Contents

Chapter 1  Introduction ................................................................. 9
  About this document .................................................................... 10
  Related documents ..................................................................... 10
  Overview of CloudLink SecureVM .............................................. 10

Chapter 2  Deployment Considerations .......................................... 13
  CloudLink SecureVM components .............................................. 14
  Keystore options .................................................................... 14
  CloudLink Center server address ............................................. 14
  Virtual machine IP addresses .................................................. 14
  Volume encryption policies ....................................................... 15
    Volume encryption policies for Windows virtual machines ........ 15
    Volume encryption policies for Linux virtual machines .......... 16
  Pre-boot authorization ............................................................ 16
  CloudLink Center server clusters ............................................ 17
  Deployment scenario ............................................................... 17
  Deployment workflow ............................................................. 18
  System requirements .............................................................. 18
    CloudLink Center requirements .......................................... 19
    Virtual machine requirements ............................................ 19

Chapter 3  Deploying and Configuring CloudLink Center .................. 21
  Overview ................................................................................ 22
  Deploying and configuring CloudLink Center for VMware vSphere ... 22
    Deploying the CloudLink Center OVF template ................... 22
    Configuring CloudLink Center ............................................. 23
  Deploying and configuring CloudLink Center for Microsoft Hyper-V .. 25
    Deploying the CloudLink Center VHD template .................. 25
    Configuring CloudLink Center ............................................ 26
Chapter 4  Preparing to Deploy SecureVM Agent .................................. 31
Overview ........................................................................................................ 32
Accessing CloudLink Center ........................................................................ 32
Setting up SecureVM licenses ...................................................................... 33
  Uploading SecureVM licenses .................................................................. 33
  Assigning SecureVM licenses .................................................................. 34
Chapter 5  Deploying CloudLink SecureVM Agent to Virtual Machines ..... 37
Overview ........................................................................................................ 38
Deploying SecureVM Agent: Standard installation to Windows or Linux virtual
  machines .................................................................................................... 39
  Downloading the SecureVM Agent installer ............................................ 39
  Running the installer ................................................................................. 40
Deploying CloudLink SecureVM: Custom installation for Windows virtual
  machines .................................................................................................... 42
  Downloading the SecureVM Agent installer for Windows ...................... 42
  Adding SecureVM Agent configuration information to the Windows Registry .... 42
  Running the SecureVM Agent installer ..................................................... 43
Deploying SecureVM Agent: Custom installation for Linux virtual machines . 44
  Downloading the SecureVM Agent deployment package ....................... 44
  Installing the SecureVM Agent deployment package ................................ 45
  Configuring SecureVM Agent .................................................................. 45
Verifying successful deployment .................................................................. 46
  On Windows virtual machines .................................................................. 46
  On Linux virtual machines ...................................................................... 46
Restarting the SecureVM Agent service ..................................................... 46
Chapter 6  Using the CloudLink Center Update Menu ............................... 49
Overview ........................................................................................................ 50
Update Menu options ................................................................................... 50
Figures

Figure 1. CloudLink deployment scenario .......................................................... 18
Figure 2. CloudLink Center virtual machine in VMware vSphere virtual machine list .......................................................... 23
Figure 3. CloudLink Center console login .......................................................... 23
Figure 4. CloudLink Center configuration for vSphere ...................................... 23
Figure 5. CloudLink Center link network configuration .................................... 24
Figure 6. CloudLink Center Summary screen ................................................ 24
Figure 7. CloudLink Center Update Menu ........................................................ 25
Figure 8. New Virtual Machine Wizard ........................................................... 25
Figure 9. CloudLink Center console login for Microsoft Hyper-V .................... 26
Figure 10. CloudLink Center configuration information ................................. 27
Figure 11. CloudLink Center link network configuration ............................... 27
Figure 12. CloudLink Center Summary screen .............................................. 28
Figure 13. CloudLink Center Update Menu .................................................... 28
Figure 14. CloudLink Center home page ....................................................... 33
Figure 15. SecureVM License panel ............................................................... 34
Figure 16. License Usage panel ................................................................... 35
Figure 17. Setup panel ................................................................................. 40
Figure 18. ProfileId registry key and value ..................................................... 43
Figure 19. SecureVM Agent Shield icon ....................................................... 46
Tables

Table 1. CloudLink SecureVM network ports ................................................................. 19
Table 2. Deployment processes ................................................................................. 39
Chapter 1 Introduction

This chapter presents the following topics:

About this document ................................................................. 10
Related documents................................................................... 10
Overview of CloudLink SecureVM ........................................ 10
Introduction

About this document

This document describes how to deploy and configure CloudLink® SecureVM. It is intended for security officers and IT administrators.

Related documents

The following EMC publications provide additional information:

- CloudLink SecureVM Deployment Guide for Microsoft Azure
- CloudLink SecureVM Administration Guide
- CloudLink SecureVM Release Notes

Overview of CloudLink SecureVM

Cloud computing offers significant benefits for deployment flexibility, infrastructure scalability, and cost-effective use of IT resources. It makes sense to take advantage of these benefits and deploy 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 residing in the cloud to address privacy and regulatory compliance requirements, and requirements related to data that might remain in the cloud after it is no longer being used.

CloudLink SecureVM secures sensitive information within virtual machines across both public and private clouds. It provides encryption for the boot partition (sometimes referred to as the boot volume in Windows environments) and additional disk encryption with pre-startup authorization for virtual machines hosted in the cloud. It provides this encryption by using native operating system encryption features: Microsoft BitLocker for Windows and eCryptfs for Linux.

BitLocker and eCryptfs 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. In the cloud, you cannot use BitLocker or eCryptfs alone to encrypt the boot partition. SecureVM is designed to solve this problem.

SecureVM enables you to use BitLocker and eCryptfs to encrypt the virtual machine boot partition and additional disks in a multitenant cloud environment. This encryption protects the integrity of the virtual machine itself against unauthorized modifications. SecureVM encrypts the virtual machine boot partition and disks with unique keys that are under the control of the enterprise security administrator. Neither cloud administrators nor other tenants on the cloud have access to the keys. Securing the virtual machine lets you define the required security policy before anyone passes the pre-startup authentication process, including verifying the integrity of the virtual machine. This offers protection against malicious tampering.

SecureVM ensures that only trusted and verified virtual machines can run and access sensitive data stored in the cloud.
As part of the SecureVM solution, CloudLink Center defines the pre-startup authentication policy, performs pre-startup authentication, and monitors all SecureVM Agents, events, and logs.
Chapter 2  Deployment Considerations

This chapter presents the following topics:

- CloudLink SecureVM components .......................................................... 14
- CloudLink Center server address ............................................................. 14
- Virtual machine IP addresses ................................................................. 14
- Volume encryption policies ...................................................................... 15
- Pre-boot authorization ............................................................................. 16
- CloudLink Center server clusters ............................................................ 17
- Deployment scenario .................................................................................. 17
- Deployment workflow ............................................................................... 18
- System requirements ............................................................................... 18
CloudLink SecureVM consists of the following main components:

- **CloudLink Center**—The web-based management interface for SecureVM that is used to manage virtual machines that belong to the SecureVM environment (those virtual machines on which SecureVM Agent has been installed). CloudLink Center communicates with the virtual machines over SSL. It manages the encryption keys used to secure the boot partition and additional disks for the virtual machines, configures the security policies, and monitors the security and operation events and collects logs.

- **CloudLink SecureVM Agent**—The agent that runs on individual virtual machines. It communicates with CloudLink Center for pre-startup authentication and decryption of BitLocker or eCryptfs encryption keys.

CloudLink SecureVM is packaged as a virtual appliance that can be deployed in the enterprise on VMware ESX or Microsoft Hyper-V.

**Keystore options**

CloudLink Center supports the following keystore options:

- **Local**—This internal keystore option stores the key inside CloudLink Center. If you plan to use the local key store, ensure that CloudLink Center is deployed in a highly available configuration.

- **Microsoft Active Directory**—This is an external keystore. Ensure that the Active Directory server is properly backed up to ensure the safety of the key.

- **Amazon S3**—This is an external keystore. Ensure that you have an Amazon Web Services (AWS) account.

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 will not be able to access any data that was encrypted using those keys.

**CloudLink Center server address**

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

EMC recommends that you specify the CloudLink Center server address as a hostname (in FQDN format, such as `cloudlinkcenter1.acme.com`) if the DNS has an entry for CloudLink Center. For more information, see the *CloudLink SecureVM Administration Guide*. If you choose to use an IP address (such as `192.168.102.11`), use a static one.

**Virtual machine IP addresses**

In some circumstances, the IP address of a virtual machine under CloudLink Center management might change, such as when IP addresses are assigned by DHCP. When
a virtual machine starts up with a changed IP address, CloudLink Center might put the virtual machine in the pending state. Before startup can continue, you must manually accept the virtual machine.

To avoid having to manually accept virtual machines in the pending state because of changed IP addresses, you can either:

- Assign static IP addresses to virtual machines
- Change the CloudLink Center global policy so that virtual machines are allowed to start up with changed IP addresses

For information about the pending state and about manually accepting virtual machines with this status and changing the CloudLink Center global policy, see the *CloudLink SecureVM Administration Guide*.

**Volume encryption policies**

During SecureVM Agent deployment, you must choose a volume encryption policy. The volume encryption policy determines whether the boot partition (Windows and Linux virtual machines), data disks (Windows virtual machines), or both the boot partition and data disks (Windows virtual machines) are automatically encrypted during SecureVM Agent deployment to a virtual machine. For Windows virtual machines, the volume encryption policy also determines whether data disks added to the virtual machine after deployment are encrypted automatically.

For Windows virtual machines, you can change the volume encryption policy after deployment. For information, see the *CloudLink SecureVM Administration Guide*.

**Volume encryption policies for Windows virtual machines**

SecureVM provides the following volume encryption policies for Windows virtual machines:

- Boot and All Data—Encrypts the boot partition and all data disks during deployment. Data disks added after deployment are automatically encrypted. When specified in a command line, the keyword for this policy is *BootAllData*.
- Boot and Manual Data—Encrypts the boot partition during deployment. Data disks available at the time of deployment or added after deployment must be manually encrypted. When specified in a command line, the keyword for this policy is *BootManualData*.
- All Data—Encrypts all data disks during deployment. The boot partition is not encrypted. Data disks added after deployment are automatically encrypted. When specified in a command line, the keyword for this policy is *AllData*.
- Manual—Performs no boot partition or data disk encryption during deployment. The boot partition and existing data disks at the time of deployment and any data disks added after deployment must be manually encrypted. When specified in a command line, the keyword for this policy is *Manual*.

**Note:** Pre-boot authorization requires that the boot partition be encrypted. For information, see *Pre-boot authorization*. 
Deployment Considerations

For information about manually encrypting the boot partition or data disks after deployment, see the CloudLink SecureVM Administration Guide.

Automatic re-encryption of previously encrypted Windows disks
You can deploy SecureVM Agent to Windows virtual machines with disks already encrypted by BitLocker. During deployment, these disks are automatically decrypted and then re-encrypted to bring the disks under CloudLink Center management.

Volume encryption policies for Linux virtual machines
SecureVM provides two volume encryption policies for Linux virtual machines that determine whether the boot partition is encrypted during deployment:

- Boot and Manual Data—Encrypts the boot partition during deployment.
- Manual—Does not encrypt the boot partition during deployment. The boot partition can be manually encrypted after deployment.

For both volume encryption policies, mounted devices that exist at the time of deployment or any mounted devices that are added after deployment must be manually encrypted.

Note: Pre-boot authorization requires that the boot partition be encrypted. For information, see Pre-boot authorization.

For information about manually encrypting the boot partition or mounted devices after deployment, see the CloudLink SecureVM Administration Guide.

Pre-boot authorization

With virtual machine pre-boot authorization, as long as certain conditions are met, CloudLink Center automatically releases encryption keys to the virtual machine when requested during startup. These conditions must be met on virtual machine startup:

- The virtual machine boot partition must be encrypted. For information, see Volume encryption policies.
  
  Note: If a virtual machine’s boot partition is not encrypted, but one or more data volumes are encrypted, the virtual machine is allowed to start up. After the virtual machine starts up, CloudLink Center determines whether encryption keys for encrypted data volumes can be released automatically.

- The virtual machine’s IP address must be identified in the Allowed IPs list.
- The virtual machine’s IP address must be the same as it was at the previous startup, or the global policy must be configured to allow virtual machines to start up with different IP addresses.
- The virtual machine’s IP address must be unique. For example, another virtual machine cannot be online with a different serial number and the same IP address.
- For Windows virtual machines, the integrity value calculated for the virtual machine must be the same as it was at the previous startup.
- The virtual machine must not have been previously removed or blocked.
• The virtual machine must not be a clone of another virtual machine that is online with the same serial number.

If a virtual machine does not meet all these conditions, it is assigned the pending state.

For information about the Allowed IPs list, global policy, removing or blocking a virtual machine, cloned virtual machines, and the pending state, see the CloudLink SecureVM Administration Guide.

CloudLink Center server clusters

A CloudLink Center server cluster provides for high availability in the event that one CloudLink Center server in the cluster becomes unavailable, whether due to planned maintenance or an unexpected issue.

A CloudLink Center server cluster is comprised of two CloudLink Center servers, where one server (referred to as the slave) is joined to another server (referred to as the master).

For information about creating a CloudLink Center server cluster, see the CloudLink SecureVM Administration Guide.

Deployment scenario

This guide assumes that CloudLink Center and the encryption keystore are deployed in the private cloud, as shown in Figure 1. SecureVM Agent is deployed to individual virtual machines hosted in the private cloud or to virtual machine instances in a supported public or hybrid cloud environment.
Deployment Considerations

CloudLink SecureVM
Components

Figure 1. CloudLink deployment scenario

When deployed, SecureVM Agent replicates the virtual machine networking configuration, as needed, to ensure that it can communicate with CloudLink Center during the startup process. This replication includes the IP configuration for available network interfaces and any static routing information. If the networking configuration is changed after deployment, you must restart the SecureVM Agent service (see Restarting the SecureVM Agent service) to synchronize the configuration.

Deployment workflow

The CloudLink SecureVM workflow is as follows:

1. Deploy CloudLink Center, as described in Chapter 3: Deploying and Configuring CloudLink Center.
2. Prepare to deploy SecureVM Agent to virtual machines, as described in Chapter 4: Preparing to Deploy SecureVM Agent.
3. Deploy SecureVM Agent to virtual machines, as described in Chapter 5: Deploying CloudLink SecureVM Agent to Virtual Machines.

Encryption based on the selected volume encryption policy begins automatically after installation.

System requirements

This section describes the system requirements for CloudLink Center and for the virtual machines to which SecureVM Agent will be deployed. Meet these requirements before deployment.
CloudLink Center requirements

System requirements for CloudLink Center are as follows:

- For VMware deployments:
  - vSphere 5.1 or later
- For Microsoft deployments:
  - Hyper-V for Windows Server 2008 or Windows Server 2012
  - 2 GB (minimum) dynamic memory (if used)
- 2 vCPU
- 2 GB vRAM
- Web browser—Microsoft Internet Explorer 10 or higher, Google Chrome 25 or higher, or Mozilla Firefox 20 or higher
  
  TLSv1.2 must be enabled in your browser settings to connect to CloudLink Center. Some web browsers (such as Microsoft Internet Explorer 11 and higher, Google Chrome 30 and higher, and Mozilla Firefox 27) enable this option by default.

Table 1 lists the network ports used by SecureVM for various services.

Table 1. CloudLink SecureVM network ports

<table>
<thead>
<tr>
<th>Port</th>
<th>TCP</th>
<th>UDP</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>Yes</td>
<td></td>
<td>Secure Shell (SSH) protocol</td>
</tr>
<tr>
<td>161</td>
<td>Yes</td>
<td>Yes</td>
<td>Simple Network Management Protocol (SNMP)</td>
</tr>
<tr>
<td>443</td>
<td>Yes</td>
<td></td>
<td>CloudLink Center web access</td>
</tr>
<tr>
<td>8443</td>
<td>Yes</td>
<td></td>
<td>CloudLink Center web access</td>
</tr>
<tr>
<td>1194</td>
<td>Yes</td>
<td></td>
<td>SecureVM Agent communication</td>
</tr>
<tr>
<td>5432</td>
<td>Yes</td>
<td></td>
<td>Clustering</td>
</tr>
<tr>
<td>8080</td>
<td>Yes</td>
<td></td>
<td>SecureVM Agent download</td>
</tr>
<tr>
<td>7</td>
<td>Yes</td>
<td></td>
<td>Syslog</td>
</tr>
<tr>
<td>123</td>
<td></td>
<td>Yes</td>
<td>Network Time Protocol (NTP)</td>
</tr>
<tr>
<td>162</td>
<td>Yes</td>
<td>Yes</td>
<td>SNMP</td>
</tr>
<tr>
<td>389</td>
<td></td>
<td>Yes</td>
<td>Microsoft Active Directory integration</td>
</tr>
<tr>
<td>514</td>
<td></td>
<td>Yes</td>
<td>Syslog</td>
</tr>
</tbody>
</table>

Virtual machine requirements

For information about currently supported platforms, see the CloudLink SecureVM Release Notes.
Deployment Considerations

If you are deploying SecureVM into an existing Linux environment and you want to retrieve the SecureVM Agent installer by using `wget`, you must install `wget` if it is not provided by default with your distribution.

**Note:** You can also retrieve the SecureVM Agent installer directly from the CloudLink Center server.
Chapter 3  Deploying and Configuring CloudLink Center

This chapter presents the following topics:

Overview ................................................................. 22
Deploying and configuring CloudLink Center for
VMware vSphere ....................................................... 22
Deploying and configuring CloudLink Center for
Microsoft Hyper-V .................................................... 25
Deploying and Configuring CloudLink Center

Overview

This chapter provides instructions for deploying and configuring CloudLink Center on VMware vSphere and on Microsoft Hyper-V.

Before deploying CloudLink Center, ensure that you are familiar with the deployment considerations, including system requirements (see Chapter 2: Deployment Considerations).

Deploying and configuring CloudLink Center for VMware vSphere

CloudLink SecureVM uses one interface to enable CloudLink Center to communicate with the SecureVM Agent that is installed on individual virtual machines. This interface, referred to as the link interface, is supported through a virtual network interface that is included in the OVF template used to deploy CloudLink Center. The link interface is configured as part of the CloudLink Center configuration process. SecureVM Agent configures this CloudLink Center network interface server address for authentication purpose.

Deploying CloudLink Center involves deploying the OVF template and configuring CloudLink Center, as described in the following sections.

Deploying the CloudLink Center OVF template

This procedure assumes that you have obtained the CloudLink Center OVF template used for deployment.

Deploy the OVF template as follows:

1. From vSphere Client, select File > Deploy OVF Template.
2. From the Deploy OVF Template window, go to the template folder, select the CloudLink Center template, and click Next.
3. Verify that the OVF template details are correct and click Next.
4. Type a name, select an inventory location for the deployed template, and click Next.
5. Select a host or cluster to run the deployed template and click Next.
6. If a series of warnings is displayed, click Yes to continue with the deployment.
7. Select a resource pool and click Next.
8. Select a location for the virtual machine files and click Next.
9. Select the disk format for the virtual disk and click Next.
10. Select a network and click Next.
11. In the Deployment Settings panel, review the selected options and click Finish.
12. When you see the Deployment Completed Successfully dialog box, click Close.

Figure 2 shows the CloudLink Center virtual machine displayed in the VMware vSphere virtual machine list.
Configuring CloudLink Center

Configure CloudLink Center as follows:

1. From vSphere Client, right-click CloudLink Center and select Power on.
2. Right-click CloudLink Center and select Open Console.
3. Log in to the CloudLink Center console with the login name gateway, as shown in Figure 3, and the default password gateway.

You can navigate the interface by using the keyboard arrow keys, the Tab key, and the Enter key.

4. Read the End User License Agreement and, if you agree to its terms, select Accept.

Use the Page Up and Page Down keys to scroll through the license agreement.

5. When prompted, type a new password for the CloudLink Center console.

You are required to change the default password. Subsequent logins to the console prompt for the new password, which you can change at any time from the Update Menu in the CloudLink Center console (see Chapter 6: Using the CloudLink Center Update Menu).

6. Review the configuration information, as shown in Figure 4, and select Confirm.
7. Type the hostname for CloudLink Center and click OK.

A valid hostname is a letter followed by letters, numbers, dashes (–), or dots (.). Letters can be lowercase or uppercase. Underscores (_) are not supported.

**Note:** If you join CloudLink Center to an Active Directory domain after deployment, as part of the configuration process, the domain name portion of the hostname might change.

8. Specify whether the CloudLink Center link network uses Dynamic Host Configuration Protocol (DHCP) or a static IP address.

**Note:** You can change the link network parameters later if necessary.

- To use DHCP, first make sure that a DHCP server is available on the CloudLink Center link network. Select DHCP, click OK, and go to step 10.
- If a DHCP server is not available, select Static, click OK, and go to step 9.

9. If you selected Static, type the IP address, network mask, and gateway address for the CloudLink Center link network interface, as shown in Figure 5, and click OK.

![Figure 5. CloudLink Center link network configuration](image)

10. Wait for the configuration to complete.

This process might take some time.

When the CloudLink Center configuration process is complete, a summary of its settings is displayed, as shown in Figure 6. These settings include the coordinates to access CloudLink Center from a web browser and the default secadmin password for logging in to CloudLink Center for the first time.

![Figure 6. CloudLink Center Summary screen](image)
After you have configured CloudLink Center, every time you log in from the CloudLink Center console, the Update Menu shown in Figure 7 is displayed. For information about the Update Menu, see Chapter 6: Using the CloudLink Center Update Menu.

![CloudLink Center Update Menu](image)

**Figure 7.  CloudLink Center Update Menu**

**Deploying and configuring CloudLink Center for Microsoft Hyper-V**

CloudLink SecureVM uses one network interface to allow CloudLink Center to communicate with the SecureVM Agent that is installed on a virtual machine. This interface, referred to as the link interface, is supported through a virtual network interface that is included in the VHD template used to deploy CloudLink Center for Microsoft Hyper-V. The link interface is configured as part of the CloudLink Center configuration process. SecureVM Agent configures this CloudLink Center network interface server address for authentication purpose.

Deploying CloudLink Center for Microsoft Hyper-V involves deploying the VHD template and configuring CloudLink Center, as described in the following sections.

**Deploying the CloudLink Center VHD template**

This procedure assumes that you have obtained the CloudLink Center VHD template used for deployment.

Deploy the CloudLink Center VHD template as follows:

1. From the Hyper-V Manager, create a CloudLink Center virtual machine by selecting **Actions > New > Virtual Machine**.
2. Type a name for the virtual machine, as shown in Figure 8.

![New Virtual Machine Wizard](image)

**Figure 8.  New Virtual Machine Wizard**
Deploying and Configuring CloudLink Center

3. Adjust the assigned memory if necessary.

4. Select the **Generation 1** option if it is available.
   This option specifies the generation of virtual machine used and depends on the version of Windows Server that you are using.

5. Select a network to connect to CloudLink Center or leave the **Not Connected** option selected.
   You can connect to the network later.

6. Connect a virtual hard disk by selecting **Use an existing virtual hard disk**, browsing to the copy of the CloudLink Center .vhd file, and then clicking **Open**.
   Do not open the master .vhd file.

7. Review the configuration and click **Finish**.

8. In the Hyper-V Manager, choose **Settings** and define the network.

9. In the Hyper-V Manager, review your **Hardware** settings for CloudLink Center.

10. Start CloudLink Center.

**Configuring CloudLink Center**

Configure CloudLink Center as follows:

1. From Hyper-V Manager, right-click CloudLink Center and select **Start**.

2. Click **Connect**.

3. Log in to the CloudLink Center console with the login name **gateway**, as shown in **Figure 9**, and the default password **gateway**.

   ![CloudLink Center console login for Microsoft Hyper-V](image)

   **Figure 9.** CloudLink Center console login for Microsoft Hyper-V

   You can navigate the interface by using the keyboard arrow keys, the Tab key, and the Enter key.

4. Read the End User License Agreement and, if you agree to its terms, select **Accept**.
   Use the Page Up and Page Down keys to scroll through the license agreement.

5. When prompted, type a new password for the CloudLink Center console.
   You are required to change the default password. Subsequent logins to the console prompt for the new password, which you can change at any time from the Update Menu in the CloudLink Center console. For information
about the Update Menu, see Chapter 6: Using the CloudLink Center Update Menu.

6. Review the configuration information (Figure 10) and select Confirm.

![Figure 10. CloudLink Center configuration information](image)

7. Enter the host FQDN for CloudLink Center and click OK.

A valid hostname is a letter followed by letters, numbers, dashes (-), or dots (.). Letters can be lowercase or uppercase. Underscores (_) are not supported.

**Note:** If you join CloudLink Center to an Active Directory domain after deployment, as part of the configuration process, the domain name portion of the hostname might change.

8. Specify whether the CloudLink Center link network uses DHCP or a static IP address.

**Note:** You can change the link network parameters later if necessary.

- To use DHCP, make sure that a DHCP server is available on the CloudLink Center link network. Select **DHCP**, click **OK**, and go to step 10.
- If a DHCP server is not available, select **Static**, click **OK**, and go to step 9.

9. If you selected **Static**, type the IP address, network mask, and gateway address for the CloudLink Center link network interface, as shown in Figure 11, and click **OK**.

![Figure 11. CloudLink Center link network configuration](image)

10. Wait for the configuration to complete.

This process might take some time.

When the CloudLink Center configuration process is complete, a summary of the settings is displayed, as shown in Figure 12. These settings include the coordinates to access CloudLink Center from a web browser and the default secadmin password for logging in to CloudLink Center for the first time.
After you have configured CloudLink Center, every time you log in by using the CloudLink Center console, the Update Menu is displayed, as shown in Figure 13. For information about the Update Menu, see Chapter 6: Using the CloudLink Center Update Menu.
Chapter 4  Preparing to Deploy SecureVM Agent

This chapter presents the following topics:

Overview ........................................................................................................................................... 32  
Accessing CloudLink Center ................................... 32  
Setting up SecureVM licenses ......................................................... 33
Preparing to Deploy SecureVM Agent

Overview

After deploying and configuring CloudLink Center, you prepare to deploy SecureVM Agent to virtual machines by accessing CloudLink Center and setting up SecureVM licenses.

Accessing CloudLink Center

With CloudLink Center deployed, use a web browser to connect to it from the virtual machine on which you plan to install SecureVM Agent, and log in.

To log in, you need the following:

- URL for CloudLink Center—The URL is available from the Summary in the Update Menu (see Chapter 6: Using the CloudLink Center Update Menu).
- Password for the secadmin user account—The first time that you log in to CloudLink Center, you are prompted for the default password and then prompted to change it. The default password is available from the Summary in the Update Menu (see Chapter 6: Using the CloudLink Center Update Menu).

You can change the password for the secadmin user account at any time following the first-time login.

EMC recommends that you configure Active Directory integration so that you can access CloudLink Center with Windows domain credentials.

For information about changing the secadmin password after the first-time login or configuring Active Directory integration, see the CloudLink SecureVM Administration Guide.

To access CloudLink Center:

1. In the address bar of a web browser, type the URL for CloudLink Center. The format is:
   
   https://clc_address:8443

   where \texttt{clc_address} represents the CloudLink Center server address (see CloudLink Center server address).

2. From the CloudLink Center home page (shown in Figure 14), type the user name (secadmin) and password (or default password for first-time login) to access CloudLink Center, and click Login.
The password must include at least 10 characters.

![CloudLink Center home page](image)

**Figure 14. CloudLink Center home page**

3. If this is the first time you have logged in, type a new password and then retype it to confirm, and click **Change Password**.

### Setting up SecureVM licenses

SecureVM license files determine the number of virtual machines that your organization can manage with CloudLink Center and the duration of the license. Before you can view and manage virtual machines in CloudLink Center, you must upload and assign one or more SecureVM license files. The number and type of license files you need depends on your SecureVM requirements.

For deployment purposes, this topic describes the basic steps for uploading and assigning a license file. For more information about SecureVM licenses, see the *CloudLink SecureVM Administration Guide*.

### Uploading SecureVM licenses

You upload licenses to make them available to CloudLink Center as follows:

1. Log in as a secadmin user.
2. In the **Topology Tree**, select **CloudLink Center**.
3. On the **System** tab, in the **Options** panel, select **SecureVM License**.
4. In the **License Registration** panel, click the **Browse** button.
5. In the **File Upload** dialog box, locate and select a license file, and click **OK**.
6. Click **Upload** to upload and display the license file in the **License Pool** panel.
Preparing to Deploy SecureVM Agent

The license appears under the “Unassigned” heading. As shown in Figure 15, the license information for new licenses includes the Type, Platform, Limit (maximum number of virtual machines), and Duration in days. The Start Date and End Date are not displayed because the license has not been assigned.

![SecureVM License Panel](image)

**Figure 15. SecureVM License panel**

**Assigning SecureVM licenses**

You can assign a license that has been uploaded to CloudLink Center (see Uploading SecureVM licenses) as follows:

1. Log in to CloudLink Center as a secadmin or admin user.
2. In the Topology Tree, select CloudLink Center.
3. On the SecureVM tab, in the Options panel, select License.
4. In the License Assignment panel, select a license from the Available Licenses list.
   
   Only valid licenses are displayed in the list.
5. Click the calendar icon, and select a start date for the storage license (present or future).
   
   The selected date is reflected in the Start Date field as YYYY-MM-DD.
6. Click Assign.
As shown in Figure 16, for each assigned license, the “License Usage” panel includes a graph heading that shows the number of virtual machines and the license expiry date. The graph shows the number of virtual machines and the valid dates for the license. Move the mouse over the starting point of a graph line to see the start date or over the end point to see the end date.

Figure 16. License Usage panel

The number of virtual machines that can be registered with CloudLink Center equals the sum of the virtual machines for all licenses valid on any given date.
This chapter presents the following topics:

Overview.................................................................................................................. 38
Deploying SecureVM Agent: Standard installation to Windows or Linux virtual machines ........................................................................................................................................................................................................................................................................................................................................................................ 39
Deploying CloudLink SecureVM: Custom installation for Windows virtual machines ........................................................................................................................................................................................................................................................................................................................................................................ 42
Deploying SecureVM Agent: Custom installation for Linux virtual machines .................................................................................................................................................................................................................................................................................................................................................. 44
Verifying successful deployment .............................................................................. 46
Restarting the SecureVM Agent service ................................................................. 46
Overview

For virtual machine pre-startup authentication and decryption of BitLocker (Windows) or eCryptfs (Linux) encryption keys, SecureVM Agent must be deployed and running on the virtual machine and connected to CloudLink Center.

You deploy CloudLink SecureVM Agent by using a standard or custom installation.

- The standard installation is an automated method that requires minimal intervention from you.
  
  The standard installation is useful for deploying SecureVM Agent to virtual machines on an individual basis. Typically, you use this method when you want encryption, based on a specified encryption policy, to begin automatically once deployment is complete.

- The custom installation requires more intervention from you, but it provides more flexibility for deployment. Unlike the standard installation, the custom installation does not automatically register the virtual machine with CloudLink Center or start the encryption process.

A custom installation is useful for the following purposes:

- Preparing a virtual machine image for encryption without starting the encryption process, allowing virtual machine clones to be deployed with a single restart
- Deploying SecureVM Agent to virtual machines before deploying CloudLink Center
- Deploying SecureVM Agent with configuration management tools

Choose either the standard or custom installation based on the level of automation or points of manual intervention you require. At a high level, deployment includes the following processes:

1. The virtual machine might automatically restart several times to install and configure BitLocker or eCryptfs, and to create a reserved partition for secure storage of volume encryption keys.

2. The virtual machine is registered with CloudLink Center.

3. Encryption, based on the specified encryption policy (see Volume encryption policies), begins.
Table 2 describes the deployment processes for each type of installation and for each operating system. This table is intended to help you determine the appropriate installation based on your deployment requirements.

Table 2. Deployment processes

<table>
<thead>
<tr>
<th>Installation type</th>
<th>SecureVM Agent for Windows</th>
<th>SecureVM Agent for Linux</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard installation</td>
<td>Download the installer. Run the installer to complete installation and configuration.</td>
<td>Download the installer. Run the installer to complete installation and configuration.</td>
</tr>
<tr>
<td>Custom installation</td>
<td>Download the installer. (Optional) Configure the volume encryption policy and CloudLink Center server address. Run the installer to complete installation. If you did not provide configuration information in step 2, you provide it when running the installer.</td>
<td>Download the operating-system-specific deployment package. Install the package. Configure the volume encryption policy and CloudLink Center server address.</td>
</tr>
</tbody>
</table>

You can view registered virtual machines in CloudLink Center and perform management operations such as changing their volume encryption policies. For information, see the *CloudLink SecureVM Administration Guide*.

**Deploying SecureVM Agent: Standard installation to Windows or Linux virtual machines**

Deploying CloudLink SecureVM Agent to Windows or Linux virtual machines using the standard installation involves the following tasks:

1. Downloading the installer using the CloudLink Center interface or directly from the server
2. Running the installer from the command line to complete installation and configuration

**Downloading the SecureVM Agent installer**

The SecureVM Agent installer is available from CloudLink Center. For Windows, the installer is provided in the securevm.bat file. For Linux, the installer is provided in the securevm.sh script.

You can download the installer in one of the following ways:

- Log in to CloudLink Center and download the installer using the CloudLink Center user interface.
- Download the installer from the CloudLink Center server without logging in.

If you are not responsible for completing the installation, provide the downloaded software to the appropriate person.
Deploying CloudLink SecureVM Agent to Virtual Machines

To download the installer using the CloudLink Center user interface:

1. Log in to CloudLink Center (see Accessing CloudLink Center).
2. On the SecureVM tab, in the Options panel, select Setup.
3. In the Setup panel, right-click the installer (securevm.bat or securevm.sh) and click Download.

Figure 17 shows the Windows installer selected for downloading.

![Setup panel](Figure 17)

4. Select Save File.
   
   For Windows, the installer is downloaded to the Downloads folder.
   
   For Linux, the installer is downloaded to the current folder.

To download the installer directly from the CloudLink Center server:

1. In a web browser, type the following:
   
   - For Windows:
     
     http://clc_address:8080/cloudlink/securevm
   
   - For Linux:
     
     http://clc_address:8080/cloudlink/securevm

   where `clc_address` is the CloudLink Center server address (see CloudLink Center server address).

2. Select Save File.
   
   For Linux, use the file name `securevm`. The installer is downloaded to the current folder.
   
   For Windows, the installer is downloaded to your Downloads folder.

   **Note:** For Linux, you can use `wget` (if installed) to download the installer directly from the CloudLink Center server. When specifying the installer location, type the following: `http://clc_address:8080/cloudlink/securevm`

**Running the installer**

After downloading the SecureVM Agent installer from CloudLink Center, you run it from the command line, providing the CloudLink Center server address and the volume encryption policy you want applied. For Linux, you can optionally specify whether you want to force the virtual machine to restart when installation is...
Deploying CloudLink SecureVM Agent to Virtual Machines

complete. A restart that is required before encryption, based on the applied volume encryption policy, begins automatically.

For Windows
To run the installer for a Windows virtual machine:

1. In a command window, go to the folder where you downloaded the SecureVM Agent installer.
   
   By default, the installer is downloaded to the Downloads folder.
2. From the command line, type the following:
   
   securevm.bat /S clc_address /p volume_encryption_policy

   where

   /S clc_address specifies the CloudLink Center server address (see CloudLink Center server address).

   /p volume_encryption_policy identifies the volume encryption policy (see Volume encryption policies) to be applied during deployment. The value is one of the following:

   - BootAllData
   - BootManualData
   - AllData
   - Manual

3. Wait for the installation to complete.

For Linux
To run the installer for a Linux virtual machine, from the command line on the virtual machine, in the location where the installer was downloaded (by default, to the current folder), type the following:

   sudo sh securevm -S clc_address [-B] [-r]

   where

   -S clc_address specifies the CloudLink Center server address (see CloudLink Center server address).

   -B specifies that the Boot with Manual Data volume encryption policy (see Volume encryption policies) is to be applied during deployment.

   -r forces the virtual machine to restart after registration with CloudLink Center. If you do not specify this option, encryption does not begin until the next time that the virtual machine is restarted. You cannot access the virtual machine until encryption is complete.
Deploying CloudLink SecureVM Agent to Virtual Machines

Deploying CloudLink SecureVM: Custom installation for Windows virtual machines

Deploying CloudLink SecureVM Agent to Windows virtual machines using the custom installation involves the following tasks:

1. Downloading the SecureVM Agent installer
2. (Optional) Adding the SecureVM Agent configuration information to the Windows Registry Editor
3. Running the SecureVM Agent installer

Downloading the SecureVM Agent installer for Windows

To download the SecureVM Agent Installer for Windows:

1. Log in to CloudLink Center.
2. On the SecureVM tab, in the Options panel, select Setup.
3. In the Setup panel, right-click securevm-windows-x64.msi and click Download.
4. Select Save File.

The installer is downloaded to your Downloads folder.

Adding SecureVM Agent configuration information to the Windows Registry

As a deployment option, you might want to specify the information necessary to configure SecureVM Agent before running the .msi file. If you do not specify this configuration information prior to running the .msi file, you define it when running the .msi file from the command line (see Running the SecureVM Agent installer).

In the Windows Registry, you define the following:

- CloudLink Center server address (see CloudLink Center server address)
- SecureVM volume encryption policy

If the SecureVM volume encryption policy is not set using the Windows Registry, the Manual policy is applied to virtual machines.

To add SecureVM Agent configuration information to the Windows Registry:

1. On the virtual machine, from a command prompt window, type regedit.
2. Go to:

   HKEY_LOCAL_MACHINE\SOFTWARE\CloudLink Technologies Inc\SecureVM

3. To configure the SecureVM volume encryption policy, do the following:
   a. Add a registry key named ProfileId with the type DWORD.
   b. Set the value of the ProfileId registry key as follows:
      - For Boot and Manual Data, set the value to 101.
Deploying CloudLink SecureVM Agent to Virtual Machines

- For All Data, set the value to 102.
- For Boot and All Data, set the value to 103.
- For Manual, set the value to 104.

4. To configure the CloudLink Center address:
   a. Add a registry key named `Server` with the type `REG_SZ`.
   b. Set the value of the `Server` registry key the CloudLink Center server address (for example, 209.87.232.41 or cloudlinkcenter.mycompany.com).

5. Save and close the registry.

Figure 18 shows an example of the `ProfileId` registry key and value:

![Figure 18. ProfileId registry key and value](image)

Running the SecureVM Agent installer

After downloading the SecureVM Agent installer (the securevm-windows-x64.msi file) from CloudLink Center, you can run it from the command line or by using Windows Installer tools.

To run the SecureVM Agent installer:

1. Go to the folder where the SecureVM Agent installer is located.
2. From the command line, type one of the following, depending on whether you have already configured SecureVM Agent (see Adding SecureVM Agent configuration information to the Windows Registry):
   - If you have not configured SecureVM Agent:
Deploying CloudLink SecureVM Agent to Virtual Machines

```shell
msiexec /i securevm-windows-x64.msi
[CLOUDLINKCENTER=clc_address]
[VOLUMEENCRYPTIONPOLICY=volume_encryption_policy]
```

- If you have configured SecureVM Agent:
  ```shell
  msiexec /i securevm-windows-x64.msi
  [CLOUDLINKCENTER=clc_address]
  ```

where
- `CLOUDLINKCENTER=clc_address` specifies the CloudLink Center server address (see CloudLink Center server address).
  
  If you do not specify the CloudLink Center server address, the virtual machine is not registered with CloudLink Center.
- `VOLUMEENCRYPTIONPOLICY=volume_encryption_policy` identifies the volume encryption policy (see Volume encryption policies) to be applied during deployment. The value is one of:
  - BootAllData
  - BootManualData
  - AllData
  - Manual

If you do not specify the CloudLink Center server address and have not already configured SecureVM Agent (see Adding SecureVM Agent configuration information to the Windows Registry), no encryption is initiated as part of the deployment process.

3. When the SecureVM Setup wizard is displayed, click Install.
4. When the wizard completes, click Finish.
5. Wait for the installation to complete.
   
   The virtual machine automatically restarts one or more times.
6. Restart the CloudLink SecureVM service (see Restarting the SecureVM Agent service).

Deploying SecureVM Agent: Custom installation for Linux virtual machines

Deploying SecureVM Agent using the custom installation involves the following tasks:

1. Downloading the SecureVM Agent deployment package
2. Installing the SecureVM Agent deployment package
3. Configuring SecureVM Agent

Download the SecureVM Agent deployment package

SecureVM Agent deployment packages are available as deb or rpm files that you download from CloudLink Center to the current folder.
To download the SecureVM Agent deployment package:

1. Log in to CloudLink Center.
2. On the SecureVM tab, in the Options panel, select Setup.
3. In the Setup panel, right-click the deployment package you want to use and click Download.
4. Select Save File.

The deployment package is downloaded to the current folder.

Installing the SecureVM Agent deployment package

After downloading the deployment package for your operating system from CloudLink Center, install the package using the package manager for your platform.

Configuring SecureVM Agent

Installation of the deployment package installs the svm installer, which provides two svm subcommands for configuring SecureVM Agent. Both commands register the virtual machine with CloudLink Center during configuration. Only one command applies the Boot with Manual Data volume encryption policy (see Volume encryption policies) during deployment.

For information about manually encrypting the boot partition (if the Boot with Manual Data volume encryption policy is not used), manually encrypting mounted devices (which neither command encrypts), or svm subcommand options and variables, see the CloudLink SecureVM Administration Guide.

- To install SecureVM Agent and encrypt the boot partition:
  1. Type the following command:
     \[ svm \[-v \] \[-s \] \[-B \] \[-S \] clc_address \]
  2. Restart the virtual machine.
     You cannot access the VM until encryption is complete.

- To install SecureVM Agent without encrypting the boot partition, type the following:
  \[ svm \[-v \] \[-s \] \[-R \] \[-S \] clc_address \]

for these commands:

\[ -v \] uses verbose mode.

\[ -s \] uses script mode to disable any interactive prompts.

\[ -B \] encrypts the boot partition.

\[ -R \] registers the VM with CloudLink Center.

\[ -S \] clc_address represents the CloudLink Center server address (see CloudLink Center server address).
Deploying CloudLink SecureVM Agent to Virtual Machines

Verifying successful deployment

Confirm that SecureVM Agent has been successfully deployed by logging in to CloudLink Center and viewing the virtual machine status. For information about managing virtual machines, including viewing their status, see the CloudLink SecureVM Administration Guide.

You can also confirm successful deployment from the virtual machine.

On Windows virtual machines

Confirm that SecureVM Agent has successfully installed using the SecureVM Agent Shield icon in the Windows taskbar, as shown in Figure 19. The tooltip displays a message indicating that the virtual machine is connected.

![SecureVM Status: Connected](image)

Figure 19. SecureVM Agent Shield icon

On Linux virtual machines

Confirm successful deployment from the virtual machine command line by typing:

```
sudo service svmd status
```

The command returns a message indicating that the SecureVM daemon (svmd) is running.

Restarting the SecureVM Agent service

You must restart the SecureVM Agent service under the following deployment-related circumstances:

- During the custom installation of the SecureVM Agent on a Windows virtual machine
- After deployment, if the networking configuration for a Windows or Linux virtual machine with an encrypted boot partition is changed

To restart the SecureVM Agent service for a Windows virtual machine custom installation or networking change, do one of the following:

- From the virtual machine command line, type the following two commands:
  ```
  netstop SecureVMSvc
  netstart SecureVMSvc
  ```
- From the Services panel, restart the SecureVM Agent service.

To restart the SecureVM Agent service for a Linux virtual machine networking configuration change:

- From the virtual machine command line, type the following two commands:
  ```
  service network restart
  svm
  ```
Chapter 6  Using the CloudLink Center Update Menu

This chapter presents the following topics:

Overview ........................................................................................................................................ 50
Update Menu options .................................................................................................................... 50
Using the CloudLink Center Update Menu

Overview

After configuring CloudLink Center, every time you log in using the CloudLink Center console, the Update Menu is displayed.

Update Menu options

The Update Menu options are as follows:

- **Summary** displays a summary of CloudLink Center settings.
- **Password** changes the current password used to log in to the CloudLink Center console.
- **Network** resets the network settings, after which you can reconfigure them. If you select this option, all current network settings are removed.
- **Routes** does not apply to most deployments. For information, contact your EMC representative.
- **Diagnostics** is intended only for use as directed by your EMC representative.