

# Hitachi Ops Center

10.9.2

---

## Installation and Configuration Guide

This manual provides information for installing and configuring Hitachi Ops Center.

© 2019, 2023 Hitachi, Ltd. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including copying and recording, or stored in a database or retrieval system for commercial purposes without the express written permission of Hitachi, Ltd., or Hitachi Vantara LLC (collectively "Hitachi"). Licensee may make copies of the Materials provided that any such copy is: (i) created as an essential step in utilization of the Software as licensed and is used in no other manner; or (ii) used for archival purposes. Licensee may not make any other copies of the Materials. "Materials" mean text, data, photographs, graphics, audio, video and documents.

Hitachi reserves the right to make changes to this Material at any time without notice and assumes no responsibility for its use. The Materials contain the most current information available at the time of publication.

Some of the features described in the Materials might not be currently available. Refer to the most recent product announcement for information about feature and product availability, or contact Hitachi Vantara LLC at [https://support.hitachivantara.com/en\\_us/contact-us.html](https://support.hitachivantara.com/en_us/contact-us.html).

**Notice:** Hitachi products and services can be ordered only under the terms and conditions of the applicable Hitachi agreements. The use of Hitachi products is governed by the terms of your agreements with Hitachi Vantara LLC.

By using this software, you agree that you are responsible for:

1. Acquiring the relevant consents as may be required under local privacy laws or otherwise from authorized employees and other individuals; and
2. Verifying that your data continues to be held, retrieved, deleted, or otherwise processed in accordance with relevant laws.

**Notice on Export Controls.** The technical data and technology inherent in this Document may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Reader agrees to comply strictly with all such regulations and acknowledges that Reader has the responsibility to obtain licenses to export, re-export, or import the Document and any Compliant Products.

Hitachi and Lumada are trademarks or registered trademarks of Hitachi, Ltd., in the United States and other countries.

AIX, AS/400e, DB2, Domino, DS6000, DS8000, Enterprise Storage Server, eServer, FICON, FlashCopy, GDPS, HyperSwap, IBM, Lotus, MVS, OS/390, PowerHA, PowerPC, RS/6000, S/390, System z9, System z10, Tivoli, z/OS, z9, z10, z13, z14, z15, z16, z/VM, and z/VSE are registered trademarks or trademarks of International Business Machines Corporation.

Active Directory, ActiveX, Bing, Excel, Hyper-V, Internet Explorer, the Internet Explorer logo, Microsoft, Microsoft Edge, the Microsoft corporate logo, the Microsoft Edge logo, MS-DOS, Outlook, PowerPoint, SharePoint, Silverlight, SmartScreen, SQL Server, Visual Basic, Visual C++, Visual Studio, Windows, the Windows logo, Windows Azure, Windows PowerShell, Windows Server, the Windows start button, and Windows Vista are registered trademarks or trademarks of Microsoft Corporation. Microsoft product screen shots are reprinted with permission from Microsoft Corporation.

All other trademarks, service marks, and company names in this document or website are properties of their respective owners.

Copyright and license information for third-party and open source software used in Hitachi Vantara products can be found in the product documentation, at <https://www.hitachivantara.com/en-us/company/legal.html> or [https://knowledge.hitachivantara.com/Documents/Open\\_Source\\_Software](https://knowledge.hitachivantara.com/Documents/Open_Source_Software).

---

# Contents

- Preface.....7**
  - Intended audience..... 7
  - Product version..... 7
  - Release notes..... 7
  - Referenced documents..... 7
  - Related documents..... 7
  - Document conventions..... 8
  - Accessing product documentation..... 9
  - Getting help..... 10
  - Comments..... 10
  
- Chapter 1: Overview..... 11**
  - Overview of the Hitachi Ops Center products..... 11
  - Overview of Hitachi Ops Center Common Services..... 12
    - Linking with an Active Directory or LDAP server..... 13
    - Linking with an identity provider..... 14
  - Installation methods for Hitachi Ops Center..... 15
  - OVA files provided by Hitachi Ops Center..... 16
  - Hitachi Ops Center system configurations..... 16
    - Example configuration running on one management server..... 17
    - Example configuration running on multiple management servers..... 17
  
- Chapter 2: Installing Hitachi Ops Center products by using the OVA file..... 20**
  - Workflow for deploying and setting up Hitachi Ops Center..... 20
  - System configuration of the Hitachi Ops Center virtual machine..... 21
  - Default settings for the virtual machine and the guest operating system..... 22
  - Deploying Hitachi Ops Center..... 23
  - Running the setup tool (opsvmsetup)..... 23
  - Installing Ops Center Analyzer separately using an OVA..... 25
  - Installing the Analyzer probe server and Protector Client (VMware vSphere Client)..... 25
    - Initial setup of the guest OS or VMs..... 27
  - Upgrading after an OVA installation..... 29
  - Configuring SSL communications..... 29

Registering products in Common Services.....	29
Registering Ops Center products with Common Services (setupcommons-service).....	30
Logging in to the Hitachi Ops Center Portal.....	33
Configuring initial settings in the Hitachi Ops Center Portal.....	34
Installing OS updates and other products after deployment.....	34
<b>Chapter 3: Installing or upgrading Hitachi Ops Center products by using the Express installer.....</b>	<b>36</b>
Using the Server Express installer.....	36
Workflow for installing and setting up Hitachi Ops Center.....	36
Preparing the management server.....	37
Installing or upgrading Common Services and additional products.....	38
Configuring SSL communications.....	48
Registering products in Common Services.....	48
Registering Ops Center products with Common Services (setupcommons-service).....	49
Logging in to the Hitachi Ops Center Portal.....	51
Configuring initial settings in the Hitachi Ops Center Portal.....	51
Installing OS updates and other products after installation.....	52
Using the Client Express installer.....	53
Workflow for installing and setting up Hitachi Ops Center (Client Express installer).....	53
Preparing the server.....	53
Installing or upgrading each product.....	53
<b>Chapter 4: Installing or upgrading Hitachi Ops Center products by using the installer.....</b>	<b>59</b>
Workflow for installing and setting up Hitachi Ops Center.....	59
Preparing the management server.....	60
Installing or upgrading Common Services.....	61
Installing or upgrading each product.....	64
Configuring SSL communications.....	64
Registering products in Common Services.....	64
Registering Ops Center products with Common Services (setupcommons-service).....	65
Logging in to the Hitachi Ops Center Portal.....	68
Configuring initial settings in the Hitachi Ops Center Portal.....	68
Installing OS updates and other products after installation.....	69
<b>Chapter 5: Removing a Hitachi Ops Center product .....</b>	<b>70</b>
Removing Common Services.....	70

<b>Chapter 6: Configuring SSL communications.....</b>	<b>72</b>
Configuring SSL communications by using the SSL Setup tool.....	72
SSL Setup tool functionality.....	74
Creating a private key and a certificate signing request (SSL Setup tool)...	77
Configuring SSL server settings (SSL Setup tool).....	78
Configuring SSL server settings for an Active Directory or LDAP server.....	80
Configuring SSL server settings for an identity provider server.....	80
Configuring SSL client settings and enabling certificate verification (SSL Setup tool).....	80
Configuring SSL communications without using the SSL Setup tool.....	83
Preparing the server certificate for Common Services.....	83
Setting the path information for the server certificate and private key.....	85
Specifying SSL server settings for each product.....	86
Configuring SSL server settings for an Active Directory or LDAP server.....	86
Configuring SSL server settings for an identity provider server.....	86
Importing certificates into each product.....	86
Importing certificates into the Common Services truststore.....	87
Enabling server certificate verification.....	88
<b>Chapter 7: Configuring a link to an identity provider.....</b>	<b>90</b>
Supported identity providers.....	90
Workflow for linking with AD FS.....	90
Configuring settings to link with AD FS (OIDC).....	91
Registering Common Services in AD FS as an application group.....	91
Setting up an issuance transform rule for AD FS.....	93
Checking the OpenID Connect Discovery endpoint of AD FS.....	94
Registering AD FS with Common Services.....	95
Logging in to the Hitachi Ops Center Portal as an identity provider user.....	96
Configuring settings to link with AD FS (SAML).....	97
Checking the AD FS metadata endpoint.....	97
Registering AD FS with Common Services.....	97
Exporting Common Services metadata.....	99
Registering Common Services in AD FS as a relying party.....	99
Setting up a claim issuance policy.....	100
Logging in to the Hitachi Ops Center Portal as an identity provider user...	103
Updating the authentication certificates used with an identity provider (SAML).....	103
Overview of updating authentication certificates.....	103
Checking the next update for the Common Services certificates.....	104
Checking the dates of the next update of the AD FS certificates.....	104
Updating the Common Services certificates.....	105

Updating the AD FS certificates.....	106
If you cannot sign on with an identity provider.....	107
Updating the Common Services metadata by using AD FS.....	107
Specifying the AD FS metadata endpoint by using Common Services	108
<b>Chapter 8: Maintaining Hitachi Ops Center.....</b>	<b>109</b>
Starting or stopping the Common Services service.....	109
Checking the validity period of a certificate in the truststore.....	109
Checking the validity period of the server certificate.....	110
Checking the revocation status of the server certificate.....	110
Checking the revocation status of the server certificate by using a web browser.....	111
Checking the revocation status of the server certificate by using a command.....	111
Checking the revocation status of the server certificate on a regular basis.....	112
Outputting the revocation status check results to a file.....	112
Outputting the revocation status check results to <code>syslog</code> .....	115
Changing the management server host name, IP address, or port number....	115
Changing the port number used for internal communications.....	117
Backing up Common Services.....	119
Restoring Common Services.....	120
Stopping unnecessary product services.....	122
Resetting the trust relationship with each product.....	123
Configuring the settings for session idle timeouts.....	124
Changing the scale of the resources managed by an individual product.....	125
Settings required when using a virus detection program.....	126
Upgrading Amazon Corretto 17.....	127
Upgrading PostgreSQL 11.....	127
Applying Linux security updates using yum.....	128
<b>Appendix A: Troubleshooting.....</b>	<b>131</b>
Collecting failure information.....	131
Common Services logs.....	133
Changing the properties of logs.....	134
Common Services audit log.....	137
Changing the audit log properties.....	138
Determining the parameters for LDAP server registration.....	140

---

# Preface

This manual provides information for installing and configuring Hitachi Ops Center.

## Intended audience

This manual is intended for system administrators who manage and use Hitachi Ops Center products.

The system administrator must have the following skills:

- VMware ESXi™ and VMware vSphere® operations, and the knowledge related to setting up these products
- Basic knowledge of Oracle Linux or Red Hat Enterprise Linux
- Basic knowledge of the prerequisite software (when using the functionality to link with an external authentication server or an identity provider)

## Product version

This document revision applies to Hitachi Ops Center version 10.9.2.

## Release notes

Read the release notes before installing and using this product. They may contain requirements or restrictions that are not fully described in this document or updates or corrections to this document. Release notes are available on the Hitachi Vantara Support Website: <https://knowledge.hitachivantara.com/Documents>.

## Referenced documents

None

## Related documents

The following documents are related to this document or contain more information about the features described in this document.

### Hitachi Vantara documents

- *Hitachi Data Instance Director Quick Start Guide*, MK-93HDID015
- *Hitachi Ops Center Administrator Getting Started Guide*, MK-99ADM000
- *Hitachi Ops Center Analyzer Installation and Configuration Guide*, MK-99ANA001
- *Hitachi Ops Center API Configuration Manager REST API Reference Guide*, MK-99CFM000
- *Hitachi Ops Center Automator Installation and Configuration Guide*, MK-99AUT000
- *Hitachi Ops Center Common Services REST API Reference Guide*, MK-99OPS003
- *Hitachi Ops Center Protector Quick Start Guide*, MK-99PRT001

Hitachi Vantara Support Connect, <https://knowledge.hitachivantara.com/Documents>

## Document conventions

This document uses the following typographic conventions:

Convention	Description
<b>Bold</b>	<ul style="list-style-type: none"> <li>▪ Indicates text in a window, including window titles, menus, menu options, buttons, fields, and labels. Example: Click <b>OK</b>.</li> <li>▪ Indicates emphasized words in list items.</li> </ul>
<i>Italic</i>	<ul style="list-style-type: none"> <li>▪ Indicates a document title or emphasized words in text.</li> <li>▪ Indicates a variable, which is a placeholder for actual text provided by the user or for output by the system. Example: <pre>pairdisplay -g group</pre></li> </ul> <p>(For exceptions to this convention for variables, see the entry for angle brackets.)</p>
Monospace	Indicates text that is displayed on screen or entered by the user. Example: <code>pairdisplay -g oradb</code>
< > angle brackets	<p>Indicates variables in the following scenarios:</p> <ul style="list-style-type: none"> <li>▪ Variables are not clearly separated from the surrounding text or from other variables. Example: <pre>Status-&lt;report-name&gt;&lt;file-version&gt;.csv</pre></li> <li>▪ Variables in headings.</li> </ul>

Convention	Description
[ ] square brackets	Indicates optional values. Example: [ a   b ] indicates that you can choose a, b, or nothing.
{ } braces	Indicates required or expected values. Example: { a   b } indicates that you must choose either a or b.
vertical bar	Indicates that you have a choice between two or more options or arguments. Examples: [ a   b ] indicates that you can choose a, b, or nothing. { a   b } indicates that you must choose either a or b.

This document uses the following icons to draw attention to information:

Icon	Label	Description
	Note	Calls attention to additional information.
	Tip	Provides helpful information, guidelines, or suggestions for performing tasks more effectively.
	Important	Highlights information that is essential to the completion of a task.
	Caution	Warns the user of adverse conditions and/or consequences (for example, disruptive operations, data loss, or a system crash).
	CAUTION	Warns the user of a hazardous situation that, if not avoided, could result in major or minor injury.
	WARNING	Warns the user of a hazardous situation which, if not avoided, could result in death or serious injury.

## Accessing product documentation

Product user documentation is available on the Hitachi Vantara Support Website: <https://knowledge.hitachivantara.com/Documents>. Check this site for the most current documentation, including important updates that may have been made after the release of the product.

## Getting help

The [Hitachi Vantara Support Website](https://support.hitachivantara.com/en_us/contact-us.html) is the destination for technical support of products and solutions sold by Hitachi Vantara. To contact technical support, log on to the Hitachi Vantara Support Website for contact information: [https://support.hitachivantara.com/en\\_us/contact-us.html](https://support.hitachivantara.com/en_us/contact-us.html).

[Hitachi Vantara Community](https://community.hitachivantara.com) is a global online community for Hitachi Vantara customers, partners, independent software vendors, employees, and prospects. It is the destination to get answers, discover insights, and make connections. **Join the conversation today!** Go to [community.hitachivantara.com](https://community.hitachivantara.com), register, and complete your profile.

## Comments

Please send comments to [doc.comments@hitachivantara.com](mailto:doc.comments@hitachivantara.com). Include the document title and number, including the revision level (for example, -07), and refer to specific sections and paragraphs whenever possible. All comments become the property of Hitachi Vantara LLC.

**Thank you!**

---

## Chapter 1: Overview

The Hitachi Ops Center product enables you to optimize your data center operations through integrated configuration, analytics, automation, and copy data management. These features enable you to administer, automate, optimize, and protect your Hitachi storage infrastructure.

Hitachi Ops Center is a system consisting of multiple products. The following provides an overview of the Hitachi Ops Center product components and an overview of the system configuration.

### Overview of the Hitachi Ops Center products

A Hitachi Ops Center system consists of the following software products:

### **Hitachi Ops Center Common Services**

Hitachi Ops Center Common Services provides infrastructure functions common to Hitachi Ops Center that enable you to launch products, manage users, and enable single sign-on (SSO).

### **Hitachi Ops Center Automator**

Hitachi Ops Center Automator provides the tools to automate and simplify end-to-end processes, such as storage provisioning, for storage and data center administrators. The building blocks of the product are prepackaged automation templates known as service templates.

### **Hitachi Ops Center Analyzer**

Hitachi Ops Center Analyzer provides a comprehensive application service-level and storage performance management solution that enables you to quickly identify and isolate performance problems, determine the root cause, and provide solutions.

Hitachi Ops Center Analyzer collects the data to analyze from the Hitachi Ops Center Analyzer detail view, which processes performance and configuration data received from probes that connect to monitoring targets.

### **Hitachi Ops Center Analyzer viewpoint**

Hitachi Ops Center Analyzer viewpoint consolidates information from multiple instances of Hitachi Ops Center Analyzer and provides functions for monitoring a system that spans multiple data centers.

### **Hitachi Ops Center Administrator**

Hitachi Ops Center Administrator is a unified software management tool that reduces the complexity of managing storage systems by simplifying the setup, management, and maintenance of storage resources.

### **Hitachi Ops Center Protector**

Hitachi Ops Center Protector provides a modern, holistic approach to data protection, recovery, and retention.

### **Hitachi Ops Center API Configuration Manager**

Hitachi Ops Center API Configuration Manager provides APIs for obtaining information from and performing operations on storage systems.

## **Overview of Hitachi Ops Center Common Services**

Hitachi Ops Center Common Services is a component that provides single sign-on functionality and a portal site for Hitachi Ops Center products.

When you log in to the Hitachi Ops Center Portal, the portal shows a list of registered Hitachi Ops Center products. When you click a product-name link, the product UI opens. Because user authentication is centralized, you can access each product without additional logins.

The Hitachi Ops Center products that support the single sign-on functionality are as follows:

- Hitachi Ops Center Automator (version 10.0.1 or later)
- Hitachi Ops Center Analyzer

- Hitachi Ops Center Analyzer detail view (version 10.8.2 or later)
- Hitachi Ops Center Analyzer probe (version 10.8.2 or later)
- Hitachi Ops Center Analyzer viewpoint
- Hitachi Ops Center Administrator (version 10.1.0 or later)
- Hitachi Ops Center Protector (version 7.0 or later)

The single sign-on user information is managed by Common Services, so you can create, delete, and modify user accounts from the portal site.



**Tip:** You can also use Hitachi Ops Center products without single sign-on. For the installation and setup procedures to use in this case, see the documentation for the specific Hitachi Ops Center products that you are using.

## Linking with an Active Directory or LDAP server

By linking Common Services with an external Active Directory or LDAP server, you can consolidate actions related to authenticating Hitachi Ops Center users. You can link Common Services with an Active Directory or LDAP server from the Hitachi Ops Center Portal.

You can link Common Services with one of the following authentication servers:

- Active Directory server
- LDAP server that support LDAPv3 and LDAPS

You can link Common Services with either an Active Directory or an LDAP server. You cannot link Common Services with both types of servers.

The following conditions apply when you link Common Services with an Active Directory server or LDAP server.

### Active Directory server:

- Both LDAP(S) and Kerberos are supported as authentication protocols.
- When using Kerberos authentication, you can set only one realm.
- You can register Common Services users for objects that are located under the base DN and with an `objectclass` of `person`.
- To log in to the Hitachi Ops Center Portal, use the Active Directory `sAMAccountName` as the user name.
- You can specify groups under the base DN to import.

### LDAP server:

- Only LDAP(S) is supported as an authentication protocol.
  - You can import a maximum of 100 user accounts.
- To narrow down the users to import, you can filter the search conditions by using LDAP attributes.
- Synchronizing user groups between the LDAP server and Common Services is not supported.

**Note:**

- To use Hitachi Ops Center Analyzer viewpoint, you must specify an email address for the `mail` attribute.
- A user who has the same user name or email address as a local user of Common Services cannot log in to the Hitachi Ops Center Portal.

Before setting up the linkage, you must delete the local user in the Hitachi Ops Center Portal or change the email address of the local user.

- If the certificate of the LDAP server has expired, all users including local users of Common Services will be unable to log in to the Hitachi Ops Center Portal.

To avoid this, you must update the certificate of the LDAP server before it expires and import the certificate into the Common Services truststore.

For details on how to set up a link with an Active Directory or LDAP server and details on users and user groups, see the Hitachi Ops Center Portal Help.

## Linking with an identity provider

By linking Common Services with an external identity provider, you can use the identity provider to centrally authenticate Hitachi Ops Center users. You can also use the Multi Factor Authentication (MFA) functionality provided by the identity provider.

By linking with an identity provider, you can authenticate a user who logs in to the Hitachi Ops Center Portal on the identity provider side. If the identity provider successfully authenticates the user, the user is imported as a local user of Common Services.

Common Services supports linking with Active Directory Federation Services (AD FS). To link with AD FS, configure the settings on both the AD FS server and the Hitachi Ops Center Portal. For details, see [Configuring a link to an identity provider \(on page 90\)](#).

**Note:**

- You cannot link one Active Directory server to both a directory service and AD FS.
- Identity provider user accounts must have a unique username and email address. If an identity provider user account conflicts with a local user ID or email address, the identity provider user cannot log in. You must remove the local user from the Hitachi Ops Center Portal or change their email address before proceeding.

## Installation methods for Hitachi Ops Center

You can use one of the following methods to install Hitachi Ops Center:

- Installation by using an OVA file

Use this method when you want to easily install the products on a virtual machine.

Deploy an OVA file on a VMware ESXi server, which creates a virtual machine on which the Hitachi Ops Center product is installed.

For information about the OVA file provided by Hitachi Ops Center and about products that are installed on the virtual machine, see [OVA files provided by Hitachi Ops Center \(on page 16\)](#).

- Installation by using the Express installer

Use this method when you want to install or upgrade multiple Hitachi Ops Center products at the same time. The Express installer includes the Server Express installer and the Client Express installer, each of which installs different products. You can select specific products to install.

**The Server Express installer installs the following products and registers them with Common Services:**

- Hitachi Ops Center Common Services
- Hitachi Ops Center Administrator
- Hitachi Ops Center API Configuration Manager
- Hitachi Ops Center Protector
- Hitachi Ops Center Automator
- Hitachi Ops Center Analyzer
- Hitachi Ops Center Analyzer detail view
- Hitachi Ops Center Analyzer viewpoint

**You can use the Client Express installer to install the following products:**

- Hitachi Ops Center API Configuration Manager
- Hitachi Ops Center Protector Client
- Hitachi Ops Center Analyzer probe server

- Installation by using the installer for each product

Use this method when you want to install or upgrade Hitachi Ops Center products individually. Use the installation media for each product to perform installation.

For details on the installation method, see the following descriptions:

- [Installing Hitachi Ops Center products by using the OVA file \(on page 20\)](#)
- [Installing or upgrading Hitachi Ops Center products by using the Express installer \(on page 36\)](#)
- [Installing or upgrading Hitachi Ops Center products by using the installer \(on page 59\)](#)

## OVA files provided by Hitachi Ops Center

Hitachi Ops Center provides the following OVA files.

OVA name	Installed product
Ops Center OVA	<ul style="list-style-type: none"> <li>▪ Hitachi Ops Center Common Services</li> <li>▪ Hitachi Ops Center Automator</li> <li>▪ Hitachi Ops Center Analyzer*</li> <li>▪ Hitachi Ops Center Analyzer detail view</li> <li>▪ Hitachi Ops Center Administrator</li> <li>▪ Hitachi Ops Center Protector (Master)</li> <li>▪ Hitachi Ops Center API Configuration Manager</li> </ul>
Analyzer OVA	<ul style="list-style-type: none"> <li>▪ Hitachi Ops Center Analyzer</li> <li>▪ Hitachi Ops Center Analyzer detail view</li> </ul>
Analyzer probe OVA	<ul style="list-style-type: none"> <li>▪ Hitachi Ops Center Analyzer probe</li> <li>▪ Hitachi Ops Center Analyzer Virtual Storage Software Agent</li> <li>▪ Hitachi Ops Center Protector (Client)</li> <li>▪ Hitachi Ops Center API Configuration Manager</li> </ul>
Analyzer viewpoint OVF	<ul style="list-style-type: none"> <li>▪ Hitachi Ops Center Analyzer viewpoint</li> <li>▪ Hitachi Ops Center Common Services</li> </ul>
<p>* If you are using Hitachi Ops Center Analyzer, the Hitachi Ops Center Analyzer probe is required. Either deploy the Analyzer probe OVA, or install the Hitachi Ops Center Analyzer probe on another machine.</p>	

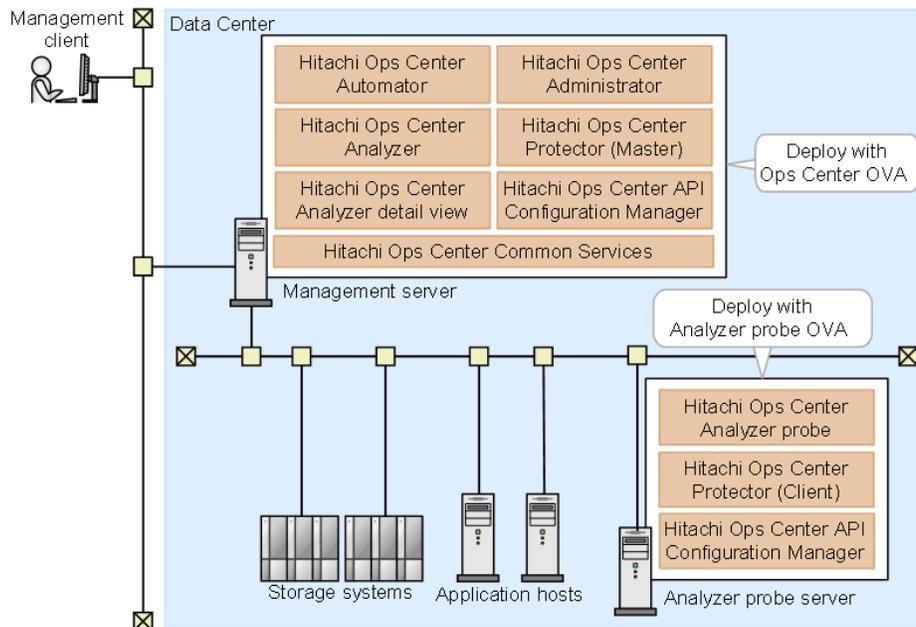
## Hitachi Ops Center system configurations

A Hitachi Ops Center system consists of one or more management servers, depending on the software you are using and the scope of resources to manage. Common Services runs on one management server, and products register with Common Services so that they can use common infrastructure functions.

The following provides basic system configuration examples and the recommended installation method for each.

## Example configuration running on one management server

The following shows an example system configuration in which Hitachi Ops Center product runs on one management server.

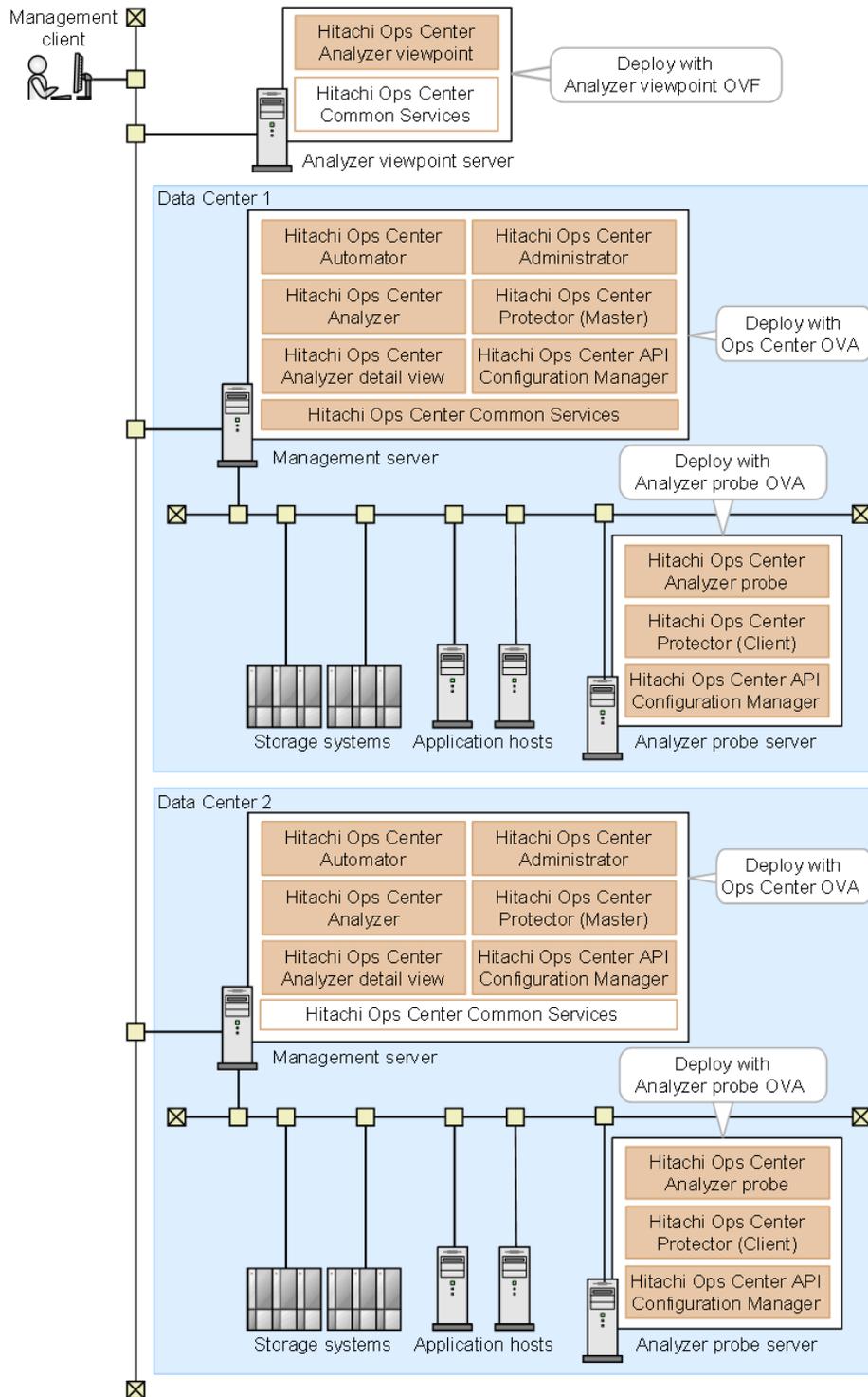


When building a system with the OVA, it's easiest to use the Ops Center OVA to install the main products, and then add the Analyzer Probe OVA.

When using an installer, you use the installer specific to the product. If you want to use the single sign-on functionality, you must also install the Common Services.

## Example configuration running on multiple management servers

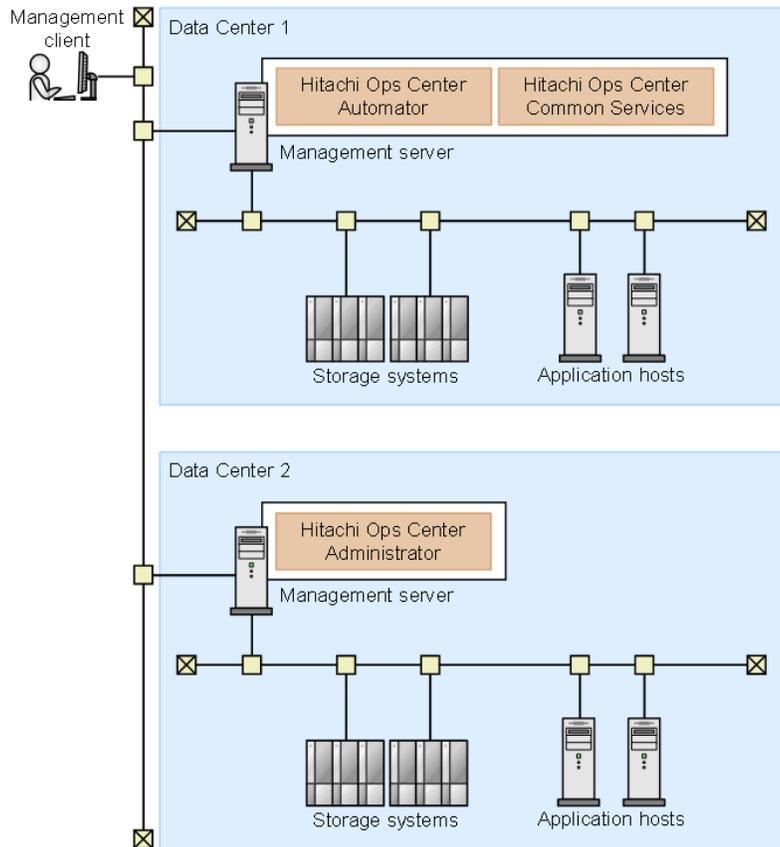
When managing resources in a large-scale data center, you can use a configuration that uses multiple management servers. The following shows this type of configuration.



If you deploy multiple OVA files, a Common Services instance is installed on each server, but the system only uses one instance. In this example configuration, the system uses the Common Services instance on the management server running in Data Center 1.

Using an installer, you can also manually install optional Hitachi Ops Center products. In this example configuration, Hitachi Ops Center Automator, Hitachi Ops Center Administrator, and Common Services are installed.

## Example configuration running on multiple management servers



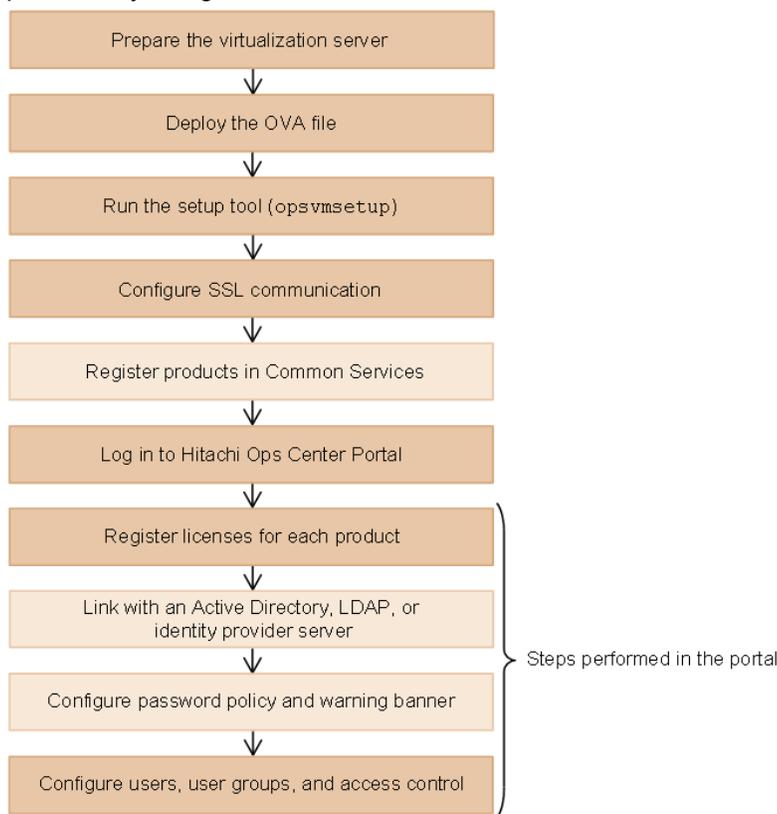
**Note:** If the Hitachi Ops Center system configuration contains multiple management servers and the system times of the management servers are not the same, you cannot start the products from the Hitachi Ops Center Portal. To keep the time synchronized, we recommend that you use NTP to correct the time automatically.

## Chapter 2: Installing Hitachi Ops Center products by using the OVA file

You can install Hitachi Ops Center products on a virtual machine by deploying the Hitachi Ops Center OVA file on a VMware ESXi server.

### Workflow for deploying and setting up Hitachi Ops Center

The following figure shows the workflow for installing and setting up the Hitachi Ops Center products by using the OVA file:



For a complete list of Hitachi Ops Center system requirements, go to the [Ops Center documentation site](#) and select Get Started with Ops Center > Hitachi Ops Center system requirements.

For details on preparing the virtualization server, see the VMware documentation.

After configuring access control, configure the settings for each product as necessary. For details on how to configure settings, see the documentation for each product.

## System configuration of the Hitachi Ops Center virtual machine

This section describes the virtual machine system configuration that is created by using the Hitachi Ops Center OVA file.

### Guest operating system

Oracle Linux is installed as the guest operating system.

### Installed products

The following products, which are components of the management server, are installed:

- Hitachi Ops Center Automator
- Hitachi Ops Center Analyzer
- Hitachi Ops Center Analyzer detail view
- Hitachi Ops Center Administrator
- Hitachi Ops Center Protector
- Hitachi Ops Center API Configuration Manager
- Hitachi Ops Center Common Services



#### Note:

- The installation directory is `/opt/hitachi`.
- The installation destination for Common Services is `/opt/hitachi/CommonService`.
- User data for Common Services is stored in the following user data directory:  
`/var/opt/hitachi/CommonService`

Hitachi Ops Center API Configuration Manager requires Command Control Interface, so it is also installed as part of the installation. The installation directory is `/opt/hitachi/ConfManager/HORCM`.



#### Note:

- For products not included in this OVA, install each product by using the separate installer or OVA provided for that product.
- Hitachi Ops Center does not support installing other software products on the management server, but allows for installing software required by corporate policy such as anti-virus programs and third-party monitoring agents. Note that Hitachi Vantara does not take responsibility for or support any interactions between the third-party programs and the Hitachi Ops Center software.

## Default settings for the virtual machine and the guest operating system

The OVA deployment sets the virtual machine and operating system settings that Hitachi Ops Center requires by default.

When you deploy the OVA file, a virtual machine with the following default settings is created. Confirm whether the virtualization server has enough resources to create the virtual machine.

Item	Settings
CPU	12 cores
Memory	36 GiB
Disk size	1050 GiB

The default settings assume that you are managing 10 storage systems. For larger-scale systems, change the settings for memory, disk size, and virtual memory, or increase the number of virtual machines.

For details on how to change the settings of virtual machines, go to the [Ops Center documentation site](#) and select Get Started with Ops Center > Hitachi Ops Center system requirements.

The following table lists the items that are set by default for the guest operating system. To change the settings for Hitachi Ops Center products after the deployment, change the operating system settings as needed.

Item	Settings
Operating system version	Oracle Linux For details about the latest operating system version, see the <i>Hitachi Ops Center System Requirements</i> .
Installed libraries	Prerequisite libraries required for the Hitachi Ops Center products included in the OVA.
Kernel parameters	Values required for the Hitachi Ops Center products included in the OVA.
Registering firewall exceptions	In addition to the ports that are registered as exceptions by the operating system, the ports that must be registered as exceptions for each of the products.

## Deploying Hitachi Ops Center

By deploying the Hitachi Ops Center OVA file, you can create a virtual machine on which the products are installed.

### Procedure

1. From a VMware vSphere client, log in to the VMware ESXi server.
2. From the VMware vSphere client, deploy the Hitachi Ops Center OVA (`OpsCenterVM_version.ova`) by selecting **File > Deploy OVF Template**, and then following the prompts.
3. To avoid IP address conflicts when the virtual machine starts, change the settings so that the machine does not connect to the network.

You can skip this step if you are sure that the IP addresses will not conflict.

When deployment is complete, the following network settings are set by default for the virtual machine:

- IP address: 172.30.197.92
  - Network mask: 255.255.0.0
  - Default gateway: 172.30.0.1
    - a. Right-click the new virtual machine, and select **Edit Settings**.
    - b. In the **Hardware** tab, select **Network adapter 1**, and then clear the **Connect at power on** check box.
4. Start the virtual machine.
  5. If you changed the settings in step 3 so that the virtual machine does not connect to the network when it starts, reselect the **Connect at power on** check box.
    - a. Right-click the virtual machine, and select **Edit Settings**.
    - b. In the **Hardware** tab, select **Network adapter 1**, and then check the **Connect at power on** check box.

## Running the setup tool (opsvmsetup)

After you complete the OVA deployment, run the setup tool (`opsvmsetup`) to complete the initial setup.

You can use the setup tool to specify the following settings:

#### Network settings

- Host name (or FQDN)
- IP address
- Default gateway
- Network mask
- DNS server (up to two servers)

#### Time settings

- Time zone
- NTP server

When you run the initial setup, the following settings are specified: the network and time settings for the guest OS, the single sign-on settings for the selected product, the settings to enable SSL communications, and the firewall settings for service ports.



#### Note:

- You can run the setup tool only once. To change the settings after running the setup tool, use the operating system commands.
- This setup tool is stored in the `/opt/OpSVM/vmtool` directory but you can run the tool from any directory.
- The setup tool specifies an IPv4 address.
- The host name (or FQDN) and IP address specified in this step is used in the URL for accessing the Hitachi Ops Center Portal. To change the host name (or FQDN) or IP address that is used to access the Hitachi Ops Center Portal, run the `cschgconnect` command after installation. For details about the `cschgconnect` command, see [Changing the management server host name, IP address, or port number \(on page 115\)](#).
- The management server on which Common Services and other relevant products are installed and the web browser used to access the Hitachi Ops Center Portal must be able to resolve and reach the host name (or FQDN) and IP address.
- You cannot specify uppercase characters in the host name (or FQDN). If you do, they are converted to lowercase characters and then registered.
- Specify the time zone in the *area/location* format. If you do not know the required values, use the following command to check the time zone values before running the setup tool:

```
timedatectl list-timezones
```

### Procedure

1. From the VMware vSphere client, log in to the guest operating system.

When you log in for the first time, use the following user ID and password:

User ID: `root`

Password: `manager`

After logging in, you must change the root password.

2. Run the setup tool: `opsvmsetup`.
3. Specify the values as indicated in the prompts.  
After you finish all items, a list of the settings is displayed.
4. Check the settings, enter `y`, and then apply the settings.

After applying the settings, the guest operating system restarts automatically.

5. If you changed the settings so that the virtual machine is not connected to the network when deployed, complete the following steps to enable the network adapter:
  - a. Log in to the guest operating system, and then stop the virtual machine by using the `shutdown` command.
  - b. From the VMware vSphere client, click **Power On the virtual machine**.

## Installing Ops Center Analyzer separately using an OVA

In a large system configuration with multiple Ops Center Analyzer servers, you can use the Analyzer OVA to deploy only Ops Center Analyzer and Analyzer detail view. This enables you to use a separate server or add another instance of Ops Center Analyzer. For information on installing the Analyzer OVA, see the Ops Center Analyzer installation documentation.

## Installing the Analyzer probe server and Protector Client (VMware vSphere Client)

By deploying the OVA file (the Analyzer probe OVA), you can create a virtual machine on which Analyzer probe server, Protector Client, and Ops Center API Configuration Manager are installed.

### Before you begin

- Review the Analyzer probe server requirements (hardware and software).
- Make sure that the ports you specify are available for communication. The default port is 8443. The default port for SSH is 22.
- If you use the Analyzer probe server in a DNS environment, exclude the domain name when specifying the host name because the Analyzer probe server does not support FQDN.

- Specify a static IP address for Analyzer probe server because the RAID Agent cannot run on hosts the use DHCP to assign IP addresses.
- When you run RAID Agent in a virtual environment:
  - Before setting up the RAID Agent, you must specify C for the LANG environment variable on the Analyzer probe server host.

At startup, RAID Agent is subject to the system LANG environment variable. If the `LC_ALL` environment variable differs from the LANG environment variable, either unset `LC_ALL` or change the value to match the LANG value. Use the following example as a reference when setting the LANG value for RAID Agent. The last line is an example of coding that unsets the `LC_ALL` value.

**Example settings:**

```
## Set Environment-variables
PATH=/sbin:/bin:/usr/bin:/opt/jplpc/bin
SHLIB_PATH=/opt/hitachi/common/lib
LD_LIBRARY_PATH=/opt/hitachi/common/lib
LIBPATH=/opt/hitachi/common/lib
HCCLIBCNF=/opt/jpl/hcclibcnf
LANG=C
export PATH SHLIB_PATH LD_LIBRARY_PATH LIBPATH HCCLIBCNF LANG
unset LC_ALL
```

- If you want to monitor VSP family, you must enable access from a guest OS to the command device. For details, see the documentation for your virtual system.



**Note:** If you do not want to collect performance information using a command device, skip these settings.

Use a VMware vSphere Client file to add a device to the guest OS. By doing so, if you designate a command device as the device to add, the command device can be accessed from the guest OS.

When configuring settings to add a device, make sure that the following requirements are met:

- Device type: Hard disk
- Disk selection: Raw device mapping
- Compatibility mode: Physical
- Virtual disks (including VMware VVols) are not used for the command device.
- When you use a virtualization system to replicate an OS environment in which the RAID Agent is running, do not apply the replicated environment to any other host. The RAID Agent startup might fail in the replicated environment.

**Procedure**

1. From a VMware vSphere client, log on to the VMware ESXi server.
2. Deploy the Analyzer probe OVA (`dcaprobe_version.ova`) by selecting **File > Deploy OVF Template**, and then following the prompts.

From the VMware vSphere client, select **File > Deploy OVF Template**, and then follow the on-screen instructions.



**Tip:** We recommend selecting **Thick Provision Lazy Zeroed** in the window for selecting the disk provisioning method.

3. Change the settings so that the virtual machine does not connect to the network when started.

This operation is not required if you are sure that the IP addresses will not conflict.

When deployment is complete, the following default network settings are used for the virtual machine:

- **IP address:** 172.30.197.101
- **Net mask:** 255.255.0.0
- **Default gateway:** 172.30.0.1
  - a. Right-click the virtual machine that you want to edit, and then select **Edit Settings**.
  - b. In the **Hardware** tab, select **Network adapter 1**, and then clear the **Connect at power on** check box.

4. Start the virtual machine.

When you log in for the first time, use the following user ID and password:

User ID: `root`

Password: `manager`

After you log in, you must change the root password.

5. Confirm that the network setting is correct.

### Next steps

Run the setup tool on the guest OS, and then specify the guest OS initial settings.



**Note:** When running the Analyzer probe server, Ops Center API Configuration Manager, and Protector Client on the same VM, all components share the same command device, but Ops Center API Configuration Manager and Protector Client must access the storage systems using different credentials. This means they must use different user accounts when accessing the storage system.



**Tip:** The Analyzer probe server and Protector Client are installed in the following directory on the virtual machine.

- Analyzer probe server: `/home`
- Protector Client: `/opt/hitachi/protector`

## Initial setup of the guest OS or VMs

After deploying the virtual appliance, run the setup tool (`opsvmsetup`) to specify the guest OS initial settings. If you want to use Protector, specify settings for Protector. If you want to use Common Services, you must manually register Analyzer probe in Common Services.

**Procedure**

1. From the VMware vSphere Client, log on to the guest OS.
2. Run the `opsvmsetup` command.

**Note:**

- You can run the setup tool only once. To change the settings after running the setup tool, use the operating system commands.
- This setup tool is stored in `/opt/OpsVM/vmtool` but you can run the tool from any location.

3. In the setup tool, you can specify the following settings:
  - **Network settings:**
    - Host name: The Analyzer probe server does not support FQDNs. Omit the domain name when specifying the host name.
    - DHCP: RAID Agent does not support the use of DHCP. If you are using RAID Agent, specify `n`.
    - IP address: The setup tool specifies an IPv4 address.
    - Default gateway
    - Network mask
    - DNS server (2 servers maximum)

- **Time settings:**

- Time zone
  - Specify the time zone in the `area/location` format. If you do not know the specifiable values, use the following command in advance to check the available time zone values:

```
timedatectl list-timezones
```

- The times and time zones of the following servers must be synchronized:
  - Analyzer server
  - Analyzer detail view server
- NTP server
- **Security setting:**
  - Server certificate
- **Protector settings:**
  - Whether to use Protector
  - Protector master host name
  - Protector master IPv4 address

4. Check the contents of the list that displays your specified settings, and then apply the settings.

After the settings are applied, the guest OS restarts automatically.

5. If the virtual machine is not connected to the network when deployed, complete the following steps to enable the network adapter:
  - a. Log on to the guest OS.
  - b. Stop the virtual machine by running the `shutdown` command.
  - c. Right-click the virtual machine that you want to stop, and then select **Edit Settings**.
  - d. In the **Hardware** tab, select **Network adapter 1**, and then select the **Connect at power on** check box.
  - e. Run the **Power On the virtual machine**.

## Upgrading after an OVA installation

The OVA is for new installations only. To perform an upgrade or overwrite installation, perform the procedures described in [Installing or upgrading Hitachi Ops Center products by using the Express installer \(on page 36\)](#) or [Installing or upgrading Hitachi Ops Center products by using the installer \(on page 59\)](#).

## Configuring SSL communications

By default, Common Services uses SSL/TLS communications. Immediately after installation, the system uses SSL communication by using a self-signed certificate. However, you must set up SSL communications to use a valid server certificate before any of the products can communicate with Common Services and the Hitachi Ops Center Portal.

For details on how to configure SSL communications, see [Configuring SSL communications \(on page 72\)](#).

### Next steps

When you finish configuring SSL communications, return to this chapter and go to the next section.

## Registering products in Common Services

To use the functions provided by Common Services, you must register products in Common Services. When you deployed the Hitachi Ops Center OVA file, each product was registered

in Common Services. This means that you only need to register your products with Common Services using the `setupcommonservice` command in the following cases:

- If you want to use a product that was installed by using a method other than the Ops Center OVA, register the product in Common Services.
- If you deployed the Ops Center OVA to multiple management servers, decide which management server to use as the Common Services host, and then reregister the products installed on the other management servers to the central Common Services instance.



**Note:** You cannot unregister a Hitachi Ops Center product using the `setupcommonservice` command. Instead, delete the product instance in the Hitachi Ops Center Portal.

### Next steps

- If you must register products in Common Services, go to the next section.
- If you do not need to register products in Common Services, go to [Logging in to the Hitachi Ops Center Portal \(on page 33\)](#).

## Registering Ops Center products with Common Services (*setupcommonservice*)

Use the `setupcommonservice` command to register Ops Center products with Common Services.

### Before you begin

- Ensure that each product can resolve the host name where Common Services is installed. If you want to use a host name that is not a fully qualified domain name (FQDN), set the IP address and the host name in the `/etc/hosts` file for name resolution. If you want to use an IP address instead of a host name, log in to the management server where Common Services is installed and run the `cschgconnect.sh` command.
- Ensure that the Ops Center product server and the Common Services server are running.
- Use a Common Services account with the "Application Administrator" role to run `setupcommonservice` command.



**Note:** Products deployed by using the Ops Center OVA are already registered in Common Services.

If you change the Common Services host name, IP address, or server port number changes, you must register each product again.

The `setupcommonservice` command also sets each Ops Center product as an authentication server that uses Common Services. You can then access the application from the portal using the Ops Center credentials.

## Administrator

Default location: /opt/rainier/bin

Command syntax:

```
setupcommonservice --csUri CommonService_URL --applicationPort port_number --  
applicationHostAddress ip_address --applicationName app_name [--appDescription  
app_description] [--csUsername CommonService_Username] [--tlsVerify --csUriCACert  
Certificate_FileName]
```

Command example:

```
setupcommonservice --csUri https://example.com/portal --csUsername sysadmin --  
tlsVerify --csUriCACert certificate.cer --applicationPort 20961 --  
applicationHostAddress 192.0.2.11 --applicationName MyAdministrator1
```

## Protector

Default location: /opt/hitachi/protector/bin/

Command syntax:

```
setupcommonservice --cs-uri CommonService_URL [--cs-username CommonService_Username] -  
-app-scheme protocol --app-hostname host_name --app-port port_number
```

Command example:

```
setupcommonservice --cs-uri https://example.com/portal --cs-username sysadmin --app-  
scheme https --app-hostname MyHost --app-port 20964
```

## Automator

### For Linux:

Default location: /opt/hitachi/Automation/bin/

Command syntax:

```
setupcommonservice {[-csUri CommonService_URL | -csUri CommonService_URL -csUsername  
CommonServiceUsername] [-appName app_name] [-appDescription app_description] [-auto]  
| -help}
```

Command example:

```
setupcommonservice -csUri https://example.com/portal -appName MyAutomator1
```

### For Windows:

Default location: *Program-Files-folder*\hitachi\Automation\bin

**Command syntax:**

```
setupcommonservice {[/csUri CommonService_URL | /csUri CommonService_URL /csUsername  
CommonServiceUsername] [/appName app_name] [/appDescription app_description] [/auto]  
| /help}
```

**Command example:**

```
setupcommonservice /csUri https://example.com/portal /appName MyAutomator1
```

**Analyzer**

**Default location:** /opt/hitachi/Analytics/bin/

**Command syntax:**

```
setupcommonservice -csUri CommonService_URL [-csUsername CommonService_Username] [-  
appPort port_number] [-appHostname ip_address_or_host_name] [-appName app_name] [-  
appDescription app_description] [-auto]
```

**Command example:**

```
setupcommonservice -csUri https://example.com/portal -appPort 22016 -appHostname  
192.0.2.10 -appName MyAnalyzer1
```

**Analyzer detail view**

**Default location:** /usr/local/megha/bin/

**Command syntax:**

```
setupcommonservice -csUri CommonService_URL -csUsername CommonService_Username -  
appHostname ip_address_or_host_name -appPort port_number -appName app_name -  
appDescription app_description
```

**Command example:**

```
setupcommonservice -csUri https://example.com/portal -csUsername sysadmin -  
appHostname MyHost -appPort 8443 -appName MyAnalyzerdetailview1 -appDescription ""
```

**Analyzer probe**

**Default location:** /usr/local/megha/bin/

**Command syntax:**

```
setupcommonservice -csUri CommonService_URL -csUsername CommonService_Username -  
appHostname ip_address_or_host_name -appPort port_number -appName app_name -  
appDescription app_description
```

Command example:

```
setupcommonservice -csUri https://example.com/portal -csUsername sysadmin -
appHostname MyHost -appPort 8443 -appName MyAnalyzerprobel -appDescription ""
```

### Analyzer viewpoint

Default location: /opt/hitachi/analyzer\_viewpoint/bin/

Command syntax:

```
setupcommonservice --csUri CommonService_URL [--csUsername CommonServiceUsername] [--
applicationName app_name]
```

Command example:

```
setupcommonservice --csUri https://example.com
```

## Logging in to the Hitachi Ops Center Portal

Log in to the Hitachi Ops Center Portal from your browser.

### Before you begin

To avoid issues with windows not displaying correctly, configure your browser settings as follows:

- Accept cookies, or register the portal URL as a trusted site.
- Enable active scripting in the security settings.

### Procedure

1. In a web browser, access the following URL:

`https://host-name-or-IP-address-of-Portal:port-number/portal/`

The default port number is 443.



**Tip:** By default, you can access the Hitachi Ops Center Portal by using both the host name and IP address. To change the settings so that users can only access the Portal by using the host name, or to change the host name or IP address used to access the Hitachi Ops Center Portal, use the **cschgconnect** command. For details about the **cschgconnect** command, see [Changing the management server host name, IP address, or port number \(on page 115\)](#).

2. Use the following built-in account to log in:

User name: sysadmin

Password: sysadmin

The Hitachi Ops Center Portal main window opens.

**Note:**

- For security, be sure to change the password of the built-in account.
- If you want to log in to the Portal by using the IP address, specify the settings so that the management server host name can also be resolved from client machines.

## Configuring initial settings in the Hitachi Ops Center Portal

After using an OVA to deploy a Hitachi Ops Center product, you must configure the following settings in the Hitachi Ops Center Portal.

Configure the following required settings:

- Apply the product licenses.

You must apply the product licenses before using the products.

- Create users and configure settings for user groups.

You must configure settings to control access to the Hitachi Ops Center Portal.

Configure the following settings as needed:

- Link with an Active Directory, LDAP, or identity provider server.

For Active Directory and LDAP, see [Linking with an Active Directory or LDAP server \(on page 13\)](#). For identity providers, see [Linking with an identity provider \(on page 14\)](#).

- Configure the password policy.

Based on your security requirements, you can configure user account password complexity and controls for locking user accounts after consecutive failed authentication attempts.

- Configure the warning banner for the Hitachi Ops Center Portal.

You can display a message on the login window of the Hitachi Ops Center Portal.

For configuration details, see the Hitachi Ops Center Portal Help.

## Installing OS updates and other products after deployment

The following table outlines the installation tasks for an operating system patch or for Hitachi Ops Center products in an environment in which the OVA is deployed.

Task	Implementation method
Apply operating system patches	Apply as needed.
Update the operating system	You can update the OS as described in <a href="#">Applying Linux security updates using yum (on page 128)</a> .

Task	Implementation method
Upgrade of OSS	<p>"Requests" incorporated in the VM image is set for the sample code of Hitachi Ops Center API Configuration Manager. If a vulnerability is found in "Requests", upgrade all of them. For details, see the <i>Hitachi Ops Center API Configuration Manager Release Notes</i>.</p>
Install additional Hitachi Ops Center products	<p>To install other Hitachi Ops Center products that are not installed on a virtual machine to which the OVA is deployed, install the products by using the installation media. Confirm the system requirements of the products, install prerequisite packages, and reconfigure kernel parameters as necessary. For details on the product system requirements, see the documentation or Release Notes for each product.</p>

---

## Chapter 3: Installing or upgrading Hitachi Ops Center products by using the Express installer

You can simultaneously install or upgrade multiple Hitachi Ops Center products by using the Express installers.

Depending on which products you want to install, you can use the Server Express installer and the Client Express installer. For details, see [Using the Server Express installer \(on page 36\)](#) or [Using the Client Express installer \(on page 53\)](#).

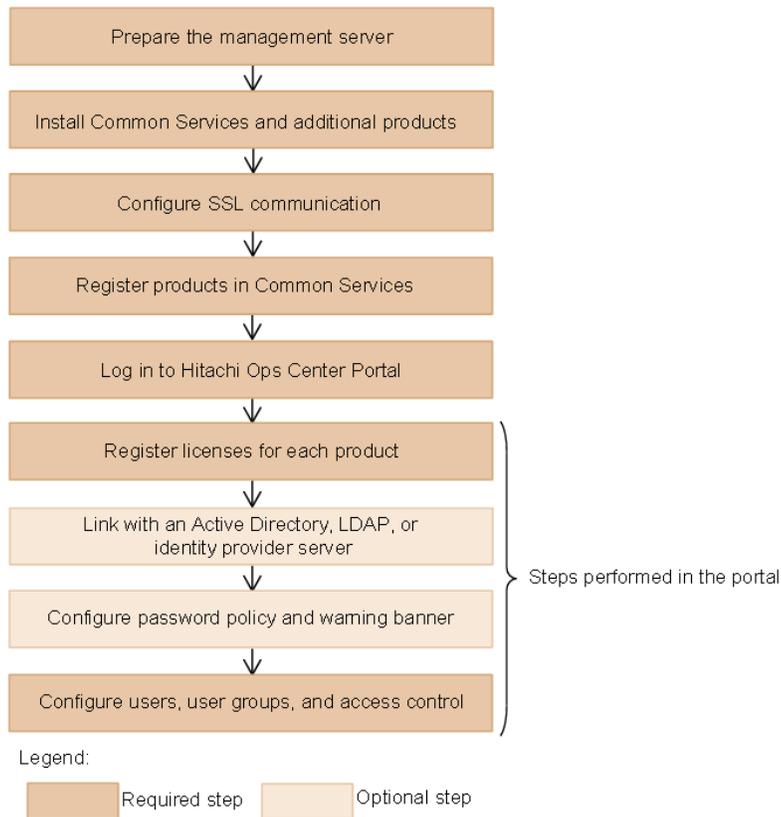
### Using the Server Express installer

Using the Server Express installer, you can simultaneously install or upgrade the following products:

- Hitachi Ops Center Common Services
- Hitachi Ops Center Administrator
- Hitachi Ops Center API Configuration Manager
- Hitachi Ops Center Protector
- Hitachi Ops Center Automator
- Hitachi Ops Center Analyzer
- Hitachi Ops Center Analyzer detail view
- Hitachi Ops Center Analyzer viewpoint

### Workflow for installing and setting up Hitachi Ops Center

The following figure shows the workflow for using the Server Express installer.



After setting up access control, configure the settings for each product as necessary. For details, see the documentation for each product.

If you are upgrading, the previous settings are preserved. If you upgrade Hitachi Ops Center products that were registered in Common Services, you do not need to configure SSL communication or perform the subsequent steps.

## Preparing the management server

Make sure that the management server on which you plan to install Hitachi Ops Center products meets the system requirements.

For the Common Services system requirements, see the Common Services Release Notes. For the system requirements of other Hitachi Ops Center products, see the documentation or Release Notes for each product.

For a complete list of Hitachi Ops Center system requirements, go to the [Ops Center documentation site](#) and select Get Started with Ops Center > Hitachi Ops Center system requirements.



**Note:**

- Hitachi Ops Center does not support installing other software products on the management server, but allows for installing software required by corporate policy such as anti-virus programs and third-party monitoring agents. Note that Hitachi Vantara does not take responsibility for or support any interactions between the third-party programs and the Hitachi Ops Center software.
- When Common Services is installed, the following RPM packages are installed:
  - Amazon Corretto 17
  - PostgreSQL 11
- Common Services starts the Common Services service by using the postgres user and postgres group created on the management server.

Configurations where postgres users and postgres groups do not exist on the management server are not supported.

If the users on the management server are managed by an external authentication server, the Common Services service cannot start when the OS starts.

Make sure that you complete the following actions on the installation destination management server:

- Specify the repository settings for the `yum` command because the Server Express installer uses the `yum` command to install prerequisite packages. For details, see the documentation for the relevant OS.
- Administrator requires a supported version of container runtime as follows:
  - Docker (for Red Hat Enterprise Linux 7 or Oracle Linux 7)  
Install Docker in advance.
  - Podman (for Red Hat Enterprise Linux 8 or Oracle Linux 8)

If a supported version of Podman is not installed on the management server, it is installed from the repository by using the `yum` command when Administrator is installed. Configure the repository settings in advance so that the package can be installed over the network. For the installation method, see the Administrator manual.



**Note:** If you run the Server Express installer, the `iptables` and `firewalld` settings are changed so that required communications can be established. If you use `nftables`, you must make the changes manually.

## Installing or upgrading Common Services and additional products

To install or upgrade Common Services and one or more products, use the Server Express installer.

**Before you begin**

- For best results, close all other programs, including:
  - Security-monitoring programs
  - Virus-detection programs
  - Process-monitoring programs

If the Services window is open, close it.

- In Common Services version 10.9.1 and later versions, a special group named support-services has been added as a default user group. This group is used for support services, so it cannot be used for standard purposes. For this reason, if you want to upgrade from version 10.9.0 or earlier, first make sure that the support-services group has not been created.
  - If the support-services group was imported by linking with an Active Directory server, delete the group. In addition, from the Hitachi Ops Center Portal, change the Group entry list setting for user directories so that the support-services group will not be imported.
  - If the system administrator created the support-services group using a method other than linking with an Active Directory server, delete or rename the group before upgrading from version 10.9.0 or earlier.



**Note:** If you upgrade Common Services from version 10.9.0 or earlier while the support-services group exists, you must delete or rename the support-services group and then perform an overwrite installation of Common Services.

**Procedure**

1. Log in to the management server as the root user.  
If you log in as an ordinary user, use the `sudo` command to complete the following procedure as the root user.
2. To start the Server Express installer, run `install.sh`, which is in the following location in the installation media:
 

```
root-directory-of-the-installation-media/install.sh
```
3. Choose the product you want to install, and then press **Enter**.  
To select multiple products, separate the numbers with commas. (Example: 2,3)
4. When performing a new installation of Analyzer, set the memory size by choosing one of the following scale values:
  - 1: Small-scale configuration
  - 2: Medium-scale configuration
  - 3: Large-scale configuration



**Note:** For details on the system requirements for each product according to the scale, see *Hitachi Ops Center System Requirements*.

5. Follow the prompts and specify the required information.

For Common Services:

Setting items	Description
Install directory	<p>For a new installation:</p> <ul style="list-style-type: none"> <li>Specify the directory in which to install Common Services.</li> </ul> <p>Common Services will be installed in the following directory:</p> <pre>specified-directory/CommonService</pre> <p>The default installation destination for Common Services is as follows:</p> <pre>/opt/hitachi/CommonService</pre> <ul style="list-style-type: none"> <li>Specify a directory by using 64 or fewer bytes and by using only the following characters: A-Z, a-z, 0-9, underscores (<code>_</code>), and forward slashes (<code>/</code>)</li> </ul> <div style="background-color: #e0f2f1; padding: 10px; border: 1px solid #ccc;"> <p> <b>Note:</b> You cannot specify the following directories:</p> <ul style="list-style-type: none"> <li><code>/usr</code></li> <li><code>/usr/local</code></li> <li><code>/var</code></li> <li>root directory (<code>/</code>)</li> </ul> </div>
Host name or IP address	<p>For a new installation:</p> <ul style="list-style-type: none"> <li>You can specify a host name in FQDN format.</li> <li>The host name (or FQDN) or IP address specified in this step is used in the URL for accessing the Hitachi Ops Center Portal. To change the host name (or FQDN) or IP address that is used to access the Hitachi Ops Center Portal, run the <code>cschgconnect</code> command after installation. For details about the <code>cschgconnect</code> command, see <a href="#">Changing the management server host name, IP address, or port number (on page 115)</a>.</li> <li>The management server on which Common Services and other relevant products are installed and the web browser used to access the Hitachi Ops Center Portal must be able to resolve and reach the host name (or FQDN) and IP address.</li> </ul>

Setting items	Description
	<ul style="list-style-type: none"> <li>▪ If you specify a host name (or FQDN), specify a value using no more than 128 characters.</li> <li>▪ You cannot specify uppercase characters in the host name (or FQDN). If you do, they are converted to lowercase characters and then registered.</li> </ul>
Port number	<p>For a new installation:</p> <ul style="list-style-type: none"> <li>▪ Specify a value in the range 1 - 65535.</li> <li>▪ Default: 443</li> </ul> <p>If you install the following products on the same management server, there will be conflicts with the default port number 443:</p> <ul style="list-style-type: none"> <li>• Hitachi Ops Center Protector</li> <li>• Hitachi Ops Center Administrator</li> </ul> <p>Change the port number so that it does not conflict between the products. If you want to change the port number for Common Services to a number other than 443, we recommend using port number 20950.</p>
Do you want to access to Ops Center Portal by using both host name and IP address ?	<p>For a new installation where a host name or FQDN is specified:</p> <ul style="list-style-type: none"> <li>▪ Specify y or n.</li> <li>▪ Default: n</li> </ul>
Do you want to back up the Common Services database first ?	<p>For an upgrade or overwrite installation:</p> <ul style="list-style-type: none"> <li>▪ Specify y or n.</li> <li>▪ Default: y</li> </ul>
Database backup location	<p>For an upgrade or overwrite installation where you want to back up the database:</p> <ul style="list-style-type: none"> <li>▪ Specify a destination by using no more than 150 bytes and only the following characters: A-Z, a-z, 0-9, underscores (<code>_</code>), and forward slashes (<code>/</code>)</li> </ul> <div style="border: 1px solid #ccc; background-color: #e0f2f1; padding: 5px; margin: 10px 0;"> <p> <b>Note:</b> You cannot specify the root directory (<code>/</code>).</p> </div> <ul style="list-style-type: none"> <li>▪ Default: <code>/var/installation-directory/backup</code></li> </ul>

Setting items	Description
Admin user name	<p>For a new installation of another product when Common Services has already been installed:</p> <p>Specify the username of the Common Services administrator.</p> <p>Specify a user who belongs to the user group to which the opscenter-system-administrator or the opscenter-security-administrator role is assigned.</p>
Password	<p>For a new installation of another product when Common Services has already been installed:</p> <p>Specify the password of the Common Services administrator.</p>

For Administrator:

Setting items	Description
IP address	<p>For a new installation:</p> <ul style="list-style-type: none"> <li>▪ Specify a value in IPv4 format.</li> <li>▪ Default: IP address of the system</li> </ul>
Port number	<p>For a new installation:</p> <ul style="list-style-type: none"> <li>▪ Specify a value in the range 1 - 65535.</li> <li>▪ Default: 20961</li> </ul>
User name	<p>For an upgrade installation:</p> <p>Default: sysadmin</p>
Password	<p>For an upgrade installation:</p> <p>Default: None</p>

For API Configuration Manager:

Setting items	Description
Install directory	<p>For a new installation:</p> <ul style="list-style-type: none"> <li>Specify the directory in which to install API Configuration Manager: <i>specified-directory/ConfManager</i></li> </ul> <p>The default installation destination for API Configuration Manager is as follows: <i>/opt/hitachi/ConfManager</i></p> <ul style="list-style-type: none"> <li>Specify a directory by using 64 or fewer bytes and by using only the following characters: A-Z, a-z, 0-9, underscores (<code>_</code>), and forward slashes (<code>/</code>)</li> </ul> <div style="background-color: #e0f2f1; padding: 10px; border: 1px solid #ccc;"> <p> <b>Note:</b> You cannot specify the following directories:</p> <ul style="list-style-type: none"> <li><code>/usr</code></li> <li><code>/usr/local</code></li> <li><code>/var</code></li> <li>root directory (<code>/</code>)</li> </ul> </div>
Do you want to back up the API Configuration Manager database first ?	<p>For an upgrade installation:</p> <ul style="list-style-type: none"> <li>Specify y or n.</li> <li>Default: y</li> </ul>

Setting items	Description
Database backup location	<p>For an upgrade installation where you want to back up the database:</p> <ul style="list-style-type: none"> <li>Specify a destination by using no more than 64 bytes and only the following characters: A-Z, a-z, 0-9, underscores (<code>_</code>), and forward slashes (<code>/</code>)</li> </ul> <div style="background-color: #e0f2f1; padding: 10px; border: 1px solid #ccc;"> <p> <b>Note:</b> You cannot specify the following directories:</p> <ul style="list-style-type: none"> <li><code>/usr</code></li> <li><code>/usr/local</code></li> <li><code>/var</code></li> <li>root directory (<code>/</code>)</li> </ul> </div> <ul style="list-style-type: none"> <li><b>Default:</b> <code>specified-directory/backup/bak_CONFIG_MGR</code></li> </ul>

For Protector:

Setting items	Description
Install directory	<p>For a new installation:</p> <p>Specify the directory in which to install Protector: <code>specified-directory/protector</code></p> <p>The default installation destination for Protector is as follows: <code>/opt/hitachi/protector</code></p>
Node name	<p>For a new installation:</p> <p>Default: Node name of the operating system</p>
User account on the local system	<p>For a new installation:</p> <p>Default: root</p>
Port number	<p>For a new installation:</p> <p>Default: 20964</p>

For Automator:

Setting items	Description
Install directory	<p>For a new installation:</p> <ul style="list-style-type: none"> <li>Specify the directory in which to install Automator. Automator will be installed in the following directory: <code>specified-directory/Automation</code></li> </ul> <p>The default installation destination for Automator is as follows: <code>/opt/hitachi/Automation</code></p> <ul style="list-style-type: none"> <li>Specify a directory by using 64 or fewer bytes and by using only the following characters: A-Z, a-z, 0-9, underscores (<code>_</code>), and forward slashes (<code>/</code>)</li> </ul> <div style="background-color: #e0f2f1; padding: 10px; border: 1px solid #ccc;"> <p> <b>Note:</b> You cannot specify the following directories:</p> <ul style="list-style-type: none"> <li><code>/usr</code></li> <li><code>/usr/local</code></li> <li><code>/var</code></li> <li>root directory (<code>/</code>)</li> </ul> </div>
Host name or IP address	<p>For a new installation:</p> <p>If you specify a host name specify a value using no more than 128 characters.</p>
Database directory	<p>For a new installation:</p> <ul style="list-style-type: none"> <li>Specify a directory by using 90 or fewer bytes and by using only the following characters: A-Z, a-z, 0-9, underscores (<code>_</code>), and forward slashes (<code>/</code>)</li> </ul> <div style="background-color: #e0f2f1; padding: 10px; border: 1px solid #ccc;"> <p> <b>Note:</b> You cannot specify the root directory (<code>/</code>).</p> </div> <ul style="list-style-type: none"> <li>Default: <code>/var/specified-directory/database</code></li> </ul>
Do you want to back up the Automator database first ?	<p>For an upgrade or overwrite installation:</p> <ul style="list-style-type: none"> <li>Specify y or n.</li> <li>Default: y</li> </ul>

Setting items	Description
Database backup location	<p>For an upgrade or overwrite installation where you want to back up the database:</p> <ul style="list-style-type: none"> <li>Specify a destination by using no more than 150 bytes and only the following characters: A-Z, a-z, 0-9, underscores (<code>_</code>), and forward slashes (<code>/</code>)</li> </ul> <p> <b>Note:</b> You cannot specify the root directory (<code>/</code>).</p> <ul style="list-style-type: none"> <li>Default: <code>/var/specified-directory/Automation_backup</code></li> </ul>

For Analyzer:

Setting items	Description
Install directory	<p>For a new installation:</p> <ul style="list-style-type: none"> <li>Specify the directory in which to install Analyzer: <code>specified-directory/Analytics</code></li> </ul> <p>The default installation destination for Analyzer is as follows: <code>/opt/hitachi/Analytics</code></p> <ul style="list-style-type: none"> <li>If you specify a directory other than the default, refer to the product manual for the requirements.</li> </ul>

For Analyzer detail view:

Setting items	Description
Installation-destination device	<p>For a new installation:</p> <ul style="list-style-type: none"> <li>A list of devices on the management server is displayed.</li> </ul> <p>Default: Devices with enough free space for the installation are displayed.</p> <ul style="list-style-type: none"> <li>If you want to use a device other than the default, specify a device name from the displayed list.</li> </ul>

Setting items	Description
Directory for storing application data	<p>For a new installation:</p> <ul style="list-style-type: none"> <li>Specify the directory where the application data will be stored.</li> </ul> <p>The default storage destination is <code>/data</code>.</p> <ul style="list-style-type: none"> <li>If you specify a directory other than the default, refer to the product manual for the requirements.</li> </ul>
HTTP access port for internal communication	<p>For a new installation:</p> <p>If port number 8080 is being used by another program, specify a value from 10000 to 65530.</p>
HTTPS access port	<p>For a new installation:</p> <p>If port number 8443 is being used by another program, specify a value from 10000 to 65530.</p>

For Analyzer viewpoint:

Setting items	Description
HTTPS access port for internal communication	If port number 25442 is being used by another program, specify a value from 1 to 65535.

**6.** Check the information you entered and the message that appears.

If both API Configuration Manager and Protector are included as products to be installed, a message related to Command Control Interface might appear. Check the message and then start the installation processing.

If there are no problems, press **y** to begin the installation.

**7.** When the installation is complete, the results are displayed:

- If all installation tasks finished successfully, **Completed successfully.** is displayed.
- If any task fails, **Failed.** is displayed.

**Note:**

- If registration with Common Services displays a **Failed.** status, you must register the product manually after the installer completes. For details, see [Registering products in Common Services \(on page 48\)](#).
- When it takes a long time to install Automator, a KNAE04747-E message might be output to the console even if the installation is successfully done. If "Hitachi Ops Center Automator installation completed successfully." is output after the KNAE04747-E message, the installation processing might have completed successfully. After waiting for a while, check if the Automator service is running, and then log in to Automator. If the Automator service is stopped, start the Automator service and log in to Automator. If the login is successful, the installation processing has completed, and you can ignore the KNAE04747-E message.

## Configuring SSL communications

By default, Common Services uses SSL/TLS communications. Immediately after installation, the system uses SSL communication by using a self-signed certificate. However, you must set up SSL communications to use a valid server certificate before any of the products can communicate with Common Services and the Hitachi Ops Center Portal.

For details on how to configure SSL communications, see [Configuring SSL communications \(on page 72\)](#).

### Next steps

When you finish configuring SSL communications, return to this chapter and go to the next section.

## Registering products in Common Services

To use the functions provided by Common Services, you must register products in Common Services.

Products installed by using the Server Express installer can be registered during installation. In the following cases, you must run the `setupcommonservice` command for each product:

- You did not register the product during installation.
- The product registration failed.
- You installed a product separately.



**Note:** You cannot unregister a Hitachi Ops Center product using the `setupcommonservice` command. Instead, delete the product instance in the Hitachi Ops Center Portal.

### Next steps

- If you must register products in Common Services, go to the next section.
- If you do not need to register products in Common Services, go to [Logging in to the Hitachi Ops Center Portal \(on page 51\)](#).

## Registering Ops Center products with Common Services (setupcommonservice)

Use the `setupcommonservice` command to register Ops Center products with Common Services.

### Before you begin

- Ensure that each product can resolve the host name where Common Services is installed. If you want to use a host name that is not a fully qualified domain name (FQDN), set the IP address and the host name in the `/etc/hosts` file for name resolution. If you want to use an IP address instead of a host name of the Ops Center portal without changing your DNS setting, log in to the server where the Ops Center portal is installed and run the `cschgconnect.sh` command.
- Ensure that the Ops Center product server and the Common Services server are running.
- Use a Common Services account with the "Application Administrator" role to run `setupcommonservice` command.



**Note:** You do not need to manually register products deployed by using the Ops Center OVA or the Server Express installer.

If you change the Common Services host name, IP address, or server port number changes, you must register each product again.

The `setupcommonservice` command also sets each Ops Center product as an authentication server that uses Common Services. You can then access the application from the portal using the Ops Center credentials.

### Administrator

Default location: `/opt/rainier/bin`

Command syntax:

```
setupcommonservice --csUri CommonService_URL --applicationPort port_number --  
applicationHostAddress ip_address --applicationName app_name [--appDescription  
app_description] [--csUsername CommonService_Username] [--tlsVerify --csUriCACert  
Certificate_FileName]
```

Command example:

```
setupcommonservice --csUri https://example.com/portal --csUsername sysadmin --  
tlsVerify --csUriCACert certificate.cer --applicationPort 20961 --  
applicationHostAddress 192.0.2.11 --applicationName MyAdministrator1
```

## Protector

Default location: /opt/hitachi/protector/bin/

Command syntax:

```
setupcommonservice --cs-uri CommonService_URL [--cs-username CommonService_Username] -  
-app-scheme protocol --app-hostname host_name --app-port port_number
```

Command example:

```
setupcommonservice --cs-uri https://example.com/portal --cs-username sysadmin --app-  
scheme https --app-hostname MyHost --app-port 20964
```

## Automator

Default location: /opt/hitachi/Automation/bin/

Command syntax:

```
setupcommonservice {[-csUri CommonService_URL | -csUri CommonService_URL -csUsername  
CommonServiceUsername] [-appName app_name] [-appDescription app_description] [-auto]  
| -help}
```

Command example:

```
setupcommonservice -csUri https://example.com/portal -appName MyAutomator1
```

## Analyzer

Default location: /opt/hitachi/Analytics/bin/

Command syntax:

```
setupcommonservice -csUri CommonService_URL [-csUsername CommonService_Username] [-  
appPort port_number] [-appHostname ip_address_or_host_name] [-appName app_name] [-  
appDescription app_description] [-auto]
```

Command example:

```
setupcommonservice -csUri https://example.com/portal -appPort 22016 -appHostname  
192.0.2.10 -appName MyAnalyzer1
```

## Analyzer detail view

Default location: /usr/local/megha/bin/

Command syntax:

```
setupcommonservice -csUri CommonService_URL -csUsername CommonService_Username -  
appHostname ip_address_or_host_name -appPort port_number -appName app_name -  
appDescription app_description
```

Command example:

```
setupcommonservice -csUri https://example.com/portal -csUsername sysadmin -
appHostname MyHost -appPort 8443 -appName MyAnalyzerdetailview1 -appDescription ""
```

### Analyzer viewpoint

Default location: /opt/hitachi/analyzer\_viewpoint/bin/

Command syntax:

```
setupcommonservice --csUri CommonService_URL [--csUsername CommonServiceUsername] [--
applicationName app_name]
```

Command example:

```
setupcommonservice --csUri https://example.com
```

## Logging in to the Hitachi Ops Center Portal

Log in to the Hitachi Ops Center Portal from your browser.

### Before you begin

To avoid issues with windows not displaying correctly, configure your browser settings as follows:

- Accept cookies, or register the portal URL as a trusted site.
- Enable active scripting in the security settings.

### Procedure

1. In a web browser, access the following URL:

```
https://host-name-or-IP-address-of-Portal:port-number/portal/
```

When entering the URL to access the portal, enter the host name or IP address and the port number that were specified during installation.

2. Use the following built-in account to log in:

User name: sysadmin

Password: sysadmin

The Hitachi Ops Center Portal main window opens.



**Note:** For security, be sure to change the password of the built-in account.

## Configuring initial settings in the Hitachi Ops Center Portal

After a new installation of a Hitachi Ops Center product, you must configure the following settings in the Hitachi Ops Center Portal.



**Note:** If you perform an upgrade installation, the previous settings will be inherited.

Configure the following required settings:

- Apply the product licenses.  
You must apply the product licenses before using the products.
- Create users and configure settings for user groups.  
You must configure settings to control access to the Hitachi Ops Center Portal.

Configure the following settings as needed:

- Link with an Active Directory, LDAP, or identity provider server.  
For Active Directory and LDAP, see [Linking with an Active Directory or LDAP server \(on page 13\)](#). For identity providers, see [Linking with an identity provider \(on page 14\)](#).
- Configure the password policy.  
Based on your security requirements, you can configure user account password complexity and controls for locking user accounts after consecutive failed authentication attempts.
- Configure the warning banner for the Hitachi Ops Center Portal.  
You can display a message on the login window of the Hitachi Ops Center Portal.

For configuration details, see the Hitachi Ops Center Portal Help.

## Installing OS updates and other products after installation

The following table outlines the installation tasks for operating system patches and Hitachi Ops Center updates where the installer is used.

Task	Implementation method
Apply operating system patches	Apply as needed.
Update the operating system	You can update the OS as described in <a href="#">Applying Linux security updates using yum (on page 128)</a> .
Upgrade Hitachi Ops Center products	For an upgrade installation or overwrite installation, use the express installer or product installer.
Install additional Hitachi Ops Center products	Confirm the system requirements of the products, install prerequisite packages, and reconfigure kernel parameters as necessary. For details on the product system requirements, see the documentation or Release Notes for each product.

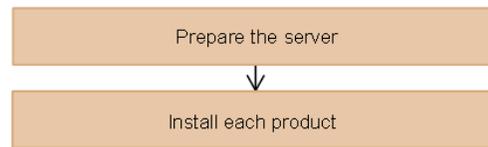
## Using the Client Express installer

Using the Client Express installer, you can simultaneously install or upgrade the following products:

- Hitachi Ops Center API Configuration Manager
- Hitachi Ops Center Protector Client
- Hitachi Ops Center Analyzer probe server

## Workflow for installing and setting up Hitachi Ops Center (Client Express installer)

The following figure shows the workflow for using the Client Express installer.



Legend:

 Required step

After installation is complete, configure the settings for each product as necessary. For details, see the documentation for each product.

## Preparing the server

Make sure that the server on which you plan to install Hitachi Ops Center products meets the system requirements that are described in the manual or Release Notes for each product.

Make sure that you complete the following actions on the installation destination:

- Specify the repository settings for the `yum` command because it is used to install prerequisite packages. For details, see the documentation for the relevant OS.
- When performing a new installation of the Analyzer probe server, do not install Analyzer detail view on the same server.



**Note:** If you run the Client Express installer, the `iptables` and `firewalld` settings are changed so that required communications can be established. If you use `nftables`, you must make the changes manually.

## Installing or upgrading each product

To install or upgrade each product, use the Client Express installer.

**Before you begin**

For best results, close all other programs, including:

- Security-monitoring programs
- Virus-detection programs
- Process-monitoring programs

If the Services window is open, close it.

**Procedure**

1. Log in to the server as the root user or use the `sudo` command.
2. To start the Client Express installer, run `install.sh`, which is in the following location in the installation media:

```
root-directory-of-the-installation-media/install.sh
```

3. Choose the product you want to install, and then press **Enter**.  
To select multiple products, separate the numbers with commas. (Example: 2,3)
4. Follow the prompts and specify the required information.

For API Configuration Manager:

Setting items	Description
Install directory	<p>For a new installation:</p> <ul style="list-style-type: none"> <li>▪ Specify the directory in which to install API Configuration Manager.</li> </ul> <p>API Configuration Manager will be installed in the following directory:</p> <pre><i>specified-directory/ConfManager</i></pre> <p>The default installation destination for API Configuration Manager is as follows:</p> <pre><i>/opt/hitachi/ConfManager</i></pre> <ul style="list-style-type: none"> <li>▪ Specify a directory by using 64 or fewer bytes and by using only the following characters: A-Z, a-z, 0-9, underscores (<code>_</code>), and forward slashes (<code>/</code>)</li> </ul> <div style="background-color: #e0f2f1; padding: 10px; border: 1px solid #ccc;"> <p> <b>Note:</b> You cannot specify the following directories:</p> <ul style="list-style-type: none"> <li>▪ <code>/usr</code></li> <li>▪ <code>/usr/local</code></li> <li>▪ <code>/var</code></li> <li>▪ root directory (<code>/</code>)</li> </ul> </div>

Setting items	Description
Whether backup is required	For an upgrade installation: <ul style="list-style-type: none"> <li>▪ Specify y or n.</li> <li>▪ Default: y</li> </ul>
Backup directory	If you selected y for the setting "Whether backup is required" for an upgrade installation: <ul style="list-style-type: none"> <li>▪ Specify the directory for the backup of the API Configuration Manager.                The API Configuration Manager is backed up in the following directory:  <code>specified-directory/backup/  bak_CONFIG_MGR</code>                The default backup destination for the API Configuration Manager is as follows:  <code>/opt/hitachi/backup/bak_CONFIG_MGR</code></li> <li>▪ Specify a directory by using 64 or fewer bytes and by using only the following characters:                A-Z, a-z, 0-9, underscores (<code>_</code>), and forward slashes (<code>/</code>)</li> </ul> <div style="background-color: #e0f2f1; padding: 10px; border: 1px solid #ccc;"> <p> <b>Note:</b> You cannot specify the following directories:</p> <ul style="list-style-type: none"> <li>▪ <code>/usr</code></li> <li>▪ <code>/usr/local</code></li> <li>▪ <code>/var</code></li> <li>▪ root directory (<code>/</code>)</li> </ul> </div>

For Protector Client:

Setting items	Description
Install directory	<p>For a new installation:</p> <ul style="list-style-type: none"> <li>Specify the directory in which to install Protector Client.</li> </ul> <p>Protector Client will be installed in the following directory:</p> <pre>specified-directory/protector</pre> <p>The default installation destination for Protector Client is as follows:</p> <pre>/opt/hitachi/protector</pre> <ul style="list-style-type: none"> <li>Specify a directory by using 64 or fewer bytes and by using only the following characters: A-Z, a-z, 0-9, underscores (<code>_</code>), and forward slashes (<code>/</code>)</li> </ul> <div style="background-color: #e0f2f1; padding: 10px; border: 1px solid #ccc;"> <p> <b>Note:</b> You cannot specify the following directories:</p> <ul style="list-style-type: none"> <li><code>/usr</code></li> <li><code>/usr/local</code></li> <li><code>/var</code></li> <li>root directory (<code>/</code>)</li> </ul> </div>
Node name	<p>For a new installation:</p> <p>Default: Node name of the operating system</p>
Master node name	<p>For a new installation:</p> <p>Specify the node name or IP address of the master OS.</p>
Internet connected	<p>For a new installation:</p> <p>Select whether to install a client node as a node connected to the internet.</p> <ul style="list-style-type: none"> <li>Specify y or n.</li> <li>Default: n</li> </ul>

For Analyzer probe server:

Setting items	Description
Application data path	<p>For a new installation:</p> <ul style="list-style-type: none"> <li>Specify the directory where the application data will be stored.</li> </ul> <p>The default storage destination is <code>/home</code>.</p> <ul style="list-style-type: none"> <li>If you specify a directory other than the default, refer to the product manual for the requirements.</li> </ul>
HTTP access port for internal communication	<p>For a new installation:</p> <p>If port number 8080 is being used by another program, specify a value from 10000 to 65530.</p>
HTTPS access port	<p>For a new installation:</p> <p>If port number 8443 is being used by another program, specify a value from 10000 to 65530.</p>
Port used for the on-demand real time monitoring module	<p>For a new installation:</p> <p>If port number 24262 is being used by another program, specify a value from 10000 to 65530.</p>
Do you want to install the Virtual Storage Software Agent?	<p>If the Virtual Storage Software Agent is not installed:</p> <p>When you want to monitor the Virtual Storage Software block, you need to install the Virtual Storage Software Agent.</p> <ul style="list-style-type: none"> <li>Specify <code>y</code> or <code>n</code>.</li> <li>Default: <code>n</code></li> </ul>
Installation destination directory for the Virtual Storage Software Agent	<p>When installing the Virtual Storage Software Agent:</p> <ul style="list-style-type: none"> <li>Specify the installation destination directory for the Virtual Storage Software Agent:</li> </ul> <pre>specified-directory/ VirtualStorageSoftwareAgent</pre> <p>The default installation destination for the Virtual Storage Software Agent is as follows:</p> <pre>/opt/hitachi/ VirtualStorageSoftwareAgent</pre> <ul style="list-style-type: none"> <li>If you specify a directory other than the default, refer to the product manual for the requirements.</li> </ul>
IP address of the Analyzer server	<p>When installing the Virtual Storage Software Agent:</p>

Setting items	Description
	<p>The IP address specified here is used when configuring the firewall.</p> <ul style="list-style-type: none"> <li>▪ Specify a value in IPv4 format.</li> <li>▪ Default: IP address of the system</li> </ul>

5. Check the information you entered and the message that appears.

If both API Configuration Manager and Protector Client are included as products to be installed, a message related to Command Control Interface might appear. Check the message and then start the installation processing.

If there are no problems, press **y** to begin the installation.



**Note:** If you are installing Analyzer probe server, the following message might appear, but you can ignore the message.

```
root@localhost's password:
```

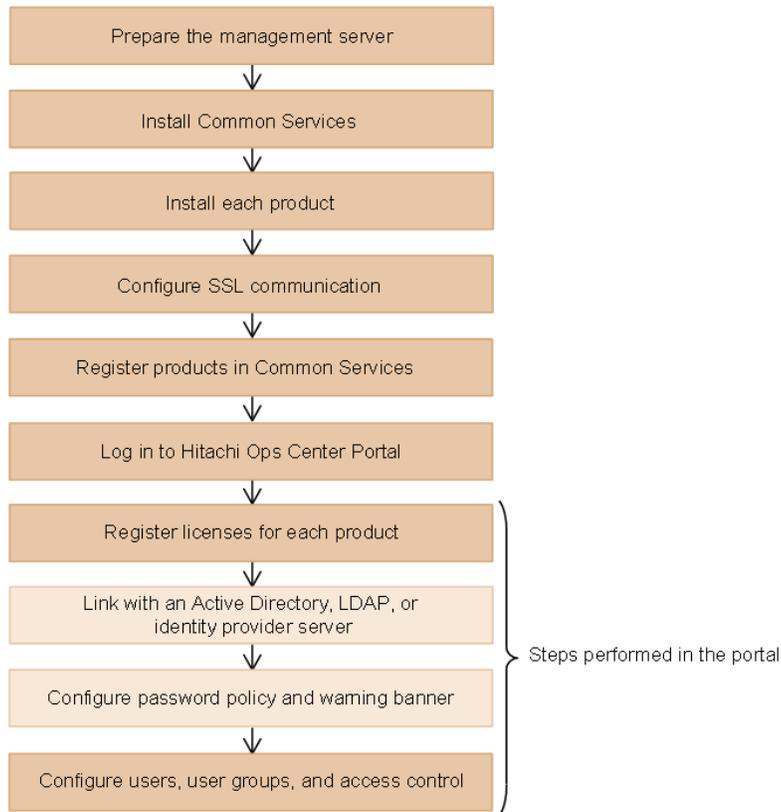
6. When the installation is complete, the results are displayed:
  - If all installation tasks finished successfully, **Completed successfully.** is displayed.
  - If any task fails, **Failed.** is displayed.

# Chapter 4: Installing or upgrading Hitachi Ops Center products by using the installer

To install or upgrade, or to create a new Hitachi Ops Center system without using the OVA, install the products by using the Common Services installer first and then install one or more products using the product installer.

## Workflow for installing and setting up Hitachi Ops Center

The general workflow for using the installer for each product is as follows:



After setting up access control, configure the settings for each product as necessary. For details, see the documentation for each product.

If you are upgrading, the previous settings are preserved. If you upgrade Hitachi Ops Center products that were registered in Common Services, you do not need to configure SSL communication or perform the subsequent steps.

## Preparing the management server

Make sure that the management server on which you plan to install Hitachi Ops Center products meets the system requirements.

For the Common Services system requirements, see the Common Services Release Notes. For the system requirements of other Hitachi Ops Center products, see the documentation or Release Notes for each product.

For a complete list of Hitachi Ops Center system requirements, go to the [Ops Center documentation site](#) and select Get Started with Ops Center > Hitachi Ops Center system requirements.



### Note:

- Hitachi Ops Center does not support installing other software products on the management server, but allows for installing software required by corporate policy such as anti-virus programs and third-party monitoring agents. Note that Hitachi Vantara does not take responsibility for or support any interactions between the third-party programs and the Hitachi Ops Center software.
- When Common Services is installed, the following RPM packages are installed:
  - Amazon Corretto 17
  - PostgreSQL 11

Common Services starts the Common Services service by using the postgres user and postgres group created on the management server.

Configurations where postgres users and postgres groups do not exist on the management server are not supported.

If the users on the management server are managed by an external authentication server, the Common Services service cannot start when the OS starts.

Make sure there are no conflicts among the following port numbers.

#### Port number used to access Common Services:

443/tcp (default)

#### Port numbers used for internal communication:

- 20951/tcp
- 20952/tcp
- 20954/tcp
- 20955/tcp
- 20956/tcp

If necessary, register the port number that is used to access Common Services in the firewall exceptions. For details on how to register firewall exceptions, see the OS documentation.

## Installing or upgrading Common Services

To install or upgrade Common Services in an existing environment or to create a Hitachi Ops Center system without using the OVA, install Common Services by using the installer.

**Note:**

- If you install Common Services version 10.9.2 or later, Amazon Corretto 17 is installed. If you upgrade Common Services, Amazon Corretto 8 (version 10.6.0 and earlier) and Amazon Corretto 11 (versions 10.6.1 to 10.9.1) that were installed with the previous version are not removed. If you no longer need Amazon Corretto 8 or Amazon Corretto 11, remove one or both by using the `rpm` command. If you cannot remove the program by using this command, use the `rpm` command with the `--noautoreun` option specified.

The package names are as follows:

- Amazon Corretto 8: `java-1.8.0-amazon-corretto-devel`
- Amazon Corretto 11: `java-11-amazon-corretto-devel`
- If the Analyzer viewpoint server was deployed by using a version of the OVF earlier than 10.5.1, you cannot use the installer to upgrade Common Services or Analyzer viewpoint on that server. In this case, deploy the newest version of the Analyzer viewpoint OVF to upgrade Analyzer viewpoint and Common Services.

For details on how to upgrade Analyzer viewpoint, see the Ops Center Analyzer documentation.

**Before you begin**

- Confirm that one of the following settings is configured on the management server installation destination:
  - The management server can access your DNS server.
  - The host name is set in the `hosts` file.

If the system cannot resolve the management server host name, it might take a long time for the Common Services to start.

- In Common Services version 10.9.1 and later versions, a special group named `support-services` has been added as a default user group. This group is used for support services, so it cannot be used for standard purposes. For this reason, if you want to upgrade from version 10.9.0 or earlier, first make sure that the `support-services` group has not been created.
  - If the `support-services` group was imported by linking with an Active Directory server, delete the group. In addition, from the Hitachi Ops Center Portal, change the Group entry list setting for user directories so that the `support-services` group will not be imported.
  - If the system administrator created the `support-services` group using a method other than linking with an Active Directory server, delete or rename the group before upgrading from version 10.9.0 or earlier.



**Note:** If you upgrade Common Services from version 10.9.0 or earlier while the `support-services` group exists, you must delete or rename the `support-services` group and then perform an overwrite installation of Common Services.

**Procedure**

1. Log in to the management server as the root user.  
If you log on as an ordinary user, use the `sudo` command to complete the following procedure as the root user.
2. Run `install.sh`, which is in the following location in the installation media:  
`root-directory-of-installation-media/COMSERV/install.sh`
3. To install Common Services, follow the prompts and specify the required information.  
You must specify the following information during installation:

**For new installations of Common Services:**

- Installation destination for Common Services
  - The default installation destination for Common Services is as follows:  
`/opt/hitachi/CommonService`
  - User data for Common Services is stored in the following user data directory:  
`/var/installation-directory-of-Common-Services`
- Host name (or FQDN) or IP address
  - The host name (or FQDN) or IP address specified in this step is used in the URL for accessing the Hitachi Ops Center Portal. To change the host name (or FQDN) or IP address that is used to access the Hitachi Ops Center Portal, run the `cschgconnect` command after installation. For details about the `cschgconnect` command, see [Changing the management server host name, IP address, or port number \(on page 115\)](#).
  - The management server on which Common Services and other relevant products are installed and the web browser used to access the Hitachi Ops Center Portal must be able to resolve and reach the host name (or FQDN) and IP address.
  - If you specify a host name (or FQDN), specify a value using no more than 128 characters.
  - You cannot specify uppercase characters in the host name (or FQDN). If you do, they are converted to lowercase characters and then registered.
- Port number of the access URL
 

If you install the following products on the same management server, there will be conflicts with the default port number 443. Change the port number so that it does not conflict between the products. If you want to change the port number for Common Services to a number other than 443, we recommend using port number 20950.

  - Hitachi Ops Center Protector (formerly Hitachi Data Instance Director)
  - Hitachi Ops Center Administrator
  - Hitachi Ops Center Analyzer viewpoint
- Whether access is possible by using an IP address
 

Specify whether an IP address can be used to access the Hitachi Ops Center Portal when a host name or FQDN is specified in the access URL.

  - To maintain the default setting of not permitting access by using an IP address, specify `y`.
  - To permit access by using an IP address, specify `n`.

An IP address acquired from the system is automatically set for the access URL.

**For overwrite or upgrade installations of Common Services:**

- Whether to back up the existing Common Services database
- If yes, the database backup destination
- If you are upgrading from version 10.9.1 or earlier, whether to continue or interrupt the installation when there is not enough free space on the disk

## Installing or upgrading each product

You install other products after you install Common Services. For details on the installation procedure, see the documentation for the individual product.

If you complete an upgrade or overwrite installation of an existing product, the installation destination is the same as the current installation destination.



**Note:** If you upgrade to Hitachi Ops Center Automator or Hitachi Ops Center Analyzer from a version earlier than 10.0, verify that SSL communication is configured.

## Configuring SSL communications

By default, Common Services uses SSL/TLS communications. Immediately after installation, the system uses SSL communication by using a self-signed certificate. However, you must set up SSL communications to use a valid server certificate before any of the products can communicate with Common Services and the Hitachi Ops Center Portal.

For details on how to configure SSL communications, see [Configuring SSL communications \(on page 72\)](#).

### Next steps

When you finish configuring SSL communications, return to this chapter and go to the next section.

## Registering products in Common Services

To use the functions provided by Common Services, you must register products in Common Services. When you use an individual installer to install each product, run the `setupcommonservice` command to register each product in Common Services.



**Note:** You cannot unregister a Hitachi Ops Center product using the `setupcommonservice` command. Instead, delete the product instance in the Hitachi Ops Center Portal.

### Next steps

- If you must register products in Common Services, go to the next section.
- If you do not need to register products in Common Services, go to [Logging in to the Hitachi Ops Center Portal \(on page 68\)](#).

## Registering Ops Center products with Common Services (setupcommonservice)

Use the `setupcommonservice` command to register Ops Center products with Common Services.

### Before you begin

- Ensure that each product can resolve the host name where Common Services is installed. If you want to use a host name that is not a fully qualified domain name (FQDN), set the IP address and the host name in the `/etc/hosts` file for name resolution. If you want to use an IP address instead of a host name, log in to the management server where Common Services is installed and run the `cschgconnect.sh` command.
- Ensure that the Ops Center product server and the Common Services server are running.
- Use a Common Services account with the "Application Administrator" role to run `setupcommonservice` command.



**Note:** Products deployed by using the Ops Center OVA are already registered in Common Services.

If you change the Common Services host name, IP address, or server port number changes, you must register each product again.

The `setupcommonservice` command also sets each Ops Center product as an authentication server that uses Common Services. You can then access the application from the portal using the Ops Center credentials.

### Administrator

Default location: `/opt/rainier/bin`

Command syntax:

```
setupcommonservice --csUri CommonService_URL --applicationPort port_number --  
applicationHostAddress ip_address --applicationName app_name [--appDescription  
app_description] [--csUsername CommonService_Username] [--tlsVerify --csUriCACert  
Certificate_FileName]
```

Command example:

```
setupcommonservice --csUri https://example.com/portal --csUsername sysadmin --  
tlsVerify --csUriCACert certificate.cer --applicationPort 443 --  
applicationHostAddress 192.0.2.11 --applicationName MyAdministrator1
```

## Protector

Default location: /opt/hitachi/protector/bin/

Command syntax:

```
setupcommonservice --cs-uri CommonService_URL [--cs-username CommonService_Username] -  
-app-scheme protocol --app-hostname host_name --app-port port_number
```

Command example:

```
setupcommonservice --cs-uri https://example.com/portal --cs-username sysadmin --app-  
scheme https --app-hostname MyHost --app-port 443
```

## Automator

### For Linux:

Default location: /opt/hitachi/Automation/bin/

Command syntax:

```
setupcommonservice {[-csUri CommonService_URL | -csUri CommonService_URL -csUsername  
CommonServiceUsername] [-appName app_name] [-appDescription app_description] [-auto]  
| -help}
```

Command example:

```
setupcommonservice -csUri https://example.com/portal -appName MyAutomator1
```

### For Windows:

Default location: *Program-Files-folder*\hitachi\Automation\bin

Command syntax:

```
setupcommonservice {[/csUri CommonService_URL | /csUri CommonService_URL /csUsername  
CommonServiceUsername] [/appName app_name] [/appDescription app_description] [/auto]  
| /help}
```

Command example:

```
setupcommonservice /csUri https://example.com/portal /appName MyAutomator1
```

## Analyzer

Default location: /opt/hitachi/Analytics/bin/

Command syntax:

```
setupcommonservice -csUri CommonService_URL [-csUsername CommonService_Username] [-  
appPort port_number] [-appHostname ip_address_or_host_name] [-appName app_name] [-  
appDescription app_description] [-auto]
```

Command example:

```
setupcommonservice -csUri https://example.com/portal -appPort 22016 -appHostname 192.0.2.10 -appName MyAnalyzer1
```

**Analyzer detail view**

Default location: /usr/local/megha/bin/

Command syntax:

```
setupcommonservice -csUri CommonService_URL -csUsername CommonService_Username -appHostname ip_address_or_host_name -appPort port_number -appName app_name -appDescription app_description
```

Command example:

```
setupcommonservice -csUri https://example.com/portal -csUsername sysadmin -appHostname MyHost -appPort 8443 -appName MyAnalyzerdetailview1 -appDescription ""
```

**Analyzer probe**

Default location: /usr/local/megha/bin/

Command syntax:

```
setupcommonservice -csUri CommonService_URL -csUsername CommonService_Username -appHostname ip_address_or_host_name -appPort port_number -appName app_name -appDescription app_description
```

Command example:

```
setupcommonservice -csUri https://example.com/portal -csUsername sysadmin -appHostname MyHost -appPort 8443 -appName MyAnalyzerprobel -appDescription ""
```

**Analyzer viewpoint**

Default location: /opt/hitachi/analyzer\_viewpoint/bin/

Command syntax:

```
setupcommonservice --csUri CommonService_URL [--csUsername CommonServiceUsername] [--applicationName app_name]
```

Command example:

```
setupcommonservice --csUri https://example.com
```

## Logging in to the Hitachi Ops Center Portal

Log in to the Hitachi Ops Center Portal from your browser.

### Before you begin

To avoid issues with windows not displaying correctly, configure your browser settings as follows:

- Accept cookies, or register the portal URL as a trusted site.
- Enable active scripting in the security settings.

### Procedure

1. In a web browser, access the following URL:

```
https://host-name-or-IP-address-of-Portal:port-number/portal/
```

When entering the URL to access the portal, enter the host name or IP address and the port number that were specified during installation.

2. Use the following built-in account to log in:

User name: `sysadmin`

Password: `sysadmin`

The Hitachi Ops Center Portal main window opens.



**Note:** For security, be sure to change the password of the built-in account.

## Configuring initial settings in the Hitachi Ops Center Portal

After a new installation of a Hitachi Ops Center product, you must configure the following settings in the Hitachi Ops Center Portal.



**Note:** If you perform an upgrade installation, the previous settings will be inherited.

Configure the following required settings:

- Apply the product licenses.  
You must apply the product licenses before using the products.
- Create users and configure settings for user groups.  
You must configure settings to control access to the Hitachi Ops Center Portal.

Configure the following settings as needed:

- Link with an Active Directory, LDAP, or identity provider server.

For Active Directory and LDAP, see [Linking with an Active Directory or LDAP server \(on page 13\)](#). For identity providers, see [Linking with an identity provider \(on page 14\)](#).

- Configure the password policy.

Based on your security requirements, you can configure user account password complexity and controls for locking user accounts after consecutive failed authentication attempts.

- Configure the warning banner for the Hitachi Ops Center Portal.

You can display a message on the login window of the Hitachi Ops Center Portal.

For configuration details, see the Hitachi Ops Center Portal Help.

## Installing OS updates and other products after installation

The following table outlines the installation tasks for operating system patches and Hitachi Ops Center updates where the installer is used.

Task	Implementation method
Apply operating system patches	Apply as needed.
Update the operating system	You can update the OS as described in <a href="#">Applying Linux security updates using yum (on page 128)</a> .
Upgrade Hitachi Ops Center products	For an upgrade installation or overwrite installation, use the express installer or product installer.
Install additional Hitachi Ops Center products	Confirm the system requirements of the products, install prerequisite packages, and reconfigure kernel parameters as necessary. For details on the product system requirements, see the documentation or Release Notes for each product.

---

## Chapter 5: Removing a Hitachi Ops Center product

To remove a Hitachi Ops Center environment or remove an unnecessary product after the OVA is deployed, use the product uninstaller. For details on how to remove products other than Common Services, see the documentation for the relevant product.

### Removing Common Services

Remove Common Services by performing the following procedure.



**Note:** If you remove Common Services, Amazon Corretto 17 and PostgreSQL 11 are not removed. If Common Services was upgraded from an earlier version, Amazon Corretto 8 (version 10.6.0 and earlier) and Amazon Corretto 11 (versions 10.6.1 to 10.9.1) might be installed on the management server. If you do not need these programs, remove them by using the `rpm` command. If you cannot remove the programs by using this command, use the `rpm` command with the `--no-preun` option specified.

The package name of each program is as follows:

- Amazon Corretto 17: `java-17-amazon-corretto-devel`
- PostgreSQL 11: `postgresql11`, `postgresql11-server`, `postgresql11-libs`
- Amazon Corretto 8: `java-1.8.0-amazon-corretto-devel`
- Amazon Corretto 11: `java-11-amazon-corretto-devel`

#### Before you begin

Before removing Common Services, complete the following:

- If necessary, back up the data.
- If any products are registered in Common Services, log in to the Hitachi Ops Center Portal, and delete all products.

#### Procedure

1. Log in to the management server as the root user.  
If you log in as an ordinary user, use the `sudo` command to complete the following procedure as the root user.
2. Move to the root directory.

3. Run the following command:

```
installation-directory-of-Common-Services/inst/uninstall.sh
```

---

## Chapter 6: Configuring SSL communications

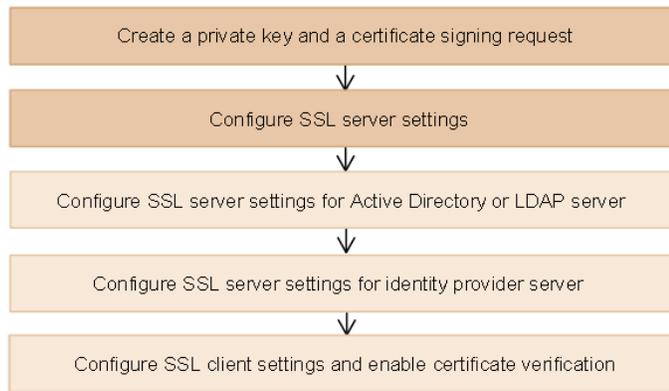
After installation, run the SSL Setup tool (`csslsetup` command) or manually perform the required procedures to configure SSL communications. By default, Common Services uses SSL/TLS communications by using a self-signed certification. So, you must set up SSL communications to use a valid server certificate.

You can use either of the following methods to configure SSL communications:

- To use the SSL setup tool (the `csslsetup` command) for each product, perform the procedure described in [Configuring SSL communications by using the SSL Setup tool \(on page 72\)](#).
- To configure SSL communications manually or use both RSA and Elliptic Curve Digital Signature Algorithm (ECDSA) as the public key encryption algorithms, perform the procedure described in [Configuring SSL communications without using the SSL Setup tool \(on page 83\)](#).

### Configuring SSL communications by using the SSL Setup tool

The following figure shows the workflow for configuring SSL communications by using the SSL Setup tool (`csslsetup` command).



Legend:



- The following Hitachi Ops Center products can be configured for SSL communications by using the `cssslsetup` command:
  - Hitachi Ops Center Common Services
  - Hitachi Ops Center Automator
  - Hitachi Ops Center Analyzer
  - Hitachi Ops Center Analyzer detail view
  - Hitachi Ops Center Analyzer viewpoint
  - Hitachi Ops Center Administrator
  - Hitachi Ops Center Protector (Master)
  - Hitachi Ops Center API Configuration Manager



**Note:**

- The `cssslsetup` command can be used for the version of each product specified in the Common Services Release Notes.
- If Hitachi Ops Center API Configuration Manager is installed by a user other than the root user, it is not displayed in the list and SSL communications cannot be configured. Configure the settings manually by referring to the Hitachi Ops Center API Configuration Manager manual.

- The `cssslsetup` command is located:
  - If Common Services is installed on the management server:  
*installation-directory-of-Common-Services/utility/bin*
  - If Common Services is not installed on the management server:  
Extract and use the files from `utility.tar`. Obtain this file either from the Common Services installation media or the Server Express installer media. The storage location is as follows:  
*root-directory-of-the-Common-Services-installation-media-or-root-directory-of-the-Server-Express-installer-media/utility.tar*  
The `cssslsetup` command is stored in the following location after the files are extracted from `utility.tar`:  
*directory-where-utility.tar-is-extracted/utility/bin*
- The following settings are not configured by the `cssslsetup` command:
  - Settings using both RSA and Elliptic Curve Digital Signature Algorithm (ECDSA) as public key encryption algorithms  
For details on how to set up such a configuration, see the procedure described in [Configuring SSL communications without using the SSL Setup tool \(on page 83\)](#).
  - Settings for storage systems and Active Directory, LDAP, and identity provider servers
  - Settings for the Analyzer probe server and Protector clients  
Configure these settings as necessary by referring to the manual for each product.

## SSL Setup tool functionality

The SSL Setup tool provides the following functions.

### Creating a private key and a certificate signing request (CSR)

The `cssslsetup` command creates a common private key and CSR that can be used by all products.



**Note:** This command only supports the RSA encryption algorithm. If you want to use both RSA and the Elliptic Curve Digital Signature Algorithm (ECDSA), perform the procedure described in [Configuring SSL communications without using the SSL Setup tool \(on page 83\)](#).

### Configuring the SSL server settings

The `cssslsetup` command configures the SSL server settings for the following:

Product	Settings
Common Services	Registers the server certificate and private key.

Product	Settings
Automator	<ul style="list-style-type: none"> <li>▪ Registers the server certificate and private key.</li> <li>▪ Enables SSL communications.</li> </ul>
Analyzer	<ul style="list-style-type: none"> <li>▪ Registers the server certificate and private key.</li> <li>▪ Enables SSL communications.</li> </ul>
Analyzer detail view	Imports the server certificate (in the PKCS#12 format) into the keystore.
Analyzer viewpoint	Registers the server certificate and private key.
Administrator	Registers the server certificate and private key.
Protector	Registers the server certificate and private key.
API Configuration Manager	<ul style="list-style-type: none"> <li>▪ Registers the server certificate and private key.</li> <li>▪ Configures notifications for storage system configuration changes.</li> </ul>

### Configuring the SSL client settings and enabling certificate verification

The `cssslsetup` command configures the SSL communication settings and enables certificate verification.

Product	Settings
Common Services	<ul style="list-style-type: none"> <li>▪ Imports the root certificate into the truststore.</li> <li>▪ Imports the root certificate of the server certificate for the Active Directory, LDAP, or an AD FS server into the truststore.</li> <li>▪ Enables certificate verification.</li> </ul>
Automator	<ul style="list-style-type: none"> <li>▪ Imports the root certificate into the truststore.</li> <li>▪ Imports the root certificate of the server certificate for the Active Directory server into the truststore.</li> <li>▪ Enables certificate verification.</li> </ul>
Analyzer	<ul style="list-style-type: none"> <li>▪ Imports the root certificate into the truststore.</li> <li>▪ Imports the root certificate of the server certificate for the Active Directory server into the truststore.</li> <li>▪ Enables certificate verification.</li> </ul>

Product	Settings
Analyzer detail view	<ul style="list-style-type: none"> <li>▪ Imports the root certificate into the truststore.</li> <li>▪ Imports the Active Directory server certificate into the truststore.</li> </ul> <div style="border: 1px solid #add8e6; background-color: #e0f7fa; padding: 10px; margin: 10px 0;"> <p> <b>Note:</b> To link with Active Directory, you must add an active directory user by using the Analyzer detail view.</p> </div> <ul style="list-style-type: none"> <li>▪ Enables certificate verification.</li> </ul> <div style="border: 1px solid #add8e6; background-color: #e0f7fa; padding: 10px; margin: 10px 0;"> <p> <b>Note:</b> If you want to use a certificate issued by a certificate authority for SSL communication for real time data collection, you must set the following Analyzer detail view server parameters in the <code>hosts</code> file on the management server to enable certificate verification:</p> <div style="border: 1px solid #add8e6; background-color: #f5f5f5; padding: 5px; margin: 5px 0; text-align: center;"> <code>IP-address hostname</code> </div> <p>For <i>hostname</i>, specify the value obtained by running the <code>hostname -f</code> command.</p> </div> <ul style="list-style-type: none"> <li>▪ Imports the server certificate of the RAID Agent server into the truststore (for on-demand real time monitoring).</li> </ul>
Analyzer viewpoint	<ul style="list-style-type: none"> <li>▪ Registers the trusted certificate into Analyzer viewpoint.</li> <li>▪ Enables certificate verification.</li> </ul>
Administrator	<p>None</p> <div style="border: 1px solid #add8e6; background-color: #e0f7fa; padding: 10px; margin: 10px 0;"> <p> <b>Note:</b></p> <ul style="list-style-type: none"> <li>▪ You must use the <code>setupcommonservice</code> command for the following tasks: <ul style="list-style-type: none"> <li>• Importing the root certificate into the truststore</li> <li>• Enabling certificate verification</li> </ul> </li> <li>▪ If you want to link with Active Directory, you must import the certificate of the Active Directory server into the truststore and register an Active Directory domain that uses the DNS server. For the configuration procedure, see the Administrator manual.</li> </ul> </div>

Product	Settings
Protector	Imports the root certificate into the truststore.   <b>Note:</b> You must use the <code>setupcommonservice</code> command to enable certificate verification.
API Configuration Manager	<ul style="list-style-type: none"> <li>▪ Specifies the certificate verification settings for storage systems.</li> <li>▪ Enables SSL communications.</li> </ul>

### Enabling or disabling certificate verification

You can enable or disable certificate verification for SSL communications maintenance.

## Creating a private key and a certificate signing request (SSL Setup tool)

Use the SSL Setup tool to create a private key and a certificate signing request (CSR) for use with all Hitachi Ops Center products.

 **Note:** If the certificate has expired or has been revoked by the certificate authority, you must renew it. Follow the procedure in this section to request a new certificate and overwrite the existing one. You must also perform the procedures in [Configuring SSL server settings \(SSL Setup tool\) \(on page 78\)](#) and [Configuring SSL client settings and enabling certificate verification \(SSL Setup tool\) \(on page 80\)](#).

### Procedure

1. Log in to the management server as the root user.  
If you log in as an ordinary user, use the `sudo` command to complete the following procedure as the root user.
2. Run the `cssslsetup` command, which is in the following location:

**If Common Services is installed on the management server:**

*installation-directory-of-Common-Services/utility/bin*

**If Common Services is not installed on the management server:**

*directory-where-utility.tar-is-extracted/utility/bin*

The main menu is displayed:

```
Main menu   Ver:cssslsetup-command-version
1. Create certificate signing request and private key.
2. Set up SSL server.
3. Set up SSL client.
```

```
4. Enable/disable certificate verification(optional).
5. Restart services for each product.
Enter a number or q to quit:
```

3. Enter **1**. You are prompted to provide the required certificate information:

- Absolute path to the file where the shared private key is output
- Absolute path to the file where the CSR is output
- Signature algorithm for RSA
- Key size
- Host name (CN)
- Organizational unit (OU)
- Organization name (O)
- Name of the city or locality (L)
- Name of the state or province (ST)
- 2-letter country code (C)
- Host name (or FQDN), IP address or both of SubjectAltName



**Note:** When you use the certificate for enabling SSL encryption for real time data collection in the Analyzer detail view server, enter the IP address of SubjectAltName and issue a certificate that includes the IP address specified in the SubjectAltName field.

4. Make sure that the settings are correct. If they are correct, enter **1. Yes**. If you want to specify the settings again, enter **2. No (Cancel)** to return to the main menu.
5. When the CSR is successfully created, the results are displayed and the main menu reappears. To exit, enter **q**.
6. Submit the CSR to the certificate authority, and request that the certificate authority issue a signed certificate. For details, follow the procedure for the certificate authority.
7. After obtaining the server certificate signed by the certificate authority, run the following command to check the results:

If Common Services is installed on the management server:

```
installation-directory-of-Common-Services/openssl/bin/openssl x509 -text -in
full-path-of-the-certificate-file
```

If Common Services is not installed on the management server:

```
directory-where-utility.tar-is-extracted/utility/lib/openssl/bin/openssl x509 -
text -in full-path-of-the-certificate-file
```

## Configuring SSL server settings (SSL Setup tool)

Use the SSL Setup tool to specify the server certificate and the private key for the Hitachi Ops Center products on the management server.

**Procedure**

1. Log in to the management server as the root user.  
If you log in as an ordinary user, use the `sudo` command to complete the following procedure as the root user.
2. Run the `cssslsetup` command, which is in the following location:

**If Common Services is installed on the management server:**

`installation-directory-of-Common-Services/utility/bin`

**If Common Services is not installed on the management server:**

`directory-where-utility.tar-is-extracted/utility/bin`

The main menu is displayed:

```
Main menu   Ver:cssslsetup-command-version
1. Create certificate signing request and private key.
2. Set up SSL server.
3. Set up SSL client.
4. Enable/disable certificate verification(optional).
5. Restart services for each product.
Enter a number or q to quit:
```

3. Enter **2**.  
A list of installed products appears.
4. Specify the target products for which you want to configure the SSL server.  
Use commas to specify multiple products.
5. Enter an absolute path to the file where the shared private key is located.
6. Enter an absolute path to the file where the shared server certificate is located.
7. Specify whether the server certificate specified is issued by an intermediate certificate authority.



**Note:** If you specified a server certificate issued by an intermediate certificate authority, create a certificate file by appending `-chained` to the file name. Do not delete this file.

8. If you specified yes in step 7, specify the absolute path of the certificate of the intermediate certificate authority.
9. To specify settings for Hitachi Ops Center Analyzer detail view or Hitachi Ops Center API Configuration Manager, use an absolute path for the root certificate of the server certificate for use with all Hitachi Ops Center products.
10. Enter the host name specified when creating the CSR.
11. To specify settings for Hitachi Ops Center Analyzer or Hitachi Ops Center Automator when ECC encryption certificate settings are enabled, specify whether to leave these settings enabled.
12. To specify settings for Hitachi Ops Center Administrator, enter the port number.
13. To specify settings for Hitachi Ops Center Administrator, enter the virtual appliance manager credentials.

14. To specify settings for Hitachi Ops Center Analyzer detail view, enter a common password for the truststore, keystore, and key manager.
15. Specify whether to use real time data collection of the Hitachi Ops Center Analyzer detail view. If you enter **1. Yes**, enter a common password for the truststore and keystore.
16. To implement the SSL server settings, enter **1. Yes**.

After the settings are implemented, a message is displayed and the main menu reappears.



**Note:** If you specify a password other than the default for real time data collection of the Hitachi Ops Center Analyzer detail view, you must manually run the following command:

```
/usr/local/megha/bin/changeSSLCertificatePassword.sh
```

17. Enter **5** to restart the services for each product.



**Note:** If you want to use the real time data collection of Hitachi Ops Center Analyzer detail view, after the Hitachi Ops Center Analyzer detail view services restarts, you must configure the SSL communication settings for the Hitachi Ops Center Analyzer probe server. For details, see the Hitachi Ops Center Analyzer manuals.

## Configuring SSL server settings for an Active Directory or LDAP server

To use LDAPS for communication with an Active Directory or LDAP server, configure SSL server settings on the Active Directory or LDAP server. For details on how to configure these settings, see the Active Directory or LDAP server documentation.

## Configuring SSL server settings for an identity provider server

To link with an identity provider, configure SSL server settings on the AD FS server. For details on how to configure these settings, see the AD FS server documentation.

## Configuring SSL client settings and enabling certificate verification (SSL Setup tool)

Use the SSL Setup tool to configure the required SSL client settings on the management server and enable certificate verification.

### Procedure

1. Log in to the management server as the root user.  
If you log in as an ordinary user, use the `sudo` command to complete the following procedure as the root user.
2. Run the `cssslsetup` command, which is in the following location:

**If Common Services is installed on the management server:**

`installation-directory-of-Common-Services/utility/bin`

**If Common Services is not installed on the management server:**

`directory-where-utility.tar-is-extracted/utility/bin`

The main menu is displayed:

```
Main menu   Ver:cssslsetup-command-version
1. Create certificate signing request and private key.
2. Set up SSL server.
3. Set up SSL client.
4. Enable/disable certificate verification(optional).
5. Restart services for each product.
Enter a number or q to quit:
```

3. Enter **3**.
4. Specify the target products for which you want to configure SSL client settings.  
Use commas to specify multiple products.
5. Import the root certificate for common use.
  - a. Specify an absolute path to the file where the root certificate is located.  
If you only want to configure the settings for linking with Active Directory, LDAP, or an AD FS server, press **Enter** without specifying anything.



**Note:** You must import the root certificate of the server certificate for Common Services.

- b. When the truststore file name is displayed, enter the truststore password. However, the truststore file name is not displayed for Analyzer viewpoint.
- c. Enter the alias name (server identification name).  
If you specify an alias name that is already used for the truststore, you are asked whether you want to re-register the alias name. Alias names are not case-sensitive. Run the following command to verify the alias name:

```
keytool -v -list -keystore path-to-truststore-file
```

6. If you want to link with Active Directory, LDAP, or an AD FS server, import the certificate associated with the server.
  - a. Enter, as an absolute path, the file name of the certificate for the Active Directory, LDAP, or AD FS server.  
If you do not want to link with Active Directory, LDAP, or AD FS server, just press **Enter**.
  - b. When the truststore file name is displayed, enter the truststore password.
  - c. Enter the alias name (server identification name).

## Configuring SSL client settings and enabling certificate verification (SSL Setup tool)

If you specify an alias name that is already used for the truststore, you are asked whether you want to re-register the alias name. Alias names are not case-sensitive. Run the following command to verify the alias name:

```
keytool -v -list -keystore path-to-truststore-file
```

7. For Hitachi Ops Center API Configuration Manager, configure SSL communications with your storage systems.
  - a. If you want to configure SSL communications, enter **1. Yes**.
  - b. Enter the storage device ID of the target storage system and use an absolute path for the server certificate.
  - c. To configure SSL communications for additional storage systems, enter **1. Yes**. If not, enter **2. No**.
  - d. Continue this procedure until you finish registering all your storage systems.

8. If you use the on-demand real time monitoring of Analyzer detail view, configure SSL communications for the Analyzer detail view server and the RAID Agent server. To configure the settings, perform the following steps:

- a. Enter **1. Yes**.
- b. When the truststore file name is displayed, specify the truststore password.
- c. Enter the alias name (server identification name).

If you specify an alias name that is already used for the truststore, you are asked whether you want to re-register the alias name. Alias names are not case-sensitive. Run the following command to verify the alias name:

```
keytool -v -list -keystore path-to-truststore-file
```

- d. Enter the file name of the server certificate of the target RAID Agent server by using the absolute path.
  - e. To configure SSL communications for an additional RAID Agent server, enter **1. Yes**. If not, enter **2. No**.
  - f. Continue this procedure until you finish registering all your RAID Agent servers.
9. Specify whether to enable certificate verification.



**Note:** If you want to enable certificate verification, you must import the certificate. Perform steps 5 to 8.

Even if you disable certificate verification, if you are using Common Services to link with Active Directory, an LDAP server, or an ID provider, you must import the root certificate of the server to which you are linking to perform authentication.

10. To implement the SSL client settings, enter **1. Yes**.

After the settings are implemented, a message is displayed and the main menu reappears.

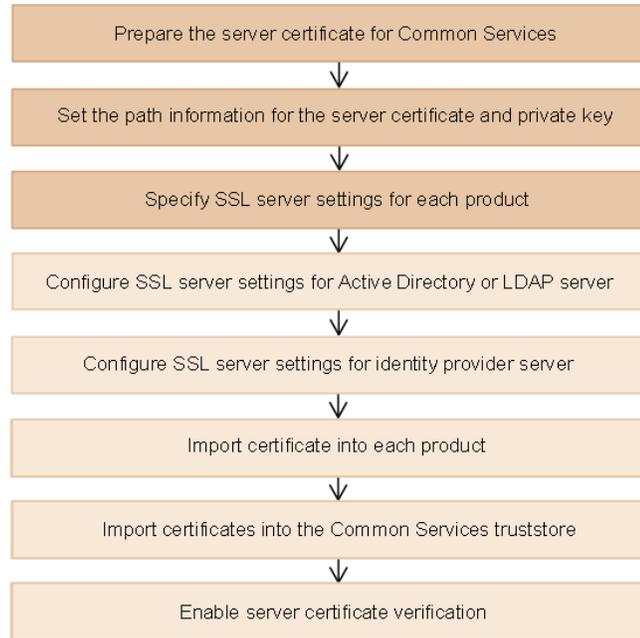
11. Enter **5** to restart the services for each product.

**Result**

The SSL communication configuration is complete.

## Configuring SSL communications without using the SSL Setup tool

The following figure shows the workflow for configuring SSL communications without using the SSL Setup tool:



Legend:



### Preparing the server certificate for Common Services

Prepare the server certificate for Common Services. Make sure the certificate has not expired. For details on how to check this, see [Checking the validity period of the server certificate \(on page 110\)](#). Common Services supports both RSA and Elliptic Curve Digital Signature Algorithm (ECDSA). You cannot configure ECDSA alone. Prepare secret keys and server certificates for RSA only or for both RSA and ECDSA.



**Note:** If you configure both RSA and ECDSA in Common Services, RSA is used for communication with Hitachi Ops Center Automator and Hitachi Ops Center Analyzer server. ECDSA is used for communication with other products.

**Procedure**

1. Log in to the management server as the root user.  
If you log in as an ordinary user, use the `sudo` command to complete the following procedure as the root user.

2. Run the following command to create a private key (in X.509 PEM format) and a certificate signing request (CSR).



**Note:** When you use the certificate for enabling SSL encryption for real time data collection in the Analyzer detail view server, enter the IP address of SubjectAltName and issue a certificate that includes the IP address specified in the SubjectAltName field.

#### Example of the command for RSA:

```
installation-directory-of-Common-Services/openssl/bin/openssl req -new -
newkey rsa:4096 -nodes -keyout privateRSA.pem -sha256 -out serverRSA.csr -
subj "/C=US/ST=xx/L=yy/O=zz/CN=host-name-or-IP-address" -addext
'subjectAltName = {DNS:host-name|IP:IP-address|DNS:host-name, IP:IP-
address}' -config installation-directory-of-Common-Services/openssl/
openssl.cnf
```

#### Example of the command for ECDSA:

```
installation-directory-of-Common-Services/openssl/bin/openssl req -new -
newkey ec:<(installation-directory-of-Common-Services/openssl/bin/openssl
ecparam -name secp384r1) -nodes -keyout privateECDSA.pem -sha256 -out
serverECDSA.csr -subj "/C=US/ST=xx/L=yy/O=zz/CN=host-name-or-IP-address" -
addext 'subjectAltName = {DNS:host-name|IP:IP-address|DNS:host-name, IP:IP-
address}' -config installation-directory-of-Common-Services/openssl/
openssl.cnf
```

When running the command, specify parameters according to the Cipher Suite supported by Common Services. For details on the Cipher Suite supported by Common Services, see the Common Services Release Notes.

Specify `/C=US/ST=xx/L=yy/O=zz` according to your environment. For `CN`, specify a host name (or FQDN) or IP address that can be used to access the Hitachi Ops Center Portal.

If you specify a host name for `CN`, specify `DNS:host-name` for `subjectAltName`. If you specify an IP address for `CN`, specify `IP:IP-address` for `subjectAltName`. If you specify a host name for `CN`, and specify that an IP address can also be used to access the Hitachi Ops Center Portal, specify `DNS:host-name, IP:IP-address` for `subjectAltName`.

To create a CSR by using the `openssl` command in the Common Services installation directory, you must specify the `-config` option to load the settings file.

3. Run the following command to check the results of creating the CSR:

```
installation-directory-of-Common-Services/openssl/bin/openssl req -text -in CSR-
file -config installation-directory-of-Common-Services/openssl/openssl.cnf
```

4. Submit the CSR to the certificate authority, and request that the certificate authority issue a signed certificate. For details, follow the procedure for the certificate authority.

5. After obtaining a server certificate signed by the certificate authority, run the following command to check the results of creating the server certificate:

```
installation-directory-of-Common-Services/openssl/bin/openssl x509 -text -in  
server-certificate-signed-by-certificate-authority
```

## Setting the path information for the server certificate and private key

In the Common Services properties file, specify the settings for the signed server certificate obtained from the certificate authority and the settings for the private key.

### Before you begin

Concatenate the signed server certificate obtained from the certificate authority and the certificate from the intermediate certificate authority into a single file as follows. If there are multiple certificates from intermediate certificate authorities, concatenate all certificates in a chain.

```
awk 1 server-certificate-signed-by-certificate-authority certificate-from-an-  
intermediate-certificate-authority [certificate-from-an-intermediate-certificate-  
authority ...] > chained-server-certificate
```

### Procedure

1. Log in to the management server as the root user.  
If you log in as an ordinary user, use the `sudo` command to complete the following procedure as the root user.
2. Transfer the signed server certificate obtained from the certificate authority and the private key to the management server in a secure manner.
3. Store the server certificate and the private key in the following location:

```
/var/installation-directory-of-Common-Services/tls/
```

For example, for an OVA install uses the following directory:

```
/var/opt/hitachi/CommonService/tls/
```

4. In the following properties file, specify the absolute paths to the server certificate file and private key file, and then save the file.

#### Properties file location

```
/var/installation-directory-of-Common-Services/userconf/  
config_user.properties
```

For example, for an OVA install uses the following file:

```
/var/opt/hitachi/CommonService/userconf/  
config_user.properties
```

**Settings**

- RSA settings:

```
CS_GW_SSL_CERTIFICATE=absolute-path-of-the-certificate-(RSA)-file
CS_GW_SSL_CERTIFICATE_KEY=absolute-path-of-the-private-key-(RSA)-file
```

- ECDSA settings:

```
CS_GW_SSL_CERTIFICATE_ECDSA=absolute-path-of-the-certificate-(ECDSA)-file
CS_GW_SSL_CERTIFICATE_KEY_ECDSA=absolute-path-of-the-private-key-(ECDSA)-file
```

5. If this is the first time configuring SSL, restart the Common Services service.



**Note:** In an environment where SSL communication settings have already been configured, if you want to change the settings in `config_user.properties` by adding ECDSA settings or reissuing a server certificate, complete the following procedures to configure SSL communication by configuring the settings for each product and Common Services, and then restarting the Common Services service. If you restart the Common Services service before configuring the settings, a communication error might occur.

## Specifying SSL server settings for each product

Configure SSL communications for each product that links with Common Services. As you did with Common Services, you must prepare the signed certificate from the certificate authority, and specify the SSL server settings.

For details on how to specify the SSL server settings, see the documentation for each product.

## Configuring SSL server settings for an Active Directory or LDAP server

To use LDAPS for communication with an Active Directory or LDAP server, configure SSL server settings on the Active Directory or LDAP server. For details on how to configure these settings, see the Active Directory or LDAP server documentation.

## Configuring SSL server settings for an identity provider server

To link with an identity provider, configure SSL server settings on the AD FS server. For details on how to configure these settings, see the AD FS server documentation.

## Importing certificates into each product

Import the root certificate of the server certificate for Common Services into each product that links with Common Services. In addition, if you import the Common Services metadata into

AD FS over the network when configuring a linkage with an identity provider, import the root certificate of the server certificate for Common Services into the AD FS server. In some cases, the certificate might already be imported.



**Note:** If you want to configure both RSA and ECDSA in Common Services, import the RSA root certificate into Hitachi Ops Center Automator. Import the ECDSA root certificate into other products.

For details on how to import a certificate, see the documentation for each product.

## Importing certificates into the Common Services truststore

Import the root certificate of the server certificate for Common Services and for each product into the Common Services truststore. If the system is linked with an Active Directory, LDAP, or identity provider server, you can also import the root certificates of these server certificates.

### Before you begin

Transfer the certificates to the management server in a secure manner.

### Procedure

1. Log in to the management server as the root user.  
If you log in as an ordinary user, use the `sudo` command to complete the following procedure as the root user.
2. Run the following command to import the root certificate of the server certificate for Common Services into the truststore.

In some cases, the certificate might already be imported.

### Format

```
keytool -importcert -alias alias-name -keystore path-to-truststore-file -storetype jks -storepass password-of-truststore-file -file path-of-the-certificate-to-be-imported
```

### Options

**-alias *alias-name***

Specify the name so that the certificate can be identified in the truststore.

**-keystore *path-to-truststore-file***

Specify the following absolute path as the path to the truststore file:

```
/var/installation-directory-of-Common-Services/tls/cacerts
```

For example, for an OVA install uses the following file:

```
/var/opt/hitachi/CommonService/tls/cacerts
```

**-storepass *password-of-truststore-file***

Specify the password of the truststore file. The default password is `changeit`.



**Note:** We recommend that you change the truststore password.

**-file *path-of-the-certificate-to-be-imported***

Specify the absolute path of the certificate to import.

3. In the same way, import the root certificate of the server certificate for each product into the truststore.
4. When you use LDAPS for communication with the Active Directory or LDAP server, import the root certificate of the server certificate for the Active Directory or LDAP server.
5. If you link Common Services with an identity provider, import the root certificate of the server certificate for the identity provider server.
6. Restart the Common Services service and the services for each product.

For details on how to restart the Common Services service, see [Starting or stopping the Common Services service \(on page 109\)](#). For details on how to restart the service of each product, see the documentation for each product.

## Enabling server certificate verification

After the initial installation of Common Services, there is no verification for server certificates from communication partners when Common Services is the SSL client. Therefore, to strengthen security, enable certificate verification immediately so that all server certificates are verified and your environment is protected from threats such as spoofing.

### Procedure

1. Log in to the management server as the root user.  
If you log in as an ordinary user, use the `sudo` command to complete the following procedure as the root user.
2. Change the following property file to enable server certificate verification:

#### Property file location

```
/var/installation-directory-of-Common-Services/userconf/
config_user.properties
```

For example, for an OVA install uses the following file:

```
/var/opt/hitachi/CommonService/userconf/
config_user.properties
```

#### Setting

```
CS_PORTAL_SSL_CERTIFICATE_CHECK=true
```

3. Restart the Common Services service.

**Result**

The SSL communication configuration is complete.

---

## Chapter 7: Configuring a link to an identity provider

By linking Common Services with an identity provider, you can delegate Hitachi Ops Center Portal authentication. You can also use the Multi Factor Authentication (MFA) functionality provided by the identity provider.

### Supported identity providers

Common Services supports the following.

Item	Description
Identity provider	Active Directory Federation Services (AD FS)
Protocol	<ul style="list-style-type: none"><li>▪ OpenID Connect (OIDC)</li><li>▪ Security Assertion Markup Language (SAML)</li></ul>
OS	The supported AD FS must support the following operating systems: <ul style="list-style-type: none"><li>▪ Windows Server 2016 Datacenter</li><li>▪ Windows Server 2019 Datacenter</li><li>▪ Windows Server 2022 Datacenter</li></ul>
Maximum number of linked providers	1

### Workflow for linking with AD FS

Use the following workflow to specify settings for AD FS:

The workflow for specifying settings depends on the protocol to be used.

**If you want to use OIDC:**

1. Register Common Services in AD FS as an application group.
2. Set up an issuance transform rule for AD FS.
3. Check the OpenID Connect Discovery endpoint of AD FS.

4. Register AD FS with Common Services.
5. Log in to the Hitachi Ops Center Portal as an identity provider user.

**If you want to use SAML:**

1. Check the AD FS metadata endpoint.
2. Register AD FS with Common Services.
3. Export Common Services metadata.
4. Register Common Services in AD FS as a relying party.
5. Set up a claim issuance policy.
6. Log in to the Hitachi Ops Center Portal as an identity provider user.

Before using Common Services to specify settings to link with the identity provider, you must finish installing and configuring AD FS.

To link with AD FS, you must specify SSL communication settings in advance for the route from Common Services to the AD FS server. For details, see [Configuring SSL communications \(on page 72\)](#).



**Note:** If you are using a host name for the Common Services access URL, the host name of the management server must be resolvable by the identity provider server.

## Configuring settings to link with AD FS (OIDC)

To link with AD FS by using the OIDC protocol, configure settings as follows.

### Registering Common Services in AD FS as an application group

By registering Common Services in AD FS as an application group, you can transfer authentication for the Hitachi Ops Center Portal to AD FS.

## Before you begin

The following settings are also necessary for registering AD FS in Common Services and should be determined in advance:

- Alias name of AD FS

The alias name is an identifier that uniquely identifies AD FS in Common Services. You can specify up to 64 characters consisting of halfwidth alphabetic characters (lowercase only), numeric characters, hyphens, and underscores. You cannot change the registered value later.

**Example:**

```
adfs_oidc_ad5
```

- URI of the Web API identifier

The Web API identifier is an identifier that AD FS uses to uniquely identify Common Services. Although you can specify any valid character string, a good practice is to use a name that is easy to identify (such as the host name of the Common Services management server).

**Example:**

```
https://common_services_host
```

## Procedure

1. Log in to the AD FS server.
2. Select **Start > Windows Administrative Tools > AD FS Management**.
3. From the tree on the left side, select **AD FS > Application Groups**. In the pane on the right side, click **Application Groups > Add Application Group**.
4. In the Welcome window, set the following items, and then click **Next**:

**Name**

A name of your choice.

**Template**

Select **Server application accessing a web API**.

5. In the Server application window, set the following items, and then click **Next**:

**Client Identifier**

Record this information for when you register AD FS in Common Services.

**Redirect URI**

Specify the host name and port number of the Common Services management server, along with the AD FS alias name:

```
https://host-name:port-number/auth/realms/opscenter/broker/  
alias-name/endpoint
```

For *alias-name*, specify the AD FS alias name that you determined in advance.

6. In the Configure Application Credentials window, select the **Generate a shared secret** check box.  
Make a note of the Secret, for when you register AD FS in Common Services.
7. Click **Next**.
8. In the Configure Web API window, for **Identifier**, specify the URI of the Web API identifier that you determined in advance, click **Add**, and then click **Next**.
9. In the Choose Access Control Policy window, specify an access control policy, and then click **Next**.
10. In the Configure Application Permissions window, select the following check boxes for **Permitted scopes**, and then click **Next**.
  - **allatclaims**
  - **email**
  - **openid**
  - **profile**
11. In the Summary window, make sure that the settings are correct, and then click **Next**.
12. In the Finish window, click **Close**.

## Setting up an issuance transform rule for AD FS

Set up an issuance transform rule for the Common Services instance registered as an application group in AD FS. The login information for the Hitachi Ops Center Portal is transmitted to Common Services is based on these settings.

### Procedure

1. Log in to the AD FS server.
2. Select **Start > Windows Administrative Tools > AD FS Management**.
3. From the tree on the left, select **AD FS > Application Groups**. In the middle pane, select the application group for Common Services, and then in the right pane, click **Properties**.  
The properties window for the application group appears.
4. For **Applications**, select **application-group-name- Web API** and then click **Edit**.  
The properties window for the Web API appears.
5. On the Issuance Transform Rules tab, click **Add Rule**.  
The Add Transform Claim Rule Wizard dialog box opens.
6. On the Select Rule Template window, select **Send LDAP Attributes as Claims for Claim rule template**, and then click **Next**.
7. On the Configure Rule window, set the following items, and then click **Finish**.

#### Claim rule name

A name of your choice

#### Attribute store

Select **Active Directory**.

### Mapping of LDAP attributes to outgoing claim types

Set the following values.

Value to specify for LDAP Attribute	Value to specify for Outgoing Claim Type
Either of the following LDAP attributes for which an email address is registered in the system: <ul style="list-style-type: none"> <li>▪ User-Principal-Name</li> <li>▪ E-Mail-Addresses</li> </ul>	E-Mail Address
Given-Name	Given Name
Surname	Surname
Token-Groups - Qualified by Domain Name	Group



**Note:** Make sure that the email address, surname, and given name of the Active Directory user for the Hitachi Ops Center Portal are set for the LDAP attributes that you specify. If this information is not set, the user cannot log in.

8. Verify that the Claim rule has been added to the Issuance Transform Rules tab, and then click **OK**.

## Checking the OpenID Connect Discovery endpoint of AD FS

Obtain the OpenID Connect Discovery endpoint needed to register AD FS in Common Services.

### Procedure

1. Log in to the AD FS server.
2. Select **Start > Windows Administrative Tools > AD FS Management**.
3. Check the OpenID Connect Discovery endpoint of AD FS.

From the tree on the left side, select **AD FS > Service > Endpoints**. From the displayed endpoint information, check the value of **URL Path** in the row where the Type is OpenID Connect Discovery.

To obtain the endpoint, simply append the base URI of AD FS to the displayed URL.

### Example:

```
https://ads.example.com/ads/.well-known/openid-configuration
```

Make a note of the OpenID Connect Discovery endpoint, because you will need it when you register AD FS in Common Services.

## Registering AD FS with Common Services

You can register AD FS with Common Services as an identity provider.

### Procedure

1. Log in to the Hitachi Ops Center Portal as the sysadmin user or as a user who belongs to the opscenter-administrators group.
2. From the navigation bar, click **Manage users**.
3. In the Users window, from the Asset type, click **Identity providers**.
4. In the Identity Providers window, click +.
5. In the wizard, enter and register the required items.

Item	Value
Provider type	Active Directory Federation Services
Federation protocol	OpenID connect 1.0
Display name	Name of the identity provider (up to 64 characters).
Alias	Alias name that was decided on in <a href="#">Registering Common Services in AD FS as an application group (on page 91)</a>
OpenID connect discovery endpoint	The endpoint that was verified in <a href="#">Checking the OpenID Connect Discovery endpoint of AD FS (on page 94)</a> .
Enabled	If you specify <b>Enable</b> , the identity provider is enabled and the <b>Log in using external identity provider</b> link appears in the login window.
Client ID	The AD FS client identifier that was displayed in <a href="#">Registering Common Services in AD FS as an application group (on page 91)</a> .
Client secret	The AD FS secret name that was displayed in <a href="#">Registering Common Services in AD FS as an application group (on page 91)</a> .
Web API identifier	URI of the Web API identifier used in <a href="#">Registering Common Services in AD FS as an application group (on page 91)</a> .
Allowed clock skew	Acceptable time difference between the management server where Common Services is installed and the AD FS server. If the time difference between the servers exceeds this value, you cannot use AD FS to log in.  Valid values are 0 to 300 (seconds).  Default: 300

Item	Value
Default group mappers	<p>Local user group used as the default. (Optional)</p> <p>When AD FS user authentication succeeds, the user is imported into Common Services as a local user, and the local user group specified for this item is assigned.</p> <p>Maximum number of groups is 10.</p>
Custom group mappers	<p>A pair consists of an AD FS user group and a local user group. (Optional)</p> <p>When AD FS user authentication succeeds, the user is imported into Common Services as a local user. If the user belongs to an AD FS user group specified in the Custom group mappers, the corresponding local user group is assigned.</p> <p>Maximum number of pairs is 10.</p> <p>Specify the AD FS user group name in Windows Domain Qualified Name format.</p> <p><b>Example:</b></p> <pre>domain\cs_admin_group</pre>

## Logging in to the Hitachi Ops Center Portal as an identity provider user

After completing the settings for linking with the identity provider, confirm that you can log in to the Hitachi Ops Center Portal from a browser as an identity provider user.

### Procedure

1. In a web browser, access the following URL:  

```
https://host-name-or-IP-address-of-Portal:port-number/portal/
```
2. In the login window, click **Log in using external identity provider**.  
The identity provider login window opens.
3. Log in as an identity provider user.  
When the identity provider user is successfully authenticated, you are logged in to the Hitachi Ops Center Portal.
4. Log in again as the sysadmin user or as a user who is a member of the opscenter-administrators group. Then, select **Manage users > Users**, and check whether the following items of the identity provider user are set correctly: the username, last name, first name, email address, and the user group specified for Default group mappers and Custom group mappers.

**Result**

This completes the settings for linking with the identity provider.

## Configuring settings to link with AD FS (SAML)

To link with AD FS by using the SAML protocol, configure settings as follows.

### Checking the AD FS metadata endpoint

Check the metadata endpoint required to register AD FS in Common Services.

**Procedure**

1. Log in to the AD FS server.
2. Select **Start > Windows Administrative Tools > AD FS Management**.
3. Check the AD FS metadata endpoints.

From the tree on the left side, select **AD FS > Service > Endpoints**. From the displayed endpoint information, check the value of URL Path in the row where the Type is Federation Metadata.

The string obtained by adding the AD FS base URI to the above URL is the AD FS metadata endpoint.

**Example:**

```
https://adfs.example.com/FederationMetadata/2007-06/
FederationMetadata.xml
```

Make note of the endpoint because you need it for registering AD FS with Common Services.

### Registering AD FS with Common Services

You can register AD FS with Common Services as an identity provider.

**Procedure**

1. Log in to the Hitachi Ops Center Portal as the sysadmin user or as a user who is a member of the opscenter-administrators group.
2. From the navigation bar, click **Manage users**.
3. In the Users window, from the Asset type, click **Identity providers**.
4. In the Identity Providers window, click +.
5. In the wizard, enter and register the required items.

Item	Value
Provider type	Active Directory Federation Services

Item	Value
Federation protocol	SAML 2.0
Display name	Name of the identity provider (up to 64 characters).
Alias	<p>Alias name used to uniquely identify the identity provider (up to 64 characters).</p> <p>Valid character types are half-width alphabetical characters (lowercase only), numbers, hyphens, and underscores.</p> <p>You cannot change the registered value later.</p>
AD FS endpoint metadata URI	Endpoint defined in <a href="#">Checking the AD FS metadata endpoint (on page 97)</a> .
Enabled	If you specify <b>Enable</b> , the identity provider is enabled and the <b>Log in using external identity provider</b> link appears in the login window.
NameID Policy Format	<p>Format used for the username when the AD FS user is imported as a Common Services local user:</p> <ul style="list-style-type: none"> <li>▪ Windows Domain Qualified Name</li> <li>▪ Email</li> <li>▪ Unspecified</li> </ul>
Allowed clock skew	<p>Acceptable time difference between the management server where Common Services is installed and the AD FS server. If the time difference between the servers exceeds this value, you cannot use AD FS to log in.</p> <p>Valid values are 0 to 300 (seconds).</p> <p>Default: 300</p>
Default group mappers	<p>Local user group used as the default. (Optional)</p> <p>When AD FS user authentication succeeds, the user is imported into Common Services as a local user, and the local user group specified for this item is assigned.</p> <p>Maximum number of groups is 10.</p>
Custom group mappers	<p>A pair consists of an AD FS user group and a local user group. (Optional)</p> <p>When AD FS user authentication succeeds, the user is imported into Common Services as a local user. If the user belongs to an AD FS user group specified in the Custom group mappers, the corresponding local user group is assigned.</p>

Item	Value
	<p>Maximum number of pairs is 10.</p> <p>Specify the AD FS user group name in Windows Domain Qualified Name format.</p> <p><b>Example:</b></p> <pre>domain\cs_admin_group</pre>

## Exporting Common Services metadata

To link with AD FS, you must register Common Services metadata into AD FS. From the Hitachi Ops Center Portal, output the metadata to a file and then send the file to the AD FS server.

### Procedure

1. Log in to the Hitachi Ops Center Portal as the sysadmin user or as a user who is a member of the opscenter-administrators group.
2. In the navigation bar, click **Manage users**.
3. In Asset type in the Users window, click **Identity providers**.
4. In the Identity Providers window, click the target AD FS.
5. In the Identity provider details window, click **Download metadata**.

The Common Services metadata file is downloaded. Transfer this file to the AD FS server.

## Registering Common Services in AD FS as a relying party

By registering Common Services in AD FS as a relying party, you can transfer authentication for the Hitachi Ops Center Portal to AD FS.

### Procedure

1. Log in to the AD FS server.
2. Select **Start > Windows Administrative Tools > AD FS Management**.
3. From the tree on the left side, select **AD FS > Relying Party Trusts**. In the pane on the right side, click **Relying Party Trusts > Adding Relying Party Trust**.
4. In the Welcome window, select **Claims aware**, and then click **Start**.
5. In the Select Data Source window, select **Import data about the relying party from file**. For **Federation metadata file location**, specify the file to which the Common Services metadata was exported, and then click **Next**.
6. In the Specifying Display Name window, specify a display name, and then click **Next**.
7. In the Choose Access Control Policy window, specify an access control policy, and then click **Next**.
8. In the Ready to Add Trust window, make sure that the settings are correct, and then click **Next**.

- In the Finish window, select the **Configure claims issuance policy for this application** check box, and then click **Close**.

## Setting up a claim issuance policy

Set up a claim issuance policy for the Common Services instance registered as a relying party in AD FS. The user attribute information imported when the user logs in to the Hitachi Ops Center Portal is transmitted to Common Services based on the claim issuance policy settings.

### Procedure

- Log in to the AD FS server.
- Select **Start > Windows Administrative Tools > AD FS Management**.
- From the tree on the left, select **AD FS > Relying Party Trusts**. In the middle pane, select the relying party trust for Common Services, and then in the right pane, click **Edit Claim Issuance Policy...**

The Edit Claim Issuance Policy dialog box opens.

- On the Issuance Transform Rules tab, click **Add Rule**.  
The Add Transform Claim Rule Wizard dialog box opens.
- Select **Transform an Incoming Claim** for the claim rule template, and then click **Next**.
- Specify the following items:

#### Claim rule name

A name of your choice

#### Outgoing claim type

The **Name ID**

#### Incoming claim type and Outgoing name ID format

Depending on the value specified for NameID Policy Format in [Registering AD FS with Common Services \(on page 97\)](#), specify the values as follows:

Value specified for NameID Policy Format	Value to specify for Incoming claim type	Value to specify for Outgoing name ID format
Windows Domain Qualified Name	Windows account name	Windows Qualified Domain Name

Value specified for NameID Policy Format	Value to specify for Incoming claim type	Value to specify for Outgoing name ID format
Email	Either of the following LDAP attributes for which an email address is registered in the system: <ul style="list-style-type: none"> <li>▪ UPN (User-Principal-Name)</li> <li>▪ E-Mail Address</li> </ul>	Email
Unspecified	UPN	UPN

**Pass through all claim values**

Select this item to turn it on.

**7. Click Finish.**

The claim rule is added to the Edit Claim Issuance Policy dialog box. The values specified here are transmitted to Common Services upon the following claim:

```
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier
```

**8. In the Edit Claim Issuance Policy dialog box, click Add Rule again.**

The Add Transform Claim Rule Wizard dialog box opens.

**9. Select Send LDAP Attributes as Claims for the claim rule template, and then click Next.****10. Specify the following items:****Claim rule name**

A name of your choice

**Attribute Store**

**Active Directory**

**Mapping of LDAP attributes to outgoing claim types**

Specify values for the following attributes:

LDAP Attribute	Value
Either of the following LDAP attributes for which an email address is registered in the system: <ul style="list-style-type: none"> <li>User-Principal-Name</li> <li>E-Mail-Addresses</li> </ul>	E-Mail Address
Given-Name	Given Name
Surname	Surname
Token-Groups - Qualified by Domain Name	Group



**Note:** Make sure that the email address, surname, and given name of the Active Directory user for the Hitachi Ops Center Portal are set for the LDAP attributes that you specify. If this information is not set, the user cannot log in.

**11. Click Finish.**

The claim rule is added to the Edit Claim Issuance Policy dialog box. The values specified are transmitted to Common Services through the following claims:

- E-Mail Address:

```
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
```

- Given Name:

```
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
```

- Surname:

```
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
```

- Group:

```
http://schemas.xmlsoap.org/claims/Group
```

**12. In the Edit Claim Issuance Policy dialog box, change the order of priority to the following, and then click OK.**

- The rule specified for the **Send LDAP Attributes as Claims**
- The rule specified for the **Transform an Incoming Claim**

**13. To make sure the specified information is correct, select AD FS > Service > Claim Descriptions.**

## Logging in to the Hitachi Ops Center Portal as an identity provider user

After completing the settings for linking with the identity provider, confirm that you can log in to the Hitachi Ops Center Portal from a browser as an identity provider user.

### Procedure

1. In a web browser, access the following URL:  
`https://host-name-or-IP-address-of-Portal:port-number/portal/`
2. In the login window, click **Log in using external identity provider**.  
The identity provider login window opens.
3. Log in as an identity provider user.  
When the identity provider user is successfully authenticated, you are logged in to the Hitachi Ops Center Portal.
4. Log in again as the sysadmin user or as a user who is a member of the opscenter-administrators group. Then, select **Manage users > Users**, and check whether the following items of the identity provider user are set correctly: the username, last name, first name, email address, and the user group specified for Default group mappers and Custom group mappers.

### Result

This completes the settings for linking with the identity provider.



**Note:** If you link with an identity provider by using the SAML protocol, you must periodically update the certificate used for user authentication. For details, see [Updating the authentication certificates used with an identity provider \(SAML\) \(on page 103\)](#).

## Updating the authentication certificates used with an identity provider (SAML)

This section explains how to check the date of the next update of a certificate, manually update a certificate, and change the number of days set as the update interval of the Common Services authentication key and AD FS Token certificates that are used with an identity provider.

If you link with an identity provider by using the OIDC protocol, you do not need to perform this procedure.

## Overview of updating authentication certificates

For identity providers, certificates used by Common Services and AD FS are used during user authentication.

Common Services certificates are called authentication keys, and AD FS certificates are called Token certificates.

Each certificate has an expiration date and certificates are automatically updated according to a defined interval (in days).

However, when a certificate is automatically updated, a discrepancy arises between the new certificate and the certificate that was registered when the link with the identity provider was configured. For this reason, you will no longer be able to log in to Common Services by using the user account of the identity provider. To prevent this problem, you must check the date of the next update of the certificate and manually update the certificate before its expiration date.

If it is inconvenient to update the authentication key of Common Services immediately, you can temporarily suppress the update by increasing the number of days set as the update interval. Although you can also change the update interval of AD FS Token certificates, the change is not applied to the certificates currently used. The new update interval is applied to the certificates that will be updated next time.



**Tip:** Specifying the same update interval for the Common Services authentication key and for the AD FS Token certificates is convenient, because this enables you to update both on the same day. Update certificates during a time when no user is logged in (such as on a holiday or during the night).

## Checking the next update for the Common Services certificates

Check the date of the next update of the authentication key for Common Services.

### Procedure

1. Log in to the Hitachi Ops Center Portal as the sysadmin user or as a user who is a member of the opscenter-administrators group.



**Note:** If the date of the next update of the authentication key will occur within 30 days, a message to that effect is displayed when you log in.

2. Select **Settings > Authentication key**, and then check the value displayed for **Authentication key next update date (UTC)**.

## Checking the dates of the next update of the AD FS certificates

Check the dates of the next update of the Token certificates of AD FS.

### Procedure

1. Log in to the AD FS server.
2. Select **Start > Windows Administrative Tools > AD FS Management**.
3. From the tree on the left side, select **AD FS > Service > Certificates**.
4. Check the value of **Expiration Date** for **Token-decrypting** and **Token-signing** in the middle pane.

## Updating the Common Services certificates

If the date of the next update of the authentication key of Common Services is approaching, update the authentication key and the metadata. You can also change the update interval of the authentication key without actually updating the key.

### Procedure

1. Log in to the Hitachi Ops Center Portal as the sysadmin user or as a user who is a member of the opscenter-administrators group.
2. Select **Settings > Authentication key**.  
The Authentication key window appears.
3. To change the update interval of the authentication key, change the value of **Authentication Key update interval (days)**.  
The default value is 180 days (with a range of 90 to 3,650). From a security standpoint, we recommend 90-180 days.
4. For **Update Authentication key now**, select **Yes**.  
If you want to change the update interval without updating the authentication key, select **No**.
5. Click **Submit**.  
If you selected **No** for **Update Authentication key now**, skip the remaining.
6. Export the metadata of Common Services. For details, see [Exporting Common Services metadata \(on page 99\)](#).
7. Log in to the AD FS server.
8. Select **Start > Windows Administrative Tools > AD FS Management**.
9. From the tree on the left side, select **AD FS > Relying Party Trusts**.
10. In **Relying Party Trusts**, check the value of **Identifier** for the Common Services instance that is registered.
11. Run the following command in PowerShell:

```
Update-AdfsRelyingPartyTrust -MetadataFile storage-location-of-the-metadata-file
-TargetIdentifier ID-of-the-relying-party
```

For *ID-of-the-relying-party*, specify the value of **Identifier** for Common Services (checked in the previous step).

#### Example of running the command:

```
Update-AdfsRelyingPartyTrust -MetadataFile metadata.xml -TargetIdentifier
https://www.example.com:8443/auth/realms/opscenter
```

For details on the command, see the AD FS documentation.

## Updating the AD FS certificates

Run the AD FS command `Update-AdfsCertificate` to update the Token certificates. After updating the certificates, you must specify the metadata endpoint for AD FS from the Hitachi Ops Center Portal, and then update the information about AD FS registered in Common Services.



**Note:** For details about Token certificates and the command, see the AD FS documentation.

### Procedure

1. Log in to the AD FS server.
2. To change the update interval of Token certificates, run the following command in PowerShell:

```
Set-AdfsProperties -CertificateDuration update-interval- (number-of-days)
```

The change will take effect the next time the Token certificates are updated after you change the update interval.

#### Example of 3 years:

```
Set-AdfsProperties -CertificateDuration 1095
```

3. If you want the change to take effect immediately, run the following command in PowerShell to update the Token certificates:

```
Update-AdfsCertificate -CertificateType Token-Decrypting -Urgent
Update-AdfsCertificate -CertificateType Token-Signing -Urgent
```

4. Log in to the Hitachi Ops Center Portal as the sysadmin user or as a user who is a member of the opscenter-administrators group.
5. In the navigation bar, click **Manage users**.
6. In Asset type in the Users window, click **Identity providers**.
7. Click the **Edit identity provider** icon for the registered identify provider.
8. For **AD FS endpoint metadata URI**, set the metadata endpoint for AD FS.  
For details on how to check the metadata endpoint, see [Checking the AD FS metadata endpoint \(on page 97\)](#).
9. Click **Next** without changing any other values.
10. In the **Edit identity provider - confirmation** window, click **Submit**.

## If you cannot sign on with an identity provider

If you cannot sign on using an identity provider, there are two possibilities:

- Certificates for Common Services were updated.

In this scenario, if you cannot log in using an identity provider, the following message is output to Applications and Services Logs > AD FS > Admin in the AD FS event log:

```
ID6013: The signature verification failed
```

For details on what to do when this message is output, see [Updating the Common Services metadata by using AD FS \(on page 107\)](#).

- Certificates for AD FS were updated.

In this scenario, if you cannot log in using an identity provider, the following message is output Common Services log file (default: /var/log/hitachi/CommonService/idp/log/server.log):

```
ERROR [org.keycloak.broker.saml.SAMLEndpoint] (default task-14) validation failed
```

For details on what to do when this message is output, see [Specifying the AD FS metadata endpoint by using Common Services \(on page 108\)](#).

## Updating the Common Services metadata by using AD FS

You can update the Common Services metadata by using AD FS.

### Procedure

1. Export the metadata of Common Services. For details, see [Exporting Common Services metadata \(on page 99\)](#).
2. Log in to the AD FS server.
3. Select **Start > Windows Administrative Tools > AD FS Management**.
4. From the tree on the left side, select **AD FS > Relying Party Trusts**.
5. In **Relying Party Trusts**, check the value of **Identifier** for the Common Services instance that is registered.
6. Run the following command in PowerShell:

```
Update-AdfsRelyingPartyTrust -MetadataFile storage-location-of-the-metadata-file -TargetIdentifier ID-of-the-relying-party
```

For *ID-of-the-relying-party*, specify the value of **Identifier** for Common Services (checked in the previous step).

### Example:

```
Update-AdfsRelyingPartyTrust -MetadataFile metadata.xml -TargetIdentifier https://www.example.com:8443/auth/realms/opscenter
```

For details on the command, see the AD FS documentation.

## Specifying the AD FS metadata endpoint by using Common Services

You can specify the AD FS metadata endpoint by using Common Services.

### Procedure

1. Log in to the Hitachi Ops Center Portal as the sysadmin user or as a user who is a member of the opscenter-administrators group.
2. In the navigation bar, click **Manage users**.
3. In Asset type in the Users window, click **Identity providers**.
4. Click the **Edit identity provider** icon for the registered identity provider.
5. For **AD FS endpoint metadata URI**, set the metadata endpoint for AD FS.  
For details on how to check the metadata endpoint, see [Checking the AD FS metadata endpoint \(on page 97\)](#).
6. Click **Next** without changing any other values.
7. In the **Edit identity provider - confirmation** window, click **Submit**.

---

## Chapter 8: Maintaining Hitachi Ops Center

The Hitachi Ops Center system administrator performs various system operation and maintenance tasks such as starting or stopping a service, backing up and restoring user data, and modifying URLs.

### Starting or stopping the Common Services service

To start or stop the Common Services service, use the `systemctl` command.

#### Procedure

1. Log in to the management server as the root user.  
If you log in as an ordinary user, use the `sudo` command to complete the following procedure as the root user.
2. Run the `systemctl` command.

#### To start the service:

```
systemctl start csportal
```

#### To stop the service:

```
systemctl stop csportal
```

#### To restart the service:

```
systemctl restart csportal
```

### Checking the validity period of a certificate in the truststore

You can check whether the validity period of a certificate in the truststore has expired.

#### Procedure

1. Run the following command and provide the keystore password when prompted:

```
installation-directory-of-Common-Services/jdk/bin/keytool -list -v -  
keystore /var/installation-directory-of-Common-Services/tls/cacerts
```

## Checking the validity period of the server certificate

You can check whether the validity period of the management server certificate has expired.



**Note:** If the certificate has expired, you must renew it. Follow the procedure in [Creating a private key and a certificate signing request \(SSL Setup tool\) \(on page 77\)](#) to request a new certificate and overwrite the existing one. You must also reconfigure the SSL server settings and SSL client settings.

### Procedure

1. Run the following command:

```
installation-directory-of-Common-Services/jdk/bin/keytool -printcert -file path-of-server-certificate
```

## Checking the revocation status of the server certificate

You can check the revocation status of the server certificate for a Hitachi Ops Center product by using the Online Certificate Status Protocol (OCSP).



**Note:** If the certificate has been revoked, you must renew it. Follow the procedure in [Creating a private key and a certificate signing request \(SSL Setup tool\) \(on page 77\)](#) to request a new certificate and overwrite the existing one. You must also reconfigure the SSL server settings and SSL client settings.

### Before you begin

Verify that the following settings are configured on the management server:

- The OCSP responder is functioning. If you are unsure whether it is functioning, contact the certificate authority.
- The server certificate has the Authority Information Access (AIA) record that includes the correct address of the OCSP responder.
- The management server can access the OCSP responder and access is not blocked by a proxy.

To check whether the AIA record includes the correct address of the OCSP responder, you can use the `openssl` command. Check the address of the `OCSP-URI` field of the AIA record. If no address is set, contact the certificate authority that signed the server certificate. The following is the command syntax and an example of the command:

Command syntax:

```
echo "Q" | installation-directory-of-Common-Services/openssl/bin/openssl s_client -connect host-name-or-ip-address-of-product-URL:port-number-of-product-URL 2> /dev/null | openssl x509 -noout -text
```

Command example:

```
echo "Q" | /opt/hitachi/CommonService/openssl/bin/openssl s_client -connect  
example.com:443 2> /dev/null | openssl x509 -noout -text
```

You can check the revocation status of the server certificate in one of the following ways:

- Web browser: [Checking the revocation status of the server certificate by using a web browser \(on page 111\)](#)
- `openssl` command: [Checking the revocation status of the server certificate by using a command \(on page 111\)](#)
- Automatically by using cron: [Checking the revocation status of the server certificate on a regular basis \(on page 112\)](#)

## Checking the revocation status of the server certificate by using a web browser

You can use the OCSP check function of your web browser to check the revocation status of the server certificate. For details on how to check the status, see the documentation for your browser.

For Firefox, you can check the status by using the following procedure.

### Procedure

1. In the settings window of Firefox, select **Privacy & Security**, and then select the **Query OCSP responder servers to confirm the current validity of certificates** check box.
2. Use Firefox to access the URL for the target product, and then check whether an error appears. If the server certificate has expired, the `SEC_ERROR_REVOKED_CERTIFICATE` error appears.



**Note:** For Hitachi Ops Center API Configuration Manager and other products that do not have a web GUI, you cannot use a web browser to check the revocation status. In such cases, see [Checking the revocation status of the server certificate by using a command \(on page 111\)](#).

## Checking the revocation status of the server certificate by using a command

You can check the revocation status of the server certificate by using the OCSP check function of the `openssl` command. For more details, see the `openssl` documentation.

### Procedure

1. On the management server, run the following `openssl` command.

Command syntax:

```
installation-directory-of-Common-Services/openssl/bin/openssl ocsp -no_nonce -  
issuer issuer-certificate -cert server-certificate -url OCSP-Responder-URI -text
```

The *issuer certificate* is either the root certificate or, if there is an intermediate certificate, specify the PEM-format certificate that combines the root and intermediate certificates.

Command example:

```
/opt/hitachi/CommonService/openssl/bin/openssl ocsp -no_nonce -issuer cacert.cer  
-cert httpsd.cer -url http://ad.example.com/ocsp -text
```

2. Check whether the value of `Cert Status` is good. If the value is `revoked`, the server certificate has expired.

## Checking the revocation status of the server certificate on a regular basis

On the management server where Hitachi Ops Center products are installed, use cron to check the revocation status of the server certificate on a regular basis. The revocation status check results can be output to a file or to `syslog`.

### Outputting the revocation status check results to a file

Output the revocation status of a server certificate to a file as follows. Register a command in cron and output the check results to a file.

#### Procedure

1. Log in to the management server as the root user.  
If you log in as an ordinary user, use the `sudo` command to complete the following procedure as the root user.
2. Modify the crontab file. Run the following command. For details on the command, see the crontab documentation.

```
crontab -u root -e
```

3. Add a command to the crontab file for each product whose revocation status you want to check. The command you set differs depending on how the server certificate of the product to be added is referenced.

**If you check by downloading the certificate file from the URL of the Hitachi Ops Center product:**

Specify the execution time, the command to download the server certificate, and the command to query the OCSP responder in the following format.

```
* * * * * command-to-download-the-server-certificate;command-to-query-the-OCSP-responder
```

- **Command syntax for downloading the server certificate:**

```
installation-directory-of-Common-Services/openssl/bin/openssl s_client -connect host-name-or-ip-address-of-product-URL:port-number-of-product-URL [-cipher Cipher-Suite] < /dev/null 2> path-of-the-standard-error-output-file | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > path-of-download-destination-of-server-certificate
```

For products that use both RSA and ECDSA server certificates, you must specify the command for RSA and again for ECDSA. For the `-cipher` option, specify an RSA or ECDSA Cipher Suite supported by the target product.

**Example:**

```
ECDHE-RSA-AES256-GCM-SHA384, ECDHE-ECDSA-AES256-GCM-SHA384
```

- **Command syntax for querying the OCSP responder:**

```
installation-directory-of-Common-Services/openssl/bin/openssl ocsp -no_nonce -issuer issuer-certificate -cert path-of-server-certificate -url OCSP-Responder-URI [ -proxy [http[s]://][userinfo-of-proxy@]host-name-or-IP-address-of-proxy[:port-number-of-proxy] [/path-of-proxy] ] [-CAfile root-certificate-of-the-OCSP-responder-server] -text -out path-of-the-file-to-which-the-results-are-output 2>> path-of-the-standard-error-output-file
```

**If you check by referencing the certificate file set for the Hitachi Ops Center product:**

Specify the execution time and the command to query the OCSP responder in the following format.

```
* * * * * command-to-query-the-OCSP-responder
```

- Command syntax for querying the OCSP responder:

```
installation-directory-of-Common-Services/openssl/bin/openssl ocspl -
no_nonce -issuer issuer-certificate -cert path-of-server-certificate -
url OCSP-Responder-URI [ -proxy [http[s]://][userinfo-of-proxy@]host-
name-or-IP-address-of-proxy[:port-number-of-proxy] [/path-of-proxy] ] [-
CAfile root-certificate-of-the-OCSP-responder-server] -text -out path-
of-the-file-to-which-the-results-are-output 2> path-of-the-standard-
error-output-file
```

**Note:**

- Specify the execution time for each command. Specify a value for "\*" \* \* \* \*". If you want to run the command every day at 4:00 a.m., specify "0 4 \* \* \*". For details, see the crontab documentation.
- Specify different paths for *path-of-the-file-to-which-the-results-are-output* and *path-of-the-standard-error-output-file* for each command.
- For the *issuer-certificate* for the command that queries the OCSP responder, either specify the root certificate or, if there is an intermediate certificate, specify the PEM-format certificate that combines the root and intermediate certificates.
- To use a proxy for the command that queries the OCSP responder, specify the `-proxy` option.
- If the `Response Verify Failure` error is output to *standard-error-output-file*, specify the `-CAfile` option.
- For details on the `openssl` command, see the `openssl` documentation.

4. Add a command for each product, specifying each command as described in step 3.

Example settings:

```
10 4 * * * command-for-product-1
20 4 * * * command-for-product-2
30 4 * * * command-for-product-3
...
```

5. After you finish specifying the commands, save the crontab file.
6. Run the following command to enable `crond.service`.

```
systemctl enable crond.service
```

- Restart the service to apply the crond settings. Run the following command.

```
systemctl restart crond
```

### Result

- At the specified time, a file is output to the directory specified in *path-of-the-file-to-which-the-results-are-output*. Check the value of `Cert Status` in the output file.
  - If the value is `good`: The server certificate is valid.
  - If the value is `revoked`: The server certificate has been revoked.
  - If the value is `unknown`: The status is unknown.
- If the output file does not include the `Cert Status` line, an error might have occurred. For details about the error, check the file output to the directory specified in *path-of-the-standard-error-output-file*.

## Outputting the revocation status check results to `syslog`

Output the revocation status of the server certificate to `syslog` as follows.

### Procedure

- Register a command in cron for each product whose revocation status you want to check. For details on how to specify the command, see [Outputting the revocation status check results to a file \(on page 112\)](#). To output the results to `syslog`, you do not need to specify the `-out` option.
- Change the crond settings. Open `crond` in a text editor such as `vi` editor and add `-s` to the `CRONDARGS` value. If you use the default value, the check results will be output to `/var/log/cron`.

```
CRONDARGS=-s
```

- Restart the service to apply the crond settings. Run the following command.

```
systemctl restart crond
```

### Result

At the specified time, the results are output to `syslog`. Search the `syslog` file for `Cert Status`. The result will be `good`, `revoked`, or `unknown`.

## Changing the management server host name, IP address, or port number

If you change the management server host name or IP address or the port number used by Common Services, run the `cschgconnect` command to change the URL for accessing the Hitachi Ops Center Portal.

## Procedure

1. Log in to the management server as the root user.  
If you log in as an ordinary user, use the `sudo` command to complete the following procedure as the root user.
2. Run the `cschgconnect` command.

### Command location

```
installation-directory-of-Common-Services/utility/bin/  
cschgconnect.sh
```

### Format

```
cschgconnect.sh [-h host-name-or-IP-address] [-p port-number] | -enableip  
{true|false} | -list
```

### Options

#### **-h *host-name-or-IP-address***

Specify the host name (or FQDN) or IP address used to access the Hitachi Ops Center Portal. If you specify a host name (or FQDN), specify a value using no more than 128 characters. For the host name (or FQDN), you cannot specify uppercase characters. If you do, they are converted to lowercase characters and then registered.

The management server on which Common Services and other relevant products are installed and the web browser used to access the Hitachi Ops Center Portal must be able to resolve and reach the host name (or FQDN) and IP address.

#### **-p *port-number***

Specify the port number used by Common Services.



**Note:** If you change the port number, you must also change the firewall setting.

#### **-enableip {*true|false*}**

Specify whether an IP address can be used when the host name or FQDN is used in the URL for the Hitachi Ops Center Portal. To specify that the portal can be accessed by using an IP address, specify `true`. To specify that the portal cannot be accessed by using an IP address, specify `false`. The IP address for accessing the portal is automatically acquired from the system.

This option and other options cannot be specified at the same time.

#### **-list**

Displays the current settings. This option and other options cannot be specified at the same time.

If you change the settings by using the `-h`, `-p`, or `-enableip` option, the settings displayed when you specify the `-list` option are not applied to the system until the Common Services service is restarted.



**Note:** If you use this command to change the host name or IP address to one that differs from the value set for `CN` or `subjectAltName` when the SSL server certificate was created, you must issue a new server certificate.

3. Restart the Common Services service.
4. Run `cschgconnect.sh -list` to check the result of the change.
5. Make sure that you can use a web browser to access the login window at the following URL:

`https://host-name-or-IP-address:port-number/portal/`

6. For each product registered in Common Services, run the `setupcommonservice` command for registering the product in Common Services again.  
For details, see the documentation for each product.

## Changing the port number used for internal communications

You can change the port number that Common Services uses for internal communications.

### Procedure

1. Log in to the management server as the root user.  
If you log in as an ordinary user, use the `sudo` command to complete the following procedure as the root user.
2. Change the port number.  
The procedure differs depending on the port number.

Port number	Change procedure
20951	<p><b>a.</b> In the following property file, specify the port number after the change, and then save the file.</p> <p><b>Property file location*</b> <code>/var/installation-directory-of-Common-Services/userconf/config_user.properties</code></p> <p><b>Settings</b></p> <pre style="background-color: #f0f0f0; padding: 5px;">CS_PORTAL_PORT=port-number-after-change CS_GW_PORTAL_PORT=port-number-after-change</pre> <p><b>b.</b> Restart the Common Services service.</p>
20952	<p><b>a.</b> In the following property file, specify the port number after the change, and then save the file.</p>

Port number	Change procedure
	<p><b>Property file location*</b>  <i>/var/installation-directory-of-Common-Services/userconf/config_user.properties</i></p> <p><b>Settings</b></p> <pre>CS_PORTAL_IDP_PORT=port-number-after-change CS_IDP_OP_HTTP_PORT=port-number-after-change CS_GW_IDP_PORT=port-number-after-change</pre> <p><b>b.</b> Restart the Common Services service.</p>
20954	<p><b>a.</b> In the following property file, specify the port number after the change, and then save the file.</p> <p><b>Property file location*</b>  <i>/var/installation-directory-of-Common-Services/userconf/config_user.properties</i></p> <p><b>Setting</b></p> <pre>CS_PORTAL_IDP_POSTGRESQL_PORT=port-number-after-change</pre> <p><b>b.</b> In the following configuration definitions file, specify the port number after the change, and then save the file.</p> <p><b>Definitions file location*</b>  <i>/var/installation-directory-of-Common-Services/pgdata/csidp/data/postgresql.conf</i></p> <p><b>Setting</b></p> <pre>port = port-number-after-change # (change requires restart)</pre> <p><b>c.</b> Stop the Common Services service.  <b>d.</b> Run the <b>systemctl</b> command to restart <code>postgresql-11@csidp</code>.  <b>e.</b> Start the Common Services service.</p>
20955	<p><b>a.</b> In the following property file, specify the port number after the change, and then save the file.</p> <p><b>Property file location*</b>  <i>/var/installation-directory-of-Common-Services/userconf/config_user.properties</i></p>

Port number	Change procedure
	<p><b>Setting</b></p> <pre>CS_PORTAL_POSTGRESQL_PORT=port-number-after-change</pre> <p><b>b.</b> In the following configuration definitions file, specify the port number after the change, and then save the file.</p> <p><b>Definitions file location*</b></p> <pre>/var/installation-directory-of-Common-Services/pgdata/csportal/data/postgresql.conf</pre> <p><b>Setting</b></p> <pre>port = port-number-after-change # (change requires restart)</pre> <p><b>c.</b> Stop the Common Services service.</p> <p><b>d.</b> Run the <code>systemctl</code> command to restart <code>postgresql-11@csportal</code>.</p> <p><b>e.</b> Start the Common Services service.</p>
20956	<p><b>a.</b> In the following property file, specify the port number after the change, and then save the file.</p> <p><b>Property file location*</b></p> <pre>/var/installation-directory-of-Common-Services/userconf/config_user.properties</pre> <p><b>Setting</b></p> <pre>CS_PORTAL_MANAGEMENT_PORT=port-number-after-change</pre> <p><b>b.</b> Restart the Common Services service.</p>
<p>* If you performed installation by using an OVA, the file is located in the following directory:</p> <pre>/var/opt/hitachi/CommonService/userconf/</pre>	

## Backing up Common Services

To back up data in Common Services, run the `csbackup` command. You can restore the backup data to an instance of Common Services in an environment that has the same installation configuration and version.

**Procedure**

1. As necessary, back up each product registered in Common Services.  
For details on how to back up each product, see the documentation for each product.
2. Log in to the management server as the root user.  
If you log in as an ordinary user, use the `sudo` command to complete the following procedure as the root user.
3. Stop the Common Services service.
4. Run the `csbackup` command.

**Command location**

```
installation-directory-of-Common-Services/utility/bin/  
csbackup.sh
```

**Format**

```
csbackup.sh -dir backup-destination-directory
```

**Option**

**-dir *backup-destination-directory***

Specify the path to the directory that stores the backup data. A relative path can be specified. A backup file, with the following file name, is output to the specified directory.

```
csbackup_YYYY-MM-DD-hh-mm-ss.jar
```



**Note:** Each time data is backed up, the number of backup files increases. For this reason, if data is backed up regularly over a long period of time, the backup files might take up a large amount of disk space. Delete backup files that are no longer necessary.

5. If the server certificate and secret key are stored in a location other than the following default, manually back up the server certificate and secret key.

```
/var/installation-directory-of-Common-Services/tls/
```

For example, for an OVA install uses the following directory:

```
/var/opt/hitachi/CommonService/tls/
```



**Note:** If SSL communication was set up by using the `cssslsetup` command, the secret key of the server certificate is stored in the location specified when the command was run.

6. Start the Common Services service.

## Restoring Common Services

To restore the Common Services backup data, run the `csrestore` command.

**Before you begin**

Make sure that the installation configuration and version of Common Services on the restoration-destination system are the same as those on the system where the backup was taken. You cannot restore backup data to a system that has a different installation configuration and version.

**Procedure**

1. Log in to the management server as the root user.  
If you log in as an ordinary user, use the `sudo` command to complete the following procedure as the root user.
2. Stop the Common Services service.
3. Run the `csrestore` command.

**Command location**

```
installation-directory-of-Common-Services/utility/bin/  
csrestore.sh
```

**Format**

```
csrestore.sh -file path-to-backup-file
```

**Option**

**-file path-to-backup-file**

Specify the path to the backup file to be restored. A relative path can be specified.

4. If the server certificate and secret key were stored in a location other than `/var/installation-directory-of-Common-Services/tls/*` and backed up manually, store the server certificate and secret key in the same location that was used for backup.

\* For example, for an OVA install uses the following directory:

```
/var/opt/hitachi/CommonService/tls/
```



**Note:** If you set up SSL communication by using the `cssslsetup` command prior to performing backup, store the server certificate and the secret key in the location you specified.

5. If the host name, IP address, or port number of Common Services at the restoration destination is changed, run the `cschgconnect` command to change the settings. For details on the `cschgconnect` command, see [Changing the management server host name, IP address, or port number \(on page 115\)](#).



**Note:** If the backup data of Common Services deployed by using the Analyzer viewpoint OVF is restored to Common Services installed by using the installer, you must change the port number of Common Services.

6. Start the Common Services service.

- As necessary, restore the backup data for each product registered in Common Services. For details on the restoration method and the prerequisites for restoring backup data, see the documentation for each product.

## Stopping unnecessary product services

After deploying the Ops Center OVA, you can stop the services of products that you do not use, and specify not to start the services when the OS starts.

After the OVA is deployed, as a best practice, we recommend that you remove any products that are not being used. If you decide not to remove them, you can use the `opsvmservicectl` command to stop multiple product services at the same time. You can also use the command to change the setting so that the services do not start when the OS starts.



**Note:** The `opsvmservicectl` command is installed when version 10.1.0 or a later version of the Ops Center OVA is deployed. If the installer or a version of the OVA earlier than 10.1.0 was used to construct the environment, uninstall any unnecessary products.

### Before you begin

After you deploy the OVA and finish the configuration using the setup tool (`opsvmsetup`).

### Procedure

- From a VMware vSphere client, log in to the guest OS as the root user.
- Run the `opsvmservicectl` command to stop the services for the products that are not needed.

#### Format

```
opsvmservicectl {disable|enable} product-name [product-name ...]
```

#### Options

##### **disable**

Stops the services for the specified products and prevents them from starting automatically when the OS starts. After you stop the services, the products remain registered in Common Services.

##### **enable**

Starts the services for the specified products and changes the setting so that the services automatically start when the OS starts.

##### ***product-name***

Specify the target products by specifying the following values. To specify multiple products, use spaces to separate the products.

Product name	Value to specify
Hitachi Ops Center Automator	Automator
Hitachi Ops Center Analyzer	Analyzer
Hitachi Ops Center Analyzer detail view	AnalyzerDetailView
Hitachi Ops Center API Configuration Manager	APIConfigurationManager
Hitachi Ops Center Protector	Protector
Hitachi Ops Center Administrator	Administrator
Hitachi Ops Center Common Services	CommonServices



**Note:** Do not perform an upgrade installation of a product that is disabled by using the `opsvmservicectl` command, because the product might not operate correctly.

3. Check the results by running the following command:

```
opsvmservicectl status
```

4. To delete the products, log in to the Hitachi Ops Center Portal and remove them.

## Resetting the trust relationship with each product

If unauthorized access to Common Services occurs or unauthorized operations are performed on the Common Services settings, information such as tokens exchanged between Common Services and each product might be leaked. In this case, reset and disable the information that might have been compromised.

### Procedure

1. Log in to the management server as the root user.  
If you log in as an ordinary user, use the `sudo` command to complete the following procedure as the root user.
2. Run the `csresettrustrelationship` command.

#### Command location

```
installation-directory-of-Common-Services/utility/bin/  
csresettrustrelationship.sh
```

**Format**

```
csresettrustrelationship.sh -f
```

**Option**

**-f**

Specify this option if you run this command. If you omit this option, the command usage is displayed.

**Output file**

The results of running the command are output to the following file:

```
/var/log/hitachi/CommonService/utility/  
result_reset_secert.json
```

**Note:**

- If you run this command, logged-in users might be forcibly logged out.
- This command runs for a period from several minutes to several tens of minutes, depending on the system configuration.
- When the command finishes running, Common Services restarts.

3. Check the content of the output file.

Make sure that the value of the `status` key is `SUCCESS` for both the `resetSecretResult` object and the `resetKeyResult` object.

If the value is `ERROR`, restart Common Services, and then rerun the command. If this does not resolve the problem, collect the failure information, and contact customer support.

4. If you are linking with the identity provider by using the SAML protocol, update the metadata for Common Services in AD FS.

This step is required because, when you reset the trust relationship, the authentication key of Common Services is forcibly updated.

For details of the procedure, see [Updating the Common Services metadata by using AD FS \(on page 107\)](#)

5. Run the `setupcommonservice` command for each product registered in Common Services.
6. Restart the service of each product registered in Common Services.

## Configuring the settings for session idle timeouts

After you log in to the Hitachi Ops Center Portal by using the single sign-on functionality of Common Services, if a specific amount of time elapses with no activity in the window, the session times out.

For the idle timeout settings, you can configure the following two settings:

- Idle timeout

Specify the amount of time that can elapse with no activity in the window before a timeout occurs. The default is 20 minutes.

- Auto refresh

Specify whether a timeout occurs if the idle timeout time elapses with no operation performed, for a window that automatically refreshes. By default, a timeout does not occur.

These settings apply to the following products: Automator, Analyzer, and Analyzer viewpoint.

You can configure the idle timeout settings by using the Hitachi Ops Center Portal. The settings will apply to each Hitachi Ops Center product within a few minutes.



**Note:**

- The idle timeout settings apply to Common Services and each Hitachi Ops Center product whose version is 10.9.0 or later (7.6.0 or later in the case of Protector). For Hitachi Ops Center products of a version earlier than 10.9.0 (earlier than 7.6.0 in the case of Protector), timeouts might not occur.
- Actual session timeouts might differ by a few minutes from the configured idle timeout time.

## Changing the scale of the resources managed by an individual product

On the management server where Common Services is installed, you can change the memory size to match the scale of the resources managed by a Hitachi Ops Center product. The target products are as follows:

- Hitachi Ops Center Analyzer
- Hitachi Ops Center Analyzer viewpoint

### Procedure

1. Log in to the management server as the root user.  
If you log in as an ordinary user, use the `sudo` command to complete the following procedure as the root user.
2. Run the `cschgscale` command.

#### Command location

```
installation-directory-of-Common-Services/utility/bin/  
cschgscale.sh
```

**Format**

```
cschgscale.sh {-scale scale-of-resources [-target Product-name] [-restart]
| -h}
```

**Options****-scale *scale-of-resources***

Specify the scale of the resources. The memory size are changed according to the specified value. Specify one of the following values. The values are not case sensitive.

- S: Small-scale configuration
- M: Medium-scale configuration
- L: Large-scale configuration

**Note:**

- You can check a detailed descriptions of the scales by using the `-h` option.
- For details on the system requirements for each product according to the scale, see *Hitachi Ops Center System Requirements*.

**-target *Product-name***

If you omit the `-target` option, all products targeted by the `cschgscale` command installed on the management server are changed. If you want to run the command for an individual product, specify the value as follows:

- `analyzer`: Hitachi Ops Center Analyzer
- `viewpoint`: Hitachi Ops Center Analyzer viewpoint



**Note:** You can use the `cschgscale` command for products whose version is 10.9.1 or later.

**-restart**

Specify this option when you are changing the product settings and want to apply the changes immediately. If you specify this option, the product service is restarted after the command is run, and the changes are applied.

**-h**

Displays usage information. This option displays a description of the options, the names of installed products for which the command can be used, and details of the `-scale` option.

## Settings required when using a virus detection program

If a virus detection program accesses database-related files used by Common Services, an error might occur for reasons such as I/O delays or file locks. To prevent such errors while Common Services is running, exclude the following directories from the targets scanned by the virus detection program:

- `/usr/pgsql-11/bin`
- `installation-directory-of-Common-Services/nginx/temp`
- `/var/installation-directory-of-Common-Services`

For details on the directories of other Ops Center products to exclude from the scanning targets, see the manual for each product.

## Upgrading Amazon Corretto 17

If a vulnerability is found in Amazon Corretto 17, upgrade Amazon Corretto 17.

### Procedure

1. Log in to the management server as the root user.  
If you log in as an ordinary user, use the `sudo` command to complete the following procedure as the root user.
2. Download Amazon Corretto 17, and store it on the management server where Common Services is installed.  
For details on the versions of Amazon Corretto 17 that are supported by Common Services, see the Common Services Release Notes.
3. Stop the Common Services service.



**Note:** If products that use Amazon Corretto 17 are installed on the management server, stop the services of those products as needed.

4. Run the `rpm` command with the `--nopost` option specified to upgrade Amazon Corretto 17.
5. Start the Common Services service.



**Note:** If products that use Amazon Corretto 17 are installed on the management server, start the services of those products as needed.

## Upgrading PostgreSQL 11

If a vulnerability is found in PostgreSQL 11, upgrade PostgreSQL 11.

### Procedure

1. Log in to the management server as the root user.  
If you log in as an ordinary user, use the `sudo` command to complete the following procedure as the root user.

2. Download PostgreSQL 11, and store it on the management server where Common Services is installed.

For details on the versions of PostgreSQL 11 that are supported by Common Services, see the Common Services Release Notes.

3. Stop the Common Services service.
4. Run the following command to stop the Common Services database:

```
systemctl stop postgresql-11@csportal.service postgresql-11@csidp.service
```

5. Run the `rpm` command to upgrade the RPM package for PostgreSQL 11.

```
rpm -Uv PostgreSQL-11-package-name postgresql11-libs-package-name postgresql11-server-package-name
```

6. Run the following command to start the Common Services database:

```
systemctl start postgresql-11@csportal.service postgresql-11@csidp.service
```

7. Start the Common Services service.

## Applying Linux security updates using yum

You can collectively (or selectively) apply OS security updates using the `yum` command. First, you must configure your server to access the RPM packages from the Linux OS media or the distribution website.

### Accessing the RPM packages using the Linux OS media

1. Mount the Linux OS media and obtain the RPM packages:

```
mkdir /media/OSImage
mount /dev/cdrom /media/OSImage
```

2. Configure the yum repository.

For Red Hat Enterprise Linux and Oracle Linux 7:

```
touch /etc/yum.repos.d/OSImage.repo
echo [dvd]>>/etc/yum.repos.d/OSImage.repo
echo name=dvd>>/etc/yum.repos.d/OSImage.repo
echo baseurl=file:///media/OSImage/>>/etc/yum.repos.d/OSImage.repo
echo gpgcheck=0>>/etc/yum.repos.d/OSImage.repo
echo enabled=1>>/etc/yum.repos.d/OSImage.repo
```

For Red Hat Enterprise Linux or Oracle Linux 8:

```
touch /etc/yum.repos.d/OSImage.repo
echo [dvd-baseos]>>/etc/yum.repos.d/OSImage.repo
echo name=dvd-baseos>>/etc/yum.repos.d/OSImage.repo
echo baseurl=file:///media/OSImage/BaseOS/>>/etc/yum.repos.d/OSImage.repo
```

```
echo gpgcheck=0>>/etc/yum.repos.d/OSImage.repo
echo enabled=1>>/etc/yum.repos.d/OSImage.repo
echo >>/etc/yum.repos.d/OSImage.repo
echo [dvd-appstream]>>/etc/yum.repos.d/OSImage.repo
echo name=dvd-appstream>>/etc/yum.repos.d/OSImage.repo
echo baseurl=file:///media/OSImage/AppStream/>>/etc/yum.repos.d/OSImage.repo
echo gpgcheck=0>>/etc/yum.repos.d/OSImage.repo
echo enabled=1>>/etc/yum.repos.d/OSImage.repo
```

## Accessing the RPM packages using the distribution website

1. Specify the repository to which the **yum** command will connect.
  - For Red Hat Enterprise Linux, register the system by using Red Hat Subscription Management. For details, see <https://access.redhat.com/articles/11258>.
  - For Oracle Linux, the initial settings are set by default (the file `repo` is already located in the directory `/etc/yum.repos.d`). For details, see <http://yum.oracle.com/getting-started.html>.
2. If you are using a proxy, specify the proxy for the **yum** command:
  - a. Add the following information to the `/etc/yum.conf` file:

```
proxy=http://host-name:port-number
proxy_username=user-name
proxy_password=password
```

- b. Clear the cache for the **yum** command.

```
yum clean all
```

## Using the yum command

To update all packages for which security-related errata are available (including packages with bug fixes or new features without security errata):

```
yum --security --exclude kernel* --exclude *podman* --exclude *containers-common*
upgrade
```

To update all packages for which security-related errata are available (ignoring any newer packages without security errata):

```
yum --security --exclude kernel* --exclude *podman* --exclude *containers-common*
upgrade-minimal
```

To update all kernel and podman packages to the latest supported versions that contain security errata, follow these examples.

For Red Hat kernel (must specify supported kernel version):

```
yum --security upgrade-minimal kernel-4.18.0-305.*
```

For Unbreakable Enterprise kernel (must specify supported uek kernel version):

```
yum --security upgrade-minimal kernel-uek-5.4.17-2102.*
```

For podman (must specify supported podman version):

```
yum --security upgrade-minimal podman-3.3.*
```

You can also update only those packages that correspond to a CVE or erratum, as in the following examples:

```
yum --cve CVE-2021-37576 upgrade-minimal
```

For Red Hat Enterprise Linux:

```
yum --advisory RHSA-2021:4056 upgrade-minimal
```

For Oracle Linux:

```
yum --advisory ELSA-2021-9474 upgrade-minimal
```

---

## Appendix A: Troubleshooting

Check the messages or log files to determine the cause of the error and take action. If you cannot determine the cause or resolve the error, collect the maintenance information about the management server and Common Services, and then contact support personnel.

### Collecting failure information

If a failure occurs while using Hitachi Ops Center, collect the failure information required to analyze the cause.

#### Procedure

1. Log in to the management server as the root user.  
If you log in as an ordinary user, use the `sudo` command to complete the following procedure as the root user.
2. To collect the failure information of Common Services, run the `csgetras` command.

#### Command location

```
installation-directory-of-Common-Services/utility/bin/  
csgetras.sh
```

#### Format

```
csgetras.sh -dir path-to-output-destination-directory
```

#### Option

**-dir** *path-to-output-destination-directory*

Specify the path to the directory to which the collected failure information is output. A relative path can be specified.

If you run the command, a file that compresses and archives the collected information is created.

3. As necessary, collect the failure information of each product registered in Common Services and the Server Express installer.  
For details on how to collect failure information, see the documentation for each product.  
For failure information for the Server Express installer, manually save the following log files.

Log file	Location	Description
ExpressInstaller_ version.hv_yyyymm dd-hhmmss.log	/tmp	The log file of the Server Express installer.
ExpressInstaller_ version.product- name_yyyymmdd- hhmmss.log	/tmp	The log files for the standard output displayed during the installation of products selected in the Server Express installer.  For <i>product-name</i> , one of the following strings is output: <ul style="list-style-type: none"> <li>▪ commonservices: Common Services</li> <li>▪ administrator: Ops Center Administrator</li> <li>▪ protector: Ops Center Protector</li> <li>▪ analyzer: Ops Center Analyzer</li> <li>▪ detailview: Ops Center Analyzer detail view</li> </ul>
ExpressInstaller_ version.command- name_yyyymmdd- hhmmss.log	/tmp	The log file output when a command is run by the Server Express installer.  For <i>command-name</i> , the following string is output: <ul style="list-style-type: none"> <li>▪ cschgscale: Output when a product is newly installed and resources have been configured.</li> </ul>
COMSERV_Report.tx t	/var/log/ hitachi/ CommonService/ inst	Installation report file that is output if Common Services is installed.

4. To collect the following failure information for work performed on a server where Common Services is not installed, log in to the server:

- Client Express installer
- SSL Setup tool (Use the `csss1setup` command in `utility.tar.`)

Manually save the following log files.

Log file	Location	Description
ClientExpressInstaller_version.hv_yyyymmdd-hhmmss.log	/tmp	The log file of the Client Express installer.
ClientExpressInstaller_version.product-name_yyyymmdd-hhmmss.log	/tmp	The log files for the standard output displayed during the installation of products selected in the Client Express installer.  For <i>product-name</i> , one of the following strings is output: <ul style="list-style-type: none"> <li>▪ probe: Ops Center Analyzer probe server</li> <li>▪ ConfManager: Ops Center API Configuration Manager</li> <li>▪ protector: Ops Center Protector Client</li> </ul>
csslsetup_YYYY-MM-DD-hh-mm-ss.log	/tmp	The log file when the SSL Setup tool ( <b>csslsetup</b> command) was run.

## Common Services logs

In Common Services, log files are output and can be used to analyze the causes of failures that occur.

Three types of log files are output for Common Services.

### Output-destination directory

/var/log/hitachi/CommonService

## Log files

Log file	Description
<code>error.log</code>	The Common Services error log is output to this file. Check the contents of this file as needed.
<code>debug.log</code>	This log file is necessary for customer support to analyze the cause of a failure when, for example, you cannot identify the cause or cannot perform recovery.
<code>server.log</code>	This log file is necessary for customer support to analyze the cause of a failure when, for example, you cannot identify the cause or cannot perform recovery.

The following items are output to `error.log`.

Item	Description
Date and time	The date and time when the log was output
Level	The log level
Thread name	The name of the internal processing of Common Services
Message ID	The message ID in the following format. <code>KAOPnnnnn-Z</code> In the above, <code>nnnnn</code> is the message number. <code>Z</code> is the message type. <ul style="list-style-type: none"> <li>▪ E: Error message</li> <li>▪ W: Warning message</li> <li>▪ I: Information</li> </ul>
Message	The message corresponding to the message ID
Exception	Information about the exception that occurred

## Changing the properties of logs

You can change the properties of Common Services logs to change how the logs are output.

### Procedure

1. Log in to the management server as the root user.  
 If you log in as an ordinary user, use the `sudo` command to complete the following procedure as the root user.

2. Edit the following properties file.

```
/var/installation-directory-of-Common-Services/userconf/  
config_user.properties
```

For example, for an OVA install uses the following file:

```
/var/opt/hitachi/CommonService/userconf/config_user.properties
```

The properties of logs are as follows:

Property	Description
CS_PORTAL_LOG_LEVEL_DEBUG	<p>Specify the level for which the debug log is to be output.</p> <p>You can specify one of the following values (listed in descending order of detail level): TRACE, DEBUG, and INFO.</p> <p>Default value: DEBUG</p>
CS_PORTAL_LOG_MAX_FILESIZE	<p>Specify the maximum size of each log file.</p> <p>When the size of a log file exceeds the specified size, a new log file is created.</p> <p>The value of this property must be specified in the form of an integer and a unit.</p> <p>You can specify KB, MB, or GB for the unit. KB, MB, and GB correspond to KiB, MiB, and GiB, respectively. If you do not specify a unit, the unit is assumed to be bytes.</p> <p>Default value: 20MB</p>
CS_PORTAL_LOG_MAX_INDEX_ERROR	<p>Specify the maximum number of error log backups to keep.</p> <p>When the error log file reaches the maximum size specified for the CS_PORTAL_LOG_MAX_FILESIZE property, a backup of the file is created, where the name of the backup file is the original file name with a number appended to the end. Each time the log file reaches the maximum size, a new backup file is created until the number of backup files reaches the number specified for this property. After this number of backup files is reached, each time a new backup file is created, the oldest backup file is deleted.</p> <p>You can specify a value in the range from 1 to 21.</p>

Property	Description
	Default value: 10
CS_PORTAL_LOG_MAX_INDEX_DEBUG	<p>Specify the maximum number of debug log backups to keep.</p> <p>When the debug log file reaches the maximum size specified for the CS_PORTAL_LOG_MAX_FILESIZE property, a backup of the file is created, where the name of the backup file is the original file name with a number appended to the end. Each time the log file reaches the maximum size, a new backup file is created until the number of backup files reaches the number specified for this property. After this number of backup files is reached, each time a new backup file is created, the oldest backup file is deleted.</p> <p>You can specify a value in the range from 1 to 21.</p> <p>Default value: 20</p>
CS_PORTAL_LOG_MAX_INDEX_APPLOG	<p>Specify the maximum number of server log backups to keep.</p> <p>When the server log file reaches the maximum size specified for the CS_PORTAL_LOG_MAX_FILESIZE property, a backup of the file is created, where the name of the backup file is the original file name with a number appended to the end. Each time the log file reaches the maximum size, a new backup file is created until the number of backup files reaches the number specified for this property. After this number of backup files is reached, each time a new backup file is created, the oldest backup file is deleted.</p> <p>You can specify a value in the range from 1 to 21.</p> <p>Default value: 20</p>

- Restart the Common Services service.

## Common Services audit log

Common Services can output audit log information about who performed which operation and when. By default, the audit log output is disabled, but you can enable it and change the properties as needed.

### Output destination

The audit log is output to the `syslog`.

### Output items

The following items are output to the audit log.

Location	Item	Description	Example
PRI	Priority	A number that indicates the priority level.  This number is converted from the facility value and the log level. The facility value is converted based on the value set for the <code>CS_PORTAL_AUDIT_FACILITY</code> property.	<11>
HEADER	Date and time	The date and time when the auditing event occurred	Sep 2 13:15:04
	Host name	The name of the host for which the auditing event occurred	WIN-00ABCD11EFG
MSG	Process ID	The process ID	5828
	Thread ID	The thread ID	http-nio-8081-exec-2
	Log level	The log level, such as <code>ERROR</code> or <code>DEBUG</code>	ERROR
	Date and time	The date and time when the audit log was output	2019-09-02T13:15:04.362+0900
	Message ID	The message ID	KAOP91111-E
	Type of auditing event	The auditing event type, such as <code>StartStop</code> or <code>Authentication</code>	Authentication

Location	Item	Description	Example
	Result of the auditing event	The result of the event, such as whether the event was successful or not	Success
	Subject-identifying information	Information such as the user ID or a URI	User ID=system,URI=/portal
	Message	The message	KAOP91111-E Audit Log.

The auditing event types that are output and their corresponding severity levels are as follows. You can change the properties of the audit log to narrow down the severity levels that are output.

Type of auditing event	Description	Corresponding severity level
Authentication	Indicates an auditing event that is related to login or authentication	If the event is successful: 6 If the event fails: 4
ConfigurationAccess	Indicates an auditing event that is related to the creation, referencing, modification, or deletion of a user account or user group	If the event is successful: 6 If the event fails: 3

## Changing the audit log properties

You can change the Common Services audit log properties to change the output.

### Procedure

1. Log in to the management server as the root user.  
If you log in as an ordinary user, use the `sudo` command to complete the following procedure as the root user.
2. Edit the following properties file.

```
/var/installation-directory-of-Common-Services/userconf/  
config_user.properties
```

For example, for an OVA install uses the following file:

```
/var/opt/hitachi/CommonService/userconf/config_user.properties
```

The properties of the audit log are as follows:

Property	Description
CS_PORTAL_AUDIT_ENABLE	<p>Specify one of the following values to indicate whether to generate the audit log.</p> <ul style="list-style-type: none"> <li>▪ true: Generate the audit log.</li> <li>▪ false: Do not generate the audit log.</li> </ul> <p>Default value: false</p>
CS_PORTAL_AUDIT_SYSLOGHOST	<p>If you want audit logs output to a server other than the management server on which Common Services is installed, specify the host name or IP address of that server.</p> <p>Default value: localhost</p>
CS_PORTAL_AUDIT_PORT	<p>Specify the port number of the syslog server.</p> <p>Default value: 514</p>
CS_PORTAL_AUDIT_FACILITY	<p>Specify the information needed to identify the sender of a message.</p> <p>You can specify the following values:</p> <ul style="list-style-type: none"> <li>▪ KERN</li> <li>▪ USER</li> <li>▪ MAIL</li> <li>▪ DAEMON</li> <li>▪ AUTH</li> <li>▪ SYSLOG</li> <li>▪ LPR</li> <li>▪ NEWS</li> <li>▪ UUCP</li> <li>▪ CRON</li> <li>▪ AUTHPRIV</li> <li>▪ FTP</li> <li>▪ NTP</li> <li>▪ AUDIT</li> <li>▪ ALERT</li> <li>▪ CLOCK</li> <li>▪ LOCAL0</li> <li>▪ LOCAL1</li> <li>▪ LOCAL2</li> </ul>

Property	Description
	<ul style="list-style-type: none"> <li>▪ LOCAL3</li> <li>▪ LOCAL4</li> <li>▪ LOCAL5</li> <li>▪ LOCAL6</li> <li>▪ LOCAL7</li> </ul> <p>Default value: USER</p>
CS_PORTAL_AUDIT_LEVEL	<p>Specify the severity levels to include in the audit log output. You can specify the following values.</p> <ul style="list-style-type: none"> <li>▪ DEBUG: Output the audit log for severity levels 0 to 7.</li> <li>▪ INFO: Output the audit log for severity levels 0 to 6.</li> <li>▪ WARN: Output the audit log for severity levels 0 to 4.</li> <li>▪ ERROR: Output the audit log for severity levels 0 to 3.</li> </ul> <p>Default value: INFO</p>

3. Restart the Common Services service.

## Determining the parameters for LDAP server registration

If you want to link with an LDAP server, when you register the link with the LDAP server in Common Services, you must set parameters to import users.

Run the `ldapsearch` command on the LDAP server, and then determine the parameters based on the information returned by the search.

### Procedure

1. Log in to the LDAP server from the LDAP client and then run the `ldapsearch` command.

#### Example of the command syntax:

```
ldapsearch -h host-name-or-IP-address-of-the-LDAP-server -b base-DN-to-be-found -D bind-dn -w password-of-the-bind-DN -L -s scope-of-the-search
```

For details, see the LDAP server documentation.

#### Example of running command:

```
ldapsearch -h example.com -b "CN=Users,DC=example,DC=com" -D "CN=admin,CN=Users,DC=example,DC=com" -w sysadmin -L -s sub (objectclass=*)
```

**Example of LDIF data:**

```
dn: CN=John Smith,CN=Users,DC=example,DC=com
objectClass: person
objectClass: organizationalPerson
uid: j_smith
cn: John Smith
sn: Smith
givenName: John
distinguishedName: CN=John Smith,CN=Users,DC=example,DC=com
whenCreated: 20200710022002.0Z
whenChanged: 20210603075422.0Z
memberOf: CN=opscenter_users,CN=Users,DC=example,DC=com
mail: j_smith@example.com
objectGUID:: hMekv/PMMkyVnykQ5AeMyQ==
description: type1

dn: CN=Tom Brady,CN=Users,DC=example,DC=com
objectClass: person
objectClass: organizationalPerson
uid: t_brady
cn: Tom Brady
sn: Brady
givenName: Tom
distinguishedName: CN=Tom Brady,CN=Users,DC=example,DC=com
whenCreated: 20200710022057.0Z
whenChanged: 20210601074245.0Z
memberOf: CN=hcs_users,CN=Users,DC=example,DC=com
mail: t_brady@example.com
objectGUID:: pZtOMo29j0CSofnJrkL3EQ==
description: type2
```

2. Based on the displayed LDIF data, determine the parameter information to set in Common Services.

The following table shows an example of the correspondence between the settings in Common Services and the LDAP attributes.

Setting in Common Services	LDAP user attribute
LDAP attribute for username	uid
LDAP attribute for email	mail
LDAP attribute for last name	sn
Full name*	cn
First name*	givenName
LDAP attribute for RDN	cn

Setting in Common Services	LDAP user attribute
LDAP attribute for UUID	objectGUID
User object classes	organizationalPerson
Custom user LDAP filter	(description=type1)
*: Set one of these settings.	

You can specify a search filter in **Custom User LDAP Filter** to narrow down the users to be imported. (The syntax must conform to RFC 2254.)

**Hitachi Vantara**

Corporate Headquarters  
2535 Augustine Drive  
Santa Clara, CA 95054 USA



[HitachiVantara.com/contact](https://HitachiVantara.com/contact)