLink Center writes events to syslog using the common event format (CEF).

You can configure a syslog logger to direct all system log messages to the configured remote host. For information about network ports required, see the *CloudLink Deployment Guide* for your environment.

Task summary

Permissions	Change Syslog Configuration
Contents panel	**Server** > **Syslog**
Commands	**Change Configuration**

Syslog values

When configuring Syslog, provide the following values:

Host

Identifies the host where system logs are stored

Facility

Identifies the facility on which the syslog messages are to be logged

Changing the syslog message format

You can change the syslog message format to one of the following:

CEF (default)

The Common Event Format (CEF) uses the following message format:

CEF:0|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension

LEEF1

The Log Event Extended Format (LEEF) version 1.0 uses the following message format:

LEEF:1.0|Vendor|Product|Version|EventID|Extension

LEEF2

LEEF version 2.0 uses the following message format:

LEEF:2.0|Vendor|Product|Version|EventID|^|Extension

Custom

The custom format is defined by an input string and uses the following variables:

%d - vendor	%p - product	%v - version
%e - event ID	%n - name	%s - severity
%m - message	%a - action	%h - device hostname
%u - username	%t - clc target type	%g - clc target name
%i - clc target ID		

Task summary

Permissions	Change Syslog Configuration
Contents panel	**Server** > **Syslog**
Commands	**Change Syslog Format**

Network configuration

You can change the CloudLink Center hostname, and enable or disable SSH access to CloudLink Center.

If CloudLink Center is deployed on Microsoft Azure, Amazon Web Services, or Dimension Data, you cannot re-enable SSH access if you are blocked from the CloudLink Center console.

Viewing network configuration

You can view the CloudLink Center hostname and SSH access status on the Network Configuration panel.

Task summary

Permissions	View Server Specific Configuration
Contents panel	**Server** > **Network**

Commands	n/a

Network Configuration page information

The Network Configuration page includes the following information:

Hostname

The CloudLink Center hostname

SSH

Whether or not SSH access to CloudLink Center is enabled

Configuring hostname and SSH access

You can change the CloudLink Center server hostname and enable or disable SSH access to the CloudLink Center server.

Note

You are locked out of the CloudLink Center server if you disable SSH access and are blocked from the CloudLink Center server console.

Task summary

Permissions	Change Server Specific Configuration
Contents panel	**Server** > **Network**
Commands	**Change Hostname**

Task summary

Permissions	Change Server Specific Configuration
Contents panel	**Server** > **Network**
Commands	**Change SSH**

CloudLink Center login options

For security, CloudLink Center automatically:

- Ends a session that has been active for a specified period of time
- Logs users out after a specified period of inactivity
- Locks users out after a specified number of attempts to log in with an incorrect password

You configure these login options.

Viewing login options

You can view the current login options.

Task summary

Permissions	View System Configuration
Contents panel	**System** > **Login Options**

Commands	n/a

Changing the maximum session timeout

For security, CloudLink Center automatically ends a session that has been active for a specified period of time. You can set this maximum session timeout.

Task summary

Permissions	Change System Configuration
Contents panel	**System** > **Login Options**
Commands	**Change Max Session Timeout**

Changing the automatic logout interval

If no activity has occurred for a specified period of time, the web application automatically logs a user out. You can configure this timeout from 0 to 60 minutes, where 0 means that no automatic logout occurs.

Task summary

Permissions	Change System Configuration
Contents panel	**System** > **Login Options**
Commands	**Change UI Idle Timeout**

Changing the number of login attempts before lockout

You can specify the number of times that a user can provide an incorrect password before CloudLink Center locks the user out. For information unlocking users, see Unlocking accounts on page 35.

Task summary

Permissions	Change System Configuration
Contents panel	**System** > **Login Options**
Commands	**Change Login Attempts**

Domain Name System servers

You can configure CloudLink Center to resolve hostnames using a Domain Name System (DNS) server.

You must configure CloudLink with a DNS server if you want to use hostnames or domain names for other servers that CloudLink will interact with, such as:

- Resolving Network Time Protocol (NTP) server hostnames. For information, see Network Time Protocol servers on page 135.
- Creating a CloudLink Center cluster and use hostnames for servers in the cluster. For information, see Creating a CloudLink Center cluster on page 118.

Viewing DNS servers

You can view all configured domain name servers on the DNS Configuration panel.

Task summary

Permissions	Change Server Specific Configuration
Contents panel	**Server** > **DNS**
Commands	n/a

DNS Configuration table

The DNS Configuration table includes the following information:

IP Address

The IP address of the DNS

Type

The DNS type, which is either:

- Manual—IP addresses are static and assigned manually
- Auto—IP addresses are assigned automatically by DHCP

Setting the Primary DNS server

If more than one DNS server has been configured, one must be set as the primary DNS server.

When viewing domain name servers on the DNS Configuration panel, the DNS shown in the first row of the DNS Configuration table is the primary.

Task summary

Permissions	Change Server Specific Configuration
Contents panel	**Server** > **DNS**
Commands	**Set Primary**

Adding a DNS server

You can add a maximum of three DNS servers, if not using DHCP.

Task summary

Permissions	Change Server Specific Configuration
Contents panel	**Server** > **DNS**
Commands	**Add**

Domain Name Server values

When configuring Syslog, provide the following value:

IP Address

The IP address of the DNS server you are adding

Testing the network configuration

You can check whether CloudLink Center has network access to an external resource. You can test the network configuration from CloudLink Center. The ping option returns the same information as using the ping network utility from a command prompt.

Task summary

Permissions	Change Server Specific Configuration
Contents panel	**Server** > **DNS**
Commands	**Ping**

Deleting a DNS server

You can delete any DNS server you have previously added manually.

Task summary

Permissions	Change Server Specific Configuration
Contents panel	**Server** > **DNS**
Commands	**Delete**

Network Time Protocol servers

You can synchronize CloudLink Center with the date and time obtained from Network Time Protocol (NTP) servers. By default, CloudLink Center is configured with four global NTP servers.

Viewing NTP time

If you suspect that CloudLink Center's time is incorrect, view the NTP time value.

Task summary

Permissions	View Server Specific Configuration
Contents panel	**Server** > **Time**
Commands	n/a

Forcing NTP time synchronization

You can force synchronization with an NTP server if CloudLink Center's time is incorrect.

Task summary

Permissions	Change Server Specific Configuration

Contents panel	**Server** > **Time**
Commands	**Force Sync With NTP Server**

Adding NTP servers

When you add an NTP server, you provide its IP address or hostname. To use a hostname, ensure that you have configured at least one DNS server first. For information, see Domain Name System servers on page 133.

If DNS servers have not been configured, the NTP servers do not work.

Task summary

Permissions	Change Server Specific Configuration
Contents panel	**Server** > **Time**
Commands	**Add NTP Server**

Deleting NTP servers

You can delete any NTP server.

Task summary

Permissions	Change Server Specific Configuration
Contents panel	**Server** > **Time**
Commands	**Delete NTP Server**

Certificates

By default, the CloudLink Center uses a self-signed certificate. When connecting to CloudLink Center, the web browser may display several security warnings. These warnings are displayed because self-signed certificates do not have the same level of trust as certificates issued and signed by a trusted certification authority (CA).

To stop these warnings from being displayed, you can obtain and upload to CloudLink Center a certificate that has been signed for CloudLink by a trusted CA.

You can upload an externally generated certificate and private key, or generate a certificate signing request for a private key generated by CloudLink Center.

CloudLink supports two formats for externally generated keys and certificates:

Privacy-Enhanced Electronic Mail format

Certificates using this format are provided in files with the filename extension `.pem`. You must upload the private key file along with the certificate file.

PKCS #12 format

Certificates using this format are provided in files with the filename extension `.p12`. Along with the certificate file, the CA provides you with a password that is required to access the contents of the `.p12` file. The file contains both the certificate and the private key.

Viewing the certificate

You can view the current certificate.

Task summary

Permissions	Change Server Specific Configuration
Contents panel	**Server** > **SSL**
Commands	n/a

Uploading a new certificate

When you upload a new certificate and an optional private key, the web server restarts and the connection is terminated.

After uploading a certificate signed for CloudLink Center, verify the subject, fingerprint, and end date to ensure this is the certificate you want to use.

Task summary

Permissions	Change Server Specific Configuration
Contents panel	**Server** > **SSL**
Commands	**Upload**

Generating a certificate signing request

A certificate signing request (CSR) involves CloudLink Center generating a private key and signing the request. The request is then fulfilled by a certificate authority (CA) and the final certificate is uploaded to CloudLink Center.

Task summary

Permissions	Change Server Specific Configuration
Contents panel	**Server** > **SSL**
Commands	**Generate CSR**

Create a private key

Provide the following values when creating a private key:

Common Name

The hostname of the CloudLink Center server creating the certificate.

Organization

The organization name, such as the name of a business.

Organization Unit

The subsection of the organization creating the certificate, such as a business unit.

City/Locality

Organization address information

State/Province

Organization address information

Country

Organization address information

Simple Network Management Protocol

CloudLink Center can send Simple Network Management Protocol (SNMP) traps to a single target when CloudLink alarms are raised, updated, or lowered.

Each server in a CloudLink cluster must be configured separately, because cluster members do not synchronize SNMP configuration.

If a CloudLink alarm is set to **Ignored**, then SNMP traps are not sent for that alarm.

Configuring SNMP

You must add a target host in order to receive SNMP traps from CloudLink.

Task summary

Permissions	Change Server Specific Configuration
Contents panel	**Server** > **SNMP**
Commands	**Change Configuration**

SNMP values

When configuring SNMP, provide the following values:

Target Version

CloudLink supports SNMP version 2.

Host

The IP address or FQDN to where the SNMP traps are sent.

Port

The receiving host port number.

Community

The SNMP trap community.

Configuring an SNMP trap receiver

Download the MIB file and import or upload it to the trap receiver or network management system application. CloudLink alarms use the Object Identifier (OID) 1.3.6.1.4.1.1139 for traps.

Two traps are sent from CloudLink Center:

- alarmUpTrap when a new alarm is raised on the CloudLink Center server
- alarmDownTrap when the cause of the alarm is corrected or removed

The information about the CloudLink alarm is contained in the alarmUpTrap and the alarm identifier is contained in the alarmDownTrap.

You can use the clAlarmIdfor unique value for each alarm instance to track the raising and lowering of a specific alarm on the CloudLink Center server.

You can test your SNMP configuration to ensure the target receives SNMP traps from CloudLink.

Task summary

Permissions	Change Server Specific Configuration
Contents panel	**Server** > **SNMP**
Commands	**Download MIB** **Send Test Trap**

CHAPTER 11

Managing Licenses

This chapter presents the following topics:

CloudLink licenses

CloudLink license files determine the amount of machine instances, KMIP clients, CPU sockets, encrypted storage capacity, or physical machines with SEDs that your organization can manage using CloudLink Center. License files also define the CloudLink Center usage duration. For example, your license might allow you to run 25 machines in CloudLink Center for 365 days, or encrypt 5 TB of storage in CloudLink Center for perpetuity.

Licensing involves uploading a license file to make it available to CloudLink Center. For information, see Uploading license files on page 143.

You uploaded a license during initial server configuration. For more information, see the *CloudLink Deployment Guide* for your environment.

Viewing licenses

You can view the uploaded licenses.

Task summary

Permissions	View License
Contents panel	**System** > **License**
Commands	n/a

License table information

The License table includes the following information for each license:

Licensing

- Instance—Licensed machines for volume encryption
- Capacity—Encrypted capacity for VxFlex OS
- KMIP—Licensed KMIP clients
- SED—Number of physical machines with SEDs. A single SED license is used per physical machine regardless of the number of SEDs connected to that machine.
- Socket—Enables encryption licenses to be applied to all machines on a VMware ESXi host. For example, if an ESXi host has two sockets, adding that host to the Licensed Hosts allocates part of the socket license and allows an unlimited number of machines to be encrypted when they are deployed on that host.

Type

The license type. Either:

- Subscription—The license expires on a predefined date and time
- Perpetual—The license never expires

Limit

The maximum number of licensed machine instances, physical machines with SEDs, amount of encrypted capacity, or KMIP clients.

For Socket licenses, this is the maximum number of sockets across all VMware ESXi hosts that can be licensed.

Duration

The number of days that the license is valid

Start Date

The date that the license takes effect

End Date

The date that the license expires

License details

The following details are available, in addition to those also available in the License table.

Status

The status of the license. One of:

- Active—The license is uploaded
- Expired—The license expired

Platform

The platform to which the license is applied. All platforms are valid if the license is not specific to a machine's platform.

Uploading license files

Upload license files to make licenses available to CloudLink Center. License files must be uploaded before they can be used.

Task summary

Permissions	Upload License
Contents panel	**System** > **License**
Commands	**Upload License**

Deleting a license

You can delete a license and replace it with a new one.

Note

You can only delete CloudLink 6.5 or higher licenses.

Task summary

Permissions	Delete License
Contents panel	**System** > **License**
Commands	**Actions** > **Delete**

Licensed hosts

Using a socket-based license requires the following: a socket license, a cloud provider, and a VMware ESXi host.

Upload a socket license as described in Uploading license files on page 143. Uploading a socket license enables the Licensed Hosts panel, which is in the Location menu. You can skip this if you uploaded a socket license when you deployed CloudLink Center.

Add a cloud provider as described in Adding Cloud Providers for approved locations on page 70. It must be a VMware vCenter cloud provider.

Adding a licensed host

Add an ESXi host to use socket licenses. The number of sockets reported by the host are automatically subtracted from the total number of available licensed sockets.

Task summary

Permissions	Add Licensed Hosts
Contents panel	**Location** > **Licensed Hosts**
Commands	**Add**

Viewing a licensed host

You can view the licensed ESXi hosts you added.

Task summary

Permissions	View Licensed Hosts
Contents panel	**Location** > **Licensed Hosts**
Commands	n/a

Licensed Hosts table

The Licensed Hosts table includes the following information:

Provider

The name of the cloud provider

Host

The ESXi host added from the cloud provider

Number of Sockets

The number of licensed sockets on the ESXi host

Deleting a licensed host

You can delete a licensed host to free socket licenses.

Task summary

Permissions	Delete Licensed Hosts

Contents panel	**Location** > **Licensed Hosts**
Commands	**Actions** > **Delete**

CHAPTER 12

KMIP Servers

This chapter presents the following topics:

Managing KMIP servers

A KMIP server is used to store public and private keys for encrypted machines.

Note

The KMIP Server menu is only available in the CloudLink Center **Contents** panel after a KMIP license is uploaded.

CloudLink Center supports the Key Management Interop Protocol (KMIP) to allow applications supporting that protocol to securely store keys and certificates.

The applications, or KMIP clients, are given access to a single KMIP partition. A KMIP partition is a container for keys and certificates created by the client. Multiple clients can be assigned to the same partition. All objects within a partition are encrypted using a key saved to the partition's keystore and are stored in the CloudLink Center database.

Note

The adding KMIP clients and generating new certificates for KMIP clients functions are unavailable in Microsoft Edge and Internet Explorer. Use Mozilla Firefox or Google Chrome if you need to add or modify KMIP clients or generate a new certificate.

KMIP server information

The KMIP Server Information panel lists the details about the server certificate used to protect the KMIP protocol.

Change maximum lifetime

You can change the maximum lifetime for KMIP server certificates.

Task summary

Permissions	Change System Configuration
Contents panel	**KMIP Server** > **Information**
Commands	**Change Lifetime**

Change the server certificate

You can change the KMIP server certificate if required. This might be necessary if the hostnames in the certificate are no longer valid.

Task summary

Permissions	Change System Configuration
Contents panel	**KMIP Server** > **Information**
Commands	**Actions** > **Change Server Certificate**

Download the certificate

You can download the current KMIP server certificate.

Task summary

Permissions	Change System Configuration

Contents panel	**KMIP Server** > **Information**
Commands	**Actions** > **Download Server Certificate**

Generate a CSR

You can generate a certificate signing request (CSR), which involves CloudLink Center generating a private key and signing the request. The request is then fulfilled by a certificate authority (CA) and the final certificate is uploaded to CloudLink Center.

Task summary

Permissions	Change System Configuration
Contents panel	**KMIP Server** > **Information**
Commands	**Actions** > **Generate CA CSR**

Provide the following values when creating a private key:

Common Name

The hostname of the CloudLink Center server creating the certificate.

Organization

The organization name, such as the name of a business.

Organization Unit

The subsection of the organization creating the certificate, such as a business unit.

City/Locality

Organization address information

State/Province

Organization address information

Country

Organization address information

Upload a CA-signed certificate

When you upload a new certificate and an optional private key, the web server restarts and the connection is terminated. After uploading a certificate signed for CloudLink Center, verify the subject, end date, and fingerprint to ensure this is the certificate you want to use.

Task summary

Permissions	Change System Configuration
Contents panel	**KMIP Server** > **Information**
Commands	**Actions** > **Upload CA Signed PEM**

Server information table

The server information table includes the following information for each CloudLink Center server:

Certificate Lifetime

How long the certificate is valid.

Subject Name

Subject name values used to create the certificates.

Issuer Name

The authority that issued the certificate.

Fingerprint

Signature for the secure hash algorithm.

End Date

Expiration date for the certificates.

Subject Alternative Name

Additional host names used for the certificates.

Audit Level

Audit tracking of all key state changes, administrator access and policy changes.

Change the audit level

You can change the KMIP audit level to limit the number of KMIP logs that are generated.

Task summary

Permissions	Change System Configuration
Contents panel	**KMIP Server** > **Information**
Commands	**Actions** > **Change Audit Level**

Choose one of the following options:

All

CloudLink records all KMIP events.

Sensitive Data Access Only

CloudLink records only security-related data events. For example, KMIP client authentication events are not recorded.

Disabled

CloudLink does not record any KMIP events.

Viewing KMIP partitions

You can view the list of KMIP partitions in the KMIP Partitions panel.

Task summary

Permissions	View KMIP Partitions
Contents panel	**KMIP Server** > **Partitions**
Commands	n/a

KMIP partitions table information

The KMIP partitions table includes the following information for each partition:

Name

The unique name of the KMIP partition.

Description

A brief description of the KMIP partition.

Key ID

The encryption key ID.

Key Caching

Whether or not encryption key caching is enabled.

Managed By

The names of the roles that administer this KMIP partition.

Adding a KMIP partition

You can add a KMIP partition to store keys and certificates separately from other KMIP clients. Adding a KMIP partition involves defining its name, keystore, managing role, and providing an optional description. After adding a KMIP partition, you must add a KMIP client.

Task summary

Permissions	Add KMIP Partition
Contents panel	**KMIP Server** > **Partitions**
Commands	**Add**

KMIP partition values

Provide the following values when adding a KMIP partition:

Partition Name

A name for the KMIP partition.

Description (optional)

A brief description of the partition.

Keystore

The keystore used to store the encryption key that encrypts the KMIP objects.

Key Caching

You can choose to cache or not cache the KMIP partition protection key. Key caching stores the protection key locally in CloudLink Center.

Managed By

The names of the roles that administer this KMIP partition.

Modifying or shredding a KMIP partition

You can modify or shred a KMIP partition.

You can modify a KMIP partition to change its description, enable or disable key caching, and change the managing role.

You can shred a KMIP partition, as long as it is not assigned to a KMIP client.

Task summary

Permissions	Modify KMIP Partition

	Shred KMIP Partition
Contents panel	**KMIP Server** > **Partitions**
Commands	**Actions** > **Modify** **Actions** > **Shred**

Viewing KMIP partition objects

You can only view objects for a selected KMIP partition.

Task summary

Permissions	View KMIP Objects
Contents panel	**KMIP Server** > **Partitions**
Commands	**Actions** > **Show Objects**

Shredding KMIP partition objects

You can shred imported KMIP objects. Shredding removes the KMIP object and permanently removes the key.

Task summary

Permissions	View KMIP Objects
Contents panel	**KMIP Server** > **Partitions**
Commands	**Actions** > **Show Objects** **Shred**

Rotating encryption keys on a KMIP partition

You can rotate encryption keys to another keystore and stop key rotation if needed. Key rotation replaces all the encryption keys in a KMIP partition with new ones.

Task summary

Permissions	View KMIP Objects
Contents panel	**KMIP Server** > **Partitions**
Commands	**Actions** > **Rotate Key** **Actions** > **Stop Key Rotation**

Viewing the event history for a KMIP partition

You view only the events for a selected KMIP partition. For information about choosing the time frame in which events occurred and the information provided on the Events page, see Viewing events on page 95.

Task summary

Permissions	n/a
Contents panel	**KMIP Server** > **Partitions**
Commands	**Actions** > **Show Event History**

Adding a KMIP client

The KMIP client is used to connect to and authenticate the connection with the key management server. The adding a KMIP client function is unavailable in Microsoft Edge and Internet Explorer. Use Mozilla Firefox or Google Chrome if you need to add a KMIP client.

CloudLink supports two KMIP credential types, username and password and device credentials. Device credentials can be used to uniquely identify back-end devices.

Note

For device credentials, the combination of serial number, device ID, network ID, machine ID, and media ID must be unique.

Task summary

Permissions	Add KMIP Client
Contents panel	**KMIP Server** > **Clients**
Commands	**Add**

KMIP client values for username and password credentials

Provide the following values when adding a KMIP client that uses a username and password:

Username

Username for client authentication from the KMIP client.

Partition

The KMIP partition to which the client has access.

Credential Type

A username and password.

Password

Password for client authentication from the KMIP client.

Confirm Password

Password confirmation

KMIP client values for device credentials

Provide the following values when adding a KMIP client that uses device credentials:

Serial Number (mandatory)

A serial number, such as a device's hardware serial number.

Partition

The KMIP partition to which the client has access.

Credential Type

Device credentials

Password (optional)

An optional password or shared secret used to authenticate the device.

Confirm Password (optional)

Password confirmation

Device ID

A generic device identifier.

Network ID

A network identifier, such as a connected device's MAC address.

Machine ID

A machine identifier, such as a client aggregator identifier.

Media ID

A media identifier, such as a storage volume identifier.

Modifying or deleting a KMIP client

The KMIP client can be modified or deleted. You can change the password, create a new certificate, or remove the client. The generating a new certificate for KMIP clients function is unavailable in Microsoft Edge and Internet Explorer. Use Mozilla Firefox or Google Chrome if you need to modify KMIP clients or generate new certificates.

Task summary

Permissions	Modify KMIP Client
Contents panel	**KMIP Server** > **Clients**
Commands	**Change Password** **Generate New Certificate**

Task summary

Permissions	Delete KMIP Client
Contents panel	**KMIP Server** > **Clients**
Commands	**Delete**

Viewing the event history for a KMIP client

You view only the events for a selected KMIP client. For information about choosing the time frame in which events occurred and the information provided on the Events page, see Viewing events on page 95.

Task summary

Permissions	n/a
Contents panel	**KMIP Server** > **Clients**

Commands	**Actions** > **Show Event History**

APPENDIX A

Permissions and Roles

This appendix presents the following topic:

Permissions and roles

The following table lists the CloudLink permissions and the default roles to which they are assigned.

Table 2 Permissions and roles

Name	Role		
	SecAdmin	Admin	Observer
Users			
View Users	×	×	×
Add User	×	×	
Delete User	×	×	
Change User Roles	×	×	
Change User Password	×	×	
Change User Second Factor	×	×	
Unlock User	×	×	
Roles			
View Roles	×	×	×
Add Role	×		
Delete Role	×		
Modify Role	×		
Change Role Administration	×		
Backup and Restore			
View Backup Configuration	×	×	×
Generate Backup Key	×		
Generate Backup	×	×	
Download Backup	×	×	
Change Backup Configuration	×	×	
Restore Backup	×		
Keystores and Keys			
View Keystores	×		×
Add Keystore	×		
Delete Keystore	×		

Table 2 Permissions and roles (continued)

Modify Keystore	x		
Move Keys	x		
Machines			
View Machines	x		x
Remove Machine	x		
Control Machine Boot	x		
Change VM Encryption Policy	x		
Change Machine Encryption	x		
Change Machine Keys	x		
Shred Machine	x		
Move Machine	x		
View Approved Networks	x		x
Add Approved Network	x		
Modify Approved Network	x		
Delete Approved Network	x		
Machine Groups			
View Groups	x		x
Add Group	x		
Modify Group	x		
Delete Group	x		
View Machines Usage	x	x	x
Reset Machines Usage	x		
CloudLink Vault			
View Vault Mode	x	x	x
Change Vault Mode	x		
Set Vault Unlock Passcodes	x		
Unlock Vault	x	x	
Monitoring			
View Actions	x	x	x

Table 2 Permissions and roles (continued)

View Alarms	x	x	x
View Events	x	x	x
View Security Events	x	x	x
CloudLink Center Clusters			
View Cluster Members	x	x	x
Add Cluster Member	x		
Delete Cluster Member	x		
Join To Cluster	x		
Check cluster concurrent session	x		
CloudLink Licenses			
View Licenses	x	x	x
Upload License	x		
Assign License	x		
Delete License	x		
Configuration			
View Syslog Configuration	x	x	x
Change Syslog Configuration	x		
Update System	x		
View System Configuration	x	x	x
Change System Configuration	x	x	
View Server Specific Configuration	x	x	x
Change Server Specific Configuration	x	x	
View User Sessions	x	x	x
Terminate User Session	x	x	
View Server Logs	x		
View Server Performance	x		

Table 2 Permissions and roles (continued)

KMIP			
View KMIP Partitions	x		x
Add KMIP Partition	x		
Modify KMIP Partition	x		
Shred KMIP Partition	x		
View KMIP Objects	x		x
View KMIP Clients	x		x
Add KMIP Client	x		
Modify KMIP Client	x		
Delete KMIP Client	x		
Location			
View Providers	x		x
Add Provider	x		
Modify Provider	x		
Delete Provider	x		
View Approved Locations	x		x
Add Approved Location	x		
Modify Approved Location	x		
Delete Approved Location	x		
View Licensed Hosts	x		
Add Licensed Host	x		
Delete Licensed Host	x		
Kubernetes			
View Kubernetes Clusters	x		x
Add Kubernetes Cluster	x		x
Modify Kubernetes Cluster	x		x
Delete Kubernetes Cluster	x		x
View Kubernetes Nodes	x		x

Table 2 Permissions and roles (continued)

View Kubernetes Volumes	×		×
Control Kubernetes Volumes	×		×

APPENDIX B

Configuring Active Directory for Use as the Keystore

This appendix presents the following topics:

Configuring Active Directory for the CloudLink encryption keystore

You must deploy a Windows Server that is accessible by CloudLink Center to use Active Directory to store CloudLink encryption keys. This procedure shows you how to configure Active Directory for the CloudLink encryption keystore on a Windows Server that is configured as a domain controller.

You must provide the hostname of the Windows Server during configuration. You also must add your DNS server to CloudLink Center. For more information, see Domain Name System servers on page 133.

Procedure

1. Set up the Organization unit on Windows Server:

    a. On the Windows taskbar, click **Start** > **All Programs** > **Administrative Tools** and select **Active Directory Users and Computers**.

    b. Create an organization unit by expanding your domain name, and right-clicking **New** > **Organizational Unit**.

    c. Specify a **Name** (for example, CloudLink_OU).

    d. Right-click the **Organization Unit** (for example, CloudLink_OU), and select **New** > **Group**.

    e. Specify the **Group Name** (for example, CloudLink_Group).

    f. Select **Global and Security**.

2. Create a bind user:

    a. Right-click the **Organization Unit** (for example, CloudLink_OU), and select **New, User**.

    b. Specify the **First Name** (for example, Cloud), **Last Name** (for example, Link), and login name. Click **Next**.

    c. Specify the **Password** and click **Finish**.

    d. Right-click the **Organization Unit** (for example, CloudLink_OU) and select **Delegate Control**.

    e. Click **Next** to follow setup wizard.

    f. Click **Add** and specify the CloudLink group name (for example, CloudLink_Group). Click **OK** and then click **Next**.

    g. Select **Create a custom task** to delegate and click **Next**.

    h. Select the first bullet - **This folder, existing objects in this folder, and creation of new objects in this folder** - and select **Next**.

    i. Select **Full Control** and click **Next**.

    j. Select **Finish**.

3. Add the bind user to the security group:

    a. Double-click **Security Group**.

    b. Click the **Members** tab.

   c. Click **Add**.

   d. Type the bind user name.

   e. Click **OK**.

4. Record the DN of CloudLink:

   a. Click the **Start** button and select **Run**.

   b. Type `cmd` and select **OK**.

   c. Enter **dsquery OU** (Support tool is required) and record the DN (for example, OU=CloudLink_OU,DC=company,DC=com).

APPENDIX C

Commands for CloudLink Agent

This appendix presents the following topics:

Command actions for Linux

When performing many tasks related to CloudLink Agent on Linux machines, you use the `svm` command. This command has several subcommands used to perform actions including registering, encrypting, decrypting, reloading machines, and removing mount points.

The following table lists the actions for each `svm` subcommand and identifies the topic in the CloudLink documentation where it is referenced.

Table 3 Command actions

Action	Commands	Procedure
About CloudLink Agent	`svm about`	Displays general information about CloudLink Agent.

Decrypt boot volumes	Encrypted using CloudLink 5.5 to 6.8:
	`svm decrypt / [-v ]`
	Encrypted using CloudLink 5.0:
	`svm decrypt /target_disk [-v ]`
		See Decrypting a volume on page 84.

Decrypt mounted volumes	Encrypted using CloudLink 5.5 to 6.8:
	`svm decrypt` *`[mount_point]`*
	Encrypted using CloudLink 5.0:
	`svm decrypt` *`[mount_point] [additional_mp]`*
		See Decrypting a volume on page 84.

Encrypt	`svm encrypt` *`[mount_point]`*
	`svm encrypt` *`[device_name]`*
		Encrypt a mount point or block device. See Encrypting a volume on page 81.

Erase	`svm erase` *`[device_name]`*	Erases a device.
Generate	`svm gentechsupport` *`[script]`*	Creates a tech support file with an optional script file that runs more commands.
Manage	`svm manage` *`[device_name]`*	Take control of a self-encrypting drive.
Network status	`svm netstat`	Displays the network connection status.

Recover	`svm recover` *`[mount_point]`*
	`svm recover` *`[device_name]`*
		See Moving an encrypted disk to another machine on page 176.

Refresh	`svm refresh`	See *Refreshing the CloudLink Agent service on Linux machines* in *CloudLink Deployment Guide for Enterprise*.
Register	`svm [-v ] [-G` *`group_regcode`*`] -S` *`clc_address`*	See *Deploying CloudLink Agent: Custom installation for Linux machines* in *CloudLink Deployment Guide for Enterprise*.

Table 3 Command actions (continued)

Action	Commands	Procedure
	`svm [-v ] [-G group_regcode] -S clc_address -t`	Use the -t option to set Trusted Platform Module (TPM) mode on a physical machine that has a TPM version 2.0 chip installed. This option is only available during CloudLink Agent installation.
	`svm -S [clc_address] [-v ]`	See Changing the CloudLink Center IP address on page 90.
Release	`svm release [device_name]`	Release control of a self-encrypting drive.
Reload	`svm reload [-v ]`	Scan for new disks. See Refreshing a Linux machine's mounted devices on page 79.
Remove	`svm removemp [mount_point]`	Remove a mount point without saving any data.
Status	`svm status`	Shows the connection and mount point statuses. See *Verifying successful deployment* in *CloudLink Deployment Guide for Enterprise*.

	`svm status connection`
	or
	`svm status co`
		Shows the CloudLink cluster nodes statuses.

Uninstall	`svm uninstall`	See *Uninstalling CloudLink Agent* in *CloudLink Deployment Guide for Enterprise*.

The following table lists the options that can be used with some `svm` subcommands.

Table 4 Command options

Option	Description
-f	Force encryption or decryption. The machine will reboot when this option is used.
-h	Help with the command.
-S	Specify the server address (*clc_address*) for CloudLink Center.
-v	Use verbose mode.

Command actions for Windows PowerShell

When performing many tasks related to CloudLink Agent on Windows machines, you use the `svm` command. This command has several subcommands used to perform actions including encrypting, decrypting, setting dependencies, and showing status.

The following table lists the actions for each `svm` subcommand and identifies the topic in the CloudLink documentation where it is referenced.

Table 5 Command actions

Action	Commands	Procedure

Clear dependencies	`svm cleardeps` *`<Microsoft SQL Server service name>`*
	Example:
	`svm cleardeps MSSQLServer`
		See *CloudLink Agent for Microsoft SQL Server* in *CloudLink Deployment Guide for Enterprise*.

Decrypt	`svm decrypt` *`[disk_volume]`*	See Decrypting a volume on page 84.
Encrypt	`svm encrypt` *`[disk_volume]`*	Encrypt a mount point or block device. See Encrypting a volume on page 81.
Manage	`svm manage` *`[device_name]`*	Take control of a self-encrypting drive.
Register	`clagent.bat /S` *`[clc_address]`* `[/g` *`[group_regcode]`*`] [/t]`	Use the /t option to set Trusted Platform Module (TPM) mode on a physical machine that has a TPM version 2.0 chip installed. This option is only available during CloudLink Agent installation.
Release	`svm release` *`[device_name]`*	Release control of a self-encrypting drive.

Set dependencies	`svm setdeps` *`<Microsoft SQL Server service name>`*
	Example:
	`svm setdeps MSSQLServer`
		See *CloudLink Agent for Microsoft SQL Server* in *CloudLink Deployment Guide for Enterprise*.

Show dependencies	`svm showdeps`	See *CloudLink Agent for Microsoft SQL Server* in *CloudLink Deployment Guide for Enterprise*.
Status	`svm status`	See *Verifying successful deployment* in *CloudLink Deployment Guide for Enterprise*.

Command variables

The following table lists variables that are used with one or more `svm` subcommands.

Table 6 Command variables

Parameter	Description
additional_mp	The device used to temporarily store data during a decryption operation for a volume (Linux) encrypted using CloudLink 5.0 or earlier.
device_name	The device must be identified when it is not mounted and listed in `/etc/fstab`.
disk_volume	Drive C:, D:, and so on.
mount_point	The mount point to be encrypted.
SED	The self-encrypting drive you want to control with CloudLink Center.
target_disk	The device used to store data during a decryption operation for a boot volume (Linux) encrypted using CloudLink 5.0 or earlier.

APPENDIX D

Installing the Redirect Application

This appendix presents the following topic:

Installing the Redirect application

In some circumstances, a machine registered with CloudLink Center may not be able to start up because the machine is unable to connect to CloudLink Center. For example, this situation occurs if the IP address of CloudLink Center changes and DNS is not configured for CloudLink Center. The IP address for CloudLink Center may change if a CloudLink Center server was replaced. The IP address may also change if CloudLink Center has been deployed in a cloud environment. The public IP address of a machine may change when it is shut down and restarted. A new IP address is typically assigned from the same subnet as the previous address.

When a machine loses its connection to CloudLink Center, CloudLink Agent scans its subnet (/24 mask) to locate CloudLink Center by hostname on port 1194. If CloudLink Center is found, CloudLink Agent reconnects automatically and updates its configuration with the current connection information for CloudLink Center.

If CloudLink Agent cannot find CloudLink Center, it scans the same subnet for a Ubuntu server that is running CloudLink's Redirect application. When contacted by a CloudLink Agent, this application sends CloudLink Agent to the active CloudLink Center server. The machine's configuration is updated with the current connection information for this CloudLink Center.

Procedure

1. On the Ubuntu server, type the following:

   ```
   wget http://clc_address/cloudlink/securevm/agenttools
   ```

2. Type the following:

   ```
   chmod +x agenttools
   ```

3. Run the Redirect application by typing:

   ```
   ./agenttools
   ```

4. Type `1` to select **Recovery**.

   Type the IP address of the active CloudLink Center server.

Results

After installation, the Redirect application runs as a console application, displaying a message each time it redirects a machine.

Machines are redirected to the new CloudLink Center to restart. However, the machine is assigned the disconnected state in CloudLink Center. You must manually change the CloudLink Center server address on the machine. For information, see Changing the CloudLink Center IP address on page 90.

APPENDIX E

Moving an Encrypted Disk to Another Machine

This appendix presents the following topic:

Moving an encrypted disk to another machine

In some circumstances, you may need to move an encrypted disk from one machine registered with CloudLink Center to another registered machine. For example, if a machine cannot boot, you can move its encrypted disk to another machine.

After moving the disk, you must register the new machine with the same CloudLink Center instance as the original machine. On startup, CloudLink Center determines whether to release keys for the moved disk based on the **Moved Volume** key release policy. For information, see Changing key release policies for a machine group on page 64.

If CloudLink Center cannot release keys for the moved volume based on the current **Moved Volume** key release policy, it puts the machine in the pending state and locks the volume. You must manually accept the moved volume. After it is accepted, CloudLink Center allows the machine to start up and puts it in the connected state. CloudLink Center unlocks the volume and displays it as encrypted.

For the purposes of the following procedures, assume that VM-A is the machine with the encrypted disk (/data1/dir1) that you want to move to VM-B.

Steps for Windows

Procedure

1. Detach the disk from VM-A.
2. Attach the disk to VM-B.

   If the machine is put in the pending state because CloudLink Center cannot release keys for the moved volume, manually accept the moved volume, as follows:

   a. In CloudLink Center, select **Machines**.

   b. Select the machine with the moved volume.

   c. Select **Actions** > **Pending Volumes**.

   d. Select the moved volume and click **Accept**.

Steps for Linux

Procedure

1. Detach the disk from VM-A.
2. Attach the disk to VM-B.
3. Type the following command or reboot VM-B.

   ```
   svm reload
   ```

4. Create a mount point on VM-B for the disk from VM-A.

   Example:

   ```
   mkdir -p  /data1/dir
   ```

5. Type this command: `svm recover /mount_point /device`

   Example:

   ```
   svm recover /data1/dir /dev/sdb1
   ```

   For information about svm parameters, see Commands for CloudLink Agent on page 167

6. Restart the CloudLink Agent service. For more information, see Restarting the CloudLink Agent service on Linux machines on page 81.

7. If the machine is put in the pending state because CloudLink Center cannot release keys for the moved volume, you need to manually accept the moved volume, as follows:

   a. In CloudLink Center, go to **Machines**.

   b. Select the machine with the moved volume.

   c. Select **Actions** > **Pending Volumes**.

   d. Select the moved volume and click **Accept**.

8. Verify that the encrypted volume is accessible.

9. In CloudLink Center, verify that the mount points attached to VM-B are identified as encrypted.

APPENDIX F

Recovering an Encrypted Linux Boot Volume

This appendix presents the following topic:

Recovering an encrypted Linux boot volume

Use the following procedure to restore an encrypted Linux boot volume. This procedure can be used to restore Linux boot volumes encrypted with CloudLink version 5.5 or higher.

Procedure

1. Shut down the machine with the encrypted Linux boot volume (CloudLinkVM-1) that needs to be restored.
2. Deploy a Linux machine (CloudLinkVM-2) that uses the same distribution and release version.

   Note

   When you create CloudLinkVM-2, use a template different from the one used for CloudLinkVM-1.

3. Install CloudLink Agent on the new machine (CloudLinkVM-2).
4. Connect the new machine (CloudLinkVM-2) to the same CloudLink Center used by the old machine (CloudLinkVM-1).
5. Attach the encrypted boot volume from the old machine (CloudLinkVM-1) to the new machine (CloudLinkVM-2).
6. Use the new machine's Linux shell to find the added disk label. For example, the added disk is displayed as `/dev/sdb`.

   Use the following command to restart CloudLink Agent on CloudLinkVM-2 if the newly added disk is not seen on CloudLinkVM-2:

   ```
   svm reload
   ```

   Note

   DO NOT restart CloudLinkVM-2 because it can cause a Linux kernel panic.

7. Mount the new disk to a directory such as `/data1/diskb`.

   Note

   The attached disk is seen on the new machine (CloudLinkVM-2) as a new data volume in an encrypted state. If the attached disk does not appear on the new machine (CloudLinkVM-2), DO NOT restart the new machine (CloudLinkVM-2) because that can cause a Linux kernel panic. Instead, run this command:

   ```
   svm reload
   ```

8. When the attached disk is available on the new machine (CloudLinkVM-2), run the following command:

   ```
   svm recover /data1/diskb /dev/sdb
   ```

The data on the restored encrypted boot volume is now accessible.

9. After the data is restored, detach the restored boot disk from the new machine (CloudLinkVM-2).

   After the restored encrypted boot disk is removed from CloudLinkVM-2, you can restart the machine if necessary.