

Hitachi Ops Center Automator

10.8.3

Installation and Configuration Guide

Ops Center Automator is a software solution that provides the necessary tools to automate and simplify end-to-end processes, such as storage provisioning, for storage and data center administrators. This manual describes how to install and configure Ops Center Automator.

© 2019, 2022 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.

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.

AI/3, 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, z/VM, and z/VSE are registered trademarks or trademarks of International Business Machines Corporation.

Active Directory, ActiveX, Bing, Edge, Excel, Hyper-V, Internet Explorer, the Internet Explorer logo, Microsoft, 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.

Contents

Preface.....	8
Intended audience.....	8
Product version.....	8
Release notes.....	8
Referenced documents.....	8
Document conventions.....	8
Conventions for storage capacity values.....	10
Accessing product documentation.....	11
Getting help.....	11
Comments.....	11
Chapter 1: Overview	12
Product overview.....	12
About related Hitachi Ops Center products.....	12
Ops Center Automator system configuration.....	13
Ops Center Automator installation and configuration workflow.....	13
Authentication methods in Ops Center Automator.....	14
Chapter 2: System requirements	15
System requirements for installing on Windows.....	15
System requirements for installing on Linux.....	16
Hardware and disk space requirements.....	22
Port requirements.....	24
Maximum resource support.....	32
Web client requirements	32
Virtualization and cluster support.....	33
Management target requirements.....	34
Chapter 3: Installing and upgrading Ops Center Automator.....	36
Installation prerequisites.....	36
Changing the server time	37
Changing the name resolution setting.....	38
Avoiding port conflicts.....	39
Installing and upgrading Ops Center Automator (Windows OS).....	39

Installing and upgrading Ops Center Automator in a cluster environment (Windows OS).....	40
About using Ops Center Automator in a cluster environment.....	40
Cluster installation workflow.....	41
Verifying the cluster configuration using the cluster management software..	42
Setting up Ops Center Automator clustering on an active node.....	42
Setting up Ops Center Automator clustering on a standby node.....	44
Registering the services and initializing the cluster installation.....	45
Installing and upgrading Ops Center Automator (Linux OS).....	46
Required settings when using a virus detection program.....	46
Post-installation tasks	47
Confirming the registered URL (Windows OS).....	48
Confirming the registered URL (Linux OS).....	48
Verifying the installation.....	48
Registering a license.....	49
Changing the system account password	49
Setting an e-mail address for the System account.....	49
Stopping and starting Common Component and Ops Center Automator services.....	50
Stopping and starting all services from a command prompt (Windows OS).....	50
Stopping and starting all services from a command prompt (Linux OS).....	50
Stopping and starting only the Ops Center Automator services from the command prompt (Windows OS).....	51
Stopping and starting only the Ops Center Automator services from the command prompt (Linux OS).....	51
Configuring single sign-on in Common Services.....	51
Registering Ops Center Automator with Ops Center Common Services.....	51
setupcommonservice command.....	52
Chapter 4: Configuring Ops Center Automator.....	54
Changing management server system settings.....	54
Changing the port number used for management server communication with management clients	54
Common Component property updates for port number changes.....	56
Changing the information of the server managing the user account.....	58
Changing the management server host name.....	59
Changing the management server IP address.....	60
Changing the Ops Center Automator management server URL.....	60
Configuring secure communications.....	61
About Ops Center Automator security settings.....	61
Secure communication routes for Ops Center Automator.....	62

Configuring security for management clients.....	63
About secure communications for management clients.....	64
Setting up SSL on the server for secure client communication (Windows OS).....	64
Setting up SSL on the server for secure client communication (Linux OS).....	69
Setting up SSL on web-based management clients.....	75
Setting up secure communication for an external authentication server.....	75
Importing a certificate into the truststore for Common Component.....	76
Changing the authenticator connection port number for the primary Common Component server.....	77
Setting up secure communications with Ops Center Common Services.....	78
Setting up secure communication with an Ops Center API Configuration Manager REST API server.....	79
Setting up secure communication with an Ops Center Administrator server.....	79
Setting up secure communication with an Ops Center Protector server.....	80
Setting up secure communication with an Ops Center Analyzer server.....	81
Setting up secure communication with a VMware vCenter server.....	82
Importing certificates for secure communication with external web servers.....	83
Verifying the server certificate expiration date.....	84
Deleting Common Component truststore certificates.....	85
Audit logging.....	86
Configuring the audit log.....	86
Enabling audit logging.....	88
Settings in the auditlog.conf file.....	89
Sample auditlog.conf file.....	91
Format of data output to the audit log.....	91
Changing the system configuration	94
Configuring the performance mode.....	106
Configuring email notifications	106
Changing the password policy	108
About account locking.....	111
About account locking policies.....	111
Setting account locking policies.....	112
Automatically locking the System account.....	112
Unlocking accounts.....	113
Operating systems supporting remote connections	114
Configuring remote machine connection information for plug-ins and services.....	116
Windows OS prerequisites for agentless connections.....	122
SSH prerequisites for agentless connections.....	123

Password authentication.....	124
Public key authentication.....	124
Keyboard interactive authentication.....	126
Setting the java heap memory size on the Ops Center API Configuration Manager server.....	126

Chapter 5: User management on an external authentication server.... 128

About linking to an external authentication server.....	128
About linking to an external authorization server.....	128
Workflow for user authentication on an LDAP directory server.....	129
Workflow for user authentication on a RADIUS server.....	129
Workflow for user authentication on a Kerberos server.....	130
About the data structures of user entries.....	131
About the BaseDN.....	131
About the hierarchical structure model.....	132
About the flat model.....	132
Configurations when multiple external authentication servers are linked.....	132
Registering an external authentication server and an external authorization server.....	134
Setup items in the exauth.properties file for LDAP authentication.....	137
Examples of setting the exauth.properties file for LDAP authentication.....	145
Setup items in the exauth.properties file for RADIUS authentication.....	148
Examples of setting the exauth.properties file for RADIUS authentication	157
Setup items in the exauth.properties file for Kerberos authentication.....	159
Examples of setting the exauth.properties file for Kerberos authentication.....	166
About LDAP search user accounts.....	168
Conditions for LDAP search user account.....	169
Registering an LDAP search user account.....	170
Deleting an LDAP search user account.....	173
Verifying the LDAP directory server that registered the LDAP search user account.....	173
Registering a shared secret.....	174
Deleting a shared secret.....	174
Verifying the RADIUS server that registered a shared secret on the management server.....	175
Verifying connections to an external authentication server and an external authorization server.....	176
Command notes for setting up a link to an external authentication server.....	178
Encryption types for Kerberos authentication.....	179

Chapter 6: Backing up and restoring Ops Center Automator..... 180

Overview of backup and restore.....	180
-------------------------------------	-----

Backing up Ops Center Automator.....	180
Restoring Ops Center Automator.....	181
Moving Ops Center Automator to another host.....	183
Chapter 7: Removing Ops Center Automator.....	187
Removing Ops Center Automator (Windows OS)	187
Removing Ops Center Automator software in a cluster environment.....	188
Deleting authentication data (Windows OS).....	190
Removing Ops Center Automator (Linux OS)	191
Deleting authentication data (Linux OS).....	192
Appendix A: Ops Center Automator file location and ports.....	193
Ops Center Automator file location.....	193
Port settings.....	195
Appendix B: Ops Center Automator processes.....	199
Ops Center Automator processes (Windows)	199
Ops Center Automator processes (Linux).....	199
Appendix C: Troubleshooting.....	201
Collecting maintenance information.....	201
Collecting the log files.....	201
Appendix D: Notices.....	202
Notices.....	202
Index.....	206

Preface

This document describes how to install and configure Hitachi Ops Center Automator.

Intended audience

This document provides instructions for storage administrators, who are responsible for storage, services, and applications within the storage environment.

Product version

This document revision applies to Hitachi Ops Center Automator v10.8.3-00 or later.

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

Hitachi Ops Center Automator documents:

- *Hitachi Ops Center Automator User Guide*, MK-99AUT001
- *Hitachi Ops Center Automator Release Notes*, RN-99AUT00


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






Document conventions

This document uses the following typographic conventions:

Convention	Description
Bold	<ul style="list-style-type: none"> Indicates text in a window, including window titles, menus, menu options, buttons, fields, and labels. Example: Click OK. Indicates emphasized words in list items.
<i>Italic</i>	<ul style="list-style-type: none"> Indicates a document title or emphasized words in text. Indicates a variable, which is a placeholder for actual text provided by the user or for output by the system. Example: <pre>pairedisplay -g group</pre> (For exceptions to this convention for variables, see the entry for angle brackets.)
Monospace	Indicates text that is displayed on screen or entered by the user. Example: <code>pairedisplay -g oradb</code>
< > angle brackets	<p>Indicates variables in the following scenarios:</p> <ul style="list-style-type: none"> Variables are not clearly separated from the surrounding text or from other variables. Example: <pre>Status-<report-name><file-version>.csv</pre> Variables in headings.
[] 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	<p>Indicates that you have a choice between two or more options or arguments. Examples:</p> <p>[a b] indicates that you can choose a, b, or nothing.</p> <p>{ a b } indicates that you must choose either a or b.</p>

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

Icon	Label	Description
	Note	Calls attention to additional information.

Icon	Label	Description
	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.

Conventions for storage capacity values

Physical storage capacity values (for example, disk drive capacity) are calculated based on the following values:

Physical capacity unit	Value
1 kilobyte (KB)	1,000 (10^3) bytes
1 megabyte (MB)	1,000 KB or $1,000^2$ bytes
1 gigabyte (GB)	1,000 MB or $1,000^3$ bytes
1 terabyte (TB)	1,000 GB or $1,000^4$ bytes
1 petabyte (PB)	1,000 TB or $1,000^5$ bytes
1 exabyte (EB)	1,000 PB or $1,000^6$ bytes

Logical capacity values (for example, logical device capacity, cache memory capacity) are calculated based on the following values:

Logical capacity unit	Value
1 block	512 bytes
1 cylinder	Mainframe: 870 KB

Logical capacity unit	Value
	Open-systems: <ul style="list-style-type: none"> ▪ OPEN-V: 960 KB ▪ Others: 720 KB
1 KB	1,024 (2 ¹⁰) bytes
1 MB	1,024 KB or 1,024 ² bytes
1 GB	1,024 MB or 1,024 ³ bytes
1 TB	1,024 GB or 1,024 ⁴ bytes
1 PB	1,024 TB or 1,024 ⁵ bytes
1 EB	1,024 PB or 1,024 ⁶ bytes

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.

[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, register, and complete your profile.

Comments

Please send comments to 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

This module gives an overview of the Ops Center Automator software.

Product overview

Hitachi Ops Center Automator is a software solution that gives 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. These preconfigured templates are customized to your specific environment and processes for creating services that automate complex tasks such as resource provisioning. When configured, Ops Center Automator integrates with existing applications to automate common infrastructure management tasks by utilizing your existing infrastructure services.

Ops Center Automator includes the following features:

- Preconfigured service templates that help in creating automation services
- Automation services for intelligent provisioning of volumes from different storage classes
- Role-based access to defined services
- Performance-based pool selection that chooses the best performing pools from infrastructure groups and gives pool information to each task for specifying the volume usage details
- Common service management attributes that can be assigned and shared across all automation services

About related Hitachi Ops Center products

Ops Center Automator is a part of Hitachi Ops Center, which includes the following components:

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

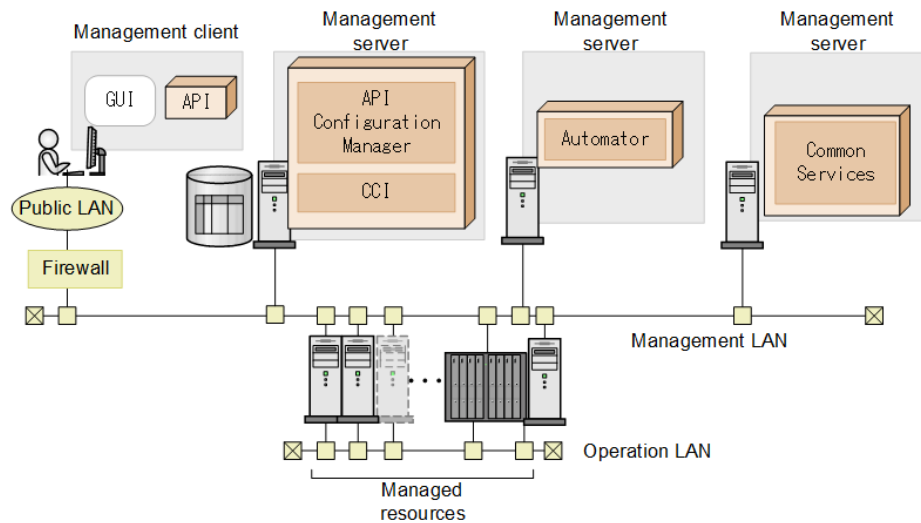
If you install Ops Center Automator along with other Hitachi Ops Center products, you can use common settings to manage users and security.

Ops Center Automator system configuration

The following gives information on the basic Ops Center Automator system configuration.

Configuration when using Ops Center API Configuration Manager

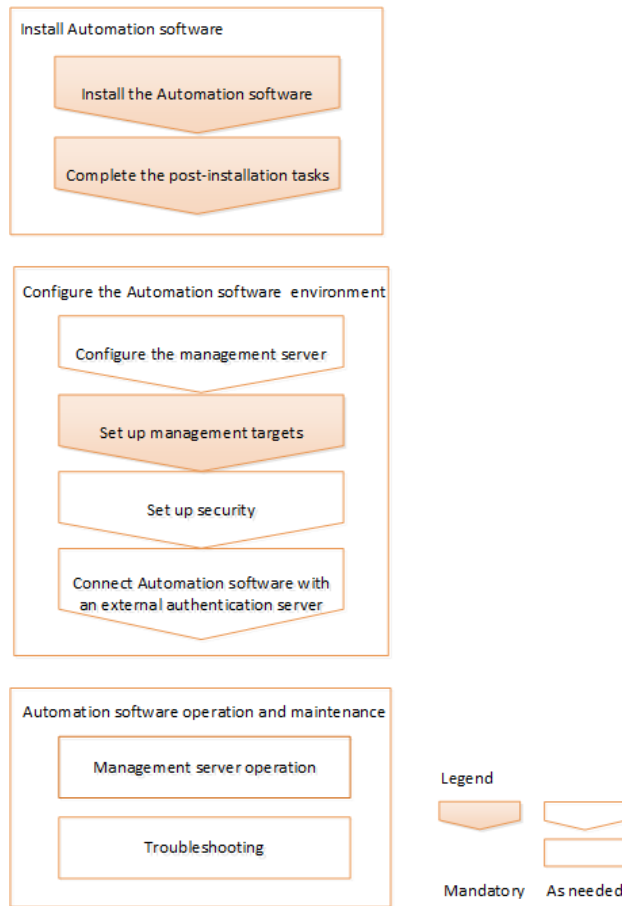
When using Ops Center Automator with Ops Center API Configuration Manager, you can install Ops Center Automator on one server and install Ops Center API Configuration Manager on another server, or you can install Ops Center Automator and Ops Center API Configuration Manager on the same server. The following figure shows the basic system configuration when using Ops Center API Configuration Manager.



Ops Center Automator supports version 10.0.0 or later of Hitachi Ops Center Common Services.

Ops Center Automator installation and configuration workflow

The following figure shows an overview workflow, which includes installing and configuring Ops Center Automator.



This guide includes system installation, setup, management, and maintenance information. For details about using the management UI to create, manage, and automate services, see the *Hitachi Ops Center Automator User Guide*.

Authentication methods in Ops Center Automator

When using Ops Center Automator, you can use the following authentication methods.

Ops Center Common Services

Select this method to use other Ops Center products.

External authentication

Select this method to use external authentication (LDAP authentication, RADIUS authentication, or Kerberos authentication).

Local user authentication

Select this method to use Automator's own user authentication.

Chapter 2: System requirements

This module gives the system requirements for installation.

If you are installing by using the Hitachi Ops Center OVA, see the *Hitachi Ops Center Installation and Configuration Guide*.

System requirements for installing on Windows

The following lists the server requirements for installing on Windows.

Supported operating systems



Note: No functional differences due to differing operating systems exist. Windows supports installations via Remote Desktop/Terminal Client with Console connection session.

OS name	Edition	SP	Architecture
<ul style="list-style-type: none">Windows Server 2012Windows Server 2012 R2 <p>Note: Server core and Minimal Server Interface are not supported.</p>	<ul style="list-style-type: none">StandardDatacenter	No SP	x64
<ul style="list-style-type: none">Windows Server 2016Windows Server 2019Windows Server 2022 <p>Note: Server core and Nano Server are not supported.</p>	<ul style="list-style-type: none">StandardDatacenter	No SP	x64

Prerequisite software

None.

IPv6 support

All installations on Windows servers support IPv6.

System requirements for installing on Linux

The following lists the server requirements for installing on Linux.

Supported operating systems

Each supported OS includes a list of RPM packages that are required for installing Ops Center Automator. When you install the software, the installation script notifies you if any of the packages are missing. If no RPM packages are missing, the installation proceeds.

- Red Hat Enterprise Linux 7.1 - 7.9, Oracle Linux 7.2 - 7.9, CentOS 7.2

After installing the default OS, the following packages are required:

- glibc-2.17-xx.el7.i686.rpm or later
- libstdc++-4.8.x-xx.el7.i686.rpm or later
- glibc-2.17-55.el7.x86_64.rpm or later
- libgcc-4.8.2-16.el7.x86_64.rpm or later
- libstdc++-4.8.2-16.el7.x86_64.rpm or later
- nss-softokn-freebl-3.15.4-2.el7.x86_64.rpm or later
- alsa-lib-1.0.27.2-3.el7.x86_64.rpm or later
- net-tools-2.0-0.17.20131004git.el7.x86_64.rpm or later
- tcsh-6.18.01-7.el7.x86_64.rpm or later
- ncurses-5.9-13.xx.el7.x86_64.rpm or later
- hostname-3.13-x.el7.x86_64.rpm or later
- tar-1.26-xx.el7.x86_64.rpm or later
- gzip-1.5-7.el7.x86_64.rpm or later
- perl-5.16.3-283.el7.x86_64.rpm or later
- policycoreutils-python-2.2.5-15.el7.x86_64.rpm or later
- policycoreutils-2.2.5-15.el7.x86_64.rpm or later
- coreutils-8.22-11.el7.x86_64.rpm or later
- libselinux-utils-2.2.2-6.el7.x86_64.rpm or later
- chkconfig-1.3.61-4.el7.x86_64.rpm or later
- gawk-4.0.2-4.el7.x86_64.rpm or later
- grep-2.20-1.el7.x86_64.rpm or later
- iproute-3.10.0-21.el7.x86_64.rpm or later
- procps-ng-3.3.10-3.el7.x86_64.rpm or later
- sed-4.2.2-5.el7.x86_64.rpm or later
- nss-softokn-freebl-3.16.2.3-9.el7.i686.rpm or later

- Red Hat Enterprise Linux 8.1, 8.2, 8.4, Oracle Linux 8.1, 8.2, 8.4

After installing the default OS, the following packages are required:

- glibc-2.28-72.el8.i686.rpm or later
- glibc-2.28-72.el8.x86_64.rpm or later
- libgcc-8.3.1-4.5.el8.i686.rpm or later
- libstdc++-8.3.1-4.5.el8.i686.rpm or later
- alsa-lib-1.1.9-4.el8.x86_64.rpm or later
- bzip2-libs-1.0.6-26.el8.x86_64.rpm or later
- expat-2.2.5-3.el8.x86_64.rpm or later
- freetype-2.9.1-4.el8.x86_64.rpm or later
- libnsl-2.28-72.el8.x86_64.rpm or later
- libpng-2:1.6.34-5.el8.x86_64.rpm or later
- libuuid-2.32.1-17.el8.x86_64.rpm or later
- zlib-1.2.11-10.el8.x86_64.rpm or later
- libxcrypt-4.1.1-4.el8.x86_64.rpm or later
- tcsh-6.20.00-9.el8.x86_64.rpm or later
- net-tools-2.0-0.51.20160912git.el8.x86_64.rpm or later
- ncurses-6.1-7.20180224.el8.x86_64.rpm or later
- glibc-langpack-en-2.28-xx.el8.x86_64.rpm or later
- tar-1.30-4.el8.x86_64.rpm or later
- hostname-3.20-6.el8.x86_64.rpm or later
- libgcc-8.3.1-4.5.el8.x86_64.rpm or later
- libstdc++-8.3.1-4.5.el8.x86_64.rpm or later
- gzip-1.9-9.el8.x86_64.rpm or later
- perl-5.26.3-416.el8.x86_64.rpm or later
- policycoreutils-python-utils-2.9-3.el8.noarch.rpm or later
- policycoreutils-2.9-3.el8.x86_64.rpm or later
- coreutils-8.30-6.el8.x86_64.rpm or later
- libselinux-utils-2.9-2.1.el8.x86_64.rpm or later
- chkconfig-1.11-1.el8.x86_64.rpm or later
- gawk-4.2.1-1.el8.x86_64.rpm or later
- grep-3.1-6.el8.x86_64.rpm or later
- iproute-4.18.0-15.el8.x86_64.rpm or later
- procps-ng-3.3.15-1.el8.x86_64.rpm or later
- sed-4.5-1.el8.x86_64.rpm or later

- nss-sofokn-freebl-3.44.0-8.el8.i686.rpm or later

Prerequisite software

None.

Kernel parameters and shell restrictions

In Linux, you must set the following kernel parameter and shell restriction values:

File*	Parameter	Value to be set
/etc/sysctl.conf	fs.file-max kernel.threads kernel.msgmni kernel.sem (4th and 2nd paramter) kernel.shmmax kernel.shmmni kernel.shmall	See "Kernel parameter and shell restriction details" below.
/etc/security/limits.conf	soft nofile hard nofile	See "Kernel parameter and shell restriction details" below.
/etc/security/limits.d/20-nproc.conf	soft nproc hard nproc	See "Kernel parameter and shell restriction details" below.
/etc/systemd/system.conf	DefaultLimitNOFILE	Specify the same value as nofile in limits.conf.
/etc/systemd/system.conf	DefaultLimitNPROC	Specify the same value as nproc in 20-nproc.conf.
* The file path differs according to the environment. In addition, note that kernel parameters and shell restrictions can also be set for files that are not listed here.		

Kernel parameter and shell restriction details**Red Hat Enterprise Linux and Oracle Linux****Table 1 Red Hat Enterprise Linux and Oracle Linux version 7.x and 8.x**

Parameters		Operating System Initial Value	Ops Center Automator	Common Component	Embedded database
kernel parameters (/etc/sysctl.conf) *	fs.file-max	99,483	133,384	42,276	42,276
	kernel.thread s-max	16,384	615	142	576
	kernel.msgm ni	1,978	53	44	44
	4th parameter of kernel.sem	128	1,235	9	1,024
	2nd parameter of kernel.sem	32,000	8,646	80	7,200
	kernel.shmm ax	4,294,967,295	238,248,346	24,372,224	200,000,000
	kernel.shmm ni	4,096	2,400	0	2,000
	kernel.shmall	268,435,456	175,963,623	23,793,664	24,372,224
shell restrictions (/etc/security/limits.conf) *	nofile (soft / hard)	4,096	1,104	1,346	8,192
shell restrictions (/etc/security/limits.d/20-nproc.conf) *	nproc (soft / hard)	8,192	1,398	198	512
*: For the calculation formula of /etc/sysctl.conf, /etc/security/limits.conf, and /etc/security/limits.d/20-nproc.conf, see the following sections.					

Values for /etc/sysctl.conf

For kernel.shmmax:

```
kernel-parameter-value-to-be-set =
Max{
    Max{
        value-that-is-enabled-in-the-system
        ,
        initial-value-of-the-OS
    }
    ,
    value-for-Common-Component
+ value-for-Automator
    ,
    value-for-embedded-database
}
```

For kernel.shmall:

```
kernel-parameter-value-to-be-set =
Max{
    value-that-is-enabled-in-the-system
    ,
    initial-value-of-the-OS
}
+ value-for-Common-Component
+ value-for-Automator
+ value-for-embedded-database
```

Other kernel parameters and shell restrictions:

```
kernel-parameter-value-to-be-set =
Max{
    Max{
        value-that-is-enabled-in-the-system
        ,
        initial-value-of-the-OS
    }
    + value-for-Common-Component
    + value-for-Automator
    ,
    value-for-embedded-database
}
```

**Note:** Max{x, y, z} indicates the maximum value among x, y, and z.

Values for /etc/security/limits.conf and /etc/security/limits.d/20-nproc.conf

The following formula is for calculating the values for the shell restriction:

```
shell-restrictions-value-to-be-set =
Max{
    Max{
        value-that-is-enabled-in-the-system
        ,
        initial-value-of-the-OS
    }
    + value-for-Common-Component
    + value-for-Automator
    ,
    value-for-embedded-database
}
```



Note: Max{x, y, z} indicates the maximum value among x, y, and z.

IPv6 support

The following Linux versions support IPv6:

- Red Hat Enterprise Linux versions 7.1-7.9, 8.1, 8.2, and 8.4
- Oracle Linux versions 7.2-7.9, 8.1, 8.2, and 8.4



Note: You must evaluate the Linux version before using it on a cluster or VMware environment.

Hardware and disk space requirements

The hardware and disk space requirements for the management server are as follows:

Hardware

Item	Ops Center Automator	
	Standard mode	High performance mode
CPU	(Minimum) Dual-core processor (Suggested) Quad-core processor or better	8-core processor or better
Physical memory	(Minimum) 8 GB (Suggested) 10 GB or higher	16 GB or higher

Item		Ops Center Automator	
		Standard mode	High performance mode
Disk	Free space required for use	(Minimum) 3000 MB*	
		(Suggested) 30 GB or higher	
	Ops Center Automator installation folder	4100 MB	
	Database space required for use	3000 MB	

*:

- Average size of service template: 2 MB
- The number of service templates: 500
- Average size of task log: 1 MB
- The number of tasks: 2000
- Total size: 3 GB (2 MB * 500 + 1 MB * 2000)

Hitachi Ops Center products cannot be installed on a disk that has a logical sector size of 4,096 bytes (4K native). If a disk that has a logical sector size of 4,096 bytes is used, change the logical sector size to 512 bytes, and then install.

Table 2 Disk space required for installation (Windows)

Component folder	Default installation folder	Ops Center Automator
Ops Center Automator installation folder	<i>Program-Files-folder</i> \hitachi	4100 MB
Ops Center Automator database storage folder	<i>Program-Files-folder</i> \hitachi\database\Automation	3000 MB

Table 3 Disk space required for installation (Linux)

Component directory	Default installation directory	Ops Center Automator
Ops Center Automator installation directory	/opt/hitachi	2440 MB
	/var/opt/hitachi	1660 MB
Ops Center Automator database storage directory	/var/opt/hitachi/database/x64/Automation	3000 MB

Virtual memory requirements

For management server stability, you must allocate virtual memory capacity for products and for the operating system and other programs. If insufficient virtual memory is allocated on the management server, Common Component products and other installed programs can become unstable or might not start. For the management server, allocate the total virtual memory capacity of Common Component plus the sum of the virtual memory capacities of all the installed Common Component products. The suggested virtual memory capacity is shown in the following table. Important: When you install both 64-bit and 32-bit products in the management server, you must reserve enough virtual memory to equal the total value of the virtual memory for all the products.

The following are the suggested amounts of virtual memories for each component:

- Common Component: 2501 MB
- Ops Center Automator: 7000 MB

Port requirements

Before you install the Ops Center Automator server, review the port and firewall requirements.

Table 4 Common Component reception ports

Port number	Description	Register firewall exception	Originator	
22015/tcp	<p>Used for accessing the HBase 64 Storage Mgmt Web Service when communicating with management clients (GUI).</p> <p>This port number can be changed.</p> <p>This port is also used when SSL is enabled. To interrupt non-SSL communication from outside the network to the management server, edit the <code>user_httpsd.conf</code> file.</p>	Yes	Client	Ops Center Automator server
22016/tcp	<p>Used for accessing the HBase 64 Storage Mgmt Web Service when performing SSL communication with management clients (GUI).</p> <p>This port number can be changed.</p>	Yes	Client	Ops Center Automator server

Port number	Description	Register firewall exeption	Originator	
22017/tcp to 22030/tcp 22033/tcp 22034/tcp	Reserved for Common Component.	No	-	-
22032/tcp	Used internally for Common Component communication (HiRDB). This port number can be changed.	No	-	-
22035/tcp	Used internally for Common Component communication (communication with the Web server).	No	-	-
22036/tcp	Used internally for Common Component communication (HiRDB). This port number can be changed.	No	-	-
22037/tcp	Used internally for Common Component communication (communication with the Web server). This port number can be changed.	No	-	-

Port number	Description	Register firewall exception	Originator	
22038/tcp	Used internally for Common Component communication (communication with the Web server). This port number can be changed.	No	-	-
22121/tcp	Used internally for Common Component communication (communication with the Web server). This port number can be changed.	No	-	-
22122/tcp	Used internally for Common Component communication (naming service). This port number can be changed.	No		
22123/tcp 22124/tcp 22125/tcp	Used internally for Common Component communication (communication with the Web server). This port number can be changed.	No	-	-

Port number	Description	Register firewall exeption	Originator	
22126/tcp	Used internally for Common Component communication (naming service). This port number can be changed.	No	-	-
22127/tcp 22128/tcp	Used internally for Common Component communication (communication with the Web server). This port number can be changed.	No	-	-

Table 5 Ops Center Automator ports

Port number	Description	Register firewall exeption	Originator	
22170/tcp	Used internally for Common Component communication (communication with the Web server).	No	-	-
22171/tcp	Used internally for Common Component communication (naming service). This port number can be changed.	No	-	-

Port number	Description	Register firewall exception	Originator	
22172/tcp	Used internally for Common Component communication (communication with the Web server). This port number can be changed.	No	-	-
22173/tcp	Used internally for Common Component communication (communication with the Web server). This port number can be changed.	No	-	-

Table 6 Reception ports of virtualization server

Type	Port number	Description	Register firewall exception	Originator	
VMware ESXi	443/tcp	This setting is required when a virtual WWN is assigned to a virtual machine by using NPIV.	Yes	Management server	Ops Center Automator

Type	Port number	Description	Register firewall exception	Originator	
VMware vCenter Server that manages VMware ESXi	443/tcp	This setting is required when a virtual WWN is assigned to a virtual machine by using NPIV.	Yes	Management server	Ops Center Automator

Table 7 Reception ports of operation targets (servers)

Port number	Description	Register firewall exception	Originator	
22/tcp	Used for SSH. cjstartsv uses this port.	Yes	Management server	Ops Center Automator
23/tcp	Used for Telnet. cjstartsv uses this port.	Yes	Management server	Ops Center Automator
445/tcp or udp	Used for Windows administrative shares. cjstartsv uses this port.	Yes	Management server	Ops Center Automator
135/tcp and 139/tcp	Used for Windows administrative shares. cjstartsv uses this port.	Yes	Management server	Ops Center Automator

Table 8 Reception ports of mail servers

Port number	Description	Register firewall exception	Originator	
25/tcp	Used for mail transmission. This port number can be changed. cjstartsv uses this port.	Yes	Management server	Ops Center Automator

Table 9 Reception ports of external authentication servers

Port number	Description	Register firewall exception	Originator	
88/tcp	Used for communication with the management server and Kerberos server. This port number is generally used. However, a different port number might be used for an external authentication server.	Yes	Management server	Ops Center Automator
88/udp	Used for communication with the management server and Kerberos server. This port number is generally used. However, a different port number might be used for an external authentication server.	Yes	Management server	Ops Center Automator
389/tcp	Used for communication with the management server and LDAP directory server. This port number is generally used. However, a different port number might be used for an external authentication server.	Yes	Management server	Ops Center Automator

Port number	Description	Register firewall exception	Originator	
1812/udp	Used for communication with the management server and RADIUS server. This port number is generally used. However, a different port number might be used for an external authentication server.	Yes	Management server	Ops Center Automator

Maximum resource support

Maximum resource support

This section lists the maximum number of resources that Ops Center Automator can manage. Best practice is not to exceed these limits.

- Number of the controllable tasks: 5,000
- Number of service templates: 1,000
- Number of controllable Agentless Remote Connections: 10,000

Web client requirements

The following browsers are supported:

Table 10 Supported browsers

Web browser/other	Version
Firefox	ESR 91
Internet Explorer	11*
Microsoft Edge	Latest version of stable channel
Chrome Browser for enterprise	Latest version of stable channel
* Browser subwindows may open behind the main (parent) window.	

Table 11 IPv6

OS	OS Name	Ops Center Automator
Windows	<ul style="list-style-type: none"> Windows Server 2012 Windows Server 2012 R2 Windows Server 2016 Windows Server 2019 Windows Server 2022 	Supported *
* Evaluation is needed before using this version in a cluster environment or in a VMware environment.		

Virtualization and cluster support

Virtualization software

All Windows and Linux server installations support the following versions of VMware ESXi. No functional differences due to differing operating systems exist. All versions of Windows support Remote Desktop/Terminal Client with Console connection session installations.

Linux does not support web console installations.

- 6.5, 6.5u1, 6.5u2, 6.5u3
- 6.7, 6.7u1, 6.7u2, 6.7u3
- 7.0, 7.0u1, 7.0u2, 7.0u3

The following Windows installations support the following versions of Hyper-V.

OS Name	OS Version	Virtualization Version
Windows Server 2012	<ul style="list-style-type: none"> Standard Edition Datacenter Edition 	Windows Server 2012 Hyper-V
		Windows Server 2012 R2 Hyper-V
		Windows Server 2016 Hyper-V
		Windows Server 2019 Hyper-V
		Windows Server 2022 Hyper-V
Windows Server 2012	<ul style="list-style-type: none"> Standard Edition R2 Datacenter Edition R2 	Windows Server 2012 R2 Hyper-V
		Windows Server 2016 Hyper-V
		Windows Server 2019 Hyper-V
		Windows Server 2022 Hyper-V

OS Name	OS Version	Virtualization Version
Windows Server 2016	<ul style="list-style-type: none"> Standard Edition Datacenter Edition 	Windows Server 2012 R2 Hyper-V
		Windows Server 2016 Hyper-V
		Windows Server 2019 Hyper-V
		Windows Server 2022 Hyper-V
Windows Server 2019	<ul style="list-style-type: none"> Standard Edition Datacenter Edition 	Windows Server 2016 Hyper-V
		Windows Server 2019 Hyper-V
		Windows Server 2022 Hyper-V
Windows Server 2022	<ul style="list-style-type: none"> Standard Edition Datacenter Edition 	Windows Server 2019 Hyper-V
		Windows Server 2022 Hyper-V

Cluster software

All Windows server installations support WSFC cluster (Bundle version).

Management target requirements

Storage System	Interface (Interface between the host and storage subsystem)	Ops Center Automator
VSP 5200, 5600, 5200H, 5600H	Fibre Channel	All versions are supported
	iSCSI	
VSP 5100, 5500, 5100H, 5500H	Fibre Channel	90-01-42-00/xx or later
	iSCSI	90-01-42-00/xx or later
VSP G1000	Fibre Channel	80-01-21-00/00 or later
	iSCSI	80-02-01-XX/XX or later
VSP G1500	Fibre Channel	80-05-0X-XX/XX or later
	iSCSI	80-05-0X-XX/XX or later
VSP G200, G400, G600, G800	Fibre Channel	All versions are supported
	iSCSI	All versions are supported

Storage System	Interface (Interface between the host and storage subsystem)	Ops Center Automator
VSP G350, G370, G700, G900	Fibre Channel	All versions are supported
	iSCSI	All versions are supported
VSP F1500	Fibre Channel	All versions are supported
	iSCSI	All versions are supported
VSP F400, F600, F800	Fibre Channel	All versions are supported
	iSCSI	All versions are supported
VSP F350, F370, F700, F900	Fibre Channel	All versions are supported
	iSCSI	All versions are supported
VSP N400, N600, N800	Fibre Channel	All versions are supported
	iSCSI	All versions are supported
VSP E1090, E1090H	Fibre Channel	All versions are supported
	iSCSI	All versions are supported
VSP E590, E790, E990, E590H, E790H	Fibre Channel	All versions are supported
	iSCSI	All versions are supported
VSP	Fibre Channel	70-01-0x-xx/xx or later
HUS VM	Fibre Channel	73-00-00-xx/xx or later

Chapter 3: Installing and upgrading Ops Center Automator

This module describes how to install and upgrade Ops Center Automator for Microsoft® Windows® OS in both cluster and non-cluster environments and Red Hat Enterprise Linux (RHEL)/CentOS/Oracle Linux OS in a non-cluster environment.

If you are installing Automator as part of the Hitachi Ops Center OVA, see the *Hitachi Ops Center Installation and Configuration Guide*.



Note: The following elements cannot be carried over or have been changed for Ops Center Automator v10.8.0 or later:

- The `SSLProtocol` and `SSLCipherSuite` parameters in `user_httpsd.conf` cannot be carried over.
- The `hcmds64chgjdk` command to switch to Oracle JDK is no longer supported when you upgrade, the existing JDK will be replaced with the Hitachi JDK.
- The internal port number of `webserver.connector.ajp13.port` will not be carried over if it has been changed.



Note: If you are upgrading, you can skip the steps in [Post-installation tasks \(on page 47\)](#) and [Configuring single sign-on in Common Services \(on page 51\)](#) because the previous settings are preserved.

Installation prerequisites

Before installing Ops Center Automator complete the following tasks:

- Verify that the environment and the management server meet all hardware and software requirements. For details on the system requirements, see Chapter 2: [System requirements \(on page 15\)](#).
- Ensure the ports used by Ops Center Automator are available. Verify that the ports on the management server are not in use by other products and no conflicts exist. If a port is in use by another product, neither product may operate correctly.
- Resolve the IP addresses and host names of the related machines.
- Ensure Windows administrator permissions are obtained to complete the installation and configuration tasks included in this guide.
- Ensure Linux root permissions are obtained to complete the installation and configuration tasks included in this guide.

- Disable any security monitoring, virus detection, or process monitoring software on the server.
- Close any Windows Services or open command prompts.
- If the server is running any other Common Component products, stop the services for those products.
- Make sure the server system time is correct. If the Common Component products and Ops Center products are installed on a different server, synchronize the management servers running the Common Component products and Ops Center products.
- For RHEL/CentOS/Oracle Linux OS, manually re-add firewall exceptions as needed for Ops Center Automator. These exceptions do not automatically get reconfigured during installation.

Changing the server time

The Ops Center Automator task and alert occurrence times are based on the management server time setting. Therefore, it is important that you verify the accuracy of the server OS time setting and reset it if necessary before installing Ops Center Automator. If you change the Ops Center Automator server time while the Common Component and Common Component product services are running, Ops Center Automator might not operate correctly.



Important: The Ops Center Automator server OS time setting must be synchronized with the management servers running Common Component products and Ops Center products.



Note: When Common Services and Automator are running on different hosts, launching Automator from the Ops Center portal fails if there is a time lag between the host where Common Services is installed and the host where Automator is installed. You must synchronize the time on the Common Services host with the time on the Automator host. Use NTP to keep the time synchronized between the hosts.

If you plan to use a service such as NTP, which automatically adjusts the server time, you must configure the service as follows:

- Configure the settings so that the time is adjusted when the service discovers a time discrepancy.
- The service adjusts the time setting only as long as the time difference remains within a specific range. Based on the maximum range value, set the frequency so that the time difference never exceeds the fixed range.

An example of a service that can adjust the time as long as the time difference does not exceed a fixed range is the Windows Time service.



Note: When running Ops Center Automator in a U.S. or Canadian time zone, you must configure the management server OS so that it supports the new Daylight Savings Time (DST) rules. Ops Center Automator cannot support the new DST rules unless the server gives support.

If you cannot use the functionality that adjusts the server time automatically, or to manually change the system time, perform these steps:

1. Stop the Common Component and all Common Component product services, for example:
 - HBase 64 Storage Mgmt Web Service
 - HBase 64 Storage Mgmt Web SSO Service
 - HBase 64 Storage Mgmt SSO Service
 - HBase 64 Storage Mgmt Common Service
 - HCS Device Manager Web Service
 - HiCommand Suite Tuning Manager
 - HiCommand Performance Reporter
 - HCS Tuning Manager REST Application Service
 - HAutomation Engine Web Service
 - HiCommand Server
 - HiCommand Tiered Storage Manager
2. Record the current time of the management server, and then reset the time.
3. Determine when to restart the services.
 - If you set the time of the machine back (meaning that the server time was ahead), wait until the server clock shows the time you recorded (the time on the server when you made the change) and then restart the machine.
 - If you set the machine time forward, restart the machine now.

Verify that the Ops Center Automator management server reflects the correct time.

Changing the name resolution setting

If you install Ops Center Automator and the Common Component product on two different machines, you must resolve the name of the Ops Center Automator server that connects to the client.

You must also resolve the name of the machine where Ops Center Automator is installed.

If you install Ops Center Automator on the same machine as the Common Component product, you must resolve the names of the machine on which you want to run the browser to access Ops Center Automator.

Update your configuration settings so that the system can resolve the IP address from the management server host name that is set as the `ServerName` property on the first line of the `user_httpsd.conf` file. To verify that the IP address resolves to the host name, run the following command:

```
ping management-server-host-name
```

Avoiding port conflicts

Before a new installation of Ops Center Automator, verify that the ports that Ops Center Automator will use on the management server are not in use by other products. If a port is being used by another product, neither product might operate correctly.

To ensure that the necessary ports are not in use, use the `netstat` or `ss` command.

You must verify that port numbers 22170 - 22173 are not used by other products because this causes a new or upgrade installation to fail.

Installing and upgrading Ops Center Automator (Windows OS)

You use the product installer to install or upgrade the Ops Center Automator software.

If you are upgrading your software, ensure that you back up the existing system configuration and data using the `backupsystem` command. For information on running this command, see the *Hitachi Ops Center Automator User Guide*.

Procedure

1. Ensure that your system meets all management server prerequisites as listed in the pre-installation checklist.
2. If the server is running any products that use the Common Component, stop the following services:
 - HBase 64 Storage Mgmt Web Service
 - HBase 64 Storage Mgmt Web SSO Service
 - HBase 64 Storage Mgmt SSO Service
 - HBase 64 Storage Mgmt Common Service
 - HCS Device Manager Web Service
 - HiCommand Suite Tuning Manager
 - HiCommand Performance Reporter
 - HCS Tuning Manager REST Application Service
 - HAutomation Engine Web Service
 - HiCommand Server
 - HiCommand Tiered Storage Manager
3. Access the installation media.
4. Start the installation wizard by running the following command:

```
Installation-media:\Windows\HAD_SERVER\setup.exe
```

5. Follow the prompts and specify the required information.
In most cases, accept the default installation selections.



Note: If the following message is displayed, check the release notes:

An Analyzer server prior to 10.7.0, Hitachi Ops Center Automator prior to 10.8.0, or Hitachi Command Suite prior to 8.8.3 is already installed on this server. Make sure to upgrade the relevant products by referring to the Release Notes. Abort the installation?

The **Install Complete** window opens.

6. Click **Finish**.

Result

Ops Center Automator is now installed.



Note: If you are upgrading, you can skip the steps in [Post-installation tasks \(on page 47\)](#) and [Configuring single sign-on in Common Services \(on page 51\)](#) because the previous settings are preserved.

Installing and upgrading Ops Center Automator in a cluster environment (Windows OS)

You can install or upgrade Ops Center Automator in a Windows cluster environment.



Note: Ops Center Automator supports Windows cluster environments only. Ops Center Automator does not support clustering in a Linux OS environment.



Note: If you are upgrading, you can skip the steps in [Post-installation tasks \(on page 47\)](#) and [Configuring single sign-on in Common Services \(on page 51\)](#) because the previous settings are preserved.

About using Ops Center Automator in a cluster environment

When using Ops Center Automator, you can increase reliability by setting up a failover management server using Microsoft Windows Server Failover Clustering.



Note: Ops Center Automator does not support installing in a cluster that spans multiple subnets.

When you use Ops Center Automator in a cluster environment, you designate one Ops Center Automator server as the active node and another as the standby node as follows:

- Active node

The active node is the host that is running services in a system that uses a cluster.

If a failure occurs, the cluster services implements a failover, and the standby node takes over running the system resources so that there is no interruption of services.

- Standby node

The standby node is the host that takes over running system resources from the active node if a failure occurs.

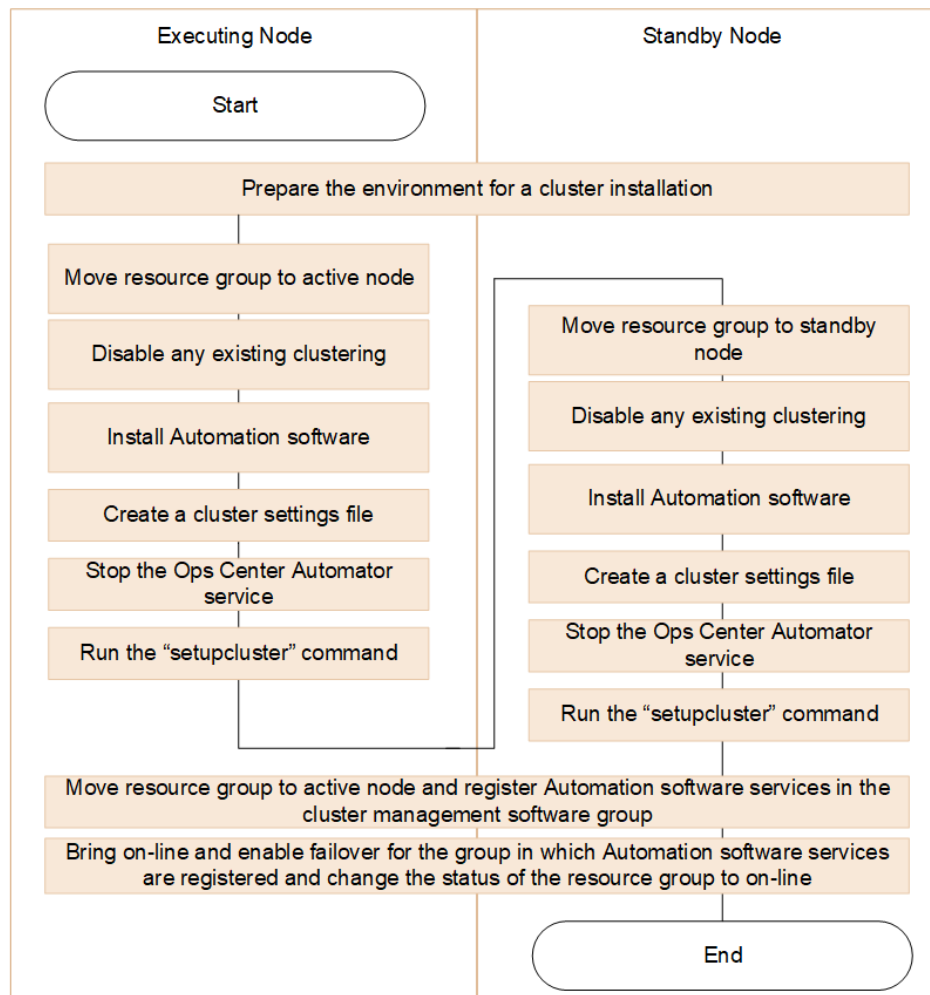


Note: If an active node fails over to the standby node, any tasks that are running fail and you must run the tasks again on the standby node.

Cluster installation workflow

When installing Ops Center Automator in a cluster configuration, you must follow a series of steps to prepare both the active node and the standby nodes.

The following shows the general workflow for setting a up cluster environment:



When installing Ops Center Automator to a cluster environment for the first time or when migrating from a noncluster environment to a cluster environment, make sure that every node in the cluster has the same disk configuration, and all Common Component products are installed in the same location (including drive letter, path, and so on) on each node.

If you are upgrading your software, ensure that you back up the existing system configuration and data using the `backupsystem` command. For information on running this command, see the *Hitachi Ops Center Automator User Guide*.



Note: When upgrading Ops Center Automator that is already installed in a cluster configuration, you must disable the resource script before running the upgrade installation.

Verifying the cluster configuration using the cluster management software

When setting up Ops Center Automator in a cluster environment, you must use the cluster management software to verify the current environment settings and to configure additional settings.

Use the cluster management software to verify the following items before setting up Ops Center Automator in a cluster environment:

- Verify whether a group exists in which other Common Component product services are registered.

If a group in which Common Component services are registered already exists, use that group. Verify that the group consists only of resources related to Common Component products.

If no group in which Common Component services are registered exists, use the cluster management software to create a group to register the Ops Center Automator services.



Note: Group names cannot contain the following characters: ! " % &) * ^ | ; = , < >

- Verify that the group in which you plan to register services includes the shared disk and client access point that can be inherited between the active and standby nodes. The client access point is the cluster management IP address and the logical host name.
- Verify that you can allocate, delete, and monitor resources by using the cluster management software without any problems.

Services that are used in a cluster environment can be failed over together by registering them as a group in the cluster management software. These groups might be referred to by different names, such as "resource groups" or "roles," depending on the versions of the cluster management software and the OS.

Setting up Ops Center Automator clustering on an active node

You can complete a new installation of Ops Center Automator on the management server on an active node in a cluster configuration.

Procedure

1. Bring online the cluster management IP address and shared disk. Make sure that the resource group for the cluster installation is moved to the active node.
2. If you created the cluster environment using another Common Component product, use the following command to take offline and disable failover for the cluster group in which Common Component product services are registered:

```
Common-Component-installation-directory\ClusterSetup
\hcnds64clustersrvstate /soff /r cluster-group-name
```

where

r - specifies the name of the group in which the Common Component product services are registered. If the group name contains spaces, you must enclose the group name in quotation marks (""). For example, if the group name is Automator cluster, specify "Automator cluster".

3. Complete a new installation of Ops Center Automator on the active node.
If another Common Component product already exists in the cluster environment, verify the following before installing Ops Center Automator, specify the IP address of the logical host as the IP address of the management server.

If no other Common Component products exist in the cluster environment, verify the following before installing Ops Center Automator, specify the IP address of the active node as the IP address of the management server.
4. Register the licenses for the products you plan to use. Access the IP address of the active node.
5. If you already have a Common Component product configured in the cluster, skip to the next step. If Ops Center Automator is the first Common Component product in the cluster, do the following:
 - a. Add the following information to a blank text file:

```
mode=online
virtualhost=logical-host-name
onlinehost=active-node-host-name
standbyhost=standby-node-host-name
```



Note: On an active node, you must specify `online` for mode.

Save the file as `cluster.conf` in `Common-Component-installation-folder\conf`.

6. Use the following command to ensure that the Ops Center Automator service is stopped:


```
Common-Component-installation-folder\bin\hcnds64srv /stop /server
AutomationWebService
```
7. Run the **setupcluster /exportpath** command where the `exportpath` specifies the absolute or relative folder path.

Setting up Ops Center Automator clustering on a standby node

After setting up the clustering installation on an active node, you can complete installation of Ops Center Automator on the management server on a standby node in a cluster configuration.

Procedure

1. In the cluster management software, move the group containing the Ops Center Automator resources to the standby node by right-clicking the group, selecting **Move**, and then selecting either **Select Node** or **Move this service or application to another node**.
2. If you created the cluster environment using another Common Component product, use the following command to take offline and disable failover for the cluster group in which Common Component product services are registered:

```
Common-Component-installation-directory\ClusterSetup
\hcnds64clustersrvstate /soff /r cluster-group-name
```

where

r - specifies the name of the group in which the Common Component product services are registered. If the group name contains spaces, you must enclose the group name in quotation marks (""). For example, if the group name is Automator cluster, specify "Automator cluster".

3. Complete a new installation of Ops Center Automator on the standby node.
Before installing Ops Center Automator on the standby node, be aware of the following requirements:
 - You must install Ops Center Automator in the same location as on the active node.
 - If other Common Component products already exist and are active in the cluster environment, specify the logical host name (the virtual host name allocated to the cluster management IP address) as the IP address of the management server. If there are no other Common Component products in the cluster environment, specify the IP address or the host name of the standby node.
4. Register the licenses for the products you plan to use.
5. If you already have a Common Component product configured within the cluster, skip to the next step. If Ops Center Automator is the first Common Component product in the cluster, add the following information to a blank text file:

```
mode=standby
virtualhost=logical-host-name
onlinehost=active-node-host-name
standbyhost=standby-node-host-name
```

Save the file as `cluster.conf` in *Common-Component-installation-folder* \conf.



Note: On a standby node, you must specify `standby` for mode.

6. Use the following command to ensure that the Ops Center Automator service is stopped:
`hcnds64srv /stop /server AutomationWebService`
7. Run the **setupcluster /exportpath** command where the `exportpath` specifies the absolute or relative folder path.

Registering the services and initializing the cluster installation

After installing Ops Center Automator on the active and standby nodes in a cluster configuration, you can register the services and scripts and then bring the clustering online as described in the following steps:

Procedure

1. In the cluster management software, move the group containing the Ops Center Automator resources to the active node by right-clicking the group, selecting **Move**, and then selecting either **Select Node** or **Move this service or application to another node**.
2. Register the Ops Center Automator services in the cluster management software group by using the following command:

```
Common-Component-installation-directory\ClusterSetup
\hcnds64clustersrvupdate /sreg /r cluster-group-name /sd drive-
letter-of-shared-disk /ap resource-name-for-client-access-point
```

where

`r` - specifies the name of the group in which the Common Component product services including Ops Center Automator will be registered. If the group name contains spaces, you must enclose the group name in quotation marks ("). For example, if the group name is Automator cluster, specify "Automator cluster".

`sd` - specifies the drive letter of the shared disk that is registered to the cluster management software. You cannot specify multiple drive letters for this option. If the database of Common Component products is divided into multiple shared disks, run the `hcnds64clustersrvupdate` command for each shared disk.

`ap` - specifies the name of the resource for the client access point that is registered to the cluster management software.

3. On the active node, bring online and enable failover for the group in which Common Component services including Ops Center Automator are registered using the following command:

```
Common-Component-installation-folder\ClusterSetup
\hcnds64clustersrvstate /son /r cluster-group-name
```

where

`r` - specifies the name of the group in which the Common Component product services including Ops Center Automator are registered. If the group name contains spaces, you must enclose the group name in quotation marks ("). For example, if the group name is Automator cluster, specify "Automator cluster".

4. Change the status of the resource group to **online** in the cluster software.

Installing and upgrading Ops Center Automator (Linux OS)

You use the product installer to install or upgrade the Ops Center Automator software.

If you are upgrading your software, ensure that you back up the existing system configuration and data using the `backupsystem` command. For information on running this command, see the *Hitachi Ops Center Automator User Guide*.



Note: To install Ops Center Automator with other Common Component products, ensure that your system meets the installation requirements for all the products.

Install Ops Center Automator by running `install.sh`.



Note: If the following message is displayed, check the release notes:

```
An Analyzer server prior to 10.7.0, Hitachi Ops Center Automator prior to
10.8.0, or Hitachi Command Suite prior to 8.8.3 is already installed on
this server. Make sure to upgrade the relevant products by referring to
the Release Notes. Abort the installation?
```

The default Ops Center Automator installation directory for Linux OS is: `/opt/hitachi/Automation`



Note: If you are upgrading, you can skip the steps in [Post-installation tasks \(on page 47\)](#) and [Configuring single sign-on in Common Services \(on page 51\)](#) because the previous settings are preserved.

Required settings when using a virus detection program

If a virus detection program accesses the files used by Ops Center Automator, operations such as I/O delays or file locks can cause errors. To prevent these problems, exclude the following directories from the targets scanned by the virus detection program while installing and running Ops Center Automator.



Note: The following directories are default paths that can be changed during installation.

Directories to be excluded during installation

▪ Windows:

```
system-drive\Program Files\hitachi\Automation
system-drive\Program Files\hitachi\database
system-drive\Program Files\hitachi\Base64
```

▪ Linux:

```
/opt/hitachi/Automation
/var/opt/hitachi/Automation
/var/opt/hitachi/Base64
/var/opt/hitachi/database
```

Directories to be excluded during operation

▪ Windows:

```
system-drive\Program Files\hitachi\Automation
system-drive\Program Files\hitachi\database
system-drive\Program Files\hitachi\Base64\HDB
```

▪ Linux:

```
/opt/hitachi/Automation
/var/opt/hitachi/Automation
/var/opt/hitachi/Base64/HDB
/var/opt/hitachi/database
```

Post-installation tasks

After installing Ops Center Automator, complete the following post-installation tasks:

1. If the server that manages the user account uses SSL communication, run the **hcnds64prmset** command to set the port number of the server (as needed).
2. Confirm the registered URL.
3. Verify access to the Ops Center Automator management server.
4. Run the **setupcommonservice** command to set up Common Services.

For details about the **setupcommonservice** command, see [setupcommonservice command \(on page 52\)](#).



Note: In a cluster configuration, **setupcommonservice** must only be run on the active node.

5. Register the license.
6. Change the System account password.
7. Set an email address for the System account.

8. Stop and restart Common Component and Ops Center Automator services (as needed).
You must change the System account password.

Confirming the registered URL (Windows OS)

Confirm the registered URL after installing Ops Center Automator.

Procedure

1. Confirm the registered URL by using the following command:
2. Verify the host name in the URL. In a noncluster environment, the host name must be a physical host name. In a cluster environment, the host name must be a logical host name. If the registered URL is incorrect, change the URL by using the following command:

```
Common-Component-installation-folder\bin\hcmts64chgurl /list
```

```
Common-Component-installation-folder\bin\hcmts64chgurl /change  
http://incorrect-IP-address-or-host-name:port-number http://  
correct-IP-address-or-host-name:port-number
```



Note: If you want to link with Common Services, change the registered URL by using the following command:

```
Common-Component-installation-folder\bin\hcmts64chgurl /change  
https://IP-address-or-host-name:22016 /type Automation
```

Confirming the registered URL (Linux OS)

Confirm the registered URL after installing Ops Center Automator.

Procedure

1. Confirm the registered URL by using the following command:
2. Verify the host name in the URL. If the registered URL is incorrect, change the URL by using the following command:

```
Common-Component-installation-directory/bin/hcmts64chgurl -list
```

```
Common-Component-installation-directory/bin/hcmts64chgurl -change  
http://incorrect-IP-address-or-host-name:port-number http://  
correct-IP-address-or-host-name:port-number
```



Note: If you want to link with Common Services, change the registered URL by using the following command:

```
Common-Component-installation-folder/bin/hcmts64chgurl -change  
https://IP-address-or-host-name:22016 -type Automation
```

Verifying the installation

When installation is complete, verify that the installation was successful using a web browser.

Procedure

1. Open a web browser that is supported by Ops Center Automator.
2. In the address bar, specify the URL for Ops Center Automator in the following format:
`http://automation_software-server-address:22015/Automation/`

Result

The logon window opens, verifying that you can access the management server.

Registering a license

When you log on initially, you must specify a valid license key.



Note: You must obtain the Ops Center Automator server license from your Hitachi Vantara representative.

Procedure

1. From the logon window, click **Licenses**.
2. Enter the license key, or click **Choose File** to browse to the license file.
3. Click **Save**.

Changing the system account password

The System account is a default account that has user management and execute permission for Ops Center Automator. When you install Ops Center Automator for the first time, you must change the System account password.



Note: This procedure only changes the local system account password. To change the Hitachi Ops Center system password, see the *Hitachi Ops Center Online Help*.

Procedure

1. From a management client, log on using the following credentials:
 User ID: system
 Password (default): manager
2. On the **Administration** tab, click **User Profile**.
3. Click **Change Password**, type the required passwords, then click **OK**.

Setting an e-mail address for the System account

Before Ops Center Automator can send e-mail notifications about Ops Center Automator system operations to the System, you must set up a System account e-mail account.

Procedure

1. On the Administration tab, click **User Profile**.

2. In the **User Profile** window, click **Edit Profile**, type the full name and the e-mail address, then click **OK**.

Result

The System account e-mail address is set up.

To receive email notifications, you must set up the System Settings to specify the Email SMTP server connection information (host name or IP address, user ID, password, and port are all required) and turn Email Notifications ON in the system parameter settings. For more detailed information, see the *Hitachi Ops Center Automator User Guide*.

Stopping and starting Common Component and Ops Center Automator services

You can start and stop Ops Center Automator services from the command prompt.

Stopping and starting all services from a command prompt (Windows OS)

The following procedure stops and starts all Common Component and Ops Center Automator services:

Procedure

1. At the command prompt, navigate to *Common-Component-installation-folder* \bin.
2. To stop the services, enter the following command:
`hcnds64srv.exe /stop`
To start services, enter the following command:
`hcnds64srv.exe /start`

Stopping and starting all services from a command prompt (Linux OS)

The following procedure stops and starts all Common Component and Ops Center Automator services:

Procedure

1. At the command prompt, navigate to *Common-Component-installation-directory*/bin.
2. To stop the services, enter the following command:
`hcnds64srv -stop`
To start services, enter the following command:
`hcnds64srv -start`

Stopping and starting only the Ops Center Automator services from the command prompt (Windows OS)

Procedure

1. Navigate to *Common-Component-installation-folder\bin*.
2. Start or stop services:
 - To stop services, enter the following command:
`hcmds64srv.exe /stop /server AutomationWebService`
 - To start services, enter the following command:
`hcmds64srv.exe /start /server AutomationWebService`

Stopping and starting only the Ops Center Automator services from the command prompt (Linux OS)

Procedure

1. Navigate to *Common-Component-installation-directory/bin*.
2. Start or stop services:
 - To stop services, enter the following command:
`hcmds64srv -stop -server AutomationWebService`
 - To start services, enter the following command:
`hcmds64srv -start -server AutomationWebService`

Configuring single sign-on in Common Services

To use the Ops Center portal single sign-on (SSO) functionality, you must register Automator with Common Services. If you deployed the Ops Center OVA, Automator is already registered in Common Services.

Registering Ops Center Automator with Ops Center Common Services

To use Common Services that is installed on a different host, or to use Common Services that was installed by using the installer, you must register Ops Center Automator with Common Services by running a command on the Ops Center Automator server.

Procedure

1. Run the `setupcommonservice` command with the `auto` option specified to register Ops Center Automator in Common Services.
For details about the `setupcommonservice` command, see [setupcommonservice command \(on page 52\)](#).

setupcommonservice command

The **setupcommonservice** command is a setting command for linking with Common Services. The **setupcommonservice** command registers Ops Center Automator as an application in Common Services and sets Ops Center Automator as an authentication server that uses Common Services.



Note: You must use the Ops Center portal to remove an Ops Center Automator registered in Common Services.

Functions

The **setupcommonservice** command registers the Ops Center Automator URL in Common Services. The URL to be registered uses the URL registered in the **hcnds64chgurl** command. Confirm in advance that the URL registered in **hcnds64chgurl** can be resolved by the browser, then run the **setupcommonservice** command.

This command needs a secure connection between Ops Center Common Services and Ops Center Automator. See the *Hitachi Ops Center Installation and Configuration Guide* for more information.

Syntax

Windows syntax:

```
setupcommonservice {[/csUri CommonServiceUri | /csUri CommonServiceUri /csUsername  
CommonServiceUsername] [/appName ApplicationName]  
[/appDescription ApplicationDescription] [ /auto ] | /help }
```

Linux syntax:

```
setupcommonservice {[-csUri CommonServiceUri | -csUri CommonServiceUri -csUsername  
CommonServiceUsername] [-appName ApplicationName]  
[-appDescription ApplicationDescription] [ -auto ] | -help }
```



Note: You are prompted to enter the password in interactive mode.

Options

Option	Description
csUri	Specify the URL of Common Services. (For example: https://common.service/portal)

Option	Description
csUsername	<p>Specify a user with opscenter-security-administrator privileges to be managed by Common Services. The username can be 1-byte alphanumeric characters. This includes (! # \$ % & ') * + , - = @ ^ _). The length is from 1 to 255 characters. Usernames are case-sensitive.</p> <p>You are prompted to enter the password when you run the command with this option.</p>
appName	<p>Specify the name of the Ops Center Automator to be displayed by Common Services. The name is specified with 1 to 128 characters.</p> <p>If <code>appName</code> is omitted at the time of new registration, the host name or IP address of Ops Center Automator is set as the name. If <code>appName</code> is omitted when updating, the name is not changed.</p>
appDescription	<p>Specify a description of the Ops Center Automator displayed by Common Services. The description can be from 0 to 512 characters.</p>
auto	<p>Automatically start and stop the services and databases of Ops Center Automator.</p>

Chapter 4: Configuring Ops Center Automator

This module gives information on how to configure Ops Center Automator.

Changing management server system settings

This module gives information about changing Ops Center Automator management server system settings.

Changing the port number used for management server communication with management clients

To change the port number used for communication between the Ops Center Automator management server and management clients (Web browsers), you must edit the definition file and configure exceptions in the firewall. For a cluster system, complete the same procedure on both the active server and standby server.



Note: For information on other ports used with Ops Center Automator, see the Port settings reference topic.

To change the port number between the Ops Center Automator management server and management clients:

Procedure

1. Stop Ops Center Automator.
2. Change the port number settings by editing the keys in the definition files.
 - For HTTPS, go to Step 3.
 - For HTTP, change the port number settings by editing the keys in the definition files as follows:

- a. Modify the `Listen` key lines in the `user_httpsd.conf` file:

Windows-based OS

Common-Component-installation-folder\uCPSB11\httpsd\conf\user_httpsd.conf

Linux OS

Common-Component-installation-directory/uCPSB11/httpsd/conf/user_httpsd.conf

Specify the new port number in place of 22015 in the following lines:

```
Listen 22015

Listen [::]:22015

#Listen 127.0.0.1:22015
```

- b. Modify the `command.http.port` lines in the `command_user.properties` file.

The folder that contains this definition file is different for cluster systems.

Windows-based OS (non-cluster)

Automation_software-installation-folder\conf

Windows-based OS (cluster)

shared-folder-name\Automation\conf

Linux OS

/opt/hitachi/Automation/conf

- c. Modify the `server.http.port` lines in the `config_user.properties` file.

The folder that contains this definition file is different for cluster systems.

Windows-based OS (non-cluster)

Automation_software-installation-folder\conf

Windows-based OS (cluster)

shared-folder-name\Automation\conf

Linux OS

/opt/hitachi/Automation/conf

- d. Go to Step 4.

3. For HTTPS, change the port number settings by editing the keys in the definition file as follows:

- a. Open the `user_httpsd.conf` file.

Windows-based OS

```
Common-Component-installation-folder\uCPSB11\httpsd\conf
\user_httpsd.conf
```

Linux OS

```
Common-Component-installation-directory/uCPSB11/httpsd/conf/
user_httpsd.conf
```

- b. Modify the `Listen` key lines by specifying the new port number in place of 22016 in the following lines:

```
Listen 22016

Listen [::]:22016

VirtualHost *22016
```

4. Configure firewall exceptions:

- If the OS is Windows, run the `hcmds64fwcancel` command to configure exceptions in the firewall.
- If the OS is Linux, configure exceptions according to the OS specifications. For details about the procedure, see the OS documentation.

5. Start Ops Center Automator.

6. Run the `hcmds64chgurl` command to update the URL for accessing Ops Center Automator.

7. If you use Common Services, run the `setupcommonservice` command to apply the change.

See "setupcommonservice command" in the *Hitachi Ops Center Automator User Guide* for more information.

Common Component property updates for port number changes

To change Common Component port numbers, you must update the Common Component properties that are listed in the following table.

Update the property files and then restart all Common Component and Ops Center Automator services.

Port number (default)	Properties file path: Common Component installation folder	Location
22015/TCP	\uCPSB11\httpsd\conf \user_httpsd.conf	Listen
		Listen [::]:
		#Listen 127.0.0.1:

Port number (default)	Properties file path: Common Component installation folder	Location
22016/TCP	\uCPSB11\httpsd\conf \user_httpsd.conf	<i>host-name:port-number</i> in the VirtualHost tag
		Listen
		Listen [::]:
22031/TCP	\uCPSB11\httpsd\conf \user_hssso_httpsd.conf	Listen
22032/TCP	\HDB\CONF\emb\HiRDB.ini	PDNAMEPORT
	\HDB\CONF\pdsys	pd_name_port
	\database\work\def_pdsys	pd_name_port
22035/TCP	\uCPSB11\CC\server\usrconf\ejb \HBase64StgMgmtSSOService \usrconf.properties*	webserver.connector.n io_http.port
22036/TCP	\uCPSB11\CC\server\usrconf\ejb \HBase64StgMgmtSSOService \usrconf.properties	ejbserver.rmi.naming. port
22037/TCP	\uCPSB11\CC\server\usrconf\ejb \HBase64StgMgmtSSOService \usrconf.properties	ejbserver.http.port
22038/TCP	\uCPSB11\CC\server\usrconf\ejb \HBase64StgMgmtSSOService \usrconf.properties	ejbserver.rmi.remote. listener.port
22170/TCP	\uCPSB11\CC\server\userconf\ejb \AutomationWebService \usrconf.properties*	webserver.connector.n io_http.port
22171/TCP	\uCPSB11\CC\server\userconf\ejb \AutomationWebService \usrconf.properties	ejbserver.rmi.naming. port
22172/TCP	\uCPSB11\CC\server\userconf\ejb \AutomationWebService \usrconf.properties	ejbserver.http.port
22173/TCP	\uCPSB11\CC\server\userconf\ejb \AutomationWebService \usrconf.properties	ejbserver.rmi.remote. listener.port

Port number (default)	Properties file path: Common Component installation folder	Location
<p>*: When changing <code>webserver.connector.nio_http.port</code>, the following configuration files need to be modified in addition to the corresponding line in <code>usrconf.properties</code>.</p> <ul style="list-style-type: none"> ▪ <code>reverse_proxy.conf</code> ▪ <code>reverse_proxy_before.conf</code> ▪ <code>reverse_proxy_after.conf</code> ▪ <code>hssso_reverse_proxy.conf</code> <p>If the target port number is not described in the property file, no modification is required.</p>		

Changing the information of the server managing the user account

You can change the information of the server managing the user account, if necessary.



Note: The user accounts are managed by the Common Component on the host you specified during the installation.

Procedure

1. If SSL is not set for HBase 64 Storage Mgmt Web Service on the server managing the user account, run this command:

Windows OS:

```
Common-Component-installation_folder\bin\hcnds64prmset /host
Server-Managing-User-Account-IP-address-or-host-name /port
HBase-64-Storage_Mgmt-Web-Service-of-Server-Managing-User-
Account-non-SSL-portnumber
```

Linux OS:

```
Common-Component-installation-directory/bin/hcnds64prmset -host
Server-Managing-User-Account-IP-address-or-host-name -port
HBase-64-Storage-Mgmt-Web-Service-of-Server-Managing-User-
Account-non-SSL-portnumber
```

2. If SSL is set for HBase 64 Storage Mgmt Web Service on the server managing the user account, run this command:

Windows OS:

```
Common-Component-installation_folder\bin\hcnds64prmset /host
Server-Managing-User-Account-host-name /sslport HBase-64-Storage-
Mgmt-Web-Service-of-Server-Managing-User-Account-SSL-portnumber
```

Linux OS:

```
Common-Component-installation-directory/bin/hcnds64prmset -host
Server-Managing-User-Account-host-name -sslport HBase-64-Storage-
Mgmt-Web-Service-of-Server-Managing-User-Account-SSL-portnumber
```

Changing the management server host name

You can change the host name of the management server after installing Ops Center Automator.

The management server host name cannot exceed 128 characters and is case-sensitive.

Procedure

1. Make a note of the new management server host name.
If you must verify the host name on a Windows machine, use the `ipconfig /all` command to display the host name.
2. Run the `hcnds64srv /stop` command to stop all Common Component services.
3. Edit the `user_httpsd.conf` file to change the value of the `ServerName` parameter to the new host name.

The `user_httpsd.conf` file is stored in the following location:

- Windows OS

```
Common-Component-installation-folder\uCPSB11\httpsd\conf
```

- Linux OS

```
Common-Component-installation-directory/uCPSB11/httpsd/conf
```

If SSL settings are enabled, re-obtain the SSL server certificate and change the value of the `ServerName` parameter in the `VirtualHost` parameter to the new host name.

4. Edit the `command_user.properties` file to change the value of the `command_hostname` parameter to the new host name.

The `command_user.properties` is stored in the following location:

- Windows OS (non-cluster)

```
Automation_software-installation-folder\conf
```

- Windows OS (cluster)

```
shared-folder-name\Automation\conf
```

- Linux OS

```
Automation_software-installation-directory/conf
```

5. If you are running other Common Component products, revise the settings for those products as needed.
6. Change the host name of the management server. After making the change, restart the server.
7. If you use the host name to access the management server from a browser, run the `hcnds64chgurl` command to update the Common Component URL.

8. If you use Common Services, run the `setupcommonservice` command to apply the change.

Changing the management server IP address

You can change the IP address of the management server after installing Ops Center Automator.

Procedure

1. In the **Tasks** window, check the tasks. If any tasks are running, (In Progress, Waiting for Input, Long Running, In Progress (with Error), or In Progress (Terminating)), stop the tasks or wait until the task ends (Completed, Failed, or Canceled).
2. Run the `hcnds64srv /stop` command to stop all Common Component services.
3. Change the IP address of the management server.
4. Run the `hcnds64srv /start` command to start all Common Component services.
5. If you use the IP address to access the management server from a browser, run the `hcnds64chgurl` command to update the URL.
6. If you use Common Services, run the `setupcommonservice` command to apply the change.

Changing the Ops Center Automator management server URL

You must change the Ops Center Automator management server URL if you change the management server host name or IP address, the Ops Center Automator ports, or any SSL settings. If Ops Center Automator runs on the same management server as other Common Component products, you can change all of the Common Component URLs with one command.



Note: You must use a complete URL, which includes a protocol and a port number, for example, `http://HostA:22015`.

Procedure

1. Verify the current URL using the following command:
`Common-Component-installation-folder\bin\hcnds64chgurl /list`
2. If Ops Center Automator is installed on a standalone server, change only the Ops Center Automator URL using the following command:
`Common-Component-installation-folder\bin\hcnds64chgurl /change new-URL /type Automation`
3. If Ops Center Automator is installed on the same server, change all Common Component URLs that are running on this management server using the following command:
`Common-Component-installation-folder\bin\hcnds64chgurl /change old-URL new-URL`

Use the following format for the URL:

`Protocol://Management-server-IP-address-or-host-name:port-number`

Where:

- *Protocol* is `http` for non-SSL communication and `https` for SSL communication.
- *Management-server-IP-address-or-host-name* is the IP address or host name of the management server on which Ops Center Automator is installed.
- *port-number* is the port number that is set for `Listen` line in the `user_httpsd.conf` file.

For non-SSL communication, specify the port number for non-SSL communication (default: 22015).

For SSL communication, specify the port number for SSL communication (default: 22016).

The `user_httpsd.conf` file is in the *Common-Component-installation-folder\uCPSB11\httpsd\conf* folder.

4. Verify that you can access Ops Center Automator using the new URL.
5. If you use Common Services, run the `setupcommonservice` command to apply the change.

Configuring secure communications

This module describes how to configure secure communications for Ops Center Automator.

About Ops Center Automator security settings

You can increase security by using secure communication for Ops Center Automator. Secure communication enables Ops Center Automator to increase security by using Secure Sockets Layer (SSL) or Transport Layer Security (TLS) for Ops Center Automator network communication. SSL or TLS enable Ops Center Automator to verify communication partners, enhance authentication for identifying partners, and detect falsified data within sent and received information. In addition, communication channels are encrypted so that data is protected from eavesdropping.

Ops Center Automator can use secure communications using SSL or TLS for the following types of communication:

- Communication between the management server and management clients
- Communication between the management server and an external authentication server (LDAP directory server)
- Communication between the management server and management targets

In addition, you can restrict access so that only specific management clients can access the management server.



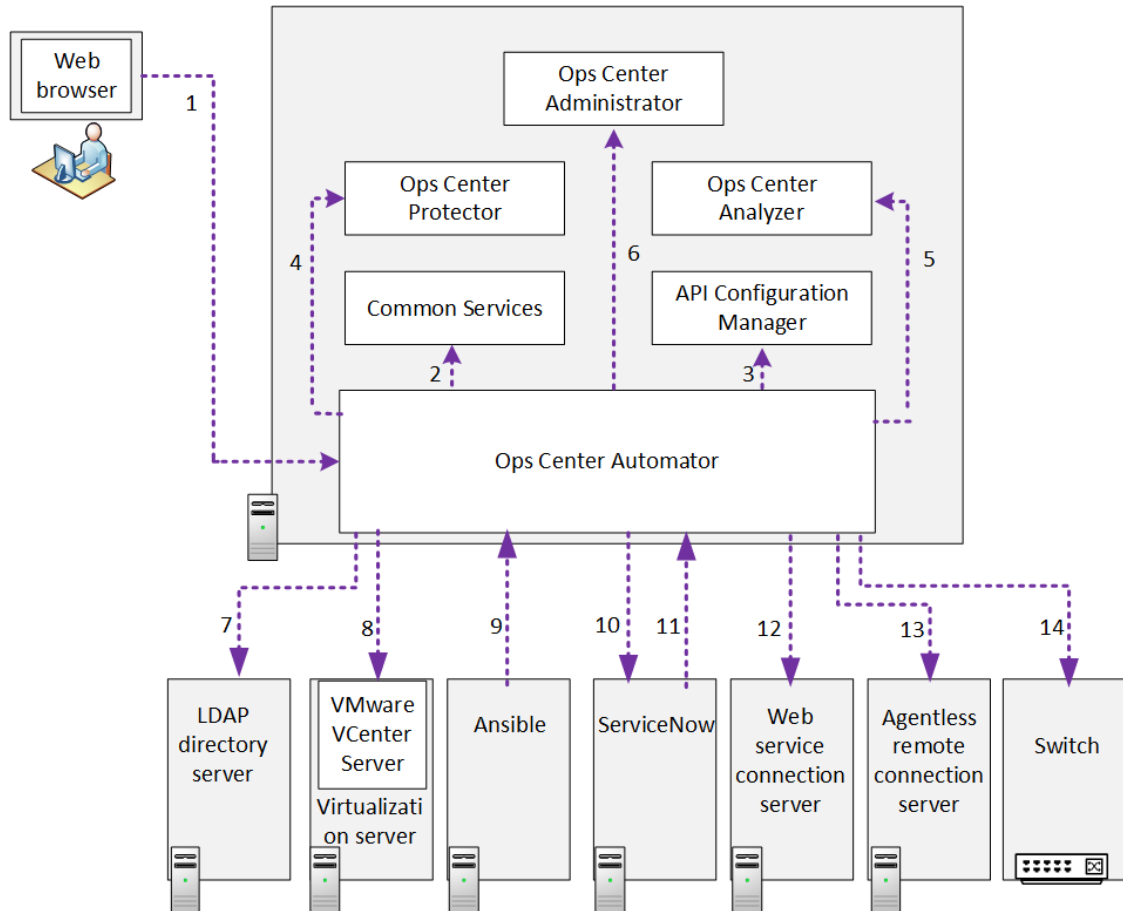
Note: When you use Ops Center Automator with security enabled, make sure that the server certificate is not expired. If the server certificate is expired, you must register a valid certificate to Ops Center Automator because users might not be able to connect to the server.



Note: For secure communication between the management server and management target, import the certificates issued by the Certificate authority, Intermediate certificate authority, or Root certificate authority into the Common Component trust store. If you want to re-register the certificates, you must delete the certificates by referring to [Deleting Common Component truststore certificates \(on page 85\)](#) and then import the certificates again.

Secure communication routes for Ops Center Automator

The following shows the secure communication routes for Ops Center Automator.



The following shows the secure communication routes that can be used in Ops Center Automator and the supported protocols for each route that is used. Note that the number in the table corresponds with the number in the figure.

Route	Server (program)	Client	Protocol
1	Ops Center Automator ¹	Management client (Web browser)	HTTPS ²
2	Ops Center Common Services ¹	Ops Center Automator ¹	HTTPS

Route	Server (program)	Client	Protocol
3	Ops Center API Configuration Manager ¹	Ops Center Automator ¹	HTTPS ²
4	Ops Center Protector ¹	Ops Center Automator ¹	HTTPS
5	Ops Center Analyzer ¹	Ops Center Automator ¹	HTTPS ²
6	Ops Center Administrator ¹	Ops Center Automator ¹	HTTPS
7	LDAP directory server	Ops Center Automator ¹	StartTLS ³
8	VMware vCenter Server	Ops Center Automator ¹	HTTPS
9	Ops Center Automator ¹	Ansible ⁵	HTTPS
10	ServiceNow	Ops Center Automator ¹	HTTPS
11	Ops Center Automator ¹	ServiceNow ⁶	HTTPS
12	Web service connection server (for example, DCNM)	Ops Center Automator ¹	HTTPS ²
13	Agentless remote connection server	Ops Center Automator ¹	SSH ⁴
14	Brocade Fabric OS	Ops Center Automator ¹	HTTPS ²
<ol style="list-style-type: none"> 1. You can configure this component by using the <code>cssslsetup</code> command if the products are installed on the same management server as Common Services. 2. HTTP can also be used in addition to HTTPS. 3. LDAP can also be used in addition to StartTLS. 4. Telnet or SMB and RPC can also be used in addition to SSH. 5. If you use a Common Services user to access Ops Center Automator, the SSL setting between Ansible and Common Services is also required. 6. If you use a Common Services user to access Ops Center Automator, the SSL setting between ServiceNow and Common Services is also required. 			

- For security settings for communication route 9 with Ansible, see the *Hitachi Ops Center Automator User Guide*.
- For security settings for communication route 10 and 11 with ServiceNow, see the *Hitachi Ops Center Automator User Guide*.

Configuring security for management clients

This module gives information about setting up secure communication between the management server and management clients.

About secure communications for management clients

Implement secure communication between the Ops Center Automator management server and management clients using SSL. To implement SSL, first set up SSL on the management server and then on the management clients. The process for setting up SSL on web-based clients is different from CLI clients.

Setting up SSL on the server for secure client communication (Windows OS)

To implement secure communication between the management server and management clients, you must set up SSL on the management server.



Note: After a new installation, SSL settings are enabled. The same certificate is used as when the `hcnds64ssltool` command is run without any options. In the case of an upgrade installation, keep the current SSL settings.

The `hcnds64ssltool` command creates two types of private keys: certificate signing requests, and self-signed certificates supporting RSA ciphers and elliptic curve ciphers (ECC). The certificate signing request is created in PEM format. Although you can use this command to create a self-signed certificate, you should use a self-signed certificate for testing purposed only.

Before you begin

Log on as a user with Administrator permissions.

Collect the following information:

- Requirements for the certificate signing request specified by the certificate authority.
- Web browser version running on the management client.

The Web browser must use X.509 PEM format and support the signature algorithm of the server certificates used on the management client (GUI).

- Existing storage directories for private keys, certificate signing requests, and self-signed certificates, if you are recreating them.

If a file with the same name already exists in the output location, the command does not overwrite the file. Therefore, when you recreate a private key, certificate signing request, or self-signed certificate, you must output it to a folder other than existing storage folders or delete the existing files.

Procedure

1. To create a private key (`httpsdkey.pem`), a certificate signing request (`httpsd.csr`), and a self-signed certificate (`httpsd.pem`) for the Common Component, use the following command:


```
Common-Component-installation-folder\bin\hccmds64ssltool [/key
private-key-file] [/csr certificate-signed-request-file] [/cert
self-signed-certificate-file] [/certtext self-signed-certificate-
content-file] [/validity expiration-date] [/sigalg RSA-server-
certificate-signature-algorithm] [/eccsigalg ECC-server-
certificate-signature-algorithm] [/ecckeysize ECC-private-key-
size] [/ext extension-information-for-the-X.509-certificate]
```

where

- **key** specifies the absolute path of the private key file that is created. If you omit this option, the files are output to the default output destination path[#] with the file name `httpsdkey.pem` (for RSA) and `ecc-httpsdkey.pem` (for ECC).
- **csr** specifies the absolute path of the certificate signing request file that is created. If you omit this option, the files are output to the default output destination path[#] with the file name `httpsd.csr` (for RSA) and `ecc-httpsd.csr` (for ECC).
- **cert** specifies the absolute path of the self-signed certificate file that is created. If you omit this option, the files are output to the default output destination path[#] with the file name `httpsd.pem` (for RSA) and `ecc-httpsd.pem` (for ECC).
- **certtext** specifies the absolute path of the self-signed certificate content file that is created. If you omit this option, the files are output to the default output destination path[#] with the file name `httpsd.txt` (for RSA) and `ecc-httpsd.txt` (for ECC).
- **validity** specifies the expiration date of the self-signed certificate by using the number of days. If you omit this option, the default of 3,650 days is used.
- **sigalg** specifies the signature algorithm of the RSA certificate as `SHA256withRSA`, or `SHA1withRSA`. If you omit this option, the default of `SHA256withRSA` is used.
- **eccsigalg** specifies the signature algorithm of the ECC certificate as `SHA512withECDSA`, `SHA384withECDSA`, `SHA256withECDSA`, or `SHA1withECDSA`. If you omit this option, the default of `SHA384withECDSA` is used.
- **ecckeysize** specifies the key size of the private key for the ECC server certificates in bits as 256 or 384. If you omit this option, the default of 384 is used.
- **ext** specifies the extension information for the X.509 certificate. To set SAN (Subject Alternative Name) on the self-signed certificate and certificate signing request, specify this option. The specification method is based on the **ext** option of the **keytool** command in Java. Note, however, that the only extension that can be specified in Ops Center Automator is SAN. If you specify the **ext** option multiple times, the first specification takes effect.

The following is an example of specifying the extension information.

- To specify `www.example.com` as the host name:

```
hccmds64ssltool /ext san=dns:www.example.com
```

- To specify `www.example.com` and `www.example.net` as multiple host names:

```
hccmds64ssltool /ext san=dns:www.example.com,
dns:www.example.net
```

This command outputs the RSA and ECC files to the specified output destination path. RSA files are output with the specified file name, and ECC files output with a prefix of "ecc-".

#The default output destination when you omit the key, csr, cert, or certtext options is as follows:

```
Common-Component-installation-folder\uCPSB11\httpsd\conf\ssl  
\server
```

2. When prompted, enter the following information after the colon(:).
 - Server Name (management server host name) - for example, Automator-SC1.
 - Organizational Unit (section) - for example, Ops Center Automator.
 - Organization Name (company) - for example, Hitachi.
 - City or Locality Name - for example, Santa Clara.
 - State or Province Name (full name) - for example, California.
 - Country Name (2 letter code) - for example, US.

To leave a field blank, type a period (.). To select a default value visible within the brackets ([]), press **Enter**.

3. Send the certificate signing request (`httpsd.csr`) to the certificate authority to apply for a server certificate.



Note: This step is not required if you plan to use a self-signed certificate, but you should use a signed server certificate in a production environment.

The server certificate issued by the certificate authority is usually sent by email. Ensure that you save the email and the server certificate sent by the certificate authority.

4. Stop Ops Center Automator.
5. Copy the private key (`httpsdkey.pem`) and the server certificate or the self-signed certificate (`httpsd.pem`) to the following folder:

```
Common-Component-installation-folder\uCPSB11\httpsd\conf\ssl  
\server
```

6. Open the `user_httpsd.conf` file from the following location:

```
Common-Component-installation-folder\uCPSB11\httpsd\conf  
\user_httpsd.conf
```

7. Within the `user_httpsd.conf` file, do the following:

- a. Uncomment the following lines by removing the hash [#] signs:

```
#Listen 22016  
  
#<VirtualHost *:22016>  
  
through  
  
#</VirtualHost>
```

with the exception of #SSLCACertificateFile and #Header set Strict-Transport-Security max-age=31536000, which must remain commented out.

The following is an example of how to edit the user_httpsd.conf file. If you are using SSL ECC, also uncomment the following lines:

#SSLCertificateKeyFile

#SSLCertificateFile

```
ServerName host-name
Listen 22015
Listen [::]:22015
#Listen 127.0.0.1:22015
SSLEngine Off
Listen 22016
#Listen [::]:22016
<VirtualHost *:22016>
ServerName host-name
SSLEngine On
SSLProtocol +TLSv1.2 +TLSv1.3
SSLCipherSuite TLSv1.3
TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256
# SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-
SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES256-GCM-
SHA384:AES128-GCM-SHA256
SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-
SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256
SSLCertificateKeyFile
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/server/
httpsdkey.pem"
SSLCertificateFile
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/server/
httpsd.pem"
#SSLCertificateKeyFile
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/server/ecc-
httpsdkey.pem"
#SSLCertificateFile
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/server/ecc-
httpsd.pem"
# SSLCACertificateFile
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/cacert/
anycert.pem"
# Header set Strict-Transport-Security max-age=31536000
</VirtualHost>
#HWSLogSSLVerbose On
```

- b. Edit the following lines as required:

ServerName in the first line

ServerName in the <VirtualHost> tag

SSLCertificateKeyFile

SSLCertificateFile

#SSLCACertificateFile

When using a chained server certificate issued from a certificate authority, delete the hash sign (#) from the line "# SSLCACertificateFile", and specify the chained certificate file (created by certificate authority) by using an absolute path.



Note:

To block non-SSL communication from external servers to the management server, comment out the lines `Listen 22015` and `Listen [::]:22015` by adding a hash mark (#) to the beginning of each line. After you comment out these lines, remove the hash mark (#) from the line `#Listen 127.0.0.1:22015`.

For an IPv6 environment, remove the hash mark (#) at the beginning of the lines `#Listen [::]:22016`.

When editing directives, be aware of the following:

- Do not specify the same directive twice.
- Do not enter a line break in the middle of a directive.
- When specifying paths in the following directives, do not specify symbolic links or junction points.
- When specifying certificates and private key files in the following directives, specify PEM-format files.
- Do not edit `httpsd.conf` or `hssso_httpsd.conf`.
- Do not remove the hash mark (#) from the beginning of the following line.

```
# Header set Strict-Transport-Security max-age=31536000
```

The following is an example of how to edit the `user_httpsd.conf` file. The numbers represent the default ports.

```
ServerName host-name
Listen 22015
Listen [::]:22015
#Listen 127.0.0.1:22015
SSLEngine Off
Listen 22016
#Listen [::]:22016
<VirtualHost *:22016>
ServerName host-name
SSLEngine On
SSLProtocol +TLSv1.2 +TLSv1.3
SSLCipherSuite TLSv1.3
TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256
# SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDSA-AES128-GCM-
SHA256:ECDSA-RSA-AES256-GCM-SHA384:ECDSA-RSA-AES128-GCM-SHA256:AES256-GCM-
```

```
SHA384:AES128-GCM-SHA256
SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-
RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256
SSLCertificateKeyFile
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/server/
httpsdkey.pem"
SSLCertificateFile
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/server/server-
certificate-or-self-signed-certificate-file"
#SSLCertificateKeyFile
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/server/ecc-
httpsdkey.pem"
#SSLCertificateFile
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/server/ecc-
httpsd.pem"
SSLCACertificateFile
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/cacert/
certificate-file-from-certificate-authority"
# Header set Strict-Transport-Security max-age=31536000
</VirtualHost>
#HWSLogSSLVerbose On
```

8. Start Ops Center Automator.
9. Update the Ops Center Automator URL by using the `hcnds64chgurl` to do the following:
 - Change the protocol from `http:` to `https:`
 - Change the port number used for secure communication.
10. If you use Common Services, run the `setupcommonservice` command to apply the change.

Result

SSL is now implemented on the Ops Center Automator server.

Setting up SSL on the server for secure client communication (Linux OS)

To implement secure communication between the management server and management clients, you must set up SSL on the management server.



Note: After a new installation, SSL settings are enabled. The same certificate is used as when the `hcnds64ssltool` command is run without any options. In the case of an upgrade installation, keep the current SSL settings.

The `hcnds64ssltool` command creates two types of private keys: certificate signing requests, and self-signed certificates supporting RSA ciphers and elliptic curve ciphers (ECC). The certificate signing request is created in PEM format. Although you can use this command to create a self-signed certificate, best practice is to use a self-signed certificate for testing purposed only.

Before you begin

Log on as a root user.

Collect the following information:

- Requirements for the certificate signing request specified by the certificate authority.
- Web browser version running on the management client.

The Web browser must use X.509 PEM format and support the signature algorithm of the server certificates used on the management client (GUI).

- Existing storage directories for private keys, certificate signing requests, and self-signed certificates, if you are recreating them.

If a file with the same name already exists in the output location, the command does not overwrite the file. Therefore, when you recreate a private key, certificate signing request, or self-signed certificate, you must output it to a directory other than existing storage directory or delete the existing files.

Procedure

1. To create a private key (`httpsdkey.pem`), a certificate signing request (`httpsd.csr`), and a self-signed certificate (`httpsd.pem`) for the Common Component, use the following command:

```
Common-Component-installation-directory/bin/hcmds64ssltool [-key
private-key-file] [-csr certificate-signed-request-file] [-cert
self-signed-certificate-file] [-certtext self-signed-certificate-
content-file] [-validity expiration-date] [-sigalg RSA-server-
certificate-signature-algorithm] [-eccsigalg ECC-server-
certificate-signature-algorithm] [-ecckeysize ECC-private-key-
size] [-ext extension-information-for-the-X.509-certificate]
```

where

- `key` specifies the absolute path of the private key file that is created. If you omit this option, the files are output to the default output destination path[#] with the file name `httpsdkey.pem` (for RSA) and `ecc-httpsdkey.pem` (for ECC).
- `csr` specifies the absolute path of the certificate signing request file that is created. If you omit this option, the files are output to the default output destination path[#] with the file name `httpsd.csr` (for RSA) and `ecc-httpsd.csr` (for ECC).
- `cert` specifies the absolute path of the self-signed certificate file that is created. If you omit this option, the files are output to the default output destination path[#] with the file name `httpsd.pem` (for RSA) and `ecc-httpsd.pem` (for ECC).
- `certtext` specifies the absolute path of the self-signed certificate content file that is created. If you omit this option, the files are output to the default output destination path[#] with the file name `httpsd.txt` (for RSA) and `ecc-httpsd.txt` (for ECC).
- `validity` specifies the expiration date of the self-signed certificate by using the number of days. If you omit this option, the default of 3,650 days is used.

- `sigalg` specifies the signature algorithm of the RSA certificate as SHA256withRSA, or SHA1withRSA. If you omit this option, the default of SHA256withRSA is used.
- `eccsigalg` specifies the signature algorithm of the ECC certificate as SHA512withECDSA, SHA384withECDSA, SHA256withECDSA, or SHA1withECDSA. If you omit this option, the default of SHA384withECDSA is used.
- `ecckeysize` specifies the key size of the private key for the ECC server certificates in bits as 256 or 384. If you omit this option, the default of 384 is used.
- `ext` specifies the extension information for the X.509 certificate. To set SAN (Subject Alternative Name) on the self-signed certificate and certificate signing request, specify this option. The specification method is based on the `ext` option of the `keytool` command in Java. Note, however, that the only extension that can be specified in Ops Center Automator is SAN. If you specify the `ext` option multiple times, the first specification takes effect.

The following is an example of specifying the extension information.

- To specify `www.example.com` as the host name:

```
hccmds64ssltool -ext san=dns:www.example.com
```

- To specify `www.example.com` and `www.example.net` as multiple host names:

```
hccmds64ssltool -ext san=dns:www.example.com,  
dns:www.example.net
```

This command outputs the RSA and ECC files to the specified output destination path. RSA files are output with the specified file name, and ECC files output with a prefix of "ecc".

#The default output destination when you omit the `key`, `csr`, `cert`, or `certtext` options is as follows:

```
Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/  
server
```

2. When prompted, enter the following information after the colon(:).
 - Server Name (management server host name) - for example, Automator-SC1.
 - Organizational Unit (section) - for example, Ops Center Automator.
 - Organization Name (company) - for example, Hitachi.
 - City or Locality Name - for example, Santa Clara.
 - State or Province Name (full name) - for example, California.
 - Country Name (2 letter code) - for example, US.

To leave a field blank, type a period (.). To select a default value visible within the brackets ([]), press **Enter**.

3. Send the certificate signing request (`httpsd.csr`) to the certificate authority to apply for a server certificate.



Note: This step is not needed if you plan to use a self-signed certificate, but best practice is to use a signed server certificate in a production environment.

The server certificate issued by the certificate authority is usually sent by email. Ensure that you save the email and the server certificate sent by the certificate authority.

4. Stop Ops Center Automator.
5. Copy the private key (`httpsdkey.pem`) and the server certificate or the self-signed certificate (`httpsd.pem`) to the following directory:

```
Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/
server
```

6. Open the `user_httpsd.conf` file from the following location:

```
Common-Component-installation-directory/uCPSB11/httpsd/conf/
user_httpsd.conf
```

7. Within the `user_httpsd.conf` file, do the following:
 - a. Uncomment the following lines by removing the hash [#] signs:

```
#Listen 22016

#<VirtualHost *:22016>

through

#</VirtualHost>
```

with the exception of `#SSLCACertificateFile` and `#Header set Strict-Transport-Security max-age=31536000`, which must remain commented out.

The following is an example of how to edit the `user_httpsd.conf` file. If you are using SSL ECC, also uncomment the following lines:

```
#SSLCertificateKeyFile
```

```
#SSLCertificateFile
```

```
ServerName host-name
Listen 22015
Listen [::]:22015
#Listen 127.0.0.1:22015
SSLEngine Off
Listen 22016
#Listen [::]:22016
<VirtualHost *:22016>
ServerName host-name
SSLEngine On
SSLProtocol +TLSv1.2 +TLSv1.3
SSLCipherSuite TLSv1.3
TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256
# SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDSA-AES128-
GCM_SHA256:ECDSA-AES256-GCM-SHA384:ECDSA-AES128-GCM-SHA256:
GCM_SHA384:AES128-GCM-SHA256
SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDSA-AES128-
GCM_SHA256:ECDSA-AES256-GCM-SHA384:ECDSA-AES128-GCM-SHA256
SSLCertificateKeyFile
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/server/
```



```
httpsdkey.pem"
SSLCertificateFile
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/server/
httpsd.pem"
#SSLCertificateKeyFile
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/server/ecc-
httpsdkey.pem"
#SSLCertificateFile
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/server/ecc-
httpsd.pem"
# SSLCACertificateFile
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/cacert/
anycert.pem"
# Header set Strict-Transport-Security max-age=31536000
</VirtualHost>
#HWSLogSSLVerbose On
```

b. Edit the following lines as required:

ServerName in the first line

ServerName in the <VirtualHost> tag

SSLCertificateKeyFile

SSLCertificateFile

#SSLCACertificateFile

When using a chained server certificate issued from a certificate authority, delete the hash sign (#) from the line "# SSLCACertificateFile", and specify the chained certificate file (created by certificate authority) by using an absolute path.



Note:

To block non-SSL communication from external servers to the management server, comment out the lines `Listen 22015` and `Listen [::]:22015` by adding a hash mark (#) to the beginning of each line. After you comment out these lines, remove the hash mark (#) from the line `#Listen 127.0.0.1:22015`.

For an IPv6 environment, remove the hash mark (#) at the beginning of the lines `#Listen [::]:22016`.

When editing directives, be aware of the following:

- Do not specify the same directive twice.
- Do not enter a line break in the middle of a directive.
- When specifying paths in the following directives, do not specify symbolic links or junction points.
- When specifying certificates and private key files in the following directives, specify PEM-format files.

- Do not edit `httpsd.conf` or `hssso_httpsd.conf`.
- Do not remove the hash mark (#) from the beginning of the following line.

```
# Header set Strict-Transport-Security max-age=31536000
```

The following is an example of how to edit the `user_httpsd.conf` file. The numbers represent the default ports.

```
ServerName host-name
Listen 22015
Listen [::]:22015
#Listen 127.0.0.1:22015
SSLEngine Off
Listen 22016
#Listen [::]:22016
<VirtualHost *:22016>
ServerName host-name
SSLEngine On
SSLProtocol +TLSv1.2 +TLSv1.3
SSLCipherSuite TLSv1.3
TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256
# SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-
GCM_SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES256-
GCM_SHA384:AES128-GCM-SHA256
SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-
SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256
SSLCertificateKeyFile
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/server/
httpsdkey.pem"
SSLCertificateFile
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/server/server-
certificate-or-self-signed-certificate-file"
#SSLCertificateKeyFile
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/server/ecc-
httpsdkey.pem"
#SSLCertificateFile
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/server/ecc-
httpsd.pem"
SSLCACertificateFile
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/cacert/
certificate-file-from-certificate-authority"
# Header set Strict-Transport-Security max-age=31536000
</VirtualHost>
#HWSLogSSLVerbose On
```

8. Start Ops Center Automator.

9. Update the Ops Center Automator URL by using the `hcmds64chgurl` command to do the following:
 - Change the protocol from `http:` to `https:`
 - Change the port number used for secure communication.
10. If you use Common Services, run the `setupcommonservice` command to apply the change.

Result

SSL is now implemented on the Ops Center Automator server.

Setting up SSL on web-based management clients

To implement secure communications between the management server and management clients, you must set up SSL on all Ops Center Automator management clients that access the Ops Center Automator web-based user interface. You must first set up SSL on the management server before setting up the management clients. You are only required to follow this procedure the first time you access the management server from this client.

Before you begin

If the signature algorithm used is SHA256 with RSA, the Web browser in use must support a server certificate that has an SHA256 with RSA signature.

Procedure

1. From the management web client, access the management server using an SSL connection by using the following URL:


```
https://automation-software-management-server-name:port-number-for-SSL-communication/Automation/
```
2. Install the SSL certificate.

Result

The SSL certificate is registered on the management client so it can communicate with the management server using SSL.

Setting up secure communication for an external authentication server

In a Windows environment, use the StartTLS protocol to implement secure communication between the Ops Center Automator management server and the LDAP directory server. To implement StartTLS, you must update the properties in the `exauth.properties` file and import the LDAP directory server certificate into the management server.

See [Importing a certificate into the truststore for Common Component \(on page 76\)](#) for details.



Note: If you specify an IPV6 address in a Linux OS environment, you are required to enclose the address with square brackets [].

Importing a certificate into the truststore for Common Component

To import a certificate to the truststore (ldapcacerts or jssecacerts), use the **hcnds64keytool** utility (for Windows) or the **keytool** utility (for Linux).

Before you begin

- Prepare a certificate

Securely obtain the certificate.

- For communication with an LDAP directory server:

The certificates issued by all the authorities from the authority that issued an LDAP directory server certificate to the root certificate authority must form a certificate chain. The certificate must satisfy the product requirements for Common Component.

- When using a certificate authority:

The certificates issued by all the authorities from the authority which issued the Common Component server certificate to the root certificate authority must form a certificate chain.

- When using a self-signed certificate:

Obtain a Common Component self-signed certificate.

- Verify the following information:

- Path of the truststore file
- Password to access the truststore, if the truststore already exists

Procedure

1. Run the following command:

In Windows:

```
Common-Component-installation-folder\bin\hcnds64keytool -import -  
alias alias-name -file certificate-file-name -keystore  
truststore-file-name -storepass truststore-password -storetype  
JKS
```

In Linux:

```
Common-Component-installation-directory/uCPSB11/jdk/bin/keytool -  
import -alias alias-name -file certificate-file-name -keystore  
truststore-file-name -storepass truststore-password -storetype  
JKS
```

Where:

- **alias:** Specify the name used to identify the certificate in the truststore. If there are two or more server certificates, specify an alias name which is not used in the truststore.
- **keystore:** Specify the truststore file path of the import destination. If no truststore file exists, one will be automatically created.

You should import LDAP directory server certificates into `ldapcacerts`. To share a certificate with other programs, you can import the certificate into `jssecacerts`.

- Specify the password used to access the truststore.



Note: When you use the `hcnds64keytool` or `keytool` utility to specify a unique name in the truststore, the truststore file name, and the password:

- Do not use the following symbols in the file name:
`: , ; * ? " < > |`
- Specify the file name as a character string of no more than 255 bytes.
- Do not include double quotation marks (") in the unique name in the truststore or the password.

2. Restart the Common Component services.

Changing the authenticator connection port number for the primary Common Component server

After you set up secure communication with an external authentication server, you must change the authenticator connection port number.

To change the authenticator connection port number, run the `hcnds64prmset` command as follows:

- Windows:

```
Common-Component-installation-folder\bin\hcnds64prmset /host  
primary_server_hostname /sslport SSL_port_number
```

- Linux:

```
Common-Component-installation-directory/bin/hcnds64prmset -host  
primary_server_hostname -sslport SSL_port_number
```

where:

- `primary_server_hostname` is the same name as the Common Name (CN) for the credentials.
- `ssl_port_number` is the same as the SSL Common Component port number. The default is 22016.

Setting up secure communications with Ops Center Common Services

Ops Center Automator and Ops Center Common Services must communicate over an SSL connection.



Tip: If Common Services is on the same server as Ops Center Automator, the `cssslsetup` command is available. By using the `cssslsetup` command, you can configure SSL communication for Hitachi Ops Center products installed on the same management server using a common secret key and server certificate. For more information on the usage and support scope of the `cssslsetup` command, refer to "Configuring SSL communications by using the `cssslsetup` command" in the *Hitachi Ops Center Installation and Configuration Guide*.

Before you begin

- Set up SSL on the Ops Center Automator server between the management server and management client. For details, see ["Setting up SSL on the server for secure client communication \(Windows OS\)" \(on page 64\)](#) or ["Setting up SSL on the server for secure client communication \(Linux OS\)" \(on page 69\)](#).
- Set up SSL on the Common Services server. For details, see "Configuring SSL for a multi-server configuration" in the *Hitachi Ops Center Installation and Configuration Guide*.

Procedure

1. Import the certificates into the Common Component truststore by running the following command:

For Windows:

```
Common-Component-installation-folder\bin\hcmds64keytool -import -alias
alias-name -keystore Common-Component-installation-folder\uCPSB11
\jdk\jdk\lib\security\jssecacerts -storepass truststore-password -file
certificate-file -storetype JKS
```

For Linux:

```
Common-Component-installation-directory/uCPSB11/jdk/bin/keytool -import -alias
alias-name -keystore Common-Component-installation-directory/uCPSB11/
jdk/jdk/lib/security/jssecacerts -storepass truststore-password -file
certificate-file -storetype JKS
```

To import the certificates in Java, ensure that the truststore password includes six or more characters. In addition, ensure that the new alias name does not conflict with an existing alias name.

2. (Optional) If you want to enable SSL verification, edit the `sso.https.certification` parameter to `true` in the `automation_software_install_dir/conf/config_user.properties` file.
3. Restart the services by running the `hcmds64srv` command.

Setting up secure communication with an Ops Center API Configuration Manager REST API server

You can set up SSL communication to be used between the Ops Center Automator server and the Ops Center API Configuration Manager REST API server by using a self-signed certificate or a certificate issued by a certificate authority.

Before you begin

If you already set up SSL on the Ops Center API Configuration Manager server, including creating the certificates, go to step 2. Otherwise, start at step 1.

Procedure

1. Set up SSL on the Ops Center API Configuration Manager REST API server. For details, see “Specifying settings for using SSL communication between REST API clients and the REST API server (when using a self-signed certificate)” or “Specifying settings for using SSL communication between REST API clients and the REST API server (when using a server certificate issued by a certificate authority)” in the *Hitachi Ops Center API Configuration Manager REST API Reference Guide*.
2. Import the certificates into the Common Component truststore by running the following command:

For Windows:

```
Common-Component-installation-folder\bin\hcmds64keytool -import -alias  
alias-name -keystore Common-Component-installation-folder\uCPSB11  
\jdk\jdk\lib\security\jssecacerts -storepass truststore-password -file  
certificate-file -storetype JKS
```

For Linux:

```
Common-Component-installation-directory/uCPSB11/jdk/bin/keytool -import -alias  
alias-name -keystore Common-Component-installation-directory/uCPSB11/  
jdk/jdk/lib/security/jssecacerts -storepass truststore-password -file  
certificate-file -storetype JKS
```

To import the certificates in Java, ensure that the truststore password includes six or more characters. In addition, ensure that the new alias name does not conflict with an existing alias name.

3. Restart the services by running the **hcmds64srv** command.

Setting up secure communication with an Ops Center Administrator server

You can set up SSL communication to be used between the Ops Center Automator server and the Ops Center Administrator server by using a self-signed certificate or a certificate issued by a certificate authority.

Before you begin

If you already set up SSL on the Ops Center Administrator server, including creating the certificates, go to step 2. Otherwise, start at step 1.

Procedure

1. Set up SSL on the Ops Center Administrator server. For details, see “Setting up SSL” in the *Hitachi Ops Center Administrator Getting Started Guide*.
2. Import the certificates into the Common Component truststore by running the following command:

For Windows:

```
Common-Component-installation-folder\bin\hcmds64keytool -import -alias
alias-name -keystore Common-Component-installation-folder\uCPSB11
\hjdk\jdk\lib\security\jssecacerts -storepass truststore-password -file
certificate-file -storetype JKS
```

For Linux:

```
Common-Component-installation-directory/uCPSB11/jdk/bin/keytool -import -alias
alias-name -keystore Common-Component-installation-directory/uCPSB11/
hjdk/jdk/lib/security/jssecacerts -storepass truststore-password -file
certificate-file -storetype JKS
```

To import the certificates in Java, ensure that the truststore password includes six or more characters. In addition, ensure that the new alias name does not conflict with an existing alias name.

3. Restart the services by running the **hcmds64srv** command.

Setting up secure communication with an Ops Center Protector server

You can set up SSL communication between the Ops Center Automator server and the Ops Center Protector server by using a self-signed certificate or a certificate issued by a certificate authority.

Before you begin

If you already set up SSL on the Ops Center Protector server, including creating the certificates, go to step 2. Otherwise, start at step 1.

Procedure

1. Set up SSL on the Ops Center Protector server. See "How to configure a server side SSL certificate" in the *Hitachi Ops Center Protector User Guide*.
2. Import the certificates into the Common Component truststore by running the following command:

For Windows:

```
Common-Component-installation-folder\bin\hcmds64keytool -import -alias
alias-name -keystore Common-Component-installation-folder\uCPSB11
\hjdk\jdk\lib\security\jssecacerts -storepass truststore-password -file
certificate-file -storetype JKS
```

For Linux:

```
Common-Component-installation-directory/uCPSB11/jdk/bin/keytool -import -alias
alias-name -keystore Common-Component-installation-directory/uCPSB11/
hjdk/jdk/lib/security/jssecacerts -storepass truststore-password -file
certificate-file -storetype JKS
```

To import the certificates in Java, ensure that the truststore password includes six or more characters. In addition, ensure that the new alias name does not conflict with an existing alias name.

3. Restart the services by running the **hcmds64srv** command.

Setting up secure communication with an Ops Center Analyzer server

You can set up SSL communication to be used between the Ops Center Automator server and the Ops Center Analyzer server by using a self-signed certificate or a certificate issued by a certificate authority.

Before you begin

If you already set up SSL on the Ops Center Analyzer server, including creating the certificates, go to step 2. Otherwise, start at step 1.

Procedure

1. Set up SSL on the Ops Center Analyzer server. For details, see “Configuring an SSL certificate (Analyzer server)” in the *Hitachi Ops Center Analyzer Installation and Configuration Guide*.
2. Import the certificates into the Common Component truststore by running the following command:

For Windows:

```
Common-Component-installation-folder\bin\hcmds64keytool -import -alias
alias-name -keystore Common-Component-installation-folder\uCPSB11
\hjdk\jdk\lib\security\jssecacerts -storepass truststore-password -file
certificate-file -storetype JKS
```

For Linux:

```
Common-Component-installation-directory/uCPSB11/jdk/bin/keytool -import -alias
alias-name -keystore Common-Component-installation-directory/uCPSB11/
```

```
hjdk/jdk/lib/security/jssecacerts -storepass truststore-password -file
certificate-file -storetype JKS
```

To import the certificates in Java, ensure that the truststore password includes six or more characters. In addition, ensure that the new alias name does not conflict with an existing alias name.

3. Restart the services by running the **hcnds64srv** command.

Setting up secure communication with a VMware vCenter server

As with all web service connections that use secure communication, you must import the VMware vCenter Server root certificates to the Ops Center Automator Common Component truststore that Ops Center Automator references. However, if you plan to use the ESX cluster service templates, you must also install the VMware vCenter Server root certificates into the OS truststore in order to configure secure communication for the prerequisite software in the service templates.



Note: If you do not plan to use the ESX cluster service templates, you do not need to complete this procedure.

To install the VMware vCenter Server root certificates:

Procedure

1. Download the VMware vCenter Server root certificates as follows:
 - a. Using a web browser, access the vCenter user interface.
 - b. In the right-side window, select **Download trusted root CA certificates**.
 - c. Select a download location on the server where the Ops Center Automator Common Component truststore resides and confirm the download.
2. On the server with the Common Component truststore, go to the location in which you downloaded the zip file and unzip the file.



Note: If the downloaded file does not have a .zip extension, change the extension to .zip.

- In Windows, the result is a **.certs** folder that contains both certificate files.
 - In Linux, the includes a directory named **lin** that contains a file with a .0 extension (xxx.0).
3. Import the VMware vCenter Server root certificates into the Common Component truststore by running the following command:

For Windows:

```
Common-Component-installation-folder\bin\hcnds64keytool -import -alias
alias-name -keystore Common-Component-installation-folder\uCPSB11
\hjdk\jdk\lib\security\jssecacerts -storepass truststore-password -file
certificate-file -storetype JKS
```

For Linux:

```
Common-Component-installation-directory/uCPSB11/jdk/bin/keytool -import -alias
alias-name -keystore Common-Component-installation-directory/uCPSB11/
hjdk/jdk/lib/security/jssecacerts -storepass truststore-password -file
certificate-file -storetype JKS
```

To import the certificates in Java, ensure that the truststore password includes six or more characters. In addition, ensure that the new alias name does not conflict with an existing alias name.

4. Install the certificates into the OS truststore.

In Windows:

- a. Right-click the file with the `.crt` extension and select **Install Certificate**. The Import Certificate Wizard opens.
- b. Select **Local Machine**, then click **Next**.
- c. Select **Place all certificates in the following store**.
- d. Click **Browse**, select **Trusted Root Certification Authorities**, then click **Finish**.
- e. Repeat steps a through d on the file with the `.cer` extension.

In Linux:

- a. Copy the "xxx.0" file to the following directory:
`/etc/pki/tls/certs`

5. Restart the services by running the `hcnds64srv` command.



Note: If you plan to use the ESX cluster service templates, you must also install Python as described in the *Hitachi Ops Center Automator User Guide*.

Importing certificates for secure communication with external web servers

You must import the certificates into the Common Component truststore to enable SSL communication between the external web server and Ops Center Automator.

- BNA
- Brocade FC switch
- DCNM
- ServiceNow
- Other web service connections

In Windows OS, use the `hcnds64keytool` command. For Linux OS, use the standard `keytool`. To import the certificate in Java, ensure that the truststore password includes six or more characters. In addition, ensure that the new alias name does not conflict with an existing alias name.

For Windows OS:

```
Common-Component-installation-folder\bin\hcmds64keytool -import -alias alias-name -
keystore Common-Component-installation-folder\uCPSB11
\hjdk\jdk\lib\security\jssecacerts -storepass truststore-password -file certificate-
file -storetype JKS
```

Restart the services by running the **hcmds64srv** command.

For Linux OS:

```
Common-Component-installation-directory/uCPSB11/jdk/bin/keytool -import -alias alias-
name -keystore Common-Component-installation-directory/uCPSB11/hjdk/jdk/lib/security/
jssecacerts -storepass truststore-password -file certificate-file -storetype JKS
```

Restart the services by running the **hcmds64srv** command.

Additional guidelines

- For additional information on the security settings for another product, see the associated product documentation.
- To obtain server certificates, see the associated product documentation for information on accessing server certificates.
- After upgrading DCNM, the server certificate is initialized. You must do the steps described in "Restoring the certificates after an upgrade" in the *Cisco DCNM Installation and Upgrade Guide for SAN Deployment*.
- If you use DCNM 11.5, create a certificate by specifying an appropriate hostname to Common Name by following the steps described in "Certificates" in the *Cisco DCNM Installation and Upgrade Guide for SAN Deployment*.
- If you use a Brocade FC switch, complete the SSL settings by following the steps described in "Managing the Security Certificates Using the secCertMgmt Command" in the *Brocade Fabric OS Administration Guide*.

Verifying the server certificate expiration date

You can verify the expiration date for an SSL certificate to ensure that your certificate has not expired. You must ensure that the management server certificate does not expire to maintain secure communication with managed servers.

To verify the expiration of the Common Component server certificate, run the following command:

For Windows OS:

```
Common-Component-installation-folder\bin\hcmds64keytool -printcert -
v -file certificate-file
```

For Linux OS:

```
Common-Component-installation-directory/uCPSB11/jdk/bin/keytool -
printcert -v -file certificate-file
```



Note: The expiration date of a self-signed server certificate is not verified at the connection between servers. If you must verify the expiration date of a certificate at the connection of the Ops Center Automator server and web servers, use the certificate issued by the certificate authority. Then, import the certificates not only for the server, but also for the certificate authority, and intermediate certificate authority.

Deleting Common Component truststore certificates

To delete the certificates imported into the Common Component truststore (ldapcacerts or jssecacerts), use the **hcnds64keytool** utility (for Windows) or the **keytool** utility (for Linux).

Before you begin

Check the following information:

- Alias name of the certificate to be deleted
- Truststore file path
- Truststore password

Procedure

1. Run the following command.

In Windows

```
Common-component-installation-folder\bin\hcnds64keytool -delete -alias alias-name -keystore truststore-file-name -storepass truststore-password
```

In Linux

```
Common-component-installation-directory/uCPSB11/jdk/bin/keytool -delete -alias alias-name -keystore truststore-file-name -storepass truststore-password
```

where:

alias

Specify the certificate alias name.

keystore

Specify the truststore file path where the certificate is stored.

storepass

Specify the truststore password.

Audit logging

The audit log provides a record of all user actions on the Ops Center Automator server. The audit log tracks events from several categories such as external services, authentication, configuration access, and start and stop services. By examining the audit log, you can check the system usage status or audit for unauthorized access.

Configuring the audit log

The audit log provides a record of all user actions on the Ops Center Automator server. The audit log tracks events from several categories such as external services, authentication, configuration access, and start and stop services. By examining the audit log, you can check the system usage status or audit for unauthorized access.

For Windows, the audit log data is output to the event log files (application log files). For Linux, the data is output to the `syslog` file.

The following table lists and describes the categories of audit log data that can be generated from products that use the Common Component. Different products generate different types of audit log data.

Categories	Description
StartStop	Events indicating starting or stopping of hardware or software: <ul style="list-style-type: none"> Starting or shutting down an OS Starting or stopping a hardware component (including micro components) Starting or stopping software on a storage system or SVP, and products that use the Common component
Failure	Events indicating hardware or software failures: <ul style="list-style-type: none"> Hardware failures Software failures (memory error, etc.)
LinkStatus	Events indicating link status among devices: Whether a link is up or down
ExternalService	Events indicating the results of communication with external services: <ul style="list-style-type: none"> Communication with an external server, such as NTP or DNS Communication with a management server (SNMP)

Categories	Description
Authentication	<p>Events indicating that a device, administrator, or end user succeeded or failed in connection or authentication:</p> <ul style="list-style-type: none"> ▪ Fibre Channel login ▪ Device authentication (Fibre Channel - Security Protocol authentication, iSCSI login authentication, SSL server/client authentication) ▪ Administrator or end user authentication
AccessControl	<p>Events indicating that a device, administrator, or end user succeeded or failed in gaining access to resources:</p> <ul style="list-style-type: none"> ▪ Access control for devices ▪ Access control for the administrator or end users
ContentAccess	<p>Events indicating that attempts to access important data succeeded or failed:</p> <ul style="list-style-type: none"> ▪ Access to important files on NAS or to contents when HTTP is supported ▪ Access to audit log files
ConfigurationAccess	<p>Events indicating that the administrator succeeded or failed in performing an allowed operation:</p> <ul style="list-style-type: none"> ▪ Reference or update of the configuration information ▪ Update of account settings including addition or deletion of accounts ▪ Security configuration ▪ Reference or update of audit log settings
Maintenance	<p>Events indicating that a performed maintenance operation succeeded or failed:</p> <ul style="list-style-type: none"> ▪ Addition or deletion of hardware components ▪ Addition or deletion of software components
AnomalyEvent	<p>Events indicating that an anomaly, such as a threshold being exceeded, occurred:</p> <ul style="list-style-type: none"> ▪ A network traffic threshold was exceeded ▪ A CPU load threshold was exceeded ▪ Pre-notification that a limit is being reached or a wraparound occurred for audit log data temporarily saved internally

Categories	Description
	<p>Events indicating that abnormal communication occurred:</p> <ul style="list-style-type: none"> ▪ SYN flood attacks to a regularly used port, or protocol violations ▪ Access to an unused port (port scanning, etc.)

Enabling audit logging

To enable the audit log of the Ops Center Automator server and change the audit events to be output to the audit log, first configure the environment configuration file (`auditlog.conf`) for the Common component. Then you must restart the Ops Center Automator server.



Note:

- If the Ops Center Automator server is installed by using a virtual appliance, the audit log is enabled by default.
If the Ops Center Automator server is installed by using the installer, the audit log is disabled by default. Enable the settings as required.
- A large volume of audit log data might be output. Change the log file size and back up or archive the generated log files accordingly.

Procedure

1. Log on to Ops Center Automator as a user with Administrator permission (Windows) or root permission (Linux).
2. Open the `auditlog.conf` file, which is located in one of the following locations:

In Windows:

```
Common-component-installation-destination-folder\conf\sec
\auditlog.conf
```

In Linux:

```
Common-component-installation-destination-directory/conf/sec/
auditlog.conf
```



Note: The `auditlog.conf` file is an environment configuration file for the Common component. Therefore, if another product that uses the Common component is installed on the same host as the Ops Center Automator server, the audit log settings will be shared among both products.

3. To enable audit logging, specify the audit event categories for the `Log.Event.Category` property in the `auditlog.conf` file.
4. To disable audit logging, delete all audit even categories specified for the `Log.Event.Category` property in the `auditlog.conf` file.
5. Restart the Ops Center Automator services.

Settings in the auditlog.conf file

You can set the following values in the `auditlog.conf` file.

Log.Facility (Linux only)

Specify a numeric value for the facility (the log type) required to output audit log data to the `syslog` file in Linux. (Default value: 1)

`Log.Facility` is ignored in Windows, even if it is specified. If an invalid value or a non-numeric character is specified, the default value is used.

The following table shows the correspondence between the specifiable values for `Log.Facility` and the facility defined in the `syslog.conf` file.

Specifiable value for <code>Log.Facility</code>	Facility defined in the <code>syslog.conf</code> file
1	user
2	mail*
3	daemon
4	auth*
6	lpr*
16	local0
17	local1
18	local2
19	local3
20	local4
21	local5
22	local6
23	local7
*: Although you can specify this value, we do not recommend that you specify it.	

To filter audit logs output to the `syslog` file, you can combine the facility specified for `Log.Facility` and the severity specified for each audit event.

The following table shows the correspondence between the severity of audit events and the severity defined in the `syslog.conf` file.

Severity of audit events	Severity defined in the <code>syslog.conf</code> file
0	emerg
1	alert
2	crit
3	err
4	warning
5	notice
6	info
7	debug

Log.Event.Category

Specify the audit event categories to be output. (Default value: none)

When specifying multiple categories, use commas (,) to separate them. In this case, do not insert spaces between categories and commas. If `Log.Event.Category` is not specified, audit log data is not output. `Log.Event.Category` is not case-sensitive. If an invalid category name is specified, the specified file name is ignored.

Valid categories: `StartStop`, `Failure`, `LinkStatus`, `ExternalService`, `Authentication`, `AccessControl`, `ContentAccess`, `ConfigurationAccess`, `Maintenance`, or `AnomalyEvent`

Log.Level (Effective in Windows only)

Specify the severity level of audit events to be output. (Default value: 6)

Events with the specified severity level or lower will be output to the event log file.

For details about the severity of each audit event, see the list of audit events output to the audit log.

`Log.Level` has an effect in Windows only. `Log.Level` is ignored in Linux, even if it is specified. Also, if an invalid value or a non-numeric character is specified, the default value is used.

The following table shows the correspondence between the specifiable value for `Log.Level` and the levels displayed in the event log.

Specifiable value for <code>Log.Level</code>	Levels displayed in the event log
0	Error
1	

Specifiable value for Log.Level	Levels displayed in the event log
2	
3	
4	Warning
5	Information
6	
7	

Sample auditlog.conf file

The following shows an example of the `auditlog.conf` file:

```
# Specify an integer for Facility. (specifiable range: 1-23)
Log.Facility 1

# Specify the event category.
# You can specify any of the following:
# StartStop, Failure, LinkStatus, ExternalService,
# Authentication, AccessControl, ContentAccess,
# ConfigurationAccess, Maintenance, or AnomalyEvent.
Log.Event.Category StartStop,Failure,LinkStatus,ExternalService,Authentication,
AccessControl,ContentAccess,ConfigurationAccess,Maintenance,AnomalyEvent
# Specify an integer for Severity. (specifiable range: 0-7)
Log.Level 6
```

In the example above, all types of audit events are output.

For Windows, `Log.Level 6` outputs audit log data corresponding to the Error, Warning, and Information levels. For Linux, `Log.Facility 1` outputs the audit log data to the `syslog` file that is defined as the user facility in the `syslog.conf` file.

Format of data output to the audit log

The audit log data is output to the event log file in Windows or to the `syslog` file in Linux.

The following shows the format of data output to the audit log:

In Windows:

```
program-name [process-ID]: message-part
```

In Linux:

```
syslog-header-message message-part
```

The format of the *syslog-header-message* differs depending on the OS environment settings. If necessary, change the settings.

For example, if you use rsyslog and specify the following in `/etc/rsyslog.conf`, messages are output in a format corresponding to RFC5424:

```
$ActionFileDefaultTemplate RSYSLOG_SyslogProtocol23Format
```

The format and contents of *message-part* are described below. In *message-part*, a maximum of 953 single-byte characters can be displayed in a *syslog* file.

```
uniform-identifier, unified-specification-revision-number, serial-number, message-ID,
date-and-time, detected-entity, detected-location, audit-event-type, audit-event-result,
audit-event-result-subject-identification-information, hardware-identification-
information, location-information, location-identification-information, redundancy-
identification-information, agent-information, request-source-host, request-source-port-
number, request-destination-host, request-destination-port-number, batch-operation-
identifier, log-data-type-information, application-identification-information, reserved-
area, message-text
```

Item*	Description
<i>uniform-identifier</i>	Fixed to CELFSS.
<i>unified-specification-revision-number</i>	Fixed to 1.1.
<i>serial-number</i>	Serial number of audit log messages.
<i>message-ID</i>	Message ID.
<i>date-and-time</i>	The date and time when the message was output. This item is output in the format of <i>yyyy-mm-ddThh:mm:ss.stime-zone</i> .
<i>detected-entity</i>	Component or process name.
<i>detected-location</i>	Host name.
<i>audit-event-type</i>	Event type.
<i>audit-event-result</i>	Event result.
<i>audit-event-result-subject-identification-information</i>	Account ID, process ID, or IP address corresponding to the event.

Item*	Description
<i>hardware-identification-information</i>	Hardware model or serial number.
<i>location-information</i>	Identification information for the hardware component.
<i>location-identification-information</i>	Location identification information.
<i>FQDN</i>	Fully qualified domain name.
<i>redundancy-identification-information</i>	Redundancy identification information.
<i>agent-information</i>	Agent information.
<i>request-source-host</i>	Host name of the request sender.
<i>request-source-port-number</i>	Port number of the request sender.
<i>request-destination-host</i>	Host name of the request destination.
<i>request-destination-port-number</i>	Port number of the request destination.
<i>batch-operation-identifier</i>	Serial number of operations through the program.
<i>log-data-type-information</i>	Fixed to BasicLog or DetailLog.
<i>application-identification-information</i>	Program identification information.
<i>reserved-area</i>	Not output. This is a reserved space.
<i>message-text</i>	The contents vary according to the audit events. Characters that cannot be displayed are output as asterisks (*).
*: Some items are not output for some audit events.	

The following is an example of the message portion of an audit log login event:

```
CELFSS,1.1,3,KNAE20002-I,2021-09-03T21:31:56.8+09:00,HAD,managementhost,
Authentication,Success,subj:uid=sysadmin,autoAuth>Login,BasicLog,HAD,"Login was
successful."
```

Changing the system configuration

You can configure various Ops Center Automator settings such as logs and tasks by editing the `config_user.properties` file. Note that after you change and save the file, you need to restart the Ops Center Automator engine web service.

You can change the following settings by editing this file:

- Log file configuration (specify the number of logs to store).
- Task and history configuration (specify the number of tasks and task histories to store).
- Configuration regarding remote command execution (SSH/telnet port number)
- Configuration information for email notification.
- Configuration information regarding Service Builder.
- Connection timeout value setting.
- Maximum number of concurrent plug-in runs.

The file is located in the following folder:

Automation-software-installation-folder\conf

The file uses the following format:

specification-key-name=setting

When editing the properties file, take note of the following:

- Lines that begin with # are treated as comments
- Blank lines are ignored
- The encoding is ISO 8859-1
- The contents are case sensitive
- To specify \ in a character string, it must be written \\.
- If value that is not valid is entered for a setting, it is set to the default value and message **KNAE02022-W** is sent to the integrated trace log and public log
- If the same specification key is entered multiple times in a file, the last one that is specified takes effect

Table 12 Settings in the `config_user.properties` file

Category	Key name	Setting	Values	Default values
HTTP connection port number	<code>server.http.port</code>	Specifies the port number to be used for HTTP communication between the Ops Center Automator server and the Common Component.	0-65535	22015

Category	Key name	Setting	Values	Default values
Logs ¹	logger.message.server.MaxBackupIndex	Specifies the maximum number of log backup files for a server.	1 - 16	7
	logger.message.server.MaxFileSize	Specifies the maximum log file size (in KB) for a server.	4 - 2097151	1024
	logger.message.command.MaxBackupIndex	Specifies the maximum number of log backup files for a command.	1 - 16	7
	logger.message.command.MaxFileSize	Specifies the maximum log file size (in KB) for a command.	4 - 2097151	1024
	logger.TA.MaxFileSize	Specifies the maximum log file size (in KB) for a task.	4 - 2097151	10240
Task management	tasklist.autoarchive.taskRemainingPeriod	Specifies the period (in days) for tasks that have ended to remain in the task list.	1 - 90	7
	tasklist.autoarchive.executeTime	Specifies the time to run the automatic archiving task.	00:00:00 - 23:59:59	04:00:00
	tasklist.autoarchive.maxTasks	Specifies the maximum number of tasks to keep in the task list.	100 - 5000	5000
	tasklist.autodelete.maxHistories	Specifies the maximum number of history entries to retain.	100 - 30000	30000
Repeats	foreach.max_value	Specifies the maximum number of concurrent tasks that can be run by the Repeated Execution Plug-in.	1 - 99	3
Remote connection port number	ssh.port.number	Specifies the SSH port number of the target device.	0 - 65535	22

Category	Key name	Setting	Values	Default values
	telnet.port .number	Specifies the Telnet port number of the target device	0 - 65535	23
General command Remote command File-transfer Terminal connection	plugin.stdoutSize.wmi	<p>If the total size of the standard output and the standard error exceeds the property value, a plug-in error occurs.</p> <p>Note: The property value unit is in kilobytes (KB).</p> <p>This property is applied during the plug-in procedure, when the following conditions are met.</p> <ul style="list-style-type: none"> - Connection target host is Windows - Execution target plug-in is either a General Command Plug-in or the Custom Plug-in <p>In Windows OS, the plug-in can continue to run, even if the number of linefeeds exceeds 65535 or more. To take advantage of this feature, you must to set the property value accordingly. For example, if this property is set to 100 KB (default value), the plug-in cannot process the maximum number of linefeeds of 65535 or more. The plug-in stops running after it reaches the 100 KB limit.</p>	1 - 1024	100

Category	Key name	Setting	Values	Default values
	plugin.stdoutSize.ssh	<p>If the total size of the standard output and the standard error exceeds the property value, a plug-in error occurs.</p> <p>Note: The property value unit is in kilobytes (KB).</p> <p>This property is applied during the plug-in procedure when the following two major conditions are met.</p> <p>[Condition (1) (Note: The following target-based conditions must be met).]</p> <ul style="list-style-type: none"> - Connection target host is Linux OS. - Execution target plug-in is a General Command Plug-in or the custom plug-in. <p>[Condition (2) (Note: The following protocol and plug-in conditions must be met.)]</p> <ul style="list-style-type: none"> - Connection protocol is SSH. - Execution target plug-in is Terminal Connect Plug-in or Terminal Command Plug-in. 	1 - 1024	100
	plugin.stdoutSize.telnet	<p>If the total size of the standard output and the standard error exceeds the property value, a plug-in error occurs.</p>	1 - 1024	100

Category	Key name	Setting	Values	Default values
		<p>Note: The property value unit is in kilobytes (KB).</p> <p>This property is applied during the plug-in procedure when the following conditions are met.</p> <ul style="list-style-type: none"> - Connection protocol is Telnet. - The target plug-in is either Terminal Connect Plug-in or Terminal Command Plug-in. 		
	<code>plugin.removeFileAccess.retry.times</code>	<p>Specifies the number of tries for a file manipulation command run internally by a content plug-in or file-transfer plug-in. The time between tries is fixed at 100 ms.</p> <p>If a temporary file access error occurs, trying the command again might result in a successful procedure. However, if the file access error is not recovered, extra time is needed for further tries until the plug-in stops. Specify this property in an environment in which file access errors occur even if there are no problems with disks.</p>	0 - 100	0
	<code>ssh.privateKeyFile</code>	Specifies the absolute path of the private key file if public key authentication is used for SSH connections.	0 - 255 characters	"" (null character)

Category	Key name	Setting	Values	Default values
	<code>plugin.localMode</code>	Specifies whether to enable or disable local execution mode. true: enabled false: disabled	true/false	true
Terminal connection	<code>plugin.terminal.prompt.account</code>	Specifies the regular expression used to detect the user ID waiting state (1-1,024 characters). If the standard output and standard error output match the specified regular expression, the Terminal Connect Plug-in (Telnet is specified for the protocol) determines that a user ID must be entered, and then it enters a user ID.	Character string that can be used in regular expression patterns	logon Logon Name Username UserName
	<code>plugin.terminal.prompt.password</code>	Specifies the regular expression used to detect the password waiting state (1-1,024 characters). If the standard output and standard error output match the specified regular expression, the Terminal Connect Plug-in (Telnet is specified for the protocol) determines that a password must be entered, and then it enters a password.	Character string that can be used in regular expression patterns	password Password PassWord

Category	Key name	Setting	Values	Default values
	telnet.connect.wait	Specifies the waiting time (in seconds) until the standard output is returned after an Telnet connection is established with the target device.	1 - 600	60
Remote command	plugin.remoteCommand.executionDirectory.wmi	Specifies the path of the execution folder that contains the custom plug-in to run if the target host is running Windows. The execution folder must be created in advance. If the "Execution Mode" of the custom plug-in is "Script", the total string length of the specified value and the script file name do not exceed 140 characters. If the length exceeds 140 characters, transferring the script might fail. In addition, because the script file name must be specified in 90 characters or less, this value specified must be within 50 characters.	Character string of 0-128 characters	"" (null character)
	plugin.remoteCommand.executionDirectory.ssh	Specifies the path of the execution folder to run the custom plug-in if the OS of the target host is Linux OS. The execution folder must be created in advance.	Character string of 0-128 characters	"" (null character)

Category	Key name	Setting	Values	Default values
	plugin.remoteCommand.workDirectory.ssh	Specifies the working folder used when the file transfer plug-in or the custom plug-in is run if the OS of the target host is Linux OS. Enter a folder or a symbolic link as an absolute path (1 - 128 characters). In addition, the symbolic link can be included as the layer of the path.	1 - 128	/tmp/Hitachi_AO
Retry remote host connection	ssh.connect.retry.times	Specifies the number of tries in the event of a failed SSH connection to the target device.	0 - 100	3
	ssh.connect.retry.interval	Specifies the time (in seconds) between tries in the event of a failed SSH connection to the target device.	1 - 600	10
	wmi.connect.retry.times	Specifies the number of tries in the event of a failed WMI connection to the target device.	0 - 100	3
	wmi.connect.retry.interval	Specifies the time (in seconds) between tries in the event of a failed WMI connection to the target device.	1 - 600	10
	telnet.connect.retry.times	Specifies the number of tries in the event of a failed Telnet connection to the target device.	0 - 100	3
	telnet.connect.retry.interval	Specifies the time (in seconds) between tries in the event of a failed Telnet connection to the target device.	1 - 600	10

Category	Key name	Setting	Values	Default values
Retry email notification	mail.notify.retry.times	Specifies the number of tries in the event of a failure of the notification function to send an email.	0 - 100	3
	mail.notify.retry.interval	Specifies the time (in seconds) between tries in the event of a failure of the notification function to send an email.	1 - 600	10
	mail.plugin.retry.times	Specifies the number of tries, if a failure occurs, to send email in the Email Notification Plug-in.	0 - 100	3
	mail.plugin.retry.interval	Specifies the time (in seconds) between tries in the event of a failure of the Email Notification Plug-in to send an email.	1 - 600	10
Audit Log	logger.Audit.command.useLoginUserID	Specifies whether to output the Ops Center Automator logon user ID, in place of the user ID, to the subject identification information for the audit log when a command is run.	true/false	false
Window update	client.events.refreshinterval	Specifies the update time (in seconds) for events.	0 - 65535	5

Category	Key name	Setting	Values	Default values
Service Builder	client.editor.upload.maxfilesize	Specifies the maximum file size (in MB) that can be uploaded to the server from the terminal used for operating Ops Center Automator by using the Service Builder Edit window.	1 - 10	3
	client.editor.canvas.maxwidth	Specifies the maximum size (in px) of the width of Flow view.	3600 - 10000	3600
	client.editor.canvas.maxhigh	Specifies the maximum size (in px) of the height of Flow view.	2400 - 30000	2400
	server.editor.step.perTemplate.maxnum	Specifies the maximum number of steps per 1 service template.	320 - 40000	320
	server.editor.step.perLayer.maxnum	Specifies the maximum number of steps per 1 layer.	80 - 10000	80
	server.editor.publicProperty.perTemplate.maxnum	Specifies the maximum number of service properties per service template.	100 - 2000	1000
	server.editor.propertyGroup.perTemplate.maxnum	Specifies the maximum number of property groups per service template.	5 - 1000	500
Debugger	tasklist.debugger.auto delete.task RemainingPeriod	Specifies the maximum number of property groups per service template.	1 - 90	7

Category	Key name	Setting	Values	Default values
	client.debugger.tasklog.maxfilesize	Specifies the size of task logs (KB) visible in the Task Log tab.	4 - 10240	1024
	logger.debugger.TA.MaxFileSize	Specifies the maximum log file size (KB) for a debug task.	4 - 2097151	10240
LongRunningTask verify interval threshold	server.longRunning.check.interval	LongRunningTask verify the threshold between times (in minutes)	0 - 20160	2880
LongRunning Monitor interval	server.longRunning.monitor.interval	LongRunning monitor interval (in seconds)	1 - 3600	60
Web Client	plugin.http.connect.timeout	Specifies the timeout value (in seconds) when the HTTP/HTTPS connection is established. If 0 is specified, timeout does not occur.	0 - 3600	60
	plugin.http.read.timeout	Specifies the timeout value (in seconds) when reading the data after the HTTP/HTTPS connection is established. If 0 is specified, timeout does not occur.	0 - 86400	600

Category	Key name	Setting	Values	Default values
Plug-in run	plugin.threadPoolSize	Specify the maximum number of concurrent plug-in runs. When using only the built-in service templates, you can set this property value to 100. To also use a custom service template, make sure to evaluate the behavior after changing the default value and make sure that no problem occurs before you move to the production process.	1-100	10
SSO	sso.https.certification	Specifies whether to verify the certificates in SSL communication with Common Services.	true/false	false
¹ You set log output thresholds for tasks in Service Share Properties. Example logger.message.server.MaxBackupIndex = 7 logger.message.server.MaxFileSize = 1024 logger.message.command.MaxBackupIndex = 7 logger.message.command.MaxFileSize = 1024 logger.TA.MaxFileSize = 1024 tasklist.autoarchive.taskRemainingPeriod = 7 tasklist.autoarchive.executeTime = 04:00:00 tasklist.autoarchive.maxTasks = 5000 tasklist.autodelete.maxHistories = 30000 mail.notify.retry.times = 3 mail.notify.retry.interval = 10 mail.plugin.retry.times = 3 mail.plugin.retry.interval = 10 client.events.refreshinterval = 5				

Configuring the performance mode

Ops Center Automator has two modes of operation: Standard mode and High performance mode. High performance mode is suitable for multiple task runs and uses more resources than Standard mode.

To switch between Standard mode and High performance mode, use the **changemode** command. For details on how to use the **changemode** command, see “changemode command” in the *Hitachi Ops Center Automator User Guide*.



Note: When you run multiple Online migration with Configuration Manager tasks, you need to operate in high performance mode. For details, see “Online migration with Configuration Manager service templates” in the *Hitachi Ops Center Automator User Guide*.

Configuring email notifications

You configure email notification settings so that when a task fails (“Failed” status) or a task detects an error (“In Progress (with Error)” status), you receive email notification. You can configure the email address, title, and type of information you receive about the failure or problem.



Note: To ensure that email notifications are enabled for the system, you must configure the system parameters in the Administration tab. For more detailed information, see the *Hitachi Ops Center Automator User Guide*.

The email definition file, `mailDefinition`, is in XML format and is located in the following folder:

`Automation-software-installation-folder\conf`

The definition file uses the following format:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<mail xmlns="http://www.example.com/products/it/software/xml/automation/conf/
mailDefinition">
  <title>email-title</title>
  <body>email-body</body> </mail>
```

When editing the file, take note of the following:

- A read error occurs if the definition file for email notification is missing, or is not well-formed XML. In this case, the email is sent with the default title and body.
- If you specify tags outside of `<mail>`, `<title>`, and `<body>`, even if the tags are well-formed XML, the tags and their content are ignored.
- An empty string is specified if the value of a `<title>` or `<body>` tag is omitted.

- The <mail> tag cannot be omitted. If it is omitted, the format is not valid and a read error occurs.
- All entries are case sensitive.

To modify the settings, edit the email-title and email-body sections in the `mailDefinition` file.

Table 13 Email notification settings

Setting	XML element	Character string length	Default value
Title of email to use for email notifications	<title>	Character string of 0-9,999 bytes	[Ops Center Automator] \$TASK_NAME\$ has changed to \$TASK_STATUS\$
Body of email to use for email notifications	<body>	Character string of 0-9,999 bytes	Service Group Name:\$SERVICE_GROUP_NAME\$ Task Name: \$TASK_NAME\$ User Name: \$USER_NAME\$ Task Detail: \$TASK_DETAIL_URL\$

Table 14 XML entity references

Character you want in the email	Character string to enter
&	&
<	<
>	>
"	"
'	'

Table 15 Embedded characters for email notification

Embedded characters	Item	Remarks
\$SERVICE_GROUP_NAME\$	Service group name	Set to the character string representing the service group name.
\$TASK_NAME\$	Task name	Set the task name according to the format in the task properties.
\$TASK_ID\$	Task ID	
\$TASK_KIND\$	Task type	
\$SERVICE_NAME\$	Service name	
\$TASK_TAGS\$	Tag of the task	
\$TASK_STATUS\$	Task status	
\$EXECUTION_DATE\$	Date and time the process was run	
\$PLANNED_START_DATE\$	Planned date and time of start	
\$START_DATE\$	Actual date and time of start	
\$END_DATE\$	Date and time of end	
\$USER_NAME\$	User who runs the process	
\$SCHEDULE_PERIOD\$	Scheduled execution period	
\$SCHEDULE_TIME\$	Scheduled execution time	
\$SCHEDULE_TIME\$	Date execution was scheduled to start	
\$TASK_DETAIL_URL\$	URL of the Task Detail window	Set to a URL starting with http.

Changing the password policy

You configure various Ops Center Automator settings related to user password conditions and locks by editing the `security.conf` file. This enables you to customize your security settings to match your specific password policy.

The file is located in the following folder:

Common-Component-installation-folder\conf\sec

The file uses the following format:

specification-key-name=setting

When editing the file, you specify one specification key and setting per line. The following shows the default state of the security definition file:

```
# This is the minimum length of the password
# (minimum: 1 -256 characters)
password.min.length=4

# This is the minimum number of uppercase characters included in the
password
# (minimum: 0-256 characters, character type: A-Z)
password.min.uppercase=0

# This is the minimum number of lowercase characters included in the
password
# (minimum: 0-256 characters, character type: a-z)
password.min.lowercase=0

# This is the minimum number of numeric characters included in the
password
# (minimum: 0-256 characters, character type: 0-9)
password.min.numeric=0

# This is the minimum number of symbolic characters included in the
password
# (minimum: 0-256 characters, character type: ! # $ % & ' ( ) * +
- . = @ \ ^ _ |)
password.min.symbol=0

# This specifies whether the user ID can be used for the password
# (true = cannot use the user ID, false = can use the user ID)
password.check.userID=false

# This is the minimum number of login failures before an account is
locked
# (minimum: 0-10 times)
account.lock.num=0
```

Table 16 Settings in the security.conf file

Key name	Setting	Settable values	Default value
password.min.length	Specifies the minimum number of characters in a password.	1 - 256	4

Key name	Setting	Settable values	Default value
<code>password.min.uppercase</code>	Specifies the minimum number of uppercase letters that must be included in the password. If 0 is specified, there are no constraints on the number of uppercase letters.	0 - 256	0
<code>password.min.lowercase</code>	Specifies the minimum number of lowercase letters that must be included in the password. If 0 is specified, there are no constraints on the number of lowercase letters.	0 - 256	0
<code>password.min.numeric</code>	Specifies the minimum number of numeric characters that must be included in the password. If 0 is specified, there are no constraints on the number of numeric characters.	0 - 256	0
<code>password.min.symbol</code>	Specifies the minimum number of symbols that must be included in the password. If 0 is specified, there are no constraints on the number of symbols.	0 - 256	0
<code>password.check.userID</code>	Specifies whether to prevent the password from being the same as the user ID.	<ul style="list-style-type: none"> true: prevent this false: allow this 	false

Key name	Setting	Settable values	Default value
<code>account.lock.num</code>	Specifies the number of consecutive failed logons before the account is automatically locked. If 0 is specified, the account is not automatically locked after failed logon tries.	0 - 10	0

About account locking

Account locking is the locking (temporary disabling) of a user account. By enabling account locking, you can reduce the risk of unauthorized access from third parties. If you are managing user accounts by using a management server, we recommend that you enable account locking.

In Common Component products, you can automatically lock user accounts that fail to log on to the GUI many times in a row. To enable account locking, you need to set the account locking policy (the number of consecutive, unsuccessful login attempts before accounts are locked).



Tip: As a way to lock an account, you can change the lock status of a user account from the GUI.

Only users with the `Admin` (user management) permission can change the lock status.



Caution:

- Account locking cannot be performed on `System` accounts when initially installing Common Component products. `System` accounts are set with `Admin` permissions for all Common Component products. If you want to set account locking for `System` accounts to improve security, you need to change the settings.
- If an external authentication server is used to authenticate users, the settings on the external authentication server are used to control automatic locking.

About account locking policies

An account locking policy is the number of consecutive, unsuccessful login attempts before automatically locking (temporarily disabling) user accounts that fail to log in to the GUI many times in a row.

When you set an account locking policy, it is immediately applied to all Common Component products that use Single Sign-On functionality. For example, if you set the number of consecutive failed login attempts to 3 and a user fails to log in to Ops Center Automator three times, the user account is automatically locked.

Setting account locking policies

You can set an account locking policy for Common Component products in the `security.conf` file.

Procedure

1. Edit the `security.conf` file.

The `security.conf` file is stored in the following locations:

In Windows:

Common-Component-installation-folder\conf\sec\security.conf

In Linux:

Common-Component-installation-directory/conf/sec/security.conf

2. Set the `account.lock.num` parameter.

Specify the number of consecutive failed login attempts required to trigger automatic account locking. Specify a value from 0 to 10. If a user makes the specified number of unsuccessful login attempts, the account will be locked. If you specify 0, any number of unsuccessful login attempts is allowed.

Default: 0



Caution:

- If you change the number of consecutive failed login attempts, the new value takes effect from the first failed login after the change. If a user is currently logged in and you attempt to login using his or her account, but you fail the specified number of times, his or her user account will be locked. However, the user can continue to perform operations while still logged in.
- You can also set an account locking policy from the GUI. However, if the system is in a cluster configuration, the settings from the GUI are applied only to the executing node. To apply the settings to the standby node, switch the nodes, and then specify the same settings.

Result

If you change the setting values in the `security.conf` file, the new account locking policy takes effect immediately.

Automatically locking the System account

To automatically lock the `System` accounts, change the settings in the `user.conf` file.

Procedure

1. Stop the Common Component product services.
2. Open the `user.conf` file.

The `user.conf` file is stored in the following locations:

- In Windows:

Common-Component-installation-folder\conf\user.conf

- In Linux:

Common-Component-installation-directory/conf/user.conf

If the `user.conf` file does not exist, create it.

3. Use the following format to specify the `account.lock.system` property:

```
account.lock.system=true
```

4. Start the Common Component product services.

Result

Account locking is applied to `System` accounts for all Ops Center products.

Unlocking accounts

Locked user accounts can be unlocked by using the `hcnds64unlockaccount`.

Before you begin

- Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

- Confirm that the locked user account has `Admin` permissions

If the user account does not have `Admin` permissions, another user whose account has User Management Admin permissions must unlock the account.

- Check the user ID and password of the locked user account.

Procedure

1. Use the `hcnds64unlockaccount` command to unlock the account.

In Windows:

```
Common-Component-installation-folder\bin
\hcnds64unlockaccount [/user user-ID /pass password]
```

In Linux:

```
Common-Component-installation-directory/bin/
hcnds64unlockaccount [-user user-ID -pass password]
```

If the command is executed without specifying the `user` option or the `pass` option, you will be prompted to enter a user ID and password.



Caution: If any symbols are used in the user ID or password, you need to escape these symbols on the command line.

- In Windows:

If the user ID or password ends with a backslash (\), use another backslash (\) to escape that backslash (\).

Also, if the user ID or password includes an ampersand (&), vertical bar (|), or caret (^), enclose each character with a double quotation mark ("), or use a caret (^) to escape the symbols.

- In Linux:

Use a backslash (\) to escape each character.

Operating systems supporting remote connections

The following OS or versions are supported as a target of remote connections. If the OS of the target is Windows, SMB and RPC are used to connect to the target. Otherwise, SSH is used to connect to the target. When using Terminal Connect Plug-in to connect to the target, Telnet or SSH is used. SSH protocol version 2 is supported.



Note: If the OS of the connection target is Windows, communication between Ops Center Automator and the connection target can be encrypted by configuring the SMB encryption. However, when the Ops Center Automator server is running Linux, SMB encryption cannot be used, and must be disabled. When you test the connection to a Windows connection target in the Add/Edit Agentless Remote Connection window of Ops Center Automator in Linux, if SMB encryption is enabled in the connection target, the KNAE02137-E message appears.



Note: If the OS of the Ops Center Automator server is Windows, then SMB v1, v2, or v3 is used, and if it is Linux, SMB v1 or v2 is used.

- Windows
 - Windows Server 2012 Standard (x64)
 - Windows Server 2012 Datacenter (x64)
 - Windows Server 2012 R2 Standard (x64)
 - Windows Server 2012 R2 Datacenter (x64)
 - Windows Server 2016 Standard (x64)
 - Windows Server 2016 Datacenter (x64)
 - Windows Server 2019 Standard (x64)
 - Windows Server 2019 Datacenter (x64)
 - Windows Server 2022 Standard (x64)
 - Windows Server 2022 Datacenter (x64)
- Linux
 - Red Hat Enterprise Linux 7.1 - 7.9, 8.1, 8.2, 8.4 (x64)
 - Oracle Linux 7.2 - 7.9, 8.1, 8.2, 8.4 (x64)

The commands (other than the commands specified in the OS of the operation-target device) run by custom plug-ins, General Command Plug-in, and File-Transfer Plug-in when the OS is Linux are shown below. Before you use these plug-ins, make sure that these commands have already been installed.

- Custom plug-in
 - `/bin/bash, /usr/bin/id, /bin/echo, /usr/bin/find, /usr/bin/test, /bin/mkdir, /bin/chmod, /bin/gunzip, /bin/tar, /bin/rm, /bin/cp, /bin/uname, /bin/su`
- General Command Plug-in
 - `/bin/bash, /usr/bin/id, /bin/echo, /usr/bin/test, /bin/uname, /bin/su`
- File-Transfer Plug-in (Send: If the value of the plug-in property `transferMode` is "send")
 - `/bin/bash, /usr/bin/id, /usr/bin/test, /bin/mkdir, /bin/chmod, /bin/gunzip, /bin/tar, /bin/rm, /bin/cp, /bin/uname, /bin/su`
- File-Transfer Plug-in (Receive: If the value of the plug-in property `transferMode` is "receive")
 - `/bin/bash, /usr/bin/id, /usr/bin/test, /bin/mkdir, /bin/chmod, /usr/bin/zip, /bin/rm, /bin/uname, /bin/su`

The custom plug-in and File-Transfer Plug-in transfer files to the operation-target device using SCP. Make sure that the operation-target device has an environment in which files can be transferred using SCP. Note that if the operation-target device is Linux and a character string is output from `.bashrc` of the connecting user, SCP might become fail. Also, when connecting to the remote machine using SSH or telnet, do not include commands such as `stty`, `tty`, `tset`, and scripts that require an interactive environment in the login script of the connecting user. If so, change the login script or create a new user who uses the login script that does not run these commands.

Configuring remote machine connection information for plug-ins and services

Before Ops Center Automator plug-ins and services can communicate with remote machines on which the plug-ins run tasks and perform actions, you must configure remote machine connection information.

Before you begin, verify the following:

- All the files located in the following path are regarded as destination properties files.

```
Automation-software-installation-folder\Automation\conf\plugin
\destinations
```

- The file name uses the following format:

```
Host-name.properties, IPv4-address.properties, IPv6-
address.properties
```



Note: Because you cannot use the colon ":" within an IPv6 address within the file name, replace it with a dash (-); for example: change "2001::234:abcd" to "2001--234-abcd.properties".

You can view a sample file in the following location:

```
Automation-software-installation-folder\Automation\conf\plugin
\destinations\#sample.properties
```

When editing the properties file, take note of the following:

- Lines that begin with # are treated as comments.
- Blank lines are ignored.
- Encoding is ISO 8859-1.
- Contents are case sensitive
- To specify a forward slash (/) in a character string, you must use a double forward slash (\\).
- If you specify an value in the destination properties file that is not valid, an execution error occurs in the plug-in that references the destination properties file.

- If you enter the same specification key multiple times in a file, the last one you specify takes effect.
- If you edited the destination properties file, the new definitions are applied when the plug-in that references the file is run.

Use the following configuration information to connect with the target machine.

Guidelines when the target machine is part of a cluster environment

When entering information for a cluster target machine:

- If the OS of the target machine is a Windows Server cluster environment, the working folders (`wmi.workDirectory.sharedName` and `wmi.workDirectory.sharedPath`) must be set. Otherwise, the plug-in causes a connection error.
- If you run the script with the Custom Plug-in, you must specify the execution folder (`common.executionDirectory`). Otherwise, the script is not forwarded.

Key name	Setting	Valid values	Smallest value	Largest value
terminal.charset	Specifies the character set used for communication.	EUC-JP eucjp ibm-943C ISO-8859-1 MS932 PCK Shift_JIS UTF-8 windows-31j	1	64
telnet.port	Specifies the port number used for a Telnet connection by using the Terminal Connect Plug-in. This setting has priority over the "telnet.port.number" setting in the properties file (<code>config_user.properties</code>).	0-65535	0	65535
ssh.port	Specifies the port number used for an SSH connection by	0-65535	0	65535

Key name	Setting	Valid values	Smallest value	Largest value
	<p>using one of the following plug-ins:</p> <ul style="list-style-type: none"> General Command Plug-in File-Transfer Plug-in Terminal Connect Plug-in Custom Plug-in <p>This setting has priority over the "ssh.port.number" setting in the properties file (config_user.properties).</p>			
telnet.prompt.account	<p>Specifies a regular expression pattern used to detect the character string that is output for prompting the user to enter a user ID to establish a connection with the target device by using the Terminal Connect Plug-in. You can use 1 to 1,024 characters. For example, specify Username:.</p>	Character string for use in regular expression patterns.	One character	1024 characters

Key name	Setting	Valid values	Smallest value	Largest value
telnet.prompt.password	Specifies a regular expression pattern used to detect the character string that is output for prompting the user to enter a password to establish a connection with the target device by using the Terminal Connect Plug-in. You can use 1 to 1,024 characters. For example, specify Password:.	Character string for use in regular expression patterns.	One character	1024 characters
telnet.noStdout.port.list	Specifies the port number of the service that does not return the standard output after a connection is established by using the Terminal Connect Plug-in. You can use 1 to 1,024 characters. To specify multiple port numbers, use a comma as a separator.	0-65535, and commas (,)	One character	1024 characters

Key name	Setting	Valid values	Smallest value	Largest value
wmi.workDirectory.sharedName	This is a property for Windows target machines. Specifies the shared folder name of the shared folder to which the file transmitted when running a command on the target . The folder must be the same as wmi.workDirectory.sharedPath. If using this property, the administrative shared setting of a target is unnecessary. Specify a character string of 0-80 characters.	Single-byte alphanumeric characters, "-", "_", and ".".	0 characters	80 characters
wmi.workDirectory.sharedPath	This is a property for Windows target machines. Specifies the absolute path of the shared folder to which the file transmitted when running a command on the target. If using the General Command Plug-in, the execution folder becomes "\Hitachi\CMALib\HAD\home" under the path listed for this property. The folder must be the same as wmi.workDirectory.sharedName. If using this property, the administrative shared setting of a target is unnecessary. Specify a character string of 0-80 characters.	Single-byte alphanumeric characters, ":", "\", "-", "_", and ".".	0 characters	80 characters

Key name	Setting	Valid values	Smallest value	Largest value
ssh.workDirectory	<p>This is a property for Linux OS target machines. Specifies the absolute path of the directory to which the file for a transmission is placed for the File-Transfer or the Custom Plug-in. Neither the path specified in this property nor the path of the parent directory can be specified as the destination and the receiver of File-Transfer Plug-in. For the working directory, the read, write, and execute privilege for the connected user are required. If the path specified in this property does not exist when the plug-in is used, it is created when the plug-in is run. If the directory cannot be created, the plug-in execution ends abnormally. You must ensure that the access permission for the new directory is 777. Priority is given over the value of "plugin.remoteComm and.workDirectory.ssh" defined in the <code>config_user.properties</code> file. Specify</p>	Single-byte alphanumeric characters, "/", "-", "_", and ".".	0 characters	128 characters

Key name	Setting	Valid values	Smallest value	Largest value
	a character string of 0-128 characters.			
common.executionDirectory	Specifies the execution folder at the time of running the Custom Plug-in on the target. If the value of the execution folder defined in the plug-in definition is not set, the value of this property is applied. Priority is given over the value of "plugin.remoteCommand.executionDirectory.wmi" and "plugin.remoteCommand.executionDirectory.ssh" defined in the config_user.properties file. Specify a character string of 0-128 characters.	Any characters	0 characters	128 characters

Windows OS prerequisites for agentless connections

The Windows prerequisites listed in the following sections are required for using agentless connections.

Supported users

You can use the following users in an agentless connection:

- Built-in administrator
- Built-in administrator of Active Directory
- A user belonging to an administrators group
- A user belonging to the Domain Admin group of Active Directory

When using a user that belongs to an administrator group, be aware that UAC (User Access Control) elevation does not apply at the time of command execution.

You also must edit the registry. Using a registry editor, set an entry under the key of the following registry.



Note: You are not required to restart the OS.

Item	Value
Registry key	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
Registry entry	LocalAccountTokenFilterPolicy
The value set as a registry entry	1 (DWORD)

Optionally, you can enter the following command at a command prompt:

```
reg add HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion
\Policies\System /v LocalAccountTokenFilterPolicy /t REG_DWORD /d
0x1 /f
```

Administrative share setting

Using an administrative share, set an entry under the key of the following registry using a registry editor and then restart the operating system.

Item	Value
Registry key	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Lanmanserver\parameters
Registry entry	AutoShareServer
The value set as a registry entry	1 (DWORD)

Enter the following command at a command prompt:

```
reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\Lanmanserver\parameters /v AutoShareServer /t REG_DWORD /d 1
```

SSH prerequisites for agentless connections

The SSH protocol prerequisites listed in the following sections are required for using agentless connections.

The SSH prerequisites are required for the following plug-ins:

- Custom Plug-in
- General Command Plug-in
- File-Transfer Plug-in
- Terminal Connect Plug-in
- Terminal Command Plug-in
- Terminal Disconnect Plug-in



Note: SSH must support version 2.

Password authentication

You must set up password authentication to an SSH server as follows:

1. Log on to a remote process target host as root.
2. Open the `/etc/ssh/sshd_config` file.
3. Set the value of `PubkeyAuthentication` to "yes". If the `PubkeyAuthentication` line is commented out, remove the comment out hash sign (#).
4. Run the following command and restart `sshd` service.

For RHEL/Oracle Linux OS (example - RHEL 8.4): `systemctl restart sshd`



Note: These commands can change with different versions of the OS. See the OS documentation for additional information.

Public key authentication

This module describes how to authenticate a public key that connects to an SSH server.

Setting up an SSH server

To use a public key authentication, it is necessary to set a public key authentication to a SSH server.

1. Log on to a remote target host as root.
2. Open the `/etc/ssh/sshd_config` file.
3. Set the value of `PubkeyAuthentication` to "yes". If the `PubkeyAuthentication` line is commented out, remove the comment out hash sign (#).
4. Run the following command and restart the `sshd` service.

For RHEL/Oracle Linux OS (example - RHEL 8.4): `systemctl restart sshd`



Note: These commands can change with different versions of the OS. See the OS documentation for additional information.

Creating a key (for the first time)

Create a public key and a secret key. Best practice is to create the keys on an OS where Ops Center Automator is installed.



Note: If you are moving a secret key to another OS, there is a possibility that a secret key will leak and pose a security risk, as a result. However, it is also possible to use the key created on another OS.

As a reference, the following procedure creates a key on RHEL 8.4 (Linux OS).

1. Run the **ssh-keygen** command.

If creating RSA key: `ssh-keygen -t rsa`

If creating DSA key: `ssh-keygen -t dsa`

2. Decide the location and name of a secret key.

Specify a path and filename that does not contain multibyte characters. As for a default, `~/.ssh/id_rsa` is set (if creating RSA key). A secret key is set as the filename specified to a selected path. A public key is set to the same directory as a secret key with the file extension ".pub" attached to the name of the secret key.

3. Enter a pass phrase.

You will be asked to enter the pass phrase and to press the return key. You will be then asked to enter the pass phrase again. If you choose not to set a pass phrase to a secret key, press only the return key to bypass the pass phrase.

Arrange a secret key to Ops Center Automator

Arrange a secret key on the OS where Ops Center Automator is installed. Arrange at arbitrary places and set a path to `ssh.privateKeyFile` of a properties file (`config_user.properties`).

Arranging a public key to a remote target host

1. Redirect the output of the **cat** command and add the contents of the generated public key file to the public key file (`authorized_keys`) used for an authentication. (Example: `cat id_rsa.pub >> authorized_keys`)
2. Run the **chmod** command and change the attribute of `authorized_keys` to 600 (give write and read privilege only to the owner). If the attribute is not 600, an authentication might fail at the time of plug-in execution.

The arrangement place of `authorized_keys` is directly under `~/.ssh` by default. With regard to `~/.ssh`, change the attribute to 700 (give write, read, and execute privilege only to the owner).

Configuring a shared property

1. Log on to the Ops Center Automator application.
2. Select [Administration] > [Shared Properties Settings].
3. Open the Pass phrase of the private key (for SSH public key authentication).

4. Enter the pass phrase as a value.

The value is the pass phrase of the private key (for SSH public key authentication).

Keyboard interactive authentication

To use keyboard interactive authentication, it is necessary to setup authentication to a SSH server.

1. Log on to a remote target host as root.
2. Open the `/etc/ssh/sshd_config` file.
3. Setup keyboard interactive authentication as follows:

For RHEL/Oracle Linux OS:

- Set yes to the value of `ChallengeResponseAuthentication`. (If the line of `ChallengeResponseAuthentication` is commented out, remove the comment out hash sign (#).)
 - Set yes to the value of `UsePAM`. (If the `UsePAM` line is commented out, remove the comment out hash sign (#).)
4. Run the following command and restart the `sshd` service. An example command for each supported OS is shown.

For RHEL/Oracle Linux OS (example - RHEL 8.4):

```
systemctl restart sshd
```



Note: These commands can change depending on the OS version. For details, see the applicable OS manual.

Setting the java heap memory size on the Ops Center API Configuration Manager server

When you run multiple Online Migration with Configuration Manager tasks, you must change the size of the Java heap used by the Ops Center API Configuration Manager server to 6,144 MB.

Before you begin

Log on to the Ops Center API Configuration Manager server as a user with Administrator permissions (in Windows).



Tip: You can check the value that is currently set by checking the value of the `rest.java.heapMemory.size` property in the `StartupV.properties` file, which is stored in the following location.

```
Configuration-Manager-installation-folder\data\properties  
\StartupV.properties
```

If the file does not exist or the file does not contain the `rest.java.heapMemory.size` property, this indicates that the default value is set.

Procedure

1. Run the following command:

```
Configuration-Manager-installation-folder\bin\setProperty.bat  
rest.java.heapMemory.size 6144
```

After the command is run, the Ops Center API Configuration Manager server restarts. If you specify `-noRestart` at the end of the command line, the command will run without restarting the server.

When you run the **setProperty** command, the value of the `rest.java.heapMemory.size` property in the `StartupV.properties` file will be changed to 6144. If the file does not exist, it will be created.

Each time the command is run, the current `StartupV.properties` file is backed up. The backup file is created in the same directory and the name of the backup file will include the date and time of creation (for example, `StartupV_20200220-093320.properties`).

Chapter 5: User management on an external authentication server

This module explains how to set up user authentication on the external authentication server.

About linking to an external authentication server



Note: To use external authentication servers with Common Services, see *Hitachi Ops Center Installation and Configuration Guide*.

If you are using external authentication servers with Common Services to login to this product, note that User IDs and passwords for external authentication servers must meet the following criteria:

- Number of characters: 1-255.
- Characters allowed: A-Z, a-z, 0-9 ! # \$ % & ' () * + - . = @ \ ^ _ | .

Ops Center Automator allows you to log in by using user accounts registered on an external authentication server. When you link to an external authentication server, you do not need to perform login password management and account control for Ops Center Automator. You can link Ops Center Automator to the following external authentication servers:

- LDAP directory server
- RADIUS server
- Kerberos server

About linking to an external authorization server

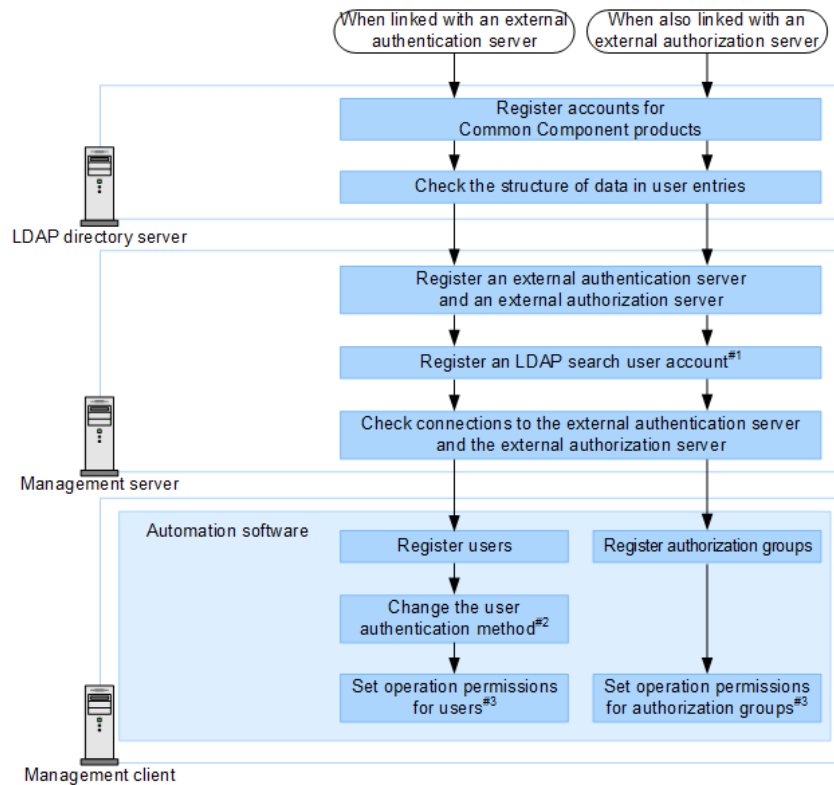
In addition to an external authentication server, if you also use an external authorization server to perform user authentication, access permissions for the management server (Common Component product) can be controlled on the external authorization server.

When an external authorization server is also linked to, you do not need to manage accounts and set permissions for individual users because Common Component products manage users by using the *authorization groups* on the external authorization server.

Common Component products can be linked to an LDAP directory server (Active Directory).

Workflow for user authentication on an LDAP directory server

To perform user authentication on an LDAP directory server, you need to register the external authentication server and the accounts to be authenticated on the management server for Common Component products.



#1: This step is not required if you want to link only to an external authentication server and the structure of the data of the user entries is a flat model.

#2: This step is required if you want to change the current user authentication method.

#3: Set permissions according to the user's job description.

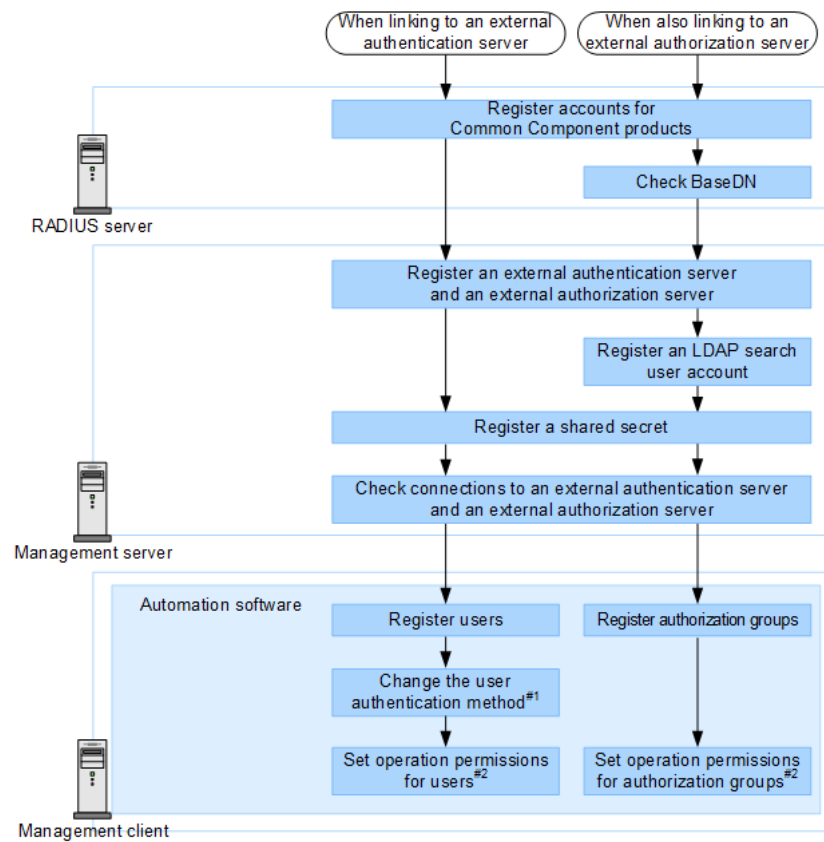
- User management
- Common Component products



Note: To use StartTLS to communicate between the LDAP directory server and the management server, you need to set up an environment specifically for this purpose to ensure secure communications.

Workflow for user authentication on a RADIUS server

To do user authentication on a RADIUS server, you need to register the external authentication server and the accounts to be authenticated on the management server for Common Component products.



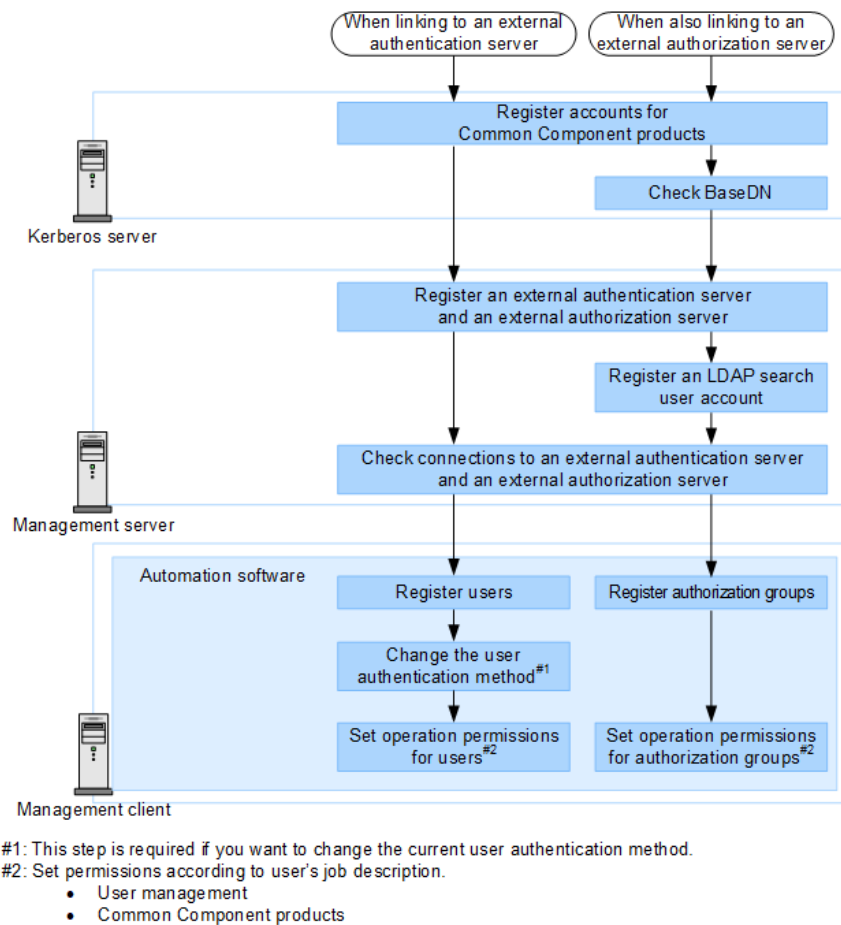
#1: This step is required if you want to change the current user authentication method.

#2: Set permissions according to the user's job description.

- User management
- Common Component products

Workflow for user authentication on a Kerberos server

To perform user authentication on a Kerberos server, you need to register the external authentication server and the accounts to be authenticated on the management server for Common Component products.



About the data structures of user entries

Two data structures of user entries for an LDAP directory server exist: the hierarchical structure model and the flat model.

When performing user authentication on an LDAP directory server, verify which data structure is being used, because information about the LDAP directory server registered on the management server and the procedures you need to perform on the management server depend on the data structure.

In addition, when performing user authentication or authorization on an LDAP directory server, also verify BaseDN, which is the start point for searching for users.

About the BaseDN

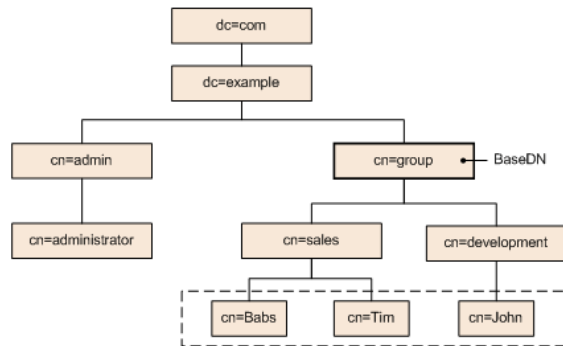
BaseDN is the starting point for searching for users during authentication or authorization.

Only user entries in the following hierarchies BaseDN are subject to authentication or authorization. In Common Component products, user entries must contain all of the users to be authenticated or authorized. BaseDN is required when registering information about the LDAP directory server on the management server.

About the hierarchical structure model

A data structure in which the following hierarchies BaseDN branch off and in which user entries are registered in another hierarchy.

If the hierarchical structure model is used, the entries in the following hierarchy BaseDN are searched for an entry that has the same login ID and user attribute value. The following figure shows an example of the hierarchical structure model.



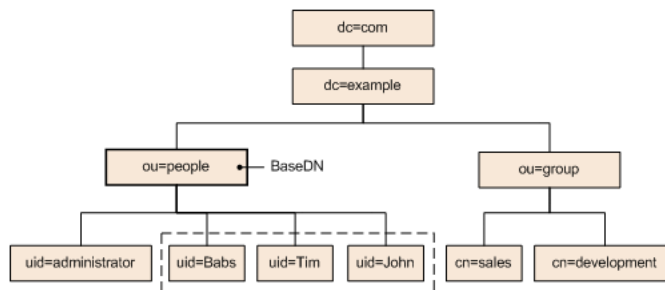
Legend: The user entities enclosed by the dotted line can be authenticated.

Figure 1 Example of the hierarchical structure model

About the flat model

A flat model is a data structure in which there are no branches in the hierarchy after BaseDN and in which user entries are registered in the hierarchy located just after BaseDN.

If the flat model is used, the entries in the hierarchy after BaseDN are searched for an entry that has the DN that consists of a combination of the login ID and BaseDN. If such a value is found, the user is authenticated. The following figure shows an example of the flat model.



Legend: The user entities enclosed by the dotted line can be authenticated.

Figure 2 Example of the flat model

Configurations when multiple external authentication servers are linked

When multiple external authentication servers are linked, user authentication is performed in a redundant configuration or a multi-domain configuration.

A redundant configuration is used when each external authentication server manages the same user information. If a failure occurs on one external authentication server, user authentication can be performed by using another external authentication server.

A multi-domain configuration is used to manage different user information for each external authentication server. If a user logs in with a user ID that includes a domain name, the user will be authenticated by an external authentication server in the domain whose name is included in the user ID. When a Kerberos server is used as an external authentication server, you can create a configuration similar to a multi-domain configuration by managing different user information for each realm.

The following table shows external authentication servers for which redundant configurations and multi-domain configurations are supported.

Table 17 Support status for redundant configurations and multi-domain configurations

External authentication server	Redundant configuration	Multi-domain configuration
LDAP directory server	Y ^{#1}	Y ^{#1}
RADIUS server	Y	N
Kerberos server	Y	Y ^{#2}

Legend:

Y: Supported

N: Not supported

#1

You can use either a redundant configuration or a multi-domain configuration.

#2

By managing different user information for each realm, you can create a configuration that is similar to a multi-domain configuration.

When an LDAP directory server is used for user authentication in a multi-domain configuration, the user authentication process varies depending on whether you log in by entering a user ID that includes a domain name.

If you log in with a user ID that includes a domain name, as in the following figure, user authentication will be performed by using the LDAP directory server of the specified domain.

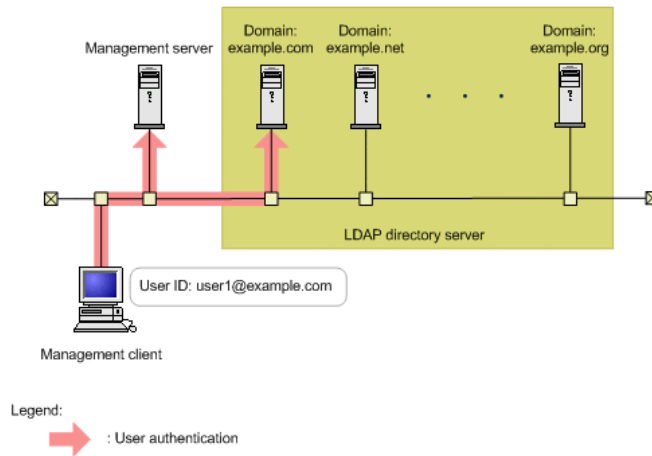


Figure 3 User authentication in a multi-domain configuration (when using a user ID that includes a domain name)

If you log in with a user ID that does not include a domain name, user authentication will be performed sequentially on all LDAP directory servers that are linked until the user is authorized, as shown in the following figure. If a large number of LDAP directory servers are linked, user authentication will take a long time. For this reason, you should log in with a user ID that includes a domain name.

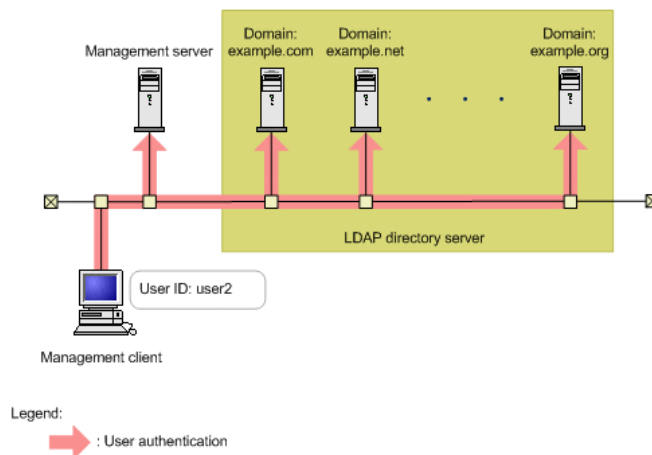


Figure 4 User authentication in a multi-domain configuration (when using a user ID that does not include a domain name)

Registering an external authentication server and an external authorization server

In the `exauth.properties` file, set the type of the external authentication server to be used, the server identification name, and the machine information about the external authentication server and external authorization server.

Before you begin

- Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).
- Copy the template of the `exauth.properties` file.

In Windows:

```
Common-Component-installation-folder\sample\conf  
\exauth.properties
```

In Linux:

```
Common-Component-installation-directory/sample/conf/  
exauth.properties
```

- Verify the data structure of user entries (for LDAP authentication).
- Set up the environment for the DNS server on the OS of the LDAP directory server.*
- Register information about the LDAP directory server to the SRV record of the DNS server.*

Verify the following information:

- Common information:
 - Type of the external authentication server
- For LDAP authentication:
 - Machine information about the external authentication server and the external authorization server (Host name or IP address, Port number)
 - BaseDN
 - Domain name for external authentication servers managed by the LDAP directory server (when linking to an external authorization server)
 - Domain name for multi-domain configurations managed by the LDAP directory server (for a multi-domain configuration)

- For RADIUS authentication
 - Machine information about the external authentication server and the external authorization server (Host name or IP address, Port number)
 - Authentication protocol
 - Host name or IP address of the management server
 - Domain name managed by the LDAP directory server (when linking to an external authorization server)
 - BaseDN (when linking to an external authorization server)
- For Kerberos authentication
 - Machine information about the external authentication server and the external authorization server (Host name or IP address, Port number)
 - Realm name
 - Domain name managed by the LDAP directory server (when linking to an external authorization server)
 - BaseDN (when linking to an external authorization server)

*: This process is required to look up the information about the LDAP directory server by using the DNS server.

Procedure

1. Specify required items in the `exauth.properties` file being copied.
2. Save the `exauth.properties` file in the following location:

In Windows:

`Common-Component-installation-folder\conf\exauth.properties`

In Linux:

`Common-Component-installation-directory/conf/
exauth.properties`

3. If the setting value of the `auth.ocsp.enable` or `auth.ocsp.responderURL` property is changed, the Common Component product services must be restarted.

If the setting value of any other property or attribute is changed, the change takes effect immediately.

Setup items in the `exauth.properties` file for LDAP authentication

In the `exauth.properties` file, set the type of the external authentication server to be used, the server identification name, and the machine information about the external authentication server.

- Common properties

See "Setup items in the `exauth.properties` file for LDAP authentication (common items)"

- Properties for an external authentication server and an external authorization server

Setup items in the `exauth.properties` file vary depending on whether information about the LDAP direx server being connected to is directly specified or looked up by using the DNS server.

- When directly specifying information about the LDAP direx server:

See "Setup items in the `exauth.properties` file for LDAP authentication (when directly specifying information about the external authentication server)" or "Setup items in the `exauth.properties` file for LDAP authentication (when an external authentication server and StartTLS are used for communication)"

- When using the DNS server to look up information about the LDAP direx server:

See "Setup items in the `exauth.properties` file for LDAP authentication (when using the DNS server to look up information about the external authentication server)"



Note:

- Make sure to distinguish between uppercase and lowercase letters for property settings.
- To use StartTLS for communication between the management server and the LDAP direx server, you need to directly specify information about the LDAP direx server to connect to in the `exauth.properties` file.
- If you use the DNS server to look up the LDAP direx server to connect to, it might take longer for users to log in.
- If the LDAP direx server to which you want to connect is in a multidomain configuration, you will not be able to look up the LDAP direx server by using the DNS server.

Table 18 Setup items in the `exauth.properties` file for LDAP authentication (common items)

Property	Details
<code>auth.server.type</code>	Specify an external authentication server type. Specify <code>ldap</code> . Default value: <code>internal</code> (used when not linking to an external authentication server)
<code>auth.server.name</code>	Specify the server identification names of LDAP direx servers. You can specify any name for this property to

Property	Details
	<p>identify which LDAP direx servers the settings such as the port number and the protocol for connecting to the LDAP direx server to which they are applied. (see "Setup items in the <code>exauth.properties</code> file for LDAP authentication (when directly specifying information about the external authentication server)" or "Setup items in the <code>exauth.properties</code> file for LDAP authentication (when using the DNS server to look up information about the external authentication server)").</p> <p><code>ServerName</code> has been set as the initial value. You must specify at least one name. To specify multiple server identification names, delimit the server identification names by using commas (.). Do not register the same server identification name more than once.</p> <p>Specifiable values: No more than 64 bytes of the following characters:</p> <p>A to Z</p> <p>a to z</p> <p>0 to 9</p> <p>! # () + - . = @ [] ^ _ { } ~</p> <p>Default value: none</p>
<code>auth.ldap.multi_domain</code>	<p>When specifying multiple server identification names for LDAP direx servers, specify, for each server, the configuration to be used.</p> <p>Specify <code>true</code> to use a multi-domain configuration.</p> <p>Specify <code>false</code> to use a redundant configuration.</p> <p>Default value: <code>false</code></p>
<code>auth.group.mapping</code>	<p>Specify whether to also link to an external authorization server.</p> <p>Specify <code>true</code> to link to an external authorization server.</p> <p>Specify <code>false</code> to not to link to an external authorization server.</p> <p>Default value: <code>false</code></p>

Table 19 Setup items in the `exauth.properties` file for LDAP authentication (when directly specifying information about the external authentication server)

Attributes	Details
<code>protocol</code>	<p>Specify the protocol for connecting to the LDAP direx server.</p> <p>This attribute is required.</p> <p>When communicating in plain text format, specify <code>ldap</code>. When using StartTLS communication, specify <code>tls</code>.</p> <p>Before specifying <code>tls</code>, make sure that one of the following encryption methods can be used on the LDAP direx server:</p> <ul style="list-style-type: none"> ▪ <code>TLS_RSA_WITH_AES_256_GCM_SHA384</code> ▪ <code>TLS_RSA_WITH_AES_256_CBC_SHA256</code> ▪ <code>TLS_RSA_WITH_AES_256_CBC_SHA</code> ▪ <code>TLS_RSA_WITH_AES_128_CBC_SHA256</code> ▪ <code>TLS_RSA_WITH_AES_128_CBC_SHA</code> ▪ <code>SSL_RSA_WITH_3DES_EDE_CBC_SHA</code> <p>You can specify <code>ldap</code> or <code>tls</code>.</p> <p>Default value: none</p> <p>When communicating by using StartTLS as the protocol for connecting to the LDAP direx server, you need to specify the security settings of Common Component.</p>
<code>host</code>	<p>Specify the host name or IP address of the LDAP direx server. If you specify the host name, make sure that the host name can be resolved to an IP address. If you specify the IP address, you can use either an IPv4 or IPv6 address. When specifying an IPv6 address, enclose it in square brackets (<code>[]</code>).</p> <p>This attribute is required.</p> <p>Default value: none</p> <p>When using StartTLS as the protocol for connecting to the LDAP direx server, in the <code>host</code> attribute specify the same host name as the value of CN in the LDAP direx server certificate. You cannot use an IP address.</p>
<code>port</code>	<p>Specify the port number of the LDAP direx server. Make sure that the port you specify is set as the listen port number on the LDAP direx server.</p> <p>Specifiable values: 1 to 65535</p> <p>Default value: 389</p>

Attributes	Details
<code>timeout</code>	<p>Specify the amount of time to wait before timing out when connecting to the LDAP direx server. If you specify 0, the system waits until a communication error occurs without timing out.</p> <p>Specifiable values: 0 to 120 (seconds)</p> <p>Default value: 15</p>
<code>attr</code>	<p>Specify the attribute (Attribute Type) to use as the user ID during authentication.</p> <ul style="list-style-type: none"> For the hierarchical structure model <p>Specify the name of the attribute containing the unique value to be used for identifying the user. The value stored in this attribute will be used as the user ID for Common Component products.</p> <p>The specified attribute must not include characters that cannot be used in a user ID of the Common Component product.</p> <p>For example, if you are using Active Directory and you want to use the Windows logon ID for the user ID of a Common Component product, specify the attribute name <code>sAMAccountName</code> in which the Windows logon ID has been defined.</p> For the flat model <p>Specify the RDN attribute name of the user entry.</p> <p>For example, if the user's DN is <code>uid=John,ou=People,dc=example,dc=com</code>, specify the <code>uid</code> that is the attribute name of the <code>uid=John</code>.</p> <p><code>sAMAccountName</code> has been set as the initial value. This attribute is required.</p> <p>Default value: none</p>
<code>basedn</code>	<p>Specify the BaseDN, which is the DN of the entry that will be used as the start point when searching for LDAP user information on the LDAP direx server. The user entries that are located in the hierarchy after this DN will be verified during authentication. If characters that need to be escaped are included in the specified BaseDN, escape all of those characters correctly because the specified value will be passed to the LDAP direx server without change.</p> <ul style="list-style-type: none"> For the hierarchical structure model <p>Specify the DN of the hierarchy that includes all of the user entries to be searched.</p> For the flat model <p>Specify the DN of the hierarchy just before the user entries to be searched.</p>

Attributes	Details
	<p>This attribute is required. Specify the DN by following the rules defined in RFC4514. For example, if any of the following characters are included in a DN, you need to use a backslash (\) to escape each character.</p> <p>Spaces # + ; , < = > \</p> <p>Default value: none</p>
<code>retry.interval</code>	<p>Specify the interval (in seconds) a failed connection to the LDAP direx server and the next try.</p> <p>Specifiable values: 1 to 60 (seconds)</p> <p>Default value: 1</p>
<code>retry.time</code>	<p>Specify the number of times to try to connect to the LDAP direx server. If you specify 0, no further tries occur.</p> <p>Specifiable values: 0 to 50</p> <p>Default value: 20</p>
<code>domain.name</code>	<p>Specify the name of a domain for external authentication servers managed by the LDAP direx server. This item is required when an external authorization server is also linked to.</p> <p>Default value: none</p>
<code>domain</code>	<p>Specify the name of a domain for multi-domain configurations managed by the LDAP direx server.</p> <p>If you log in by using a user ID that includes the domain name specified in this attribute, the LDAP direx server that belongs to the specified domain will be used as the authentication server.</p> <p>When specifying a domain name for the server identification name of each LDAP direx server, do not specify the same domain name more than once. This value is not case sensitive.</p> <p>This item is required when a multi-domain configuration is used.</p> <p>Default value: none</p>
<code>dns_lookup</code>	<p>Specify <code>false</code>.</p> <p>Default value: <code>false</code></p>
<p>Note: To specify the attributes, use the following syntax:</p> <pre>auth.ldap.auth.server.name-property-value.attribute=value</pre>	

Table 20 Setup items in the `exauth.properties` file for LDAP authentication (when an external authentication server and StartTLS are used for communication)

Property	Details
<code>auth.ocsp.enable</code>	<p>Specify whether to verify the validity of an LDAP direx server's electronic signature certificate by using an OCSP responder when the LDAP direx server and StartTLS are used for communication.</p> <p>To verify the validity of certificates, specify <code>true</code>. To not verify the validity of certificates, specify <code>false</code>.</p> <p>Default value: <code>false</code></p>
<code>auth.ocsp.responderURL</code>	<p>Specify the URL of an OCSP responder to use an OCSP responder that is not the one written in the AIA field of the electronic signature certificate to verify the validity of the electronic signature certificate. If this value is omitted, the OCSP responder written in the AIA field is used.</p> <p>Default value: <code>none</code></p>

Table 21 Setup items in the `exauth.properties` file for LDAP authentication (when using the DNS server to look up information about the external authentication server)

Attributes	Details
<code>protocol</code>	<p>Specify the protocol for connecting to the LDAP direx server.</p> <p>This attribute is required.</p> <p>Specifiable values: <code>ldap</code></p> <p>Default value: <code>none</code></p>
<code>port</code>	<p>Specify the port number of the LDAP direx server. Make sure that the port you specify is set as the listen port number on the LDAP direx server.</p> <p>Specifiable values: 1 to 65535</p> <p>Default value: 389</p>
<code>timeout</code>	<p>Specify the amount of time to wait before timing out when connecting to the LDAP direx server. If you specify 0, the system waits until a communication error occurs without timing out.</p> <p>Specifiable values: 0 to 120 (seconds)</p> <p>Default value: 15</p>

Attributes	Details
attr	<p>Specify the attribute (Attribute Type) to use as the user ID during authentication.</p> <ul style="list-style-type: none"> For the hierarchical structure model <p>Specify the name of the attribute containing the unique value to be used for identifying the user. The value stored in this attribute will be used as the user ID for Common Component products.</p> <p>The specified attribute must not include characters that cannot be used in a user ID of the Common Component product.</p> <p>For example, if you are using Active Directory and you want to use the Windows logon ID for the user ID of a Common Component product, specify the attribute name <code>sAMAccountName</code> in which the Windows logon ID has been defined.</p> For the flat model <p>Specify the RDN attribute name of the user entry.</p> <p>For example, if the user's DN is <code>uid=John,ou=People,dc=example,dc=com</code>, specify the <code>uid</code> that is the attribute name of the <code>uid=John</code>.</p> <p><code>sAMAccountName</code> has been set as the initial value. This attribute is required.</p> <p>Default value: none</p>
basedn	<p>Specify the BaseDN, which is the DN of the entry that will be used as the start point when searching for LDAP user information on the LDAP direx server. The user entries that are located in the hierarchy after this DN will be verified during authentication. If characters that need to be escaped are included in the specified BaseDN, escape all of those characters correctly because the specified value will be passed to the LDAP direx server without change.</p> <ul style="list-style-type: none"> For the hierarchical structure model <p>Specify the DN of the hierarchy that includes all of the user entries to be searched.</p> For the flat model <p>Specify the DN of the hierarchy just before the user entries to be searched.</p> <p>This attribute is required. Specify the DN by following the rules defined in RFC4514. For example, if any of the following characters are included in a DN, you need to use a backslash (\) to escape each character.</p> <p>Spaces # + ; , < = > \</p>

Attributes	Details
	Default value: none
<code>retry.interval</code>	<p>Specify the interval (in seconds) between tries to connect to the LDAP direx server.</p> <p>Specifiable values: 1 to 60 (seconds)</p> <p>Default value: 1</p>
<code>retry.time</code>	<p>Specify the number of tries to connect to the LDAP direx server. If you specify 0, no further tries occur.</p> <p>Specifiable values: 0 to 50</p> <p>Default value: 20</p>
<code>domain.name</code>	<p>Specify the name of a domain for external authentication servers managed by the LDAP direx server.</p> <p>Default value: none</p>
<code>dns_lookup</code>	<p>Specify <code>true</code>.</p> <p>However, if the following attribute values are already set, the LDAP direx server will be connected to by using the userspecified values instead of by using the DNS server to look up the information.</p> <ul style="list-style-type: none"> <code>auth.ldap.auth.server.name-property-value.host</code> <code>auth.ldap.auth.server.name-property-value.port</code> <p>Default value: <code>false</code></p>
<p>Note: To specify the attributes, use the following syntax:</p> <pre>auth.ldap.auth.server.name-property-value.attribute=value</pre>	

Examples of setting the `exauth.properties` file for LDAP authentication

This section gives examples of how to set the `exauth.properties` file when using an LDAP directory server to perform authentication.

- When directly specifying information about an LDAP directory server (when linking to only an external authentication server)

```
auth.server.type=ldap
auth.server.name=ServerName
auth.group.mapping=false
auth.ocsp.enable=false
auth.ocsp.responderURL=
auth.ldap.ServerName.protocol=ldap
auth.ldap.ServerName.host=ldap.example.com
auth.ldap.ServerName.port=389
auth.ldap.ServerName.timeout=15
auth.ldap.ServerName.attr=sAMAccountName
auth.ldap.ServerName.basedn=dc=Example,dc=com
auth.ldap.ServerName.retry.interval=1
auth.ldap.ServerName.retry.times=20
auth.ldap.ServerName.dns_lookup=false
```

- When using the DNS server to look up an LDAP directory server (when linking to only an external authentication server)

```
auth.server.type=ldap
auth.server.name=ServerName
auth.group.mapping=false
auth.ldap.ServerName.protocol=ldap
auth.ldap.ServerName.timeout=15
auth.ldap.ServerName.attr=sAMAccountName
auth.ldap.ServerName.basedn=dc=Example,dc=com
auth.ldap.ServerName.retry.interval=1
auth.ldap.ServerName.retry.times=20
auth.ldap.ServerName.domain.name=EXAMPLE.COM
auth.ldap.ServerName.dns_lookup=true
```

- When directly specifying information about the LDAP directory server (when also linking to an authorization server)

```
auth.server.type=ldap
auth.server.name=ServerName
auth.group.mapping=true
auth.ocsp.enable=false
auth.ocsp.responderURL=
auth.ldap.ServerName.protocol=ldap
auth.ldap.ServerName.host=ldap.example.com
auth.ldap.ServerName.port=389
auth.ldap.ServerName.timeout=15
auth.ldap.ServerName.attr=sAMAccountName
auth.ldap.ServerName.basedn=dc=Example,dc=com
auth.ldap.ServerName.retry.interval=1
auth.ldap.ServerName.retry.times=20
auth.ldap.ServerName.domain.name=EXAMPLE.COM
auth.ldap.ServerName.dns_lookup=false
```

- When using the DNS server to look up the LDAP directory server (when also linking to an authorization server)

```
auth.server.type=ldap
auth.server.name=ServerName
auth.group.mapping=true
auth.ldap.ServerName.protocol=ldap
auth.ldap.ServerName.timeout=15
auth.ldap.ServerName.attr=sAMAccountName
auth.ldap.ServerName.basedn=dc=Example,dc=com
auth.ldap.ServerName.retry.interval=1
auth.ldap.ServerName.retry.times=20
auth.ldap.ServerName.domain.name=EXAMPLE.COM
auth.ldap.ServerName.dns_lookup=true
```

- When using a redundant configuration

```
auth.server.type=ldap
auth.server.name=ServerName1,ServerName2
auth.ldap.multi_domain=false
auth.group.mapping=false
auth.ldap.ServerName1.protocol=ldap
auth.ldap.ServerName1.host=ldap1.example.com
auth.ldap.ServerName1.port=389
auth.ldap.ServerName1.timeout=15
auth.ldap.ServerName1.attr=sAMAccountName
auth.ldap.ServerName1.basedn=dc=Example,dc=com
auth.ldap.ServerName1.retry.interval=1
auth.ldap.ServerName1.retry.times=20
auth.ldap.ServerName2.protocol=ldap
auth.ldap.ServerName2.host=ldap2.example.com
auth.ldap.ServerName2.port=389
auth.ldap.ServerName2.timeout=15
auth.ldap.ServerName2.attr=sAMAccountName
auth.ldap.ServerName2.basedn=dc=Example,dc=net
auth.ldap.ServerName2.retry.interval=1
auth.ldap.ServerName2.retry.times=20
```

- When using a multi-domain configuration

```
auth.server.type=ldap
auth.server.name=ServerName1,ServerName2
auth.ldap.multi_domain=true
auth.group.mapping=false
auth.ldap.ServerName1.protocol=ldap
auth.ldap.ServerName1.host=ldap1.example.com
auth.ldap.ServerName1.port=389
auth.ldap.ServerName1.timeout=15
auth.ldap.ServerName1.attr=sAMAccountName
auth.ldap.ServerName1.basedn=dc=Example,dc=com
auth.ldap.ServerName1.retry.interval=1
auth.ldap.ServerName1.retry.times=20
auth.ldap.ServerName1.domain=example.com
auth.ldap.ServerName2.protocol=ldap
auth.ldap.ServerName2.host=ldap2.example.com
auth.ldap.ServerName2.port=389
auth.ldap.ServerName2.timeout=15
auth.ldap.ServerName2.attr=sAMAccountName
auth.ldap.ServerName2.basedn=dc=Example,dc=net
auth.ldap.ServerName2.retry.interval=1
auth.ldap.ServerName2.retry.times=20
auth.ldap.ServerName2.domain=example.net
```

Setup items in the `exauth.properties` file for RADIUS authentication

In the `exauth.properties` file, set the type of the external authentication server to be used, the server identification name, and the machine information about the external authentication server.

- Common properties

See "Setup items in the `exauth.properties` file for RADIUS authentication (common items)"

- Properties for an external authentication server

Specify these property values for each RADIUS server.

See "Setup items in the `exauth.properties` file for RADIUS authentication (settings for the external authentication server)"

- Properties for an external authorization server

These properties need to be set when an external authorization server is also linked to. Specify information about the LDAP directory server for each domain.

Setup items in the `exauth.properties` file vary depending on whether information about the LDAP directory server being connected to is directly specified or looked up by using the DNS server.

- When directly specifying information about the LDAP directory server

See "Setup items in the `exauth.properties` file for RADIUS authentication (common settings for the external authorization server)", "Setup items in the `exauth.properties` file for RADIUS authentication (when directly specifying information about the external authorization server)", and "Setup items in the `exauth.properties` file for RADIUS authentication (when an external authorization server and Start TLS are used for communication)"

- When using the DNS server to look up the information about the LDAP directory server

See "Setup items in the `exauth.properties` file for RADIUS authentication (common settings for the external authorization server)" and "Setup items in the `exauth.properties` file for RADIUS authentication (when using the DNS server to look up information about the external authorization server)"



Note:

- Make sure to distinguish between uppercase and lowercase letters for property settings.
- To use StartTLS for communication between the management server and the LDAP directory server, you need to directly specify information about the LDAP directory server to connect to in the `exauth.properties` file.
- If you use the DNS server to look up the LDAP directory server to connect to, it might take longer for users to log in.

Table 22 Setup items in the `exauth.properties` file for RADIUS authentication (common items)

Property names	Details
<code>auth.server.type</code>	Specify an external authentication server type. Specify <code>radius</code> . Default value: <code>internal</code> (used when not linking to an external authentication server)
<code>auth.server.name</code>	Specify the server identification names of RADIUS servers. You can specify any name for this property to identify which RADIUS servers the settings such as the port number and the protocol for connecting to the RADIUS server (see "Setup items in the <code>exauth.properties</code> file for RADIUS authentication (settings for the external authentication server)" are applied to. <code>ServerName</code> has been set as the initial value. You must specify at least one name. When configuring a redundant configuration, separate the server identification name of each server with a comma (,). Do not register the same server identification name more than once. Specifiable values: No more than 64 bytes of the following characters: A to Z a to z 0 to 9 ! # () + - . = @ [] ^ _ { } ~ Default value: none
<code>auth.group.mapping</code>	Specify whether to also link to an external authorization server. Specify <code>true</code> to link to an external authorization server. Specify <code>false</code> to not to link to an external authorization server. Default value: <code>false</code>

Table 23 Setup items in the `exauth.properties` file for RADIUS authentication (settings for the external authentication server)

Attributes	Details
<code>protocol</code>	Specify the protocol for RADIUS server authentication. This attribute is required. Specifiable values: <code>PAP</code> or <code>CHAP</code> Default value: none

Attributes	Details
<code>host</code> ¹	<p>Specify the host name or IP address of the RADIUS server. If you specify the host name, make sure beforehand that the host name can be resolved to an IP address. If you specify the IP address, you can use either an IPv4 or IPv6 address. When specifying an IPv6 address, enclose it in square brackets ([]). This attribute is required.</p> <p>Default value: none</p>
<code>port</code>	<p>Specify the port number for RADIUS server authentication. Make sure beforehand that the port you specify is set as the listen port number on the RADIUS server.</p> <p>Specifiable values: 1 to 65535</p> <p>Default value: 1812</p>
<code>timeout</code>	<p>Specify the amount of time to wait before timing out when connecting to the RADIUS server.</p> <p>Specifiable values: 1 to 65535 (seconds)</p> <p>Default value: 1</p>
<code>retry.times</code>	<p>Specify the number of times to try to connect to the RADIUS. If you specify 0, no further tries occur.</p> <p>Specifiable values: 0 to 50</p> <p>Default value: 3</p>
<code>attr.NAS-Identifier</code> ²	<p>Specify the host name of the Ops Center Automator management server. The RADIUS server uses this attribute value to identify the management server. The host name of the management server has been set as the initial value.</p> <p>Specifiable values: Specify no more than 253 bytes of the following characters:</p> <p>A to Z</p> <p>a to z</p> <p>0 to 9</p> <p>! " # \$ % & ' () * + , - . / : ; < = > ?</p> <p>@ [\] ^ _ ` { } ~</p> <p>Default value: none</p>

Attributes	Details
<code>attr.NAS-IP-Address</code> ²	<p>Specify the IPv4 address of the Ops Center Automator management server. The RADIUS server uses this attribute value to identify the management server.</p> <p>If the format of the address is not valid, this property is disabled.</p> <p>Default value: none</p>
<code>attr.NAS-IPv6-Address</code> ²	<p>Specify the IPv6 address of the Ops Center Automator management server. The RADIUS server uses this attribute value to identify the management server. Enclose the IPv6 address in square brackets ([]).</p> <p>If the format of the address is not valid, this property is disabled.</p> <p>Default value: none</p>
<ol style="list-style-type: none"> 1. When linking to an external authorization server that is running on the same computer and using StartTLS as the protocol for connecting to the LDAP directory server, in the <code>host</code> attribute specify the same host name as the value of CN in the LDAP directory server certificate. You cannot use an IP address. 2. You must specify exactly one of the following: <code>attr.NAS-Identifier</code>, <code>attr.NAS-IP-Address</code>, or <code>attr.NAS-IPv6-Address</code>. <p>Note: To specify the attributes, use the following syntax:</p> <pre>auth.radius.auth.server.name-property-value.attribute=value</pre>	

Table 24 Setup items in the `exauth.properties` file for RADIUS authentication (common settings for the external authorization server)

Attributes	Details
<code>domain.name</code>	<p>Specify the name of a domain managed by the LDAP directory server. This item is required when an external authorization server is also linked to.</p> <p>Default value: none</p>
<code>dns_lookup</code>	<p>Specify whether to use the DNS server to look up the information about the LDAP directory server.</p> <p>To directly specify information about the LDAP directory server in the <code>exauth.properties</code> file, specify <code>false</code>.</p> <p>To use the DNS server to look up the information, specify <code>true</code>.</p>

Attributes	Details
	<p>However, if the following attribute values are already set, the LDAP directory server will be connected to by using the user-specified values instead of by using the DNS server to look up the information.</p> <ul style="list-style-type: none"> <code>auth.group.domain-name.host</code> <code>auth.group.domain-name.port</code> <p>Default value: <code>false</code></p>
<p>Note: To specify the attributes, use the following syntax:</p> <pre>auth.radius.auth.server.name-property-value.attribute=value</pre>	

Table 25 Setup items in the `exauth.properties` file for RADIUS authentication (when directly specifying information about the external authorization server)

Attributes	Details
<code>protocol</code> ¹	<p>Specify the protocol for connecting to the LDAP directory server.</p> <p>When communicating in plain text format, specify <code>ldap</code>. When using StartTLS communication, specify <code>tls</code>.</p> <p>Before specifying <code>tls</code>, make sure that one of the following encryption methods can be used on the LDAP directory server.</p> <ul style="list-style-type: none"> <code>TLS_RSA_WITH_AES_256_GCM_SHA384</code> <code>TLS_RSA_WITH_AES_256_CBC_SHA256</code> <code>TLS_RSA_WITH_AES_256_CBC_SHA</code> <code>TLS_RSA_WITH_AES_128_CBC_SHA256</code> <code>TLS_RSA_WITH_AES_128_CBC_SHA</code> <code>SSL_RSA_WITH_3DES_EDE_CBC_SHA</code> <p>Specifiable values: <code>ldap</code> or <code>tls</code></p> <p>Default value: <code>ldap</code></p>

Attributes	Details
<code>host²</code>	<p>If the external authentication server and the external authorization server are running on different computers, specify the host name or IP address of the LDAP directory server. If you specify the host name, make sure beforehand that the host name can be resolved to an IP address. If you specify the IP address, you can use either an IPv4 or IPv6 address. When specifying an IPv6 address, enclose it in square brackets ([]).</p> <p>If you omit this attribute, the external authentication server and the external authorization server are assumed to be running on the same computer.</p> <p>Default value: none</p>
<code>port</code>	<p>Specify the port number of the LDAP directory server. Make sure beforehand that the port you specify is set as the listen port number on the LDAP directory server.</p> <p>Specifiable values: 1 to 65535</p> <p>Default value: 389</p>
<code>basedn</code>	<p>Specify the BaseDN, which is the DN of the entry that will be used as the start point when searching for LDAP user information on the LDAP directory server. The user entries that are located in the hierarchy after this DN will be verified during authorization.</p> <p>Specify the DN of the hierarchy that includes all of the user entries to be searched.</p> <p>Specify the DN by following the rules defined in RFC4514. For example, if any of the following characters are included in a DN, you need to use a backslash (\) to escape each character.</p> <p>Spaces # + ; , < = > \</p> <p>If characters that need to be escaped are included in the specified BaseDN, escape all of those characters correctly because the specified value will be passed to the LDAP directory server without change.</p> <p>If you omit this attribute, the value specified in the <code>defaultNamingContext</code> property of Active Directory is assumed as the BaseDN.</p> <p>Default value: none</p>
<code>timeout</code>	<p>Specify the amount of time to wait before timing out when connecting to the LDAP directory server. If you specify 0, the system waits until a communication error occurs without timing out.</p> <p>Specifiable values: 0 to 120 (seconds)</p> <p>Default value: 15</p>

Attributes	Details
<code>retry.interval</code>	Specify the interval (in seconds) between tries to connect to the LDAP directory server. Specifiable values: 1 to 60 (seconds) Default value: 1
<code>retry.times</code>	Specify the number of tries to connect to the LDAP directory server. If you specify 0, no further tries occur. Specifiable values: 0 to 50 Default value: 20
<ol style="list-style-type: none"> 1. When communicating by using StartTLS as the protocol for connecting to the LDAP directory server, you need to specify the security settings of Common Component. 2. When the external authentication server and the external authorization server are running on different computers and when using StartTLS as the protocol for connecting to the LDAP directory server, in the <code>host</code> attribute specify the same host name as the value of CN in the LDAP directory server certificate. You cannot use an IP address. <p>Note: To specify the attributes, use the following syntax:</p> <pre>auth.group.domain-name.attribute=value</pre> <p>For <i>domain-name</i>, specify the value specified for <code>auth.radius.auth.server.name-property-value.domain.name</code>.</p>	

Table 26 Setup items in the `exauth.properties` file for RADIUS authentication (when an external authorization server and StartTLS are used for communication)

Property	Details
<code>auth.ocsp.enable</code>	Specify whether to verify the validity of an LDAP directory server's electronic signature certificate by using an OCSP responder when the LDAP directory server and StartTLS are used for communication. To verify the validity of certificates, specify <code>true</code> . To not verify the validity of certificates, specify <code>false</code> . Default value: <code>false</code>
<code>auth.ocsp.responderURL</code>	Specify the URL of an OCSP responder to use an OCSP responder that is not the one written in the AIA field of the electronic signature certificate to verify the validity of the electronic signature certificate. If this value is omitted, the OCSP responder written in the AIA field is used. Default value: None

Table 27 Setup items in the `exauth.properties` file for RADIUS authentication (when using the DNS server to look up information about the external authorization server)

Attributes	Details
<code>protocol</code>	<p>Specify the protocol for connecting to the LDAP directory server.</p> <p>Specifiable values: <code>ldap</code></p> <p>Default value: <code>ldap</code></p>
<code>port</code>	<p>Specify the port number of the LDAP directory server. Make sure beforehand that the port you specify is set as the listen port number on the LDAP directory server.</p> <p>Specifiable values: 1 to 65535</p> <p>Default value: 389</p>
<code>basedn</code>	<p>Specify the BaseDN, which is the DN of the entry that will be used as the start point when searching for LDAP user information on the LDAP directory server. The user entries that are located in the hierarchy after this DN will be verified during authorization.</p> <p>Specify the DN of the hierarchy that includes all of the user entries to be searched.</p> <p>Specify the DN by following the rules defined in RFC4514. For example, if any of the following characters are included in a DN, you need to use a backslash (\) to escape each character.</p> <p>Spaces # + ; , < = > \</p> <p>If characters that need to be escaped are included in the specified BaseDN, escape all of those characters correctly because the specified value will be passed to the LDAP directory server without change.</p> <p>If you omit this attribute, the value specified in the <code>defaultNamingContext</code> property of Active Directory is assumed as the BaseDN.</p> <p>Default value: none</p>
<code>timeout</code>	<p>Specify the amount of time to wait before timing out when connecting to the LDAP directory server. If you specify 0, the system waits until a communication error occurs without timing out.</p> <p>Specifiable values: 0 to 120 (seconds)</p> <p>Default value: 15</p>
<code>retry.interval</code>	<p>Specify the interval (in seconds) between tries to connect to the LDAP directory server.</p> <p>Specifiable values: 1 to 60 (seconds)</p> <p>Default value: 1</p>

Attributes	Details
<code>retry.times</code>	<p>Specify the number of times to try to connect to the LDAP directory server. If you specify 0, no further tries occur.</p> <p>Specifiable values: 0 to 50</p> <p>Default value: 20</p>
<p>Note: To specify the attributes, use the following syntax:</p> <p><code>auth.group.domain-name.attribute=value</code></p> <p>For <i>domain-name</i>, specify the value specified for <code>auth.radius.auth.server.name-property-value.domain.name</code>.</p>	

Examples of setting the `exauth.properties` file for RADIUS authentication

The following are examples of how to set the `exauth.properties` file when using a RADIUS server to perform authentication:

- When linking to only an external authentication server

```
auth.server.type=radius
auth.server.name=ServerName
auth.group.mapping=false
auth.radius.ServerName.protocol=PAP
auth.radius.ServerName.host=radius.example.com
auth.radius.ServerName.port=1812
auth.radius.ServerName.timeout=1
auth.radius.ServerName.retry.times=3
auth.radius.ServerName.attr.NAS-Identifier=host_A
```

- When directly specifying information about an external authorization server

```
auth.server.type=radius
auth.server.name=ServerName
auth.group.mapping=true
auth.ocsp.enable=false
auth.ocsp.responderURL=
auth.radius.ServerName.protocol=PAP
auth.radius.ServerName.host=radius.example.com
auth.radius.ServerName.port=1812
auth.radius.ServerName.timeout=1
auth.radius.ServerName.retry.times=3
auth.radius.ServerName.attr.NAS-Identifier=host_A
auth.radius.ServerName.domain.name=EXAMPLE.COM
auth.radius.ServerName.dns_lookup=false
auth.group.EXAMPLE.COM.protocol=ldap
auth.group.EXAMPLE.COM.host=ldap.example.com
auth.group.EXAMPLE.COM.port=389
auth.group.EXAMPLE.COM.basedn=dc=Example,dc=com
auth.group.EXAMPLE.COM.timeout=15
auth.group.EXAMPLE.COM.retry.interval=1
auth.group.EXAMPLE.COM.retry.times=20
```

- When using the DNS server to look up an external authorization server

```
auth.server.type=radius
auth.server.name=ServerName
auth.group.mapping=true
auth.radius.ServerName.protocol=PAP
auth.radius.ServerName.host=radius.example.com
auth.radius.ServerName.port=1812
auth.radius.ServerName.timeout=1
auth.radius.ServerName.retry.times=3
auth.radius.ServerName.attr.NAS-Identifier=host_A
auth.radius.ServerName.domain.name=EXAMPLE.COM
auth.radius.ServerName.dns_lookup=true
auth.group.EXAMPLE.COM.protocol=ldap
auth.group.EXAMPLE.COM.basedn=dc=Example,dc=com
auth.group.EXAMPLE.COM.timeout=15
auth.group.EXAMPLE.COM.retry.interval=1
auth.group.EXAMPLE.COM.retry.times=20
```

- When using a redundant configuration

```
auth.server.type=radius
auth.server.name=ServerName1,ServerName2
auth.group.mapping=false
auth.radius.ServerName1.protocol=PAP
auth.radius.ServerName1.host=radius1.example.com
auth.radius.ServerName1.port=1812
auth.radius.ServerName1.timeout=1
auth.radius.ServerName1.retry.times=3
auth.radius.ServerName1.attr.NAS-IP-Address=127.0.0.1
auth.radius.ServerName2.protocol=PAP
auth.radius.ServerName2.host=radius2.example.com
auth.radius.ServerName2.port=1812
auth.radius.ServerName2.timeout=1
auth.radius.ServerName2.retry.times=3
auth.radius.ServerName2.attr.NAS-IP-Address=127.0.0.1
```

Setup items in the `exauth.properties` file for Kerberos authentication

In the `exauth.properties` file, specify the type of the external authentication server, the server identification name, and the information about the external authentication server.

- Common properties

See "Setup items in the `exauth.properties` file for Kerberos authentication (common items)"

- Properties for an external authentication server

Specify these property values for each Kerberos server.

Setup items in the `exauth.properties` file vary depending on whether information about the Kerberos server being connected to is directly specified or looked up by using the DNS server.

- When directly specifying information about the Kerberos server:

See "Setup items in the `exauth.properties` file for Kerberos authentication (when directly specifying information about the external authentication server)"

- When using the DNS server to look up information about the Kerberos server:

See "Setup items in the `exauth.properties` file for Kerberos authentication (when using the DNS server to look up information about the external authentication server)"

- Properties for an external authorization server

These properties need to be set if you directly specify information about the Kerberos server and an external authorization server is also linked. Specify the properties for each realm.

See "Setup items in the `exauth.properties` file for Kerberos authentication (settings for the external authorization server)" or "Setup items in the `exauth.properties` file for Kerberos authentication (when an external authorization server and StartTLS are used for communication)"



Note:

- Make sure to distinguish between uppercase and lowercase letters for property settings.
- To use StartTLS for communication between the management server and the LDAP directory server, you need to directly specify information about the LDAP directory server to connect to in the `exauth.properties` file.
- If you use the DNS server to look up the LDAP directory server to connect to, it might take longer for users to log in.

Table 28 Setup items in the `exauth.properties` file for Kerberos authentication (common items)

Property names	Details
<code>auth.server.type</code>	Specify an external authentication server type. Specify <code>kerberos</code> . Default value: <code>internal</code> (used when not linking to an external authentication server)
<code>auth.group.mapping</code>	Specify whether to also link to an external authorization server. Specify <code>true</code> to link to an external authorization server. Specify <code>false</code> to not to link to an external authorization server. Default value: <code>false</code>

Table 29 Setup items in the `exauth.properties` file for Kerberos authentication (when directly specifying information about the external authentication server)

Attributes	Details
<code>default_realm</code>	Specify the default realm name. If you specify a user ID but not a realm name in the login window of the GUI, the user is authenticated as a user who belongs to the realm specified for this attribute. This attribute is required. Default value: <code>none</code>
<code>dns_lookup_kdc</code>	Specify <code>false</code> . Default value: <code>false</code>
<code>default_tkt_enctypes</code>	Specify the encryption type used for Kerberos authentication. This property is enabled only if the management server OS is Windows. You can use the following encryption types: <ul style="list-style-type: none"> ▪ <code>aes128-cts</code> ▪ <code>rc4-hmac</code> ▪ <code>des3-cbc-sha1</code> ▪ <code>des-cbc-md5</code> ▪ <code>des-cbc-crc</code> To specify multiple encryption types, use a comma to separate the encryption types.

Attributes	Details
	<p>Among the specified encryption types, an encryption type that is supported by both the management server OS and a Kerberos server will be used.</p> <p>Default value: None (DES-CBC-MD5 is used for authentication.)</p>
<code>clockskew</code>	<p>Specify the acceptable range of difference between the management server time and Kerberos server time. If the difference exceeds this value, an authentication error occurs.</p> <p>Specifiable values: 0 to 300 (seconds)</p> <p>Default value: 300</p>
<code>timeout</code>	<p>Specify the amount of time to wait before timing out when connecting to the Kerberos server. If you specify 0, the system waits until a communication error occurs without timing out.</p> <p>Specifiable values: 0 to 120 (seconds)</p> <p>Default value: 3</p>
<code>realm_name</code>	<p>Specify the realm identification names. You can specify any name for this attribute to identify which realms the property attribute settings are applied to. You must specify at least one name. When specifying multiple realm identification names, separate the names with commas (,). Do not register the same realm identification name more than once.</p> <p>Default value: none</p>
<code>value-specified-for-realm_name.realm</code>	<p>Specify the name of the realm set in the Kerberos server. This attribute is required.</p> <p>Default value: none</p>
<code>value-specified-for-realm_name.kdc[#]</code>	<p>Specify the information about the Kerberos server in the following format:</p> <p><i>host-name-or-IP-address[:port-number]</i></p> <p>This attribute is required.</p>

Attributes	Details
	<p>host-name-or-IP-address</p> <p>If you specify the host name, make sure beforehand that the name can be resolved to an IP address. If you specify the IP address, use an IPv4 address. In an IPv6 environment, you must specify the host name. Note that you cannot specify the loopback address (<code>localhost</code> or <code>127.0.0.1</code>).</p> <p>port-number</p> <p>Make sure beforehand that the port you specify is set as the listen port number on the Kerberos server. If you do not specify a port number or the specified port number cannot be used in a Kerberos server, 88 is assumed.</p> <p>When configuring the Kerberos server in redundant configuration, separate the servers with commas (,) as follows:</p> <pre>host-name-or-IP-address[:port-number] , host-name-or-IP-address[:port-number],...</pre>
<p>#: When using StartTLS as the protocol for connecting to the external authorization server, specify the same host name as the value of CN in the external authorization server certificate. You cannot use an IP address.</p> <p>Note: To specify the attributes, use the following syntax:</p> <pre>auth.kerberos.attribute=value</pre>	

Table 30 Setup items in the `exauth.properties` file for Kerberos authentication (when using the DNS server to look up information about the external authentication server)

Attributes	Details
<code>default_realm</code>	<p>Specify the default realm name. If you specify a user ID but not a realm name in the login window of the GUI, the user is authenticated as a user who belongs to the realm specified for this attribute. This attribute is required.</p> <p>Default value: none</p>
<code>dns_lookup_kdc</code>	Specify <code>true</code> . This attribute is required.

Attributes	Details
	<p>However, if all the following attributes values are already set, the Kerberos server will not be looked up by using the DNS server.</p> <ul style="list-style-type: none"> ▪ <code>realm_name</code> ▪ <code>value-specified-for-realm_name.realm</code> ▪ <code>value-specified-for-realm_name.kdc</code>
<code>default_tkt_enctypes</code>	<p>Specify the encryption type used for Kerberos authentication. This property is enabled only if the management server OS is Windows.</p> <p>You can use the following encryption types:</p> <ul style="list-style-type: none"> ▪ <code>aes128-cts</code> ▪ <code>rc4-hmac</code> ▪ <code>des3-cbc-sha1</code> ▪ <code>des-cbc-md5</code> ▪ <code>des-cbc-crc</code> <p>To specify multiple encryption types, use a comma to separate the encryption types.</p> <p>Among the specified encryption types, an encryption type that is supported by both the management server OS and a Kerberos server will be used.</p> <p>Default value: None (DES-CBC-MD5 is used for authentication.)</p>
<code>clockskew</code>	<p>Specify the acceptable range of difference between the management server time and Kerberos server time. If the difference exceeds this value, an authentication error occurs.</p> <p>Specifiable values: 0 to 300 (seconds)</p> <p>Default value: 300</p>
<code>timeout</code>	<p>Specify the amount of time to wait before timing out when connecting to the Kerberos server. If you specify 0, the system waits until a communication error occurs without timing out.</p> <p>Specifiable values: 0 to 120 (seconds)</p> <p>Default value: 3</p>
<p>Note: To specify the attributes, use the following syntax:</p> <pre>auth.kerberos.attribute=value</pre>	

Table 31 Setup items in the `exauth.properties` file for Kerberos authentication (settings for the external authorization server)

Attributes	Details
<code>protocol#</code>	<p>Specify the protocol for connecting to the LDAP directory server.</p> <p>When communicating in plain text format, specify <code>ldap</code>. When using StartTLS communication, specify <code>tls</code>. StartTLS communication can be used only when directly specifying information about the Kerberos server.</p> <p>Before specifying <code>tls</code>, make sure that one of the following encryption methods can be used on the LDAP directory server.</p> <ul style="list-style-type: none"> ▪ <code>TLS_RSA_WITH_AES_256_GCM_SHA384</code> ▪ <code>TLS_RSA_WITH_AES_256_CBC_SHA256</code> ▪ <code>TLS_RSA_WITH_AES_256_CBC_SHA</code> ▪ <code>TLS_RSA_WITH_AES_128_CBC_SHA256</code> ▪ <code>TLS_RSA_WITH_AES_128_CBC_SHA</code> ▪ <code>SSL_RSA_WITH_3DES_EDE_CBC_SHA</code> <p>Specifiable values: <code>ldap</code> or <code>tls</code></p> <p>Default value: <code>ldap</code></p>
<code>port</code>	<p>Specify the port number of the LDAP directory server. Make sure beforehand that the port you specify is set as the listen port number on the LDAP directory server.</p> <p>Specifiable values: 1 to 65535</p> <p>Default value: 389</p>
<code>basedn</code>	<p>Specify the BaseDN, which is the DN of the entry that will be used as the start point when searching for LDAP user information on the LDAP directory server. The user entries that are located in the hierarchy after this DN will be verified during authorization.</p> <p>Specify the DN of the hierarchy that includes all of the user entries to be searched.</p> <p>Specify the DN by following the rules defined in RFC4514. For example, if any of the following characters are included in a DN, you need to use a backslash (<code>\</code>) to escape each character.</p> <p>Spaces <code># + ; , < = > \</code></p> <p>If characters that need to be escaped are included in the specified BaseDN, escape all of those characters correctly because the specified value will be passed to the LDAP directory server without change.</p>

Attributes	Details
	<p>If you omit this attribute, the value specified in the <code>defaultNamingContext</code> property of Active Directory is assumed as the BaseDN.</p> <p>Default value: none</p>
<code>timeout</code>	<p>Specify the amount of time to wait before timing out when connecting to the LDAP directory server. If you specify 0, the system waits until a communication error occurs without timing out.</p> <p>Specifiable values: 0 to 120 (seconds)</p> <p>Default value: 15</p>
<code>retry.interval</code>	<p>Specify the interval (in seconds) between tries to connect to the LDAP directory server.</p> <p>Specifiable values: 1 to 60 (seconds)</p> <p>Default value: 1</p>
<code>retry.times</code>	<p>Specify the number of tries to connect to the LDAP directory server. If you specify 0, no further tries occur.</p> <p>Specifiable values: 0 to 50</p> <p>Default value: 20</p>
<p>#: When communicating by using StartTLS as the protocol for connecting to the LDAP directory server, you need to specify the security settings of Common Component.</p> <p>Note: To specify the attributes, use the following syntax:</p> <p><code>auth.group.realm-name.attribute=value</code></p> <p>For <i>realm-name</i>, specify the value specified for <code>auth.kerberos.realm_name-property-value.rHealm</code>.</p>	

Table 32 Setup items in the `exauth.properties` file for Kerberos authentication (when an external authorization server and StartTLS are used for communication)

Property	Details
<code>auth.ocsp.enable</code>	<p>Specify whether to verify the validity of an LDAP directory server's electronic signature certificate by using an OCSP responder when the LDAP directory server and StartTLS are used for communication.</p> <p>To verify the validity of certificates, specify <code>true</code>. To not verify the validity of certificates, specify <code>false</code>.</p> <p>Default value: <code>false</code></p>

Property	Details
<code>auth.ocsp.responderURL</code>	Specify the URL of an OCSP responder to use an OCSP responder that is not the one written in the AIA field of the electronic signature certificate to verify the validity of the electronic signature certificate. If this value is omitted, the OCSP responder written in the AIA field is used. Default value: None

Examples of setting the `exauth.properties` file for Kerberos authentication

The following are examples of how to set the `exauth.properties` file when using a Kerberos server to perform authentication:

- When directly specifying information about a Kerberos server (when not linking to an external authorization server)

```
auth.server.type=kerberos
auth.group.mapping=false
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=false
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
auth.kerberos.realm_name=RealmName
auth.kerberos.RealmName.realm=EXAMPLE.COM
auth.kerberos.RealmName.kdc=kerberos.example.com:88
```

- When using the DNS server to look up a Kerberos server (when not linking to an external authorization server)

```
auth.server.type=kerberos
auth.group.mapping=false
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=true
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
```

- When directly specifying information about a Kerberos server (when also linking to an external authorization server)

```
auth.server.type=kerberos
auth.group.mapping=true
auth.ocsp.enable=false
auth.ocsp.responderURL=
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=false
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
auth.kerberos.realm_name=RealmName
auth.kerberos.RealmName.realm=EXAMPLE.COM
auth.kerberos.RealmName.kdc=kerberos.example.com:88
auth.group.EXAMPLE.COM.protocol=ldap
auth.group.EXAMPLE.COM.port=389
auth.group.EXAMPLE.COM.basedn=dc=Example,dc=com
auth.group.EXAMPLE.COM.timeout=15
auth.group.EXAMPLE.COM.retry.interval=1
auth.group.EXAMPLE.COM.retry.times=20
```

- When using the DNS server to look up a Kerberos server (when also linking to an external authorization server)

```
auth.server.type=kerberos
auth.group.mapping=true
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=true
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
```

- When using a redundant configuration

```
auth.server.type=kerberos
auth.group.mapping=false
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=false
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
auth.kerberos.realm_name=S1
auth.kerberos.S1.realm=EXAMPLE.COM
auth.kerberos.S1.kdc=kerberos.example.com:88,kerberos.example.net:88
```

- When specifying multiple realm identifiers

```
auth.server.type=kerberos
auth.group.mapping=false
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=false
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
auth.kerberos.realm_name=S1,S2
auth.kerberos.S1.realm=EXAMPLE.COM
auth.kerberos.S1.kdc=kerberos1.example.com:88,kerberos1.example.net:88
auth.kerberos.S2.realm=EXAMPLE.NET
auth.kerberos.S2.kdc=kerberos2.example.com:88,kerberos2.example.net:88
```

About LDAP search user accounts

An LDAP search user account is used when an account needs to be authenticated or authorized, or when searching for information within an LDAP directory server.

In the following cases, you need to register an LDAP search user account on the management server.

- When an LDAP directory server is used as an external authentication server and the data structure is the hierarchical structure model
- When an LDAP directory server is used as an external authorization server

When registering an authorization group in Common Component products by using the GUI, to verify whether the distinguished name of the authorization group is registered on the external authorization server by using a user ID such as the `System` account registered in Common Component products, you need to register a user account used to search for LDAP user information on the management server.

Except in the cases shown previously, this step is not necessary, because LDAP user information is not searched during authentication and authorization. If a user account used to search for LDAP user information has been already registered, delete it.

Conditions for LDAP search user account

Conditions for the LDAP search user account vary depending on the authentication method.

Prepare a user account that satisfies the following conditions on the LDAP directory server.

For LDAP authentication:

- The user account can bind to the DN specified for `auth.ldap.auth.server.name-property-value.basedn` in the `exauth.properties` file
- The user account can search the attributes for all entries after the DN specified for `auth.ldap.auth.server.name-property-value.basedn` in the `exauth.properties` file
- The user account can reference the DN specified for `auth.ldap.auth.server.name-property-value.basedn` in the `exauth.properties` file
- The user account can reference the authorization groups that are under the DN specified for `auth.ldap.auth.server.name-property-value.basedn` in the `exauth.properties` file (when an external authorization server is also linked to)
- The user account can search the attributes of the authorization groups that are under the DN specified for `auth.ldap.auth.server.name-property-value.basedn` in the `exauth.properties` file and search the attributes of nested groups of the authorization groups (when an external authorization server is also linked to)

For RADIUS authentication:

- The user account can bind to the DN specified for `auth.group.domain-name.basedn` in the `exauth.properties` file
- The user account can search the attributes for all entries after the DN specified for `auth.group.domain-name.basedn` in the `exauth.properties` file
- The user account can reference the DN specified for `auth.group.domain-name.basedn` in the `exauth.properties` file
- The user account can reference the authorization groups that are under the DN specified for `auth.group.domain-name.basedn` in the `exauth.properties` file.
- The user account can search the attributes of the authorization groups that are under the DN specified for `auth.group.domain-name.basedn` in the `exauth.properties` file and search the attributes of nested groups of the authorization groups

For Kerberos authentication:

- The user account can bind to the DN specified for `auth.group.realm-name.basedn` in the `exauth.properties` file
- The user account can search the attributes for all entries after the DN specified for `auth.group.realm-name.basedn` in the `exauth.properties` file
- The user account can reference the DN specified for `auth.group.realm-name.basedn` in the `exauth.properties` file
- The user account can reference the authorization groups that are under the DN specified for `auth.group.realm-name.basedn` in the `exauth.properties` file
- The user account can search the attributes of the authorization groups that are under the DN specified for `auth.group.realm-name.basedn` in the `exauth.properties` file and search the attributes of nested groups of the authorization groups

Registering an LDAP search user account

Use the `hcmds64ldapuser` command to register an LDAP search user account on the management server.

Before you begin

- Register an LDAP search user on the LDAP directory server.
- Verify the following information:
 - DN and password of the LDAP search user
 - Server identification name or the domain name for external authentication servers of the LDAP directory server (for LDAP authentication)

Specify the server identification name that was specified for the `auth.server.name` property in the `exauth.properties` file, or specify the domain name specified for `auth.ldap.value-specified-for-auth.server.name.domain.name` property in the `exauth.properties` file.

- Domain name of the RADIUS server (for RADIUS authentication)

Specify the domain name specified for `auth.radius.auth.server.name-property-value.domain.name` in the `exauth.properties` file.

- Realm name of the Kerberos server (for Kerberos authentication)

If you directly specify information about a Kerberos server in the `exauth.properties` file, specify the value specified for `auth.kerberos.default_realm` or `auth.kerberos.auth.kerberos.realm_name-property-value.realm`.

If you specify the settings in the `exauth.properties` file to use the DNS server to look up information about a Kerberos server, specify the realm name registered in the DNS server.

Procedure

1. Execute the `hcnds64ldapuser` command.

In Windows:

```
Common-Component-installation-folder\bin
\hcnds64ldapuser /set /dn DN-of-user-account-used-to-search-
for-LDAP-user-info [/pass password-of-user-account-used-to-
search-for-LDAP-user-info] /name name
```

In Linux:

```
Common-Component-installation-directory/bin/hcmds64ldapuser
-set -dn DN-of-user-account-used-to-search-for-LDAP-user-
info [-pass password-of-user-account-used-to-search-for-
LDAP-user-info] -name name
```

- **DN-of-user-account-used-to-search-for-LDAP-user-info**

Specify a DN by following the rules defined in RFC4514. For example, if the following characters are included in a DN, you need to use a backslash (\) to escape each character.

Spaces # + , ; < = > \

- **password-of-user-account-used-to-search-for-LDAP-user-info**

This is case-sensitive and must exactly match the password registered in the LDAP directory server. If you execute the command without specifying the `pass` option, you will be prompted to enter a password.

**Note:**

- In the LDAP directory server, you can use double quotation marks (") for the DN and password. In the management server, however, you need to register a user account whose DN and password do not include double quotation marks.
- If you are using Active Directory, you can use the `dsquery` command provided by Active Directory to verify the DN of a user. The following example shows how to use the `dsquery` command to verify the DN of the user `administrator`, and also shows the execution results:

```
dsquery user -name administrator
```

```
"CN=administrator,CN=admin,DC=example,DC=com"
```

- If the DN includes commas such as `cn=administrator,cn=admin,dc=example,com`, specify as follows:

In Windows:

```
hcmds64ldapuser /set /dn
"cn=administrator,cn=admin,dc=example\,com" /pass
administrator_pass /name ServerName
```

In Linux:

```
hcmds64ldapuser -set -dn
"cn=administrator,cn=admin,dc=example\\,com" -pass
administrator_pass -name ServerName
```

Deleting an LDAP search user account

Before you begin

Use the **hcmds64ldapuser** command to delete the LDAP search user account from the management server.

Verify the following information:

- Server identification name or the domain name for external authentication servers of the LDAP directory server (for LDAP authentication)
- Domain name of the RADIUS server (for RADIUS authentication)
- Realm name of the Kerberos server (for Kerberos authentication)

Procedure

1. Execute the **hcmds64ldapuser** command.

In Windows:

```
Common-Component-installation-folder\bin\hcmds64ldapuser /
delete /name name
```

In Linux:

```
Common-Component-installation-directory/bin/hcmd64ldapuser
-delete -name name
```

Verifying the LDAP directory server that registered the LDAP search user account

Use the **hcmds64ldapuser** command to verify which LDAP directory server has registered the LDAP search user account on the management server.

Procedure

1. Run the **hcmds64ldapuser** command.

In Windows:

```
Common-Component-installation-folder\bin\hcmds64ldapuser /
list
```

In Linux:

```
Common-Component-installation-directory/bin/hcmd64ldapuser
-list
```

Registering a shared secret

Before you begin

Use the `hcnds64radiussecret` command to register the RADIUS shared secret on the management server.

Verify the following information:

- Shared secret
- RADIUS server indication name

RADIUS-server-indication-name must match a server indication name specified for the `auth.server.name` property in the `exauth.properties` file.

Procedure

1. Run the `hcnds64radiussecret` command.

In Windows:

```
Common-Component-installation-folder\bin\hcnds64radiussecret
[/set shared-secret] /name RADIUS-server-indication-name
```

In Linux:

```
Common-Component-installation-directory/bin/
hcnds64radiussecret [-set shared-secret] -name RADIUS-
server-indication-name
```

- If you execute the command without specifying the `set` option, you will be prompted to enter a shared secret.

Deleting a shared secret

Before you begin

Use the `hcnds64radiussecret` command to delete the shared secret.

Verify the RADIUS server indication name.

Procedure

1. Run the `hcnds64radiussecret` command.

In Windows:

```
Common-Component-installation-folder\bin
\hcnds64radiussecret /delete /name RADIUS-server-indication-
name
```

In Linux:

```
Common-Component-installation-directory/bin/
hcnds64radiussecret -delete -name RADIUS-server-indication-
name
```

Verifying the RADIUS server that registered a shared secret on the management server

Use the `hcnds64radiussecret` command to verify which RADIUS server has registered the shared secret on the management server.

Procedure

1. Run the `hcnds64radiussecret` command.

In Windows:

```
Common-Component-installation-folder\bin  
hcnds64radiussecret /list
```

In Linux:

```
Common-Component-installation-directory/bin/  
hcnds64radiussecret -list
```

Result

The server identification name of the RADIUS server is displayed.

Verifying connections to an external authentication server and an external authorization server

Before you begin

Use the `hcmds64checkauth` command to verify whether the management server is correctly connected to the external authentication server and the external authorization server.

- Register an external authentication server and an external authorization server
- Verify the following information:

- For LDAP authentication

Verify the user accounts registered on the LDAP directory server. For user IDs, specify the value saved in the attribute specified by `auth.ldap.value-specified-in-auth.server.name.attr` in the `exauth.properties` file.

- For RADIUS authentication

Verify the user accounts registered on the RADIUS server.

- For Kerberos authentication

When linking only to an external authentication server:

Verify the user accounts that are registered in Common Component products and whose authentication method is Kerberos authentication.

When also linking to an external authorization server:

Verify the user accounts not registered in Common Component products.

In addition, if you specify a user who belongs to a realm other than the realm specified for `default_realm` in the `exauth.properties` file, also verify the realm that the user belongs to. If more than one realm name is specified in the `exauth.properties` file, verify all specified realm names.

Note that you cannot specify a user account whose *user-ID* or *password* begins with a forward slash (/) in Windows, or hyphen (-) in Linux.

Procedure

1. Run the `hcmds64checkauth` command.

In Windows:

```
Common-Component-installation-folder\bin\hcmds64checkauth [/user user-ID /pass password] [/summary]
```


In Linux:

```
Common-Component-installation-directory/bin/hcmds64checkauth
[-user user-ID -pass password] [-summary]
```

- If you run the command without specifying the `user` option or the `pass` option, you will be prompted to enter a user ID and password.
- If you run the command with the `summary` option specified, the confirmation message is displayed in summary format.



Note: When using the Kerberos authentication method, if more than one realm name is specified in the `exauth.properties` file, verify the connection for each realm name. In addition, specify user IDs according to the following:

- To specify a user belonging to a realm other than the realm set for `default_realm` in the `exauth.properties` file:
user-ID@realm-name
- To specify a user who belongs to the realm set for `default_realm` in the `exauth.properties` file:

You can omit the realm name.

- When using the LDAP authentication method, if the `hcmds64checkauth` command is executed, all connected external authentication servers are verified and the verification results for each external authentication server are displayed.

For external authentication servers for which the user account specified for the `hcmds64checkauth` command is not registered, an error message indicating that the user account is not registered is displayed in phase 3 of the verification result, and confirmation at phase 3 might fail.

When this occurs, verify the connection of each external authentication server by using a user account that is registered to that server.

Result

Settings in the `exauth.properties` file and connections to the external authentication server and external authorization server are verified, and verification results are displayed in each of four phases. The following message is displayed if the verifying in each phase finishes normally.

```
KAPM15004-I The result of the configuration check of Phase phase-number was normal.
```

Phase 1

The command verifies that common properties have been correctly specified in the `exauth.properties` file.

Phase 2

The command verifies that the properties for the external authentication server and properties for the external authorization server have been correctly specified in the `exauth.properties` file.

Phase 3

The command verifies that the external authentication server can be connected to.

Phase 4

If an external authorization server is also linked to, the command verifies that the external authorization server can be connected to and authorization groups can be searched.

Command notes for setting up a link to an external authentication server

If command line control characters are included in the arguments of commands that will be executed when specifying the settings to link to an external authentication server, escape the characters correctly according to the specifications of the command line.

Also, you need to pay attention to backslashes (`\`) included in the arguments because they are treated specially in the command line.

The following explains how to escape when running the `hcnds64dapuser` command, `hcnds64radiussecret` command, or `hcnds64checkauth` command.

In Windows:

If the following characters are included in an argument, enclose the argument in double quotation marks (`"`) or use a caret (`^`) to escape each character:

Spaces & | ^ < > ()

A backslash might be treated as an escape character depending on the character that follows it. Therefore, if a backslash and any of the previous characters are included in an argument, use a caret to escape each character rather than enclose the argument in double quotation marks.

Also, if there is a backslash at the end of an argument, escape it by using another backslash.

In Linux:

If the following characters are included in an argument, enclose the argument in double quotation marks or use a backslash to escape each character:

Spaces # & ' () ~ \ ` < > ; |

Note that a backslash in an argument is treated as an escape character even if the argument is enclosed in double quotation marks. If a backslash is included in an argument, escape it by using another backslash.

For example, if a shared secret to be registered by the `hcnds64radiussecret` command is `secret01\`, escape it as follows:

In Windows:

```
hcmds64radiussecret /set secret01\\ /name ServerName
```

In Linux:

Use either of the following formats:

```
hcmds64radiussecret -set secret01\\ -name ServerName
```

```
hcmds64radiussecret -set "secret01\\" -name ServerName
```

Encryption types for Kerberos authentication

Configure the Kerberos server so that the encryption types supported by Common Component products can be used.

In Common Component products, the following encryption types can be used for Kerberos authentication.

- AES256-CTS-HMAC-SHA1-96
- AES128-CTS-HMAC-SHA1-96
- RC4-HMAC
- DES3-CBC-SHA1
- DES-CBC-CRC
- DES-CBC-MD5

Chapter 6: Backing up and restoring Ops Center Automator

This module describes how to backup and restore Ops Center Automator.

Overview of backup and restore

Ops Center Automator allows you to backup and restore your system in case a failure occurs and your system go down.

Use cases

Periodic backup

Prepare for any failures by periodically backing up your data as part of your normal operations. Then, if a failure occurs, restore the backed up data to recover from the failure.

Re-installation of the OS on the same management server

System configuration and database information can be carried over.

Move to another host

You can use the backup and restore feature to move Ops Center Automator to another host. System configuration and database information can also be carried over.

Ops Center Automator does not support periodic automatic backup. Create a backup schedule that fits your requirements and perform a manual backup.

Backing up Ops Center Automator

Ops Center Automator allows you to back up your system configuration and database information.

Before you begin

On the Tasks tab, verify that there is no task in the In Progress, Waiting for Input, In Progress (with Error), Long Running, or In Progress (Terminating) status.

Procedure

1. Log on to the management server using Administrator privilege (for Windows) or root privilege (for Linux).

2. Stop the services or disable failover.

- For a non-cluster environment:

Stop the Ops Center Automator and Common Component services by running the **hcnds64srv /stop** command.

- For a cluster environment:

Run the following command to take the group where the Ops Center Automator and Common Component services are registered offline and disable failover.

```
Common-Component-installation-folder\ClusterSetup\hcnds64clustersrvstate.bat /soff /r group-name
```

3. Run the **backupsystem** command.

4. Start the services or enable failover.

- For a non-cluster environment:

Start the Ops Center Automator and Common Component services by running the **hcnds64srv /start** command.

- For a cluster environment:

Run the following command to take the group where the Ops Center Automator and Common Component services are registered online and enable failover.

```
Common-Component-installation-folder\ClusterSetup\hcnds64clustersrvstate.bat /son /r group-name
```

Restoring Ops Center Automator

Ops Center Automator allows you to restore your system configuration and database information.

Before you begin

On the Tasks tab, verify that there is no task in the In Progress, Waiting for Input, In Progress (with Error), Long Running, or In Progress (Terminating) status.

Procedure

1. Log on to the management server using Administrator privilege (for Windows) or root privilege (for Linux).
2. Complete a backup of Ops Center Automator on the source host.
See [Backing up Ops Center Automator \(on page 180\)](#) for the steps to do this.
3. Transfer the archived backup to the destination host.

4. Stop the services or disable failover.

- For a non-cluster environment:

Stop the Ops Center Automator and Common Component services by running the **hcnds64srv /stop** command.

- For a cluster environment:

Run the following command to take the group where the Ops Center Automator and Common Component services are registered offline and disable failover.

```
Common-Component-installation-folder\ClusterSetup\hcnds64clustersrvstate.bat /soff /r group-name
```

5. Run the **restoresystem** command to restore the backup.

6. Reconfigure the following settings to match the destination environment.

To set	See
External authentication server integration (exauth.properties ¹)	Registering an external authentication server and an external authorization server (on page 134) and Registering an LDAP search user account (on page 170)
Password policy (security.conf ²)	Changing the password policy (on page 108)
Audit log (auditlog.conf ²)	Enabling audit logging (on page 88)
Port number ³ (user_httpsd.conf) ⁴	Changing the port number used for management server communication with management clients (on page 54) and Common Component property updates for port number changes (on page 56)
Secure communications (user_httpsd.conf) ⁴	Configuring secure communications (on page 61)
Server managing the user account	Changing the information of the server managing the user account (on page 58)
Agentless connection secret key	Public key authentication (on page 124)
RADIUS server shared secret key	Registering a shared secret (on page 174)
Performance mode	Configuring the performance mode (on page 106)
Warning banner	"hcnds64banner command" in the <i>Hitachi Ops Center Automator User Guide</i>

To set	See
1. The backup source file is stored in the following location:	
<ul style="list-style-type: none"> For Windows: 	<code>Backup-destination-folder\HBase\base\conf</code>
<ul style="list-style-type: none"> For Linux: 	<code>Backup-destination-directory/HBase/base/conf</code>
2. The backup source file is stored in the following location:	
<ul style="list-style-type: none"> For Windows: 	<code>Backup-destination-folder\HBase\base\conf\sec</code>
<ul style="list-style-type: none"> For Linux: 	<code>Backup-destination-directory/HBase/base/conf/sec</code>
3: This setting is required if it had been changed from the default.	
4: The backup source file is stored in the following location:	
<ul style="list-style-type: none"> For Windows: 	<code>Backup-destination-folder\HBase\base\httpsd.conf</code>
<ul style="list-style-type: none"> For Linux: 	<code>Backup-destination-directory/HBase/base/httpsd.conf</code>

7. Remove and re-register Ops Center Automator in Common Services.
 - a. Remove Ops Center Automator from Common Services. To remove Ops Center Automator, see the *Hitachi Ops Center Installation and Configuration Guide*.
 - b. Run the `setupcommonservices` command to apply changes to Common Services.
 - c. If necessary, change permissions for user groups and service groups.
8. Restart the services by running the `hcnds64srv /start` command.

Moving Ops Center Automator to another host

If necessary, you can move Ops Center Automator from one host to another.



Note: If the host name or IP address of the replacement source and host name or IP address of the replacement destination are different, you must change the management server host name.

Before you begin

Make sure following settings are the same between the source host and the replacement destination host:

- The host name and IP address.
- The account of the OS user used by Ops Center Automator
- The Hitachi Ops Center product environment (configuration, version, and revision).
- The installation path of Ops Center Automator.

You should also make sure that no tasks are currently being processed in the "Status" column of the Tasks tab of Ops Center Automator with the indication "In Progress", "Waiting for Input", "In Progress (with Error)", "Long Running", or "In Progress (Terminating)".

Procedure

1. Log on to the management server using Administrator privilege.
2. Complete a backup of Ops Center Automator on the source host.
 - a. Stop the current services by running the **hcmds64srv /stop** command.
 - b. Run the **backupsystem** command to perform the backup.
3. Transfer the archived backup file to the replacement destination host.
4. Log on to the management server for the destination host.
5. Complete a restore of Ops Center Automator on the replacement destination host.
 - a. Stop the services by running the **hcmds64srv /stop** command.
 - b. Run the **restoresystem** command to restore the backup.
 - c. Reconfigure the following settings to match the environment of the restore destination.

To set	See
External authentication server integration (<code>exauth.properties</code> ¹)	Registering an external authentication server and an external authorization server (on page 134) and Registering an LDAP search user account (on page 170)
Password policy (<code>security.conf</code> ²)	Changing the password policy (on page 108)
Audit log (<code>auditlog.conf</code> ²)	Enabling audit logging (on page 88)
Port number ³ (<code>user_httpsd.conf</code> ⁴)	Changing the port number used for management server communication with management clients (on page 54) and Common Component property updates for port number changes (on page 56)

To set	See
Secure communications (<code>user_httpsd.conf</code> ⁴)	Configuring secure communications (on page 61)
Server managing the user account	Changing the information of the server managing the user account (on page 58)
Agentless connection secret key	Public key authentication (on page 124)
RADIUS server shared secret key	Registering a shared secret (on page 174)
Performance mode	Configuring the performance mode (on page 106)
Warning banner	"hcmds64banner command" in the <i>Hitachi Ops Center Automator User Guide</i>
<p>1. The backup source file is stored in the following location:</p> <p>For Windows:</p> <pre>backup-destination-folder\HBase\base\conf</pre> <p>For Linux:</p> <pre>backup-destination-directory/HBase/base/conf</pre> <p>2. The backup source file is stored in the following location:</p> <p>For Windows:</p> <pre>backup-destination-folder\HBase\base\conf\sec</pre> <p>For Linux:</p> <pre>backup-destination-directory/HBase/base/conf/sec</pre> <p>3. This setting is required if it has been changed from the default.</p> <p>4. The backup source file is stored in the following location:</p> <p>For Windows:</p> <pre>backup-destination-folder\HBase\base\httpsd.conf</pre>	

To set	See
For Linux:	
<code>backup-destination-directory/HBase/base/httpsd.conf</code>	

6. Remove and register Ops Center Automator from Common Services.
 - a. Remove Ops Center Automator from Common Services. To remove Ops Center Automator, see the *Hitachi Ops Center Installation and Configuration Guide*.
 - b. Run the `setupcommonservice` command to apply the changes to Common Services.
 - c. If necessary, change permissions for user groups and service groups.
7. Restart the services by running the `hcnds64srv /start` command.

Chapter 7: Removing Ops Center Automator

This module describes how to remove Ops Center Automator.

Removing Ops Center Automator (Windows OS)

You can remove Ops Center Automator in a Windows environment by completing the steps listed in the following sections.

Before you begin

- If tasks in the Status column of the Tasks tab of Ops Center Automator are in the Waiting, Waiting for Input, In Progress, Long Running, or In Progress (with Error) state, wait until the tasks stop or finish running.
- Close all of the service dialog boxes.
- Close any Windows Services or open command prompts.
- Disable any security monitoring, virus detection, or process monitoring software on the server.



Caution: If other Common Component products are installed in the same host, do not delete the shared folder (\Base64). If you delete this folder, other Common Component products will not work properly.

Procedure

1. Log on to Windows OS as the administrator.
2. Run the following command to stop all services:
`Common-Component-installation-folder\bin\hcnds64srv /stop`
3. Open the **Control Panel**, and then choose **Programs and Features** or **Uninstall a Program**.
4. Select **Hitachi Ops Center Automator**, and then click **Uninstall**, or select the program, right-click, and select **Uninstall**.
5. In the **Automation Software** window, click **Next > Remove** to start the software removal process.
The removal process deletes the Ops Center Automator installation folder.
6. If you use Common Services, delete Ops Center Automator information from Common Services.

Result

Ops Center Automator is removed from the host.

Removing Ops Center Automator software in a cluster environment

You can remove the Ops Center Automator software from the server in a cluster environment to migrate to a different server or stop Ops Center Automator processes.



Note: If you remove Ops Center Automator, the properties files, log files, and other product-related files are deleted.

Procedure

1. In the cluster management software, move the group in which the Common Component services are registered from the standby node to the active node by right-clicking the group, selecting **Move**, and then either **Select Node** or **Move this service or application to another node**.
2. Take offline and disable failover for the group in which Common Component services including Ops Center Automator are registered by using the following command:

```
Common-Component-installation-directory\ClusterSetup
\hcnds64clustersrvstate /soff /r cluster-group-name
```

where

r - specifies the name of the group in which the Common Component product services including Ops Center Automator are registered. If the group name contains spaces, you must enclose the group name in quotation marks ("). For example, if the group name is Automator cluster, specify "Automator cluster".

3. Delete the Common Component services including Ops Center Automator by using the following command:



Note: Before deleting the services, delete the "customer script" from the cluster management software.

```
Common-Component-installation-directory\ClusterSetup
\hcnds64clustersrvupdate /sdel /r cluster-group-name
```

where

r - specifies the name of the group in which the Common Component product services including Ops Center Automator are registered. If the group name contains spaces, you must enclose the group name in quotation marks ("). For example, if the group name is Automator cluster, specify "Automator cluster".



Note:

- All Ops Center Automator and Common Component product services that are registered in the group specified by the `r` option are deleted. However, the File Services Manager services are not deleted.
- If you plan to continue using Common Component products, reregister them after you remove Ops Center Automator. Deleting the Ops Center Automator services does not cause a problem.

Remember that if you changed the service resource names, all resource names are reinitialized when the services are reregistered. Therefore, you must write down the resource names for the services that you are deleting, and change the names after reregistering those services.

4. Use the following command to stop the Common Component products:
`Common-Component-installation-folder\bin\hcmds64srv /stop`
5. Remove Hitachi Ops Center Automator from the active node.
6. On the active node, delete any files and folders that are no longer required (such as those files and folders created during installation in the cluster environment).
7. In the cluster management software, move the Ops Center Automator services group to the standby node by right-clicking the group, selecting **Move**, and selecting either **Select Node** or **Move this service or application to another node**.
8. Remove Ops Center Automator from the standby node.
9. After performing the removal of the cluster installation, delete the Ops Center Automator folder and, if you no longer plan to use any other Common Component services, also delete the `Base64` folder from the standby node.
10. If the following resources are not in use by other applications, use the cluster management software to take them offline, and then delete them:
 - IP address
 - Shared disk
11. On the standby node, delete any files and folders that are no longer required (such as those files and folders created during installation in the cluster environment).

12. To continue using other Common Component products, use the following command to register the Common Component services in the cluster management software group:

```
Common-Component-installation-folder\ClusterSetup
\hcmds64clustersrvupdate /sreg /r cluster-group-name /sd drive-
letter-of-shared-disk /ap resource-name-for-client-access-point
```

where

r - specifies the name of the group in which you to plan to register the Common Component product services. If the group name contains spaces, you must enclose the group name in quotation marks ("). For example, if the group name is Automator cluster, specify "Automator cluster".

sd - specifies the drive letter of the shared disk that is registered to the cluster management software. You cannot specify multiple drive letters for this option. If the database of Common Component products is divided into multiple shared disks, run the `hcmds64clustersrvupdate` command for each shared disk.

ap - specifies the name of the resource for the client access point that is registered to the cluster management software.

13. To continue using other Common Component products, use the following command to bring online and enable failover for the group in which the Common Component services are registered:

```
Common-Component-installation-folder\ClusterSetup
\hcmds64clustersrvstate /son /r cluster-group-name
```

where

r - specifies the name of the group in which the Common Component product services are registered. If the group name contains spaces, you must enclose the group name in quotation marks ("). For example, if the group name is Automator cluster, specify "Automator cluster".

14. In the cluster management software, move the group containing the Common Component resources to the active node by right-clicking the group, selecting **Move**, and then selecting either **Select Node** or **Move this service or application to another node**.
15. If you are using Common Services, delete the Ops Center Automator information from Common Services.

Deleting authentication data (Windows OS)

If the `KNAE04574-E` warning dialog box appears although the removal completes successfully, the deletion of authentication data failed. Delete the data by running the `hcmds64intg` command on the server that administers user accounts (on the host running the product using Common Component and connected to the server)

To run the `hcmds64intg` command to delete the authentication data from a Windows host:

Procedure

1. Start all installed services of the products using Common Component products by running the following command:

```
Common-Component-installation-folder\bin\hcnds64srv /start
```

2. Delete the authentication data by running the following command: *Common-Component-installation-folder\bin\hcnds64intg /delete /type component-name /user user-id /pass password*

- */type*

Specify the name of the component that you want to delete. Automation can be specified.

- */user*

Specify the user ID of a user who has the Admin (user management) permission. If you run the command without the user option, you are prompted to specify a user ID.

- */pass*

Specify the password of a user who has the Admin (user management) permission. If you run the command without the pass option, you are prompted to specify a password.



Note: If you display a GUI window of another product using Common Component without deleting the authentication data, the following problems might occur, even after removing the Ops Center Automator server:

- User management information of the Ops Center Automator server displays.
- The button used to start the Ops Center Automator server is enabled on the dashboard. Clicking the enabled button causes a link error to appear.



Note: If you use Common Services, see the Hitachi Ops Center online help for the steps to delete a user account.

Removing Ops Center Automator (Linux OS)

You can remove Ops Center Automator in a Linux OS environment as listed in the following procedure.

Procedure

1. Move to a root directory, such as */root*.
2. Run the following command: *Directory-specified-when-installing-Automation-software/ADUninstall/uninstall.sh*
3. If you use Common Services, delete Ops Center Automator information from Common Services.

Deleting authentication data (Linux OS)

If the `KNAE04574-E` warning dialog box appears although the removal completes successfully, the deletion of authentication data failed. Delete the data by running the `hcmds64intg` command on the server that administers user accounts (on the host running the product using Common Component and connected to the server)

Procedure

1. Start all installed services of the products using Common Component product by running the following command:
`Common-Component-installation-directory/bin/hcmdsv64srv -start`
2. Delete the authentication data by running the following command: `Common-Component-installation-directory/bin/hcmdsv64intg -delete -type component-name -user user-id -pass password`
 - `-type`
Specify the name of the component that you want to delete. Automation can be specified.
 - `-user`
Specify the user ID of a user who has the Admin (user management) permission. If you run the command without the user option, you are prompted to specify a user ID.
 - `-pass`
Specify the password of a user who has the Admin (user management) permission. If you run the command without the pass option, you are prompted to specify a password.



Note: If you display a GUI window of another product using Common Component without deleting the authentication data, the following problems might occur, even after removing the Ops Center Automator server:

- User management information of the Ops Center Automator server displays.
- The button used to start the Ops Center Automator server is enabled on the dashboard. Clicking the enabled button causes a link error to appear.



Note: If you use Common Services, see the Hitachi Ops Center online help for the steps to delete a user account.

Appendix A: Ops Center Automator file location and ports

This module includes a list of all the folders or directories that Ops Center Automator creates as part of the installation. It also includes a list of ports.

Ops Center Automator file location

Installation folders

The following tables list the folders or directories that are created when Ops Center Automator is installed. The Windows folder locations column and Linux OS directory locations column lists default paths that can be changed during installation.

Windows folder details	Windows folder locations
Folder specified when installing Ops Center Automator	<code>system-drive\Program Files\hitachi</code>
Ops Center Automator installation folder	<code>system-drive\Program Files\hitachi\Automation</code>
Commands files	<code>system-drive\Program Files\hitachi\Automation\bin</code>
Configuration files	<code>system-drive\Program Files\hitachi\Automation\conf</code>
Folder for service templates	<code>system-drive\Program Files\hitachi\Automation\contents</code>
Folder for service templates and plug-ins under development	<code>system-drive\Program Files\hitachi\Automation\develop</code>
Data files	<code>system-drive\Program Files\hitachi\Automation\data</code>
Help files	<code>system-drive\Program Files\hitachi\Automation\docroot</code>
Preset property definition files	<code>system-drive\Program Files\hitachi\Automation\extra_presets</code>

Windows folder details	Windows folder locations
Temporary working folder for installation and removal	<code>system-drive\Program Files\hitachi\Automation\inst</code>
Library files	<code>system-drive\Program Files\hitachi\Automation\lib</code>
Log files	<code>system-drive\Program Files\hitachi\Automation\logs</code>
System files	<code>system-drive\Program Files\hitachi\Automation\system</code>
Working folder used by Internal command	<code>system-drive\Program Files\hitachi\Automation\webapps</code>
Working folder	<code>system-drive\Program Files\hitachi\Automation\work</code>
Common Component	<code>system-drive\Program Files\hitachi\Base64</code>

Linux OS directory details	Linux OS directory locations
Directory specified when installing Ops Center Automator	<code>/opt/hitachi</code>
Ops Center Automator installation directory	<code>/opt/hitachi/Automation</code>
Commands files	<code>/opt/hitachi/Automation/bin</code>
Configuration files	<code>/opt/hitachi/Automation/conf</code>
Directory for service templates	<code>/var/opt/hitachi/Automation/contents</code>
Directory for service templates and plug-ins under development	<code>/var/opt/hitachi/Automation/develop</code>
Data files	<code>/var/opt/hitachi/Automation/data</code>
Help files	<code>/opt/hitachi/Automation/docroot</code>
Preset property definitions files	<code>/var/opt/hitachi/Automation/extra_presets</code>
Temporary working directory for installation and removal	<code>/opt/hitachi/Automation/inst</code>
Library files	<code>/opt/hitachi/Automation/lib</code>
Log files	<code>/var/opt/hitachi/Automation/logs</code>

Linux OS directory details	Linux OS directory locations
System files	/opt/hitachi/Automation/system
Working directory used by Internal command	/opt/hitachi/Automation/webapps
Working directory	/var/opt/hitachi/Automation/work
Common Component	/opt/hitachi/Base64

Port settings

Ops Center Automator uses the following port settings:

External connection port

Port number	Firewall	Description
22/tcp	Automator --> Operation target	Used for SSH. <i>cjstartsv</i> uses this port.
23/tcp	Automator --> Operation target	Used for Telnet. <i>cjstartsv</i> uses this port.
443/tcp	Automator-->Common Services	Used to access Common Services
445/tcp or udp	Automator --> Operation target	Used for Windows administrative shares. <i>cjstartsv</i> uses this port.
135/tcp and 139/tcp	Automator --> Operation target	Used for Windows administrative shares. <i>cjstartsv</i> uses this port.
22015/tcp	Browser -> Automator	Used to access HBase 64 Storage Mgmt Web Service. In non-SSL (unsecured) communication, initial setup is a required. This port number can be changed. <i>httpsd</i> uses this port.

Port number	Firewall	Description
22016/tcp	Browser -> Automator	Use to access HBase 64 Storage Mgmt Web Service. In SSL (secured) communication, a setting is required. This port number can be changed. <code>httpsd</code> uses this port.
25/tcp	Automator -> SMTP server	Used for mail transmission. This port number can be changed. For details, see "Configuring email and log settings" in the <i>Hitachi Ops Center Automator User Guide</i> . <code>cjstartsv</code> uses this port.
88/tcp or udp	Automator -> Kerberos server	<code>cjstartsv</code> uses this port.
389/tcp	Automator -> LDAP directory server	Used for <code>ldap/tls</code> . <code>cjstartsv</code> uses this port.
1812/udp	Automator -> Radius server	Used for Radius servers. <code>cjstartsv</code> uses this port.
Various Web Service connection ports/ tcp	Automator -> Various servers	Used for the servers registered to Web Service connections.

Internal connection port

Port number	Firewall	Description
22017/tcp	Automator -> Automator	Used to access the Common Component. <code>cjstartsv</code> uses this port.
22018/tcp	Automator -> Automator	Used to access the Common Component. <code>cjstartsv</code> uses this port.
22025/tcp	Automator -> Automator	Used to access the Common Component. <code>cjstartsv</code> uses this port.

Port number	Firewall	Description
22026/tcp	Automator -> Automator	Used to access the Common Component. cjstartsv uses this port.
22031/tcp	Automator -> Automator	Used to access the Common Component. cjstartsv uses this port.
22032/tcp	Automator -> Automator	Used to access the Common Component. cjstartsv uses this port.
22035/tcp	Automator -> Automator	Used to access the Common Component. cjstartsv uses this port.
22036/tcp	Automator -> Automator	Used to access the Common Component. cjstartsv uses this port.
22037/tcp	Automator -> Automator	Used to access the Common Component. cjstartsv uses this port.
22038/tcp	Automator -> Automator	Used to access the Common Component. cjstartsv uses this port.
22170/tcp	Automator -> Automator	Used to access the Common Component. cjstartsv uses this port.
22171/tcp	Automator -> Automator	Used to access the Common Component. cjstartsv uses this port.
22172/tcp	Automator -> Automator	Used to access the Common Component. cjstartsv uses this port.
22173/tcp	Automator -> Automator	Used to access the Common Component. cjstartsv uses this port.

Port number	Firewall	Description
22220/tcp	Automator -> Automator	Used in an embedded database.



Note: These ports are "reserved" and are used only for an internal port connection.

Appendix B: Ops Center Automator processes

This module includes a list of the Ops Center Automator processes.

Ops Center Automator processes (Windows)

The following table lists the Ops Center Automator processes in Windows. This table contains the process information necessary to check Ops Center Automator status. Note that this is not a table of the Ops Center Automator process configuration.

Process name	Service name	Description
cjstartsv.exe	HAutomation Engine Web Service	Used in Common Component.
hcmdssvctl.exe		
cjstartsv.exe	HBase 64 Storage Mgmt SSO Service	Used in Common Component.
hcmdssvctl.exe		
httpd.exe	HBase 64 Storage Mgmt Web Service	Used in Common Component.
rotatelog.exe		
httpd.exe	HBase 64 Storage Mgmt Web SSO Service	Used in Common Component.
rotatelog.exe		
pdsvr.exe	HiRDB/EmbeddedEdition _HD1	Used in the Common Component database.
pdprcd.exe		
pdmlgd.exe		
pdmd.exe		

Ops Center Automator processes (Linux)

The following table lists the Ops Center Automator processes in Linux. This table contains the process information necessary to check Ops Center Automator status. Note that this is not a table of the Ops Center Automator process configuration.

Process name	Daemon name	Description
cjstartsv	hicommand64-hcs_ao	Used in Common Component.
hcs_ao		
cjstartsv	hicommand64-hcs_hssso	Used in Common Component.
hcs_hssso		
httpsd	hicommand64-hcs_web	Used in Common Component.
rotatelog		
httpsd	hicommand64-hcs_hweb	Used in Common Component.
rotatelog		
pdprcd	-	Used in the Common Component database.
pdmlgd		
pdrdmd		

Appendix C: Troubleshooting

This module describes the actions to take if an error occurs on the Ops Center Automator server. Confirm the messages or log files to determine the cause of the error, and take action accordingly.

Collecting maintenance information

If no messages are output when a problem occurs, or you cannot correct the problem even after following the instructions in the message, collect maintenance information, and then contact user support.

Collecting the log files

Procedure

1. Log on to the management server as a user with Administrator permissions (for Windows) or as a root user (for Linux).
2. Run the `hcnds64getlogs` command to collect the log files.

In Windows:

```
Common-Component-installation-folder\bin\hcnds64getlogs /dir output-folder-path
```

In Linux:

```
Common-Component-installation-directory/bin/hcnds64getlogs -dir output-directory-path
```

Result

An archive file is output to the specified destination.

See "hcnds64getlogs command" in the *Hitachi Ops Center Automator User Guide*.

Appendix D: Notices

This software product includes the following redistributable software.

Notices

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).

Portions of this software were developed at the National Center for Supercomputing Applications (NCSA) at the University of Illinois at Urbana-Champaign.

This product includes software developed by the University of California, Berkeley and its contributors.

This software contains code derived from the RSA Data Security Inc. MD5 Message-Digest Algorithm, including various modifications by Spyglass Inc., Carnegie Mellon University, and Bell Communications Research, Inc (Bellcore).

Regular expression support is provided by the PCRE library package, which is open source software, written by Philip Hazel, and copyright by the University of Cambridge, England. The original software is available from <ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/>

1. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)
2. This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)
3. This product includes software written by Tim Hudson (tjh@cryptsoft.com)
4. This product includes the OpenSSL Toolkit software used under OpenSSL License and Original SSLeay License. OpenSSL License and Original SSLeay License are as follow:

LICENSE ISSUES

=====

The OpenSSL toolkit stays under a double license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts.

OpenSSL License

/* =====

* Copyright (c) 1998-2019 The OpenSSL Project. All rights reserved.

*

* Redistribution and use in source and binary forms, with or without

* modification, are permitted provided that the following conditions

* are met:

*

* 1. Redistributions of source code must retain the above copyright

* notice, this list of conditions and the following disclaimer.

*

* 2. Redistributions in binary form must reproduce the above copyright

* notice, this list of conditions and the following disclaimer in

* the documentation and/or other materials provided with the

* distribution.

*

* 3. All advertising materials mentioning features or use of this

* software must display the following acknowledgment:

```

* "This product includes software developed by the OpenSSL Project
* for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
* endorse or promote products derived from this software without
* prior written permission. For written permission, please contact
* openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
* nor may "OpenSSL" appear in their names without prior written
* permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
* acknowledgment:
* "This product includes software developed by the OpenSSL Project
* for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS" AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* =====
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com). This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/

Original SSLeay License
-----

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
* All rights reserved.
*
* This package is an SSL implementation written
* by Eric Young (eay@cryptsoft.com).
* The implementation was written so as to conform with Netscapes SSL.
*
* This library is free for commercial and non-commercial use as long as
* the following conditions are aheared to. The following conditions
* apply to all code found in this distribution, be it the RC4, RSA,
* lhash, DES, etc., code; not just the SSL code. The SSL documentation
* included with this distribution is covered by the same copyright terms

```

* except that the holder is Tim Hudson (tjh@cryptsoft.com).

*

* Copyright remains Eric Young's, and as such any Copyright notices in

* the code are not to be removed.

* If this package is used in a product, Eric Young should be given attribution

* as the author of the parts of the library used.

* This can be in the form of a textual message at program startup or

* in documentation (online or textual) provided with the package.

*

* Redistribution and use in source and binary forms, with or without

* modification, are permitted provided that the following conditions

* are met:

* 1. Redistributions of source code must retain the copyright

* notice, this list of conditions and the following disclaimer.

* 2. Redistributions in binary form must reproduce the above copyright

* notice, this list of conditions and the following disclaimer in the

* documentation and/or other materials provided with the distribution.

* 3. All advertising materials mentioning features or use of this software

* must display the following acknowledgement:

* "This product includes cryptographic software written by

* Eric Young (eay@cryptsoft.com)"

* The word 'cryptographic' can be left out if the routines from the library

* being used are not cryptographic related :-).

* 4. If you include any Windows specific code (or a derivative thereof) from

* the apps directory (application code) you must include an acknowledgement:

* "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

*

* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND

* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE

* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE

* ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE

* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL

* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS

* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)

* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT

* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY

* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF

* SUCH DAMAGE.

*

* The licence and distribution terms for any publically available version or

* derivative of this code cannot be changed. i.e. this code cannot simply be

* copied and put under another distribution licence

* [including the GNU Public Licence.]

*/

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

This product includes software developed by IAIK of Graz University of Technology.

This product includes software developed by Daisuke Okajima and Kohsuke Kawaguchi (<http://relaxngcc.sf.net/>).

This product includes software developed by the Java Apache Project for use in the Apache JServ servlet engine project (<http://java.apache.org/>).

This product includes software developed by Andy Clark.

Java is a registered trademark of Oracle and/or its affiliates.



Other company and product names mentioned in this document may be the trademarks of their respective owners.

Index

A

- agentless 122
- audit logging 86
- audit logs (Automator server)
 - configure environment configuration file 88
 - output format 91
- auditlog.conf
 - sample 91
 - settings 89
- authentication
 - external 128
 - method 14
 - user 129, 130
- authorization group 128
- Automation Director 40, 52, 94, 106, 108, 116, 183
- automation software
 - file location 193
 - installing 39, 46
 - port settings 193, 195
 - removing 187
- Automator 40, 52, 94, 106, 108, 116, 183

B

- back up 180
- backing up 180
- backup 180
- basic system configuration 13

C

- changing security settings 108
- cluster
 - installation prerequisites 41
- cluster environment configuration, checking 42
- collecting log files 201
- conditions
 - LDAP search user account 169
- configure
 - java heap memory size 126
- configure email notification 106

- configuring
 - basic system 13
 - management server URL 60
 - server host name 59
 - server IP address 60
- connection information for remote machines 116
- cssslsetup 78

D

- definition file 106
- disk space requirements 22
- documents
 - related 8

E

- email notification 106
- exauth.properties 137, 148
- exauth.properties file
 - Kerberos server 159
- external authentication server
 - registering 134
 - verifying connections 176
- external authorization server
 - registering 134
 - verifying connections 176

F

- file location
 - automation software 193
- folder server 129

H

- hardware requirements 22
- hcmds64unlockaccount command 113
- Hitachi Ops Center products 12
- host 106, 122
- host name
 - changing 59

I

- installation prerequisites 36
- installing
 - automation software 36, 39, 46
 - avoiding port conflicts 39
 - in a cluster environment 40
 - moving the software to another host 183
 - on another host 183
- IP address
 - changing 60
- IPv6 116

J

- java heap memory size, setting 126

K

- Kerberos server
 - exauth.properties file 159

L

- LDAP 129, 137
- LDAP search user
 - registering 170
- LDAP search user account
 - conditions 169
 - deleting 173
- Linux
 - processes 199
- locking
 - System account 112
 - unlocking accounts 113
 - user accounts 112
- log file
 - collecting 201

M

- machine 122
- maintenance
 - information 201
- management 34
- management client
 - setting up SSL on web-based clients 75
 - setting up the server for secure client communication 64
- maximum resources 32
- monitor 34
- multi-domain configuration 132

N

- Name resolution 38

O

- ops center 78
- Ops Center 40, 52, 80, 94, 106, 108, 116, 183
- Ops Center Automator
 - related products 12
 - workflows 13
- Ops Center Automator 10.8.3 40, 52, 94, 106, 108, 116, 183
- Ops Center Protector 80
- overview
 - basic system configuration 13
 - related products 12
 - workflows 13
- Overview 12

P

- password policy 108
- performance mode 106
- planning
 - avoiding port conflicts 39
- port 24
- ports
 - automation software settings 193, 195
 - avoiding conflicts 39
 - properties requiring updated when ports change 56
- Post-Installation tasks 47
- Preface 8
- prerequisite 122
- processes
 - Linux 199
 - Windows 199
- product version 8
- properties 116
- Properties file (config_user.properties) 94

R

- RADIUS 129, 130, 148
- redundant configuration 132
- registering
 - Automator with Common Services 51
- Registering a license 49
- related documents 8
- remote connection
 - OS support 114
- remote connection information 116

- removing
 - automation software 187
 - automation software components 187, 191
 - software in a cluster environment 188
- requirements
 - disk space 22
 - hardware 22
- restore 180
- restored 181
- restoring 181
- S**
- secure communication 78
- secure communications 61
- security definition 108
- security settings
 - overview 61
 - secure communications for management clients 64
 - setting up SSL on web-based management clients 75
 - setting up:server for secure client communication 64
- security.conf file 108
- server 122
- service
 - starting 50
 - stopping 50
- setup 137, 148
- shared secret
 - checking 175
 - deleting 174
 - registering 174
- single-sign on 51
- SSL
 - setting up on the server for secure client communication 64
 - setting up on web-based management clients 75
 - using for secure client communication 64
- SSL communication 80
- sso 51
- starting
 - service 50
- stopping
 - service 50
- system 34
- System account
 - automatically lock 112
 - changing the password 49
- system requirements 15

T

- target 34
- troubleshooting 201

U

- uninstalling 187, 191
- URL
 - changing the management server URL 60
 - confirming, Linux 48
 - confirming, Windows 48
- user accounts
 - account locking 111
 - account locking policies 111
 - setting account locking policies 112
 - unlocking accounts 113
- user management 128

V

- verifying connections
 - external authentication server 176
 - external authorization server 176
- Verifying the installation 48
- virus detection, excluding directories
 - directory
 - excluding from virus detection 46

W

- windows 40, 122
- Windows
 - processes 199
- workflow 129, 130
- workflows
 - overview 13

Hitachi Vantara



Corporate Headquarters

2535 Augustine Drive

Santa Clara, CA 95054 USA

HitachiVantara.com | community.HitachiVantara.com

Contact Information

USA: 1-800-446-0744

Global: 1-858-547-4526

HitachiVantara.com/contact