JP1 Version 12

Job Management: Getting Started (High-speed Transfer of Huge Files)

3021-3-D40(E)

Notices

■ Relevant program products

P-2A41-9ACL JP1/Data Highway - Server version 12-00 (for Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016)

P-8141-9ACL JP1/Data Highway - Server version 12-00 (for Linux 6 (x64))

■ Trademarks

HITACHI, JP1 are either trademarks or registered trademarks of Hitachi, Ltd. in Japan and other countries.

Internet Explorer is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries.

Linux(R) is the registered trademark of Linus Torvalds in the U.S. and other countries.

Microsoft is either a registered trademark or a trademark of Microsoft Corporation in the United States and/or other countries.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

Red Hat is a trademark or a registered trademark of Red Hat Inc. in the United States and other countries.

RSA and BSAFE are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries.

Windows is either a registered trademark or a trademark of Microsoft Corporation in the United States and/or other countries.

Windows Server is either a registered trademark or a trademark of Microsoft Corporation in the United States and/or other countries.

Other company and product names mentioned in this document may be the trademarks of their respective owners.

JP1/Data Highway - Server includes RSA BSAFE(R) Cryptographic software of EMC Corporation.

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

This product includes software developed by Ben Laurie for use in the Apache-SSL HTTP server project.

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/

This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/).

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

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 Daisuke Okajima and Kohsuke Kawaguchi (http://relaxngcc.sf.net/).

This product includes software developed by Andy Clark.

Other product and company names mentioned in this document may be the trademarks of their respective owners. Throughout this document Hitachi has attempted to distinguish trademarks from descriptive terms by writing the name with the capitalization used by the manufacturer, or by writing the name with initial capital letters. Hitachi cannot attest to the accuracy of this information. Use of a trademark in this document should not be regarded as affecting the validity of the trademark.

Java is a registered trademark of Oracle and/or its affiliates.

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:

```
* 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 rouines from the library
* being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
```

■ Microsoft product screen shots

Microsoft product screen shots reprinted with permission from Microsoft Corporation.

■ Related products

JP1/Data Highway - Automatic Job Executor

A client product for transmitting and receiving data. The product automates the file transfer functionality of JP1/Data Highway - Server.

■ Restrictions

Information in this document is subject to change without notice and does not represent a commitment on the part of Hitachi. The software described in this manual is furnished according to a license agreement with Hitachi. The license agreement contains all of the terms and conditions governing your use of the software and documentation, including all warranty rights, limitations of liability, and disclaimers of warranty.

Material contained in this document may describe Hitachi products not available or features not available in your country.

No part of this material may be reproduced in any form or by any means without permission in writing from the publisher.

■ Issued

Jun. 2019: 3021-3-D40(E)

■ Copyright

Summary of amendments

The following table lists changes in this manual (3021-3-D40(E)) and product changes related to this manual.

Changes	Location
The following OS are supported: • macOS 10.13 (High Sierra)	*1.2.2*
The following web browser is change of supported version: • Mozilla Firefox ESR	*1.2.2*
The following web browser are supported: • Safari 11	*1.2.2*
The application (App) that is used to send and receive files and messages is now supported.	*2.2.4*, *Chapter 3*
The following OSs are no longer supported: • Windows Server 2008 R2	--

In addition to the above changes, minor editorial corrections were made.

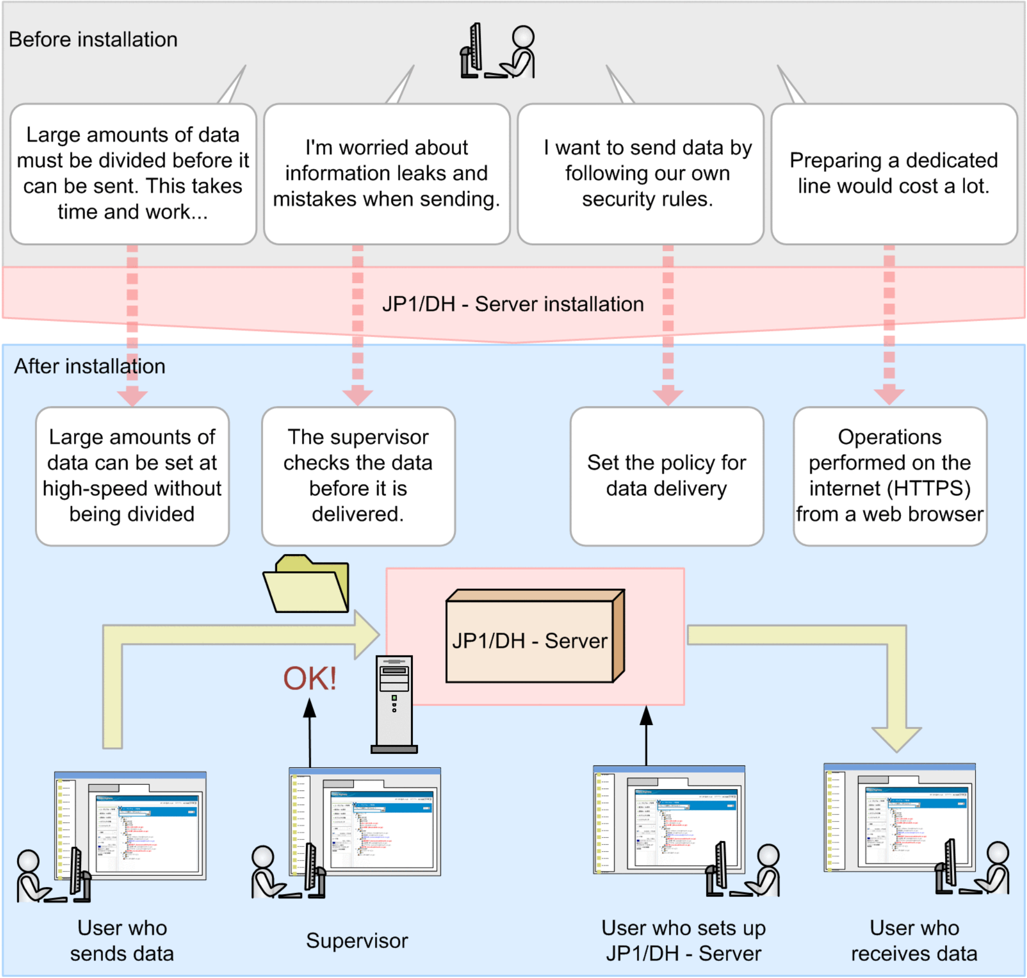
Preface

■ What you can do with JP1/Data Highway - Server

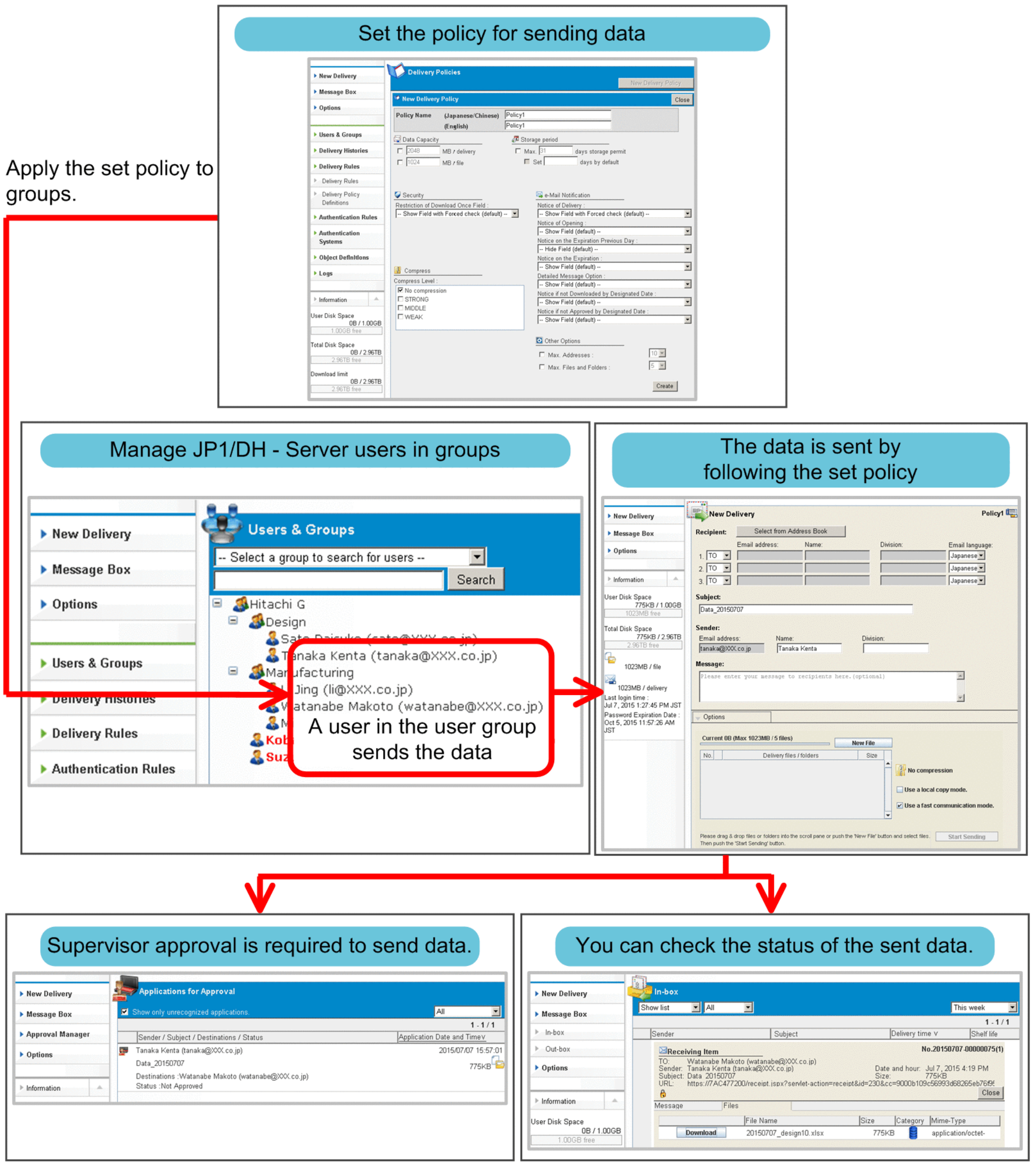
Business environments now span multiple countries: for example, between Japan and countries in Asia, Europe, and America. With companies sending an increasing amount of data across national borders each year, the ability to reliably send large amounts of data at high speeds can open up business opportunities.

Challenges also exist. For example, data leakage due to erroneous transmission has become a serious problem. Security measures are increasingly important, but cost reduction also needs to be focused on to strengthen company competitiveness.

In addition to sending data safely by using SSL communications, JP1/Data Highway - Server (hereafter called *JP1/DH - Server*) is able to send large amounts of data at high speed, using various security measures. Costs can be reduced because this product uses the Internet and web browsers which you are already using.


Before installation
Large amounts of data must be divided before it can be sent. This takes time and work...
I'm worried about information leaks and mistakes when sending.
I want to send data by following our own security rules.
Preparing a dedicated line would cost a lot.
JP1/DH - Server installation
After installation
Large amounts of data can be set at high-speed without being divided
The supervisor checks the data before it is delivered.
Set the policy for data delivery
Operations performed on the internet (HTTPS) from a web browser
JP1/DH - Server
OK!
User who sends data
Supervisor
User who sets up JP1/DH - Server
User who receives data

JP1/DH - Server provides various windows and provides wide support for the process, from operation preparation to starting the operation and onward.



Set the policy for sending data

Apply the set policy to groups.

Manage JP1/DH - Server users in groups

The data is sent by following the set policy

A user in the user group sends the data

Supervisor approval is required to send data.

You can check the status of the sent data.

■ What is explained in this manual

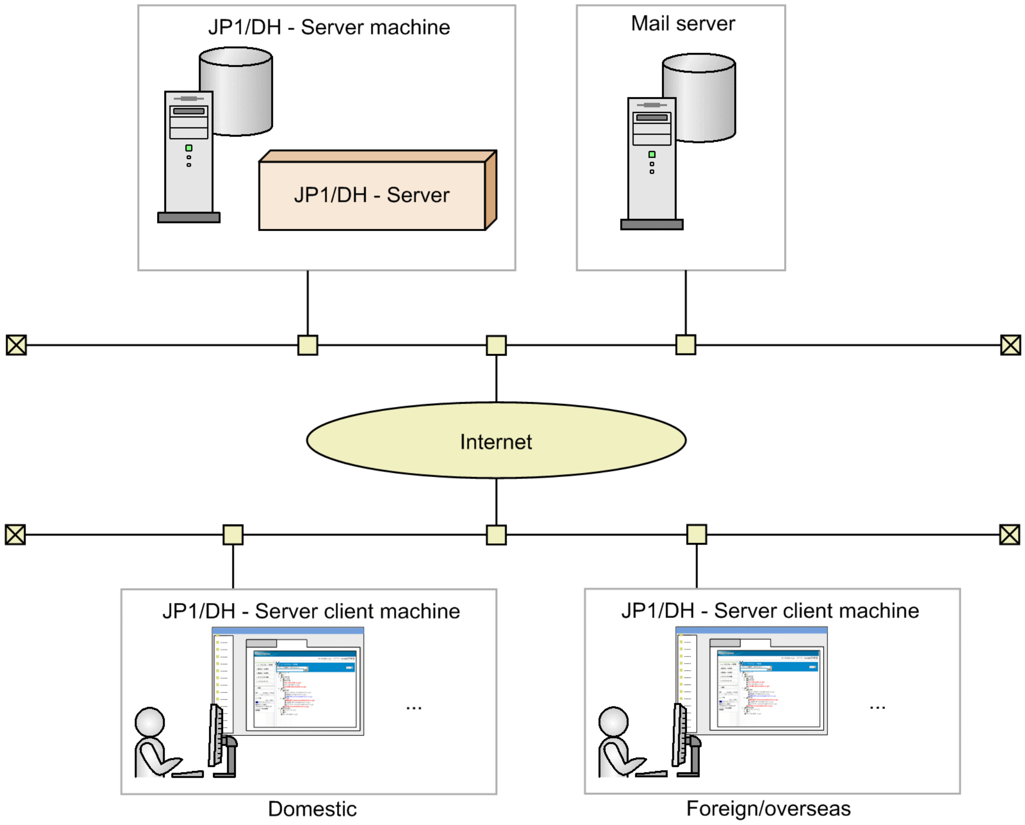
This manual aims to help the reader understand the basic tasks from installation to operation of JP1/DH - Server. The following table shows the workers that are assumed to be involved from installation to operation of JP1/DH - Server:

Worker	User authorities	Process	Details	Location in the manual
System administrator#	Administrators	Configure	Installs JP1/DH - Server and configures the system. The system administrator logs in to the computer where JP1/DH - Server will be installed as a built-in Administrator user.	*1.1* to *1.8*
	Administrators	Prepare to operate	Prepares JP1/DH - Server for day-to-day operation. The system administrator logs in to JP1/DH - Server using the fixed user ID `admin`.	*1.9* to *2.5*

Worker	User authorities	Process	Details	Location in the manual
System administrator#	Representative user (with user authorities for JP1/DH - Server)	Prepare to operate	Creates groups that are the units for managing users in JP1/DH - Server, and sets the policy (delivery policy) for sending data.	*2.6* to *2.7*
Domain-content manager	Representative user (with user authorities for JP1/DH - Server)	Prepare to operate	Determines how JP1/DH - Server will be used in a particular department. This includes what kind of policy to apply to data delivery, and who can authorize data delivery and under what conditions. To realize his or her objectives in terms of JP1/DH - Server usage, the domain-content manager sets elements such as delivery policies and users. The domain-content manager is an experienced employee at the department where JP1/DH - Server is installed.	*2.8* to *2.10*
General user	General user (with user authorities for JP1/DH - Server)	Operate	Uses JP1/DH - Server to send or receive data.	*Chapter 3*

#: The system administrator uses both the *Administrators* and *representative user* authorities.

The explanations in this manual assume the following system configuration. For operations other than this configuration, see the manuals indicated in *Appendix B.1 Related publications*.



JP1/DH - Server machine

Delivers large amounts of data at high speed. A JP1/DH - Server user accesses JP1/DH - Server to transmit and receive data. To obtain the best performance from JP1/DH - Server, in the JP1/DH - Server machine, install JP1/DH - Server only.

Note that in this manual, JP1/DH - Server is installed in the default installation folder for JP1/DH - Server.

Mail server

The mail server that is currently in operation is used. When delivering the data, JP1/DH - Server sends an email to notify the sender or recipient of the delivery status of the data.

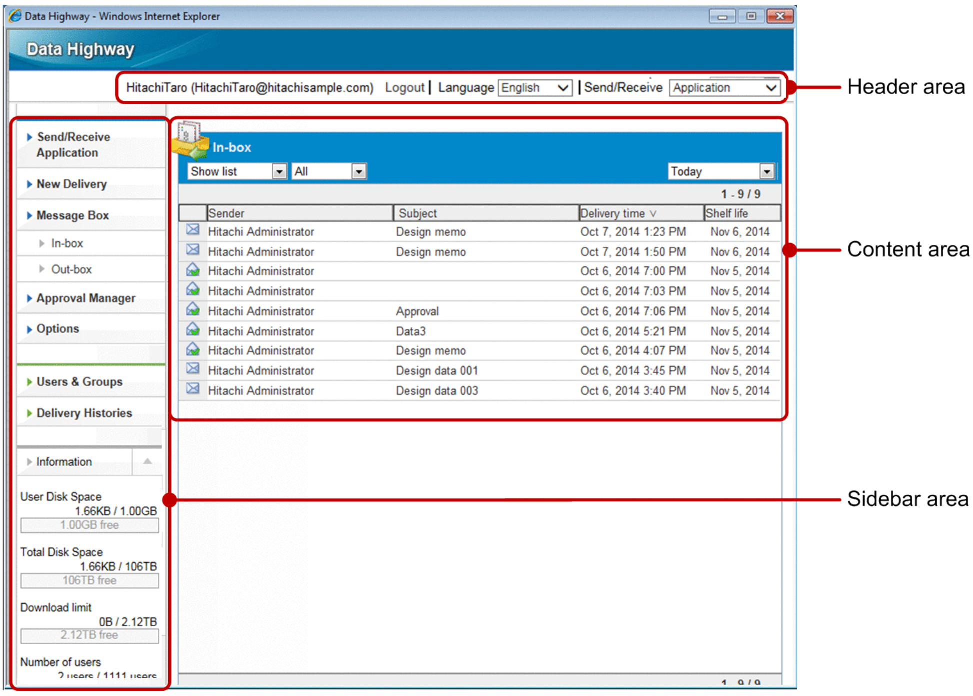
Internet

The Internet lines that are currently in operation are used. For improved communication security, JP1/DH - Server supports only SSL communication with HTTPS.

JP1/DH - Server client machines

All operations for delivering data in JP1/DH - Server can be performed by accessing JP1/DH - Server from a web browser, such as from your local machine.

Basic names in the JP1/DH - Server window:



HitachiTaro (HitachiTaro@hitachisample.com) | Language: English | Send/Receive: Application

1 - 9 / 9

Sender	Subject	Delivery time ∨	Shelf life
Hitachi Administrator	Design memo	Oct 7, 2014 1:23 PM	Nov 6, 2014
Hitachi Administrator	Design memo	Oct 7, 2014 1:50 PM	Nov 6, 2014
Hitachi Administrator		Oct 6, 2014 7:00 PM	Nov 5, 2014
Hitachi Administrator		Oct 6, 2014 7:03 PM	Nov 5, 2014
Hitachi Administrator	Approval	Oct 6, 2014 7:06 PM	Nov 5, 2014
Hitachi Administrator	Data3	Oct 6, 2014 5:21 PM	Nov 5, 2014
Hitachi Administrator	Design memo	Oct 6, 2014 4:07 PM	Nov 5, 2014
Hitachi Administrator	Design data 001	Oct 6, 2014 3:45 PM	Nov 5, 2014
Hitachi Administrator	Design data 003	Oct 6, 2014 3:40 PM	Nov 5, 2014

User Disk Space 1.66KB / 1.00GB (1.00GB free)

Total Disk Space 1.66KB / 106TB (106TB free)

Download limit 0B / 2.12TB (2.12TB free)

Number of users 2 users / 1111 users

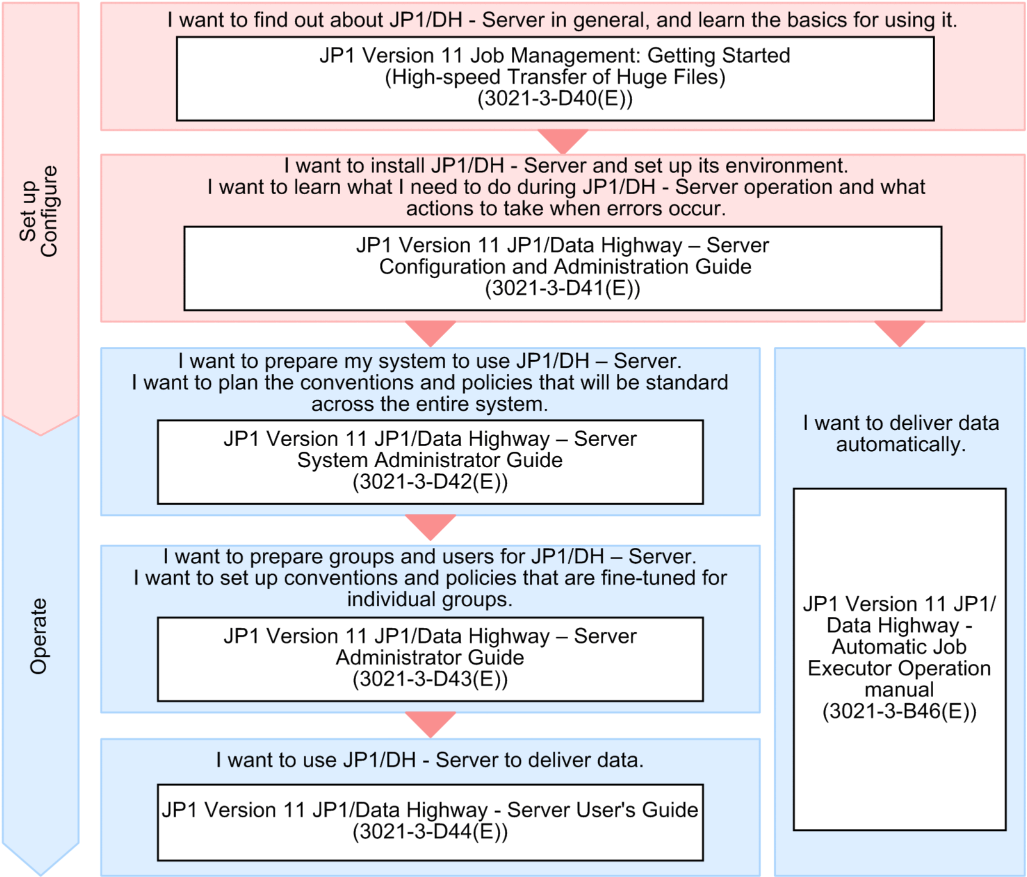
Header area

Content area

Sidebar area

■ How to read this manual

In addition to this manual, JP1/DH - Server manuals include the *Configuration and Administration Guide*, *System Administrator Guide*, *Administrator Guide*, *User's Guide*, and the *Automatic Job Executor Operation manual*. Refer to these manuals accordingly, as follows:


Set up
Configure
Operate
I want to find out about JP1/DH - Server in general, and learn the basics for using it.
JP1 Version 11 Job Management: Getting Started (High-speed Transfer of Huge Files) (3021-3-D40(E))
I want to install JP1/DH - Server and set up its environment.
I want to learn what I need to do during JP1/DH - Server operation and what actions to take when errors occur.
JP1 Version 11 JP1/Data Highway – Server Configuration and Administration Guide (3021-3-D41(E))
I want to prepare my system to use JP1/DH – Server.
I want to plan the conventions and policies that will be standard across the entire system.
JP1 Version 11 JP1/Data Highway – Server System Administrator Guide (3021-3-D42(E))
I want to prepare groups and users for JP1/DH – Server.
I want to set up conventions and policies that are fine-tuned for individual groups.
JP1 Version 11 JP1/Data Highway – Server Administrator Guide (3021-3-D43(E))
I want to use JP1/DH - Server to deliver data.
JP1 Version 11 JP1/Data Highway - Server User's Guide (3021-3-D44(E))
I want to deliver data automatically.
JP1 Version 11 JP1/ Data Highway - Automatic Job Executor Operation manual (3021-3-B46(E))

A reference to another manual is written as follows: For details about *something*, see *topic-title* in the *manual-name*. Using *topic-title* as a keyword, search for the relevant section in the target manual.

This manual assumes the following environment:

Operations on the JP1/DH - Server machine:

Windows Server 2012

Operations on the JP1/DH - Server client:

Windows 7

Internet Explorer 11

Some windows in this manual might differ from the windows of your product because of improvements made without prior notice.

■ Conventions: Fonts and symbols

The following table explains the text formatting conventions used in this manual:

Text formatting	Convention
Bold	Bold characters indicate text in a window, other than the window title. Such text includes menus, menu options, buttons, radio box options, or explanatory labels. For example: • From the **File** menu, choose **Open**. • Click the **Cancel** button.

Text formatting	Convention
Bold	• In the **Enter name** entry box, type your name.
Italic	Italic characters indicate a placeholder for some actual text to be provided by the user or system. For example: • Write the command as follows: `copy` *source-file target-file* • The following message appears: `A file was not found. (file =` *file-name*`)` Italic characters are also used for emphasis. For example: • Do *not* delete the configuration file.
`Monospace`	Monospace characters indicate text that the user enters without change, or text (such as messages) output by the system. For example: • At the prompt, enter `dir`. • Use the `send` command to send mail. • The following message is displayed: `The password is incorrect.`

The following table explains the symbols used in this manual:

Symbol	Convention
`|`	In syntax explanations, a vertical bar separates multiple items, and has the meaning of OR. For example: `A|B|C` means A, or B, or C.
`{ }`	In syntax explanations, curly brackets indicate that only one of the enclosed items is to be selected. For example: `{A|B|C}` means only one of A, or B, or C.
`[ ]`	In syntax explanations, square brackets indicate that the enclosed item or items are optional. For example: `[A]` means that you can specify `A` or nothing. `[B|C]` means that you can specify `B`, or `C`, or nothing.
`...`	In coding, an ellipsis (...) indicates that one or more lines of coding have been omitted. In syntax explanations, an ellipsis indicates that the immediately preceding item can be repeated as many times as necessary. For example: `A, B, B, ...` means that, after you specify `A, B,` you can specify B as many times as necessary.

■ Conventions: Version numbers

The version numbers of Hitachi program products are usually written as two sets of two digits each, separated by a hyphen. For example:

- Version 1.00 (or 1.0) is written as 01-00.
- Version 2.05 is written as 02-05.
- Version 2.50 (or 2.5) is written as 02-50.
- Version 12.25 is written as 12-25.

The version number might be shown on the spine of a manual as *Ver. 2.00*, but the same version number would be written in the program as *02-00*.

Contents

1 Setting up JP1/DH - Server

This chapter describes how to create an environment for using JP1/DH - Server to deliver data.

1.1 General procedure for setting up JP1/DH - Server

The table below shows the tasks required to create an environment for using JP1/DH - Server to deliver data.

Perform the tasks according to the order of the numbers shown in the table below. For details about each task, see the applicable reference.

Order	Task overview	Task details	Reference
1	Preparation before installation	Check the environment in which JP1/DH - Server will be set up.	*1.2.1*
2		Check required OSs.	*1.2.2*
3	Installing JP1/DH - Server	Install JP1/DH - Server.	*1.3*
4	Setting up the environment for JP1/DH - Server	Prepare the information required to set up the JP1/DH - Server environment.	*1.4.1*
5		Use the file digikatsuwide.xml to set up the environment.	*1.4.2*
6		Set Java heap memory sizes.	*1.4.3*
7		Set the maximum number of web client connections and the number of concurrent processes.	*1.4.4*
8		Apply the environment settings to JP1/DH - Server.	*1.4.5*
9		Define the IP address and host name of JP1/DH - Server in the hosts file.	*1.4.6*
10	Preparation for using SSL (HTTPS) communication	Create a server certificate for the test environment.	*1.5.1*
11		Create a server certificate for the production environment.	*1.5.2*
12	Setting the network configuration	Set the network configuration.	*1.6*
13	Starting JP1/DH - Server	Start JP1/DH - Server.	*1.7*
14	Checking the created environment	Verify that the environment settings of the machine on which JP1/DH - Server is installed are correct.	*1.8.1*
15		Verify that the network settings are correct.	*1.8.2*
16	Changing the password	Change the password of the system administrator.	*1.9*

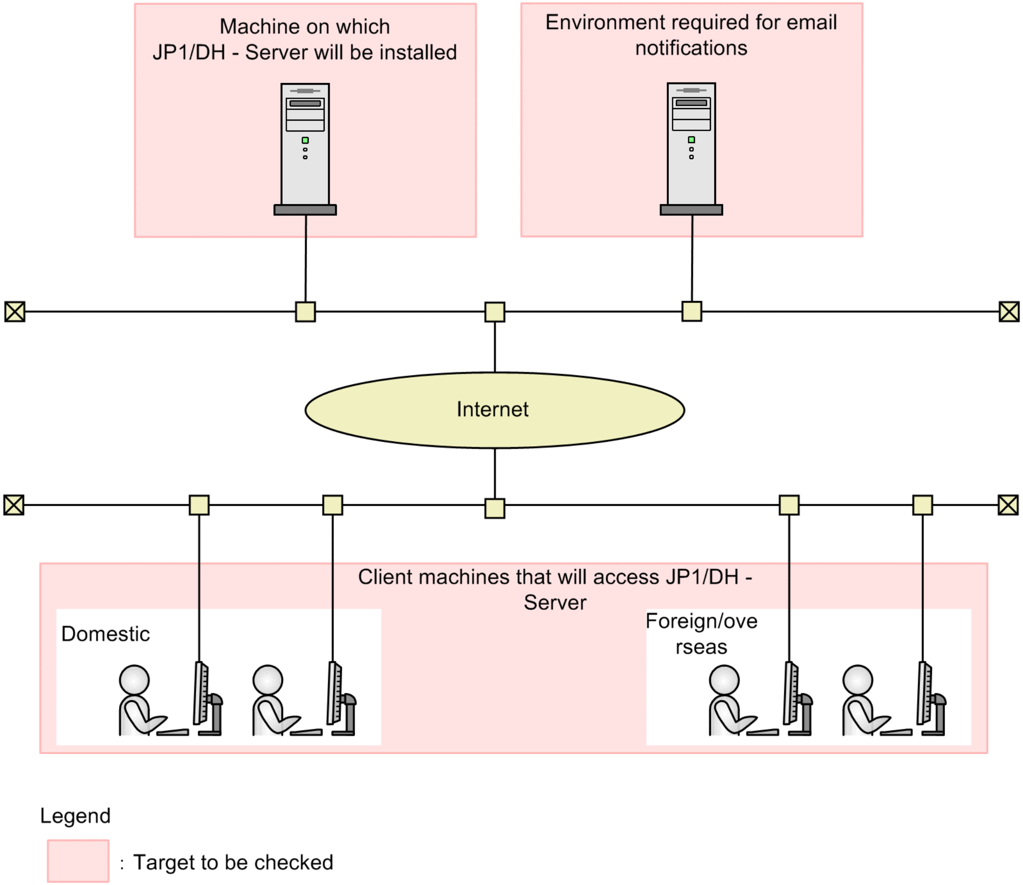
1.2 Preparation before installation

This section describes the preparation required before you install JP1/DH - Server.

1.2.1 Checking the environment in which JP1/DH - Server will be set up

Before you install JP1/DH - Server, check whether the following items are appropriate:

- Machine on which JP1/DH - Server will be installed
- Client machines that will access JP1/DH - Server
- Environment required for email notifications


Machine on which JP1/DH - Server will be installed
Environment required for email notifications
Internet
Client machines that will access JP1/DH - Server
Domestic
Foreign/overseas
Legend
: Target to be checked

(1) Checking the environment of the machine on which JP1/DH - Server will be installed

Check whether the environment of the machine on which JP1/DH - Server will be installed is appropriate.

Procedure

1. Prepare a dedicated server machine.

   Prepare a dedicated server machine for JP1/DH - Server. To enable JP1/DH - Server to provide its highest performance when delivering large amounts of data, avoid using JP1/DH - Server and other systems on the same machine.

2. Check the CPU performance. (Verify that the CPU is a dual core 64-bit CPU running at 2.4 GHz or higher.)

3. Verify that the amount of memory is 3.0 GB or more.

4. Verify that the required amount of disk space meets the conditions below.
   The disk space requirements assume the values in the following table:

Item	Assumed value
Number of users	100
Size of exchanged data	100.0 MB to 1.0 GB
Number of data items exchanged per day	100 (at a maximum)
Total size of files delivered per day	100.0 GB (at a maximum)
Data storage period	31 days

   - Installation folder: `C:\Program Files\Hitachi\jp1dh\server\`
     Disk space for application installation: 2.0 GB or more
   - Storage folder for delivery data: `C:\Program Files\Hitachi\jp1dh\server\data\`
     Disk space required to store delivery data: 3.5 TB or more#
     #:
     If you are merely trying out the software, at least 300 GB is sufficient. In this case, the data storage period will be approximately 3 days (assuming the size and number of files being stored remains unchanged). If the amount of data delivered exceeds the disk space for storing delivery data, no further data can be delivered. Data for which the storage period has been exceeded is deleted from the folder and can no longer be downloaded.
   - Disk space required for database while JP1/DH - Server is running: at least 80.5 MB
   - Disk space for log data storage: at least 5.0 GB

5. Verify that the network interface speed is 1.0 Gbps or higher.

6. Verify that no file or folder named `Program` exists in the installation target machine.
   If a file or folder named `Program` exists under the root of the system drive, the program will not run properly. If such a file or folder exists, delete it before you install JP1/DH - Server.

7. Verify that PostgreSQL is not installed and that no postgres user accounts are in the installation target machine.
   If PostgreSQL is installed on the machine, uninstall it before you install JP1/DH - Server.
   If postgres user accounts exist in the machine, delete them before you install JP1/DH - Server.

> **Important**
>
> In Windows Server 2012 ,Windows Server 2012 R2 and Windows Server 2016, Microsoft .NET Framework 3.5 must be installed to use the command prompt with the elevated privileges, which is installed together with JP1/DH - Server. For details about how to install Microsoft .NET Framework 3.5, see *Installing .NET Framework 3.5* in the *JP1/Data Highway - Server Configuration and Administration Guide*.

Related topics

- *Installing .NET Framework 3.5* in the *JP1/Data Highway - Server Configuration and Administration Guide*

(2) Checking the environments of the client machines that will access JP1/DH - Server

Verify that the environments of the machines that will access JP1/DH - Server are appropriate.

Procedure

1. Check the CPU performance. (Verify that the CPU is a dual core CPU running at 2.4 GHz or higher.)

2. Verify that the amount of memory is 3.0 GB or more.

3. Verify that the disk space available for applet log output meets the conditions below.
   The disk space for applet log output assumes the following values:

Item	Assumed value
Number of data items exchanged per day	1
Delivery data file size	1,000.0 MB (at a maximum)

   Disk space available for applet log# output: 840.0 MB or more

   #: Applet logs are output when client machines communicate with JP1/DH - Server.

4. Verify that the network interface speed is 100.0 Mbps or higher.

(3) Checking and determining the environment required for email notifications

Check and determine the environment required to use email notifications on JP1/DH - Server.

Procedure

1. Check the mail server used by the system.

   In the environment in which JP1/DH - Server will be installed, verify that the mail server that is currently in operation supports SMTP.

   JP1/DH - Server sends email notifications to users to report information such as the delivery status of data. Therefore, the mail server used by the system must support SMTP.

2. Determine the sender's email address.

   Determine the sender's email address for the email notifications sent from JP1/DH - Server to users. This email address is set in the sender field of the email notifications that are received by JP1/DH - Server users.

Postrequisites

- Check the OSs required for both the machine on which JP1/DH - Server will be installed and the client machines that will access JP1/DH - Server.
- Check the web browsers that can be used on the client machines.

Related topics

- *1.2.2 Checking required OSs*

1.2.2 Checking required OSs

Check the OSs required for both the machine on which JP1/DH - Server will be installed and the client machines that will access JP1/DH - Server.

In addition, check the web browsers that can be used on the client machines.

Procedure

1. Verify that the machine on which JP1/DH - Server is to be installed is running one of the following OSs:
   - Windows Server 2012
   - Windows Server 2012 R2
   - Windows Server 2016
   - Linux 6 (x64)

   In this manual, the operating system used in the installation procedure is Windows Server 2012.

2. Verify that the OS on each JP1/DH - Server client machine is one of the following OSs:
   - Windows 7
   - Windows 8.1
   - Windows 10
   - OS X Yosemite v10.10
   - OS X El Capitan v10.11
   - macOS 10.12 (Sierra)
   - macOS 10.13 (High Sierra)

   In this manual, the operating procedures given are for Windows 7.

3. Verify that the web browser of each JP1/DH - Server client machine is one of the following web browsers:
   - Internet Explorer 11[#1, #2]
   - Microsoft Edge
   - Mozilla Firefox(R) ESR 60
   - Google Chrome 52 or later
   - Safari 8
   - Safari 9
   - Safari 10
   - Safari 11

   In this manual, the operating procedures given are for Internet Explorer 11.

   #1: If Internet Explorer is used, you must enable the following functionality:
   - Cookies
   - JavaScript (including the Ajax and DOM functions)
   - Cascading style sheets (CSS)
   - SSL communication (encrypted HTTP communication)
   - Java applets

If the web pages are not displayed correctly due to an error such as a page layout error, change the on or off state of Compatibility View Settings in addition to enabling the above functionality.

#2: If Internet Explorer is used, specify the following web browser setting:

- Disable the enhanced protected mode
- Add the URL of this server to trusted sites and disable the protected mode for trusted sites.

> **Important**
>
> For the version of the Java software to be installed, follow the message that appears when each JP1/DH - Server client machine accesses JP1/DH - Server.

> **Note**
>
> The OS versions in this manual are accurate as of October 2018. For details about the latest OS version requirements, see the prerequisites in the *JP1/Data Highway - Server Configuration and Administration Guide* and the *JP1/Data Highway - Server System Administrator Guide*.

Postrequisites

Install JP1/DH - Server.

Related topics

- *1.3 Installing JP1/DH - Server*
- Prerequisites in the *JP1/Data Highway - Server Configuration and Administration Guide*
- Prerequisites in the *JP1/Data Highway - Server System Administrator Guide*

1.3 Installing JP1/DH - Server

Use the Hitachi Integrated Installer and follow the wizard to install JP1/DH - Server.

Procedure

1. The system administrator logs in as the built-in Administrator user to the machine on which JP1/DH - Server will be installed.

2. Exit all Windows programs (recommended).

3. Insert the Hitachi Integrated Installer distribution media that contains JP1/DH - Server, and then start the Hitachi Integrated Installer.

4. In the Hitachi Integrated Installer, select **JP1/Data Highway - Server**, and then click the **Install** button.

5. Enter the user information.

6. Verify that the installation destination folder is as follows:
   `C:\Program Files\Hitachi\jp1dh\server\`

7. In the Ready to Install window, check the entered content.

8. Click the **Install** button.
   The installation of JP1/DH - Server starts.

9. When the InstallShield Wizard Complete window appears, click the **Finish** button.

10. Click the **Finish** button to exit the Hitachi Integrated Installer.

Postrequisites

After JP1/DH - Server is installed, set the environment.

Related topics

- *1.4 Setting up the environment for JP1/DH - Server*

1.4 Setting up the environment for JP1/DH - Server

After JP1/DH - Server is installed, set up the environment required to operate JP1/DH - Server.

1.4.1 Preparing the information required to set up the JP1/DH - Server environment

By gathering the information you need to set up the JP1/DH - Server environment before starting the setup process, you can ensure that the rest of the process goes smoothly.

The following information is needed when setting up the JP1/DH - Server environment:

- The location of the `digikatsuwide.xml`, `usrconf.cfg`, and `usrconf.properties` files to be used during environment setup
- The IP address of the machine on which JP1/DH - Server is installed
- The host name and port number of the mail server that is currently in operation
- The sender address in email that JP1/DH - Server sends to users
- The FQDN and domain name of the server
- The absolute path of the storage folder for delivery data
- The network bandwidth available to JP1/DH - Server
- The maximum size of files JP1/DH - Server can deliver
- The size of the Java heap memory
- The maximum number of web clients that can connect to JP1/DH - Server, and the number of requests from web clients that JP1/DH - Server can process concurrently

Postrequisites

Use the `digikatsuwide.xml` file to set up the environment.

Related topics

- *1.4.2 Using the file digikatsuwide.xml to set up the environment*
- *1.4.3 Setting Java heap memory sizes*
- *1.4.4 Setting the maximum number of web client connections and the number of concurrent processes*

1.4.2 Using the file digikatsuwide.xml to set up the environment

According to the procedure below, edit the `digikatsuwide.xml` file to set the server IP address, the mail server, the sender's email address to be used for email notifications, the FQDN and domain name of the server, the storage folder for delivery data, network bandwidth limits, and the maximum size of files available for transfer.

Prerequisites

To perform this task, the system administrator logs in as the built-in Administrator user to the machine on which JP1/DH - Server is installed.

Procedure

1. Use a text editor to open the `digikatsuwide.xml` file.

   The `digikatsuwide.xml` file is stored in the following location:

   installation-folder`\misc\digikatsuwide\digikatsuwide\WEB-INF`

2. Set the server IP address.

   Set the IP address of the machine on which JP1/DH - Server is installed.

```
<end-point>
    <ip>server-IP-address#</ip>
</end-point>
<end-point protocol="https">
    <ip>server-IP-address#</ip>
</end-point>
```

   #

   To make the server accessible from the Internet, specify a global IP address (for example, `192.168.0.2`).

3. Set the mail server.

   Set the host name and port number of the mail server that is currently in operation. For *sender's-email-address*, set the sender's email address for the email notifications that are sent to users by JP1/DH - Server to report information such as the delivery status of data.

```
<mail-notification>
    <mail-server>
        <host>mail-server-host-name</host>
        <port>mail-server-port-number</port>
    </mail-server>
    <notification-from>
        <system-address>sender's-email-address</system-address>
    </notification-from>
    :
</mail-notification>
```

4. Set the FQDN and domain name of the server.

   Set the fully qualified domain name (FQDN) and domain name of the machine on which JP1/DH - Server is installed.

```
<biz-connect id="bizconnect">
    <service>
        :
        <bind-hostname>server-FQDN</bind-hostname>
        <bind-domainname>server-domain-name</bind-domainname>
        <bind-sub-domainname>server-subdomain-name</bind-sub-domainname>
        :
    </service>
</biz-connect>
```

Important

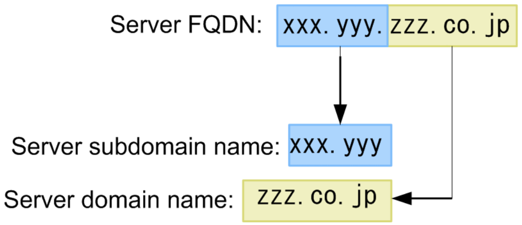
- Do not use an underscore (_) in the host name (the server FQDN). Doing so might cause a malfunction.

- If the FQDN or domain name of the server is invalid, the operation after logging in to JP1/DH - Server will not work properly. Make sure that no problems exist with the settings.

Tip

Structure of domain and subdomain names

A server FQDN consists of the following two parts: the domain name part and the subdomain name part.



For example, if a server FQDN is `jp1dhserver.foo1.foo2.co.jp`, the server domain name is `foo2.co.jp`, and the server subdomain name is `jp1dhserver.foo1`. In this example, set values in the `digikatsuwide.xml` file as follows:

```
<biz-connect id="bizconnect">
<service>
:
<bind-hostname>jp1dhserver.foo1.foo2.co.jp</bind-hostname>
<bind-domainname>foo2.co.jp</bind-domainname>
<bind-sub-domainname>jp1dhserver.foo1</bind-sub-domainname>
:
</service>
</biz-connect>
```

5. Set the storage folder for delivery data.

Set the folder for storing the data transmitted by JP1/DH - Server. The folder for storing delivery data is as follows: `C:\Program Files\Hitachi\jp1dh\server\data\`.

```
<biz-connect id="bizconnect">
    :
    <persistence>
        <storage>
            <directory>C:\Program Files\Hitachi\jp1dh\server\data\</
directory>
        </storage>
    </persistence>
    :
</biz-connect>
```

Important

You cannot use any network folder or any folder on a network drive as the storage folder for delivery data.

6. Set network bandwidth limits.

   Set the network bandwidth to be used by JP1/DH - Server.

```
<biz-connect id="bizconnect">
    <service>
        :
        <throughput-limit>
            <upload>maximum-transmission-bandwidth-for-uploading#</upload>
            <download>maximum-transmission-bandwidth-for-downloading#</
download>
        </throughput-limit>
        :
    </service>
</biz-connect>
```

   #

   The network bandwidth values are in Mbps.

   Specify a value in the range from 0 to 1,000. You cannot omit these values.

   The value `0` means *no bandwidth limit*.

   Important

   - Set the network bandwidth by considering the need for balance with other business operations. In the test and evaluation phrases, verify that the specified values are appropriate.
   - For the network bandwidth values, specify values within the range of the network bandwidth available on actual network lines. Even if you set a value that exceeds the range of the network bandwidth available on actual network lines, no error occurs, but the network bandwidth that can be used by JP1/DH - Server is limited to the network bandwidth of actual network lines.

7. Set the maximum size of files available for transfer.

   Set the maximum size of files that can be delivered per delivery and the maximum file size per file. Set these values by considering the content of your business.

```
<biz-connect id="bizconnect">
    <service>
      :
      <data-capacity>
        <per-file>maximum-size-per-delivery#</per-file>
        <per-delivery>maximum-file-size-per-file#</per-delivery>
      </data-capacity>
      :
    </service>
    :
</biz-connect>
```

   #

   The unit is GB.

   Set a value in the range from 1 to 1,024.

   Make sure that you specify the values. If you omit them, startup of JP1/DH - Server will fail.

Postrequisites

Set Java heap memory sizes in the `usrconf.cfg` file.

Related topics

- *1.4.3 Setting Java heap memory sizes*

1.4.3 Setting Java heap memory sizes

Open the `usrconf.cfg` file and then set the minimum and maximum sizes of Java heap memory, according to the procedure below.

Prerequisites

To perform this task, the system administrator logs in as the built-in Administrator user to the machine on which JP1/DH - Server is installed.

Procedure

1. Use a text editor to open the `usrconf.cfg` file.

   The `usrconf.cfg` file is stored in the following location:

   installation-folder`\misc\CC\server\usrconf\ejb\jp1dh`

2. Set Java heap memory sizes.

```
#------ JP1/DH - Server ---------
add.jvm.arg=-Xmsminimum-Java-heap-memory-size#m
add.jvm.arg=-Xmxmaximum-Java-heap-memory-size#m
```

   #

   Specify the memory sizes in MB.

   Specify 1,024 MB or more as the maximum size.

   We recommend that you specify the same value for the minimum and maximum sizes.

   > **Tip**
   >
   > Set the Java heap memory sizes by considering the transmission speed and the size of the files to be sent.
   >
   > Monitor the usage of Java heap memory during operation and, if necessary, revise the size of Java heap memory.

Postrequisites

In the `usrconf.properties` file, set the maximum number of web clients that can connect to JP1/DH - Server and the number of web client requests that JP1/DH - Server can process concurrently.

Related topics

- *1.4.4 Setting the maximum number of web client connections and the number of concurrent processes*

1.4.4 Setting the maximum number of web client connections and the number of concurrent processes

Open the `usrconf.properties` file, and then set the maximum number of web clients that can connect to JP1/DH - Server and the number of web client requests that JP1/DH - Server can process concurrently, according to the procedure below.

Prerequisites

To perform this task, the system administrator logs in as the built-in Administrator user to the machine on which JP1/DH - Server is installed.

Procedure

1. Use a text editor to open the `usrconf.properties` file.

   The `usrconf.properties` file is stored in the following location:

   installation-folder`\misc\CC\server\usrconf\ejb\jp1dh`

2. Set the maximum number of web client connections and the number of concurrent request processes.

```
#------ JP1/DH - Server ---------
webserver.connector.inprocess_http.max_connections=maximum-number-of-web-
client-connections#1
webserver.connector.inprocess_http.max_execute_threads=
number-of-concurrent-request-processes#2
```

#1

The value that can be specified for the maximum number of web client connections is 1,024 or fewer.

#2

For the number of concurrent request processes, set a value that does not exceed the maximum number of web client connections.

Postrequisites

Execute batch commands to apply the environment settings to JP1/DH - Server.

Related topics

- *1.4.5 Applying the environment settings to JP1/DH - Server*

1.4.5 Applying the environment settings to JP1/DH - Server

After you edit the environment configuration file, apply the settings to JP1/DH - Server according to the procedure below. The batch commands used in these operations are stored in the following folder:

installation-folder`\setup_util`

Prerequisites

To perform this task, the system administrator logs in as the built-in Administrator user to the machine on which JP1/DH - Server is installed.

Procedure

1. Execute `start_webcon.bat` to start JP1/DH - Server.

   When `start_webcon.bat` runs, the command prompt starts. Follow the given instructions.

   If the message below appears, JP1/DH - Server is running normally. Leave the command prompt open and go to the next step.

   ```
   KDJE30028-I The J2EE server has started. Server name = jp1dh
   ```

2. Execute `prepare_deploy.bat` to prepare to apply the environment settings.

   When `prepare_deploy.bat` runs, the command prompt starts and gives instructions. Follow the given instructions to perform operations. After you finish all operations, go to the next step.

3. Execute `stop_webcon.bat` to stop JP1/DH - Server.

   When `stop_webcon.bat` runs, the command prompt starts and gives instructions. If JP1/DH - Server stops normally, a message indicating that JP1/DH - Server stopped normally appears in the command prompt that started in step 1.

4. Perform step 1 again to start JP1/DH - Server.

5. Execute `deploy_app.bat` to apply the environment settings to JP1/DH - Server.

   When `deploy_app.bat` runs, the command prompt starts. Follow the given instructions to perform operations. After you finish all operations, go to the next step.

6. Execute `stop_webcon.bat` to stop JP1/DH - Server.

   When `stop_webcon.bat` runs, the command prompt starts. Follow the given instructions. If JP1/DH - Server stops normally, a message indicating that JP1/DH - Server stopped normally appears in the command prompt that started in step 3.

Postrequisites

- If all batch operations executed without errors, the environment settings have been applied to JP1/DH - Server. Next, add the IP address and host name of JP1/DH - Server to the hosts file.
- If a batch execution error occurred, a problem exists with the environment settings. Check whether the settings are correct, and then apply them to JP1/DH - Server again.

Related topics

- *1.4 Setting up the environment for JP1/DH - Server*
- *1.4.6 Defining the IP address and host name of JP1/DH - Server in the hosts file*

1.4.6 Defining the IP address and host name of JP1/DH - Server in the hosts file

After the environment settings can be applied to JP1/DH - Server, edit the hosts file. Note that you do not need to restart JP1/DH - Server after you edit the hosts file.

Prerequisites

To perform this task, the system administrator logs in as the built-in Administrator user to the machine on which JP1/DH - Server is installed.

Procedure

1. Use a text editor to open the hosts file.
   The hosts file is stored in the following location:
   `C:\WINDOWS\system32\drivers\etc`

2. Define the IP address and host name (FQDN) of the server.
   For the IP address, specify a server-specific IPv4 address. Do not specify a loopback address (`127.0.0.1`).

Postrequisites

Prepare to use SSL (HTTPS) communication.

Related topics

- *1.5 Preparation for using SSL (HTTPS) communication*

1.5 Preparation for using SSL (HTTPS) communication

A server certificate for SSL (HTTPS) communication is required to operate JP1/DH - Server on networks. Considering the period required from the application to the acquisition of a server certificate for SSL (HTTPS) communication, obtain the server certificate before JP1/DH - Server starts in the production environment. Until JP1/DH - Server starts in the production environment, you can use a self-signed server certificate instead to access JP1/DH - Server and create an operation environment on the intranet, and to perform tests and evaluations.

> **Tip**
>
> It might take a long time to obtain the server certificate. A self-signed server certificate can be used only for operations in the test environment, but can be used immediately after it is created. Create a self-signed server certificate first, and then prepare the official server certificate before JP1/DH - Server starts in the production environment.
>
> When JP1/DH - Server is to start in the production environment, replace the self-signed server certificate with the formal server certificate.

Related topics

- *1.5.1 Creating a server certificate for the test environment*
- *1.5.2 Creating a server certificate for the production environment*

1.5.1 Creating a server certificate for the test environment

During the test operation period, create the certificate to be used instead of the server certificate. This certificate is called a *self-signed server certificate*. A secret key and a certificate signing request (CSR) are required to create a self-signed server certificate.

(1) Creating a secret key for the test environment

Create a secret key required to create a self-signed server certificate.

Prerequisites

To perform this task, the system administrator logs in as the built-in Administrator user to the machine on which JP1/DH - Server is installed, and then starts the command prompt.

Procedure

1. Start the command prompt.
   Start the command prompt at the following location, in which the batch command for creating a secret key is stored:
   installation-folder`\bin\`

2. Execute `selfsignedkeygen.bat` with necessary arguments specified.

   ```
   selfsignedkeygen.bat
     -out secret-key-file-name
     [-bits {512|1024|2048|4096}]
   ```

   The following are details of the arguments:

`-out` *secret-key-file-name*

Specify the name of the file to which the created secret key is output.

`[-bits {512|1024|2048|4096}]`

Specify the bit length of the secret key to be created.

If you omit this argument, `2048` is used.

Keys with a bit length of `1024` or lower are becoming more dangerous with decreased safety. Therefore, specify `2048` or higher for the bit length.

Operation result

The secret key file with the name specified for `-out` is created.

(2) Creating a certificate signing request (CSR) for the test environment

Create a certificate signing request (CSR) required to create a self-signed server certificate.

Prerequisites

- To perform this task, the system administrator logs in as the built-in Administrator user to the machine on which JP1/DH - Server is installed, and then starts the command prompt.
- A secret key must be created beforehand.

Procedure

1. Start the command prompt.

   Start the command prompt at the following location, in which the batch command for creating a certificate signing request (CSR) is stored:

   installation-folder`\bin\`

2. Execute `selfsignedcertreq.bat` with necessary arguments specified.

   ```
   selfsignedcertreq.bat
     -key key-file-name
     -out CSR-file-name
     -subject "subject"
   ```

   The following are details of the arguments:

   `-key` *key-file-name*

   Specify the name of the secret key file that was created beforehand.

   `-out` *CSR-file-name*

   Specify the name of the file to which the created certificate signing request (CSR) is output.

   `-subject "`*subject*`"`

   Specify a server certificate subject name.

   The following is the format of a server certificate subject name:

   ```
   "/C=two-letter-country-code(JP for Japan)/ST=state-or-province-name/
   L=city-or-area-name/O=organization-name/OU=organization-unit-name/
   CN=server-host-name-(FQDN)"
   ```

   The following is an example of how to specify a subject name:

```
"/C=JP/ST=Tokyo/L=Shinagawa-ku/O=HitachiLtd./OU=SoftwareDevelopment/
CN=jp1dhserver.foo1.foo2.co.jp"
```

Important

You can specify values with alphanumeric characters and the following symbols:

A half space, period (`.`), hyphen (`-`), and a half comma (,)

You cannot use a forward slash (`/`).

Operation result

The certificate signing request (CSR) file with the name specified for `-out` is created.

(3) Creating a self-signed server certificate for the test environment

Create a self-signed server certificate.

Prerequisites

- To perform this task, the system administrator logs in as the built-in Administrator user to the machine on which JP1/DH - Server is installed, and then starts the command prompt.
- A secret key and a certificate signing request (CSR) must be created beforehand.

Procedure

1. Start the command prompt.

   Start the command prompt at the following location, in which the batch command for creating a self-signed server certificate is stored:

   installation-folder`\bin\`

2. Execute `selfsigned.bat` with necessary arguments specified.

```
selfsigned.bat
  -in CSR-file-name
  -out certificate-file-name
  [-sign {MD5|SHA1|SHA224|SHA256|SHA384|SHA512}]
  -signkey key-file-name
  -days number-of-days-of-validity
```

   The following are details of the arguments:

   `-in` *CSR-file-name*

   Specify the name of the certificate signing request (CSR) file that was created beforehand.

   `-out` *certificate-file-name*

   Specify the name of the file to which the created self-signed server certificate is output.

   `[-sign {MD5|SHA1|SHA224|SHA256|SHA384|SHA512}]`

   Specify the signature algorithm used for creating a self-signed server certificate. If you omit this operand, the underlined signature algorithm is used.

   - MD5: Use md5WithRSAEncryption.

   - SHA1: Use sha1WithRSAEncryption.

- SHA224: Use sha224WithRSAEncryption.
- SHA256: Use sha256WithRSAEncryption.
- SHA384: Use sha384WithRSAEncryption.
- SHA512: Use sha512WithRSAEncryption.

If you omit this operand, the underlined signature algorithm is used.

> **Important**
>
> The signature algorithms `MD5` and `SHA1` are becoming more dangerous with decreased safety. Therefore, specify a value other than them.

`-signkey` *key-file-name*

Specify the name of the secret key file that was created beforehand.

`-days` *number-of-days-of-validity*

Specify the validity period of the created self-signed server certificate, in units of days. Note that the command execution date and time are automatically set as the starting date and time of the validity period, and cannot be changed.

Operation result

The self-signed server certificate file is created with the name specified for `-out`.

Postrequisites

- If the self-signed server certificate is used to start JP1/DH - Server in the test environment, set the network configuration and install the self-signed server certificate in JP1/DH - Server.
- If you prepare to start JP1/DH - Server in the production environment, create a server certificate.

Related topics

- *1.6 Setting the network configuration*
- *1.5.2 Creating a server certificate for the production environment*

1.5.2 Creating a server certificate for the production environment

To start JP1/DH - Server operation on the Internet, you must obtain a server certificate and install it in JP1/DH - Server.

To obtain a server certificate, prepare a secret key and a certificate signing request (CSR) first.

(1) Creating a secret key for the production environment

Create a secret key required to create a server certificate.

Prerequisites

To perform this task, the system administrator logs in as the built-in Administrator user to the machine on which JP1/DH - Server is installed, and then starts the command prompt.

Procedure

1. Start the command prompt.

   Start the command prompt at the following location, in which the command for creating a secret key is stored:

installation-folder`\uCPSB\httpsd\sbin`

2. Execute the `openssl.bat` command with the necessary arguments specified.

```
openssl.bat genrsa -rand file-name [:file-name…]
      [-des|-des3]
       -out key-file-name
      [512|1024|2048|4096]
```

The following are details of the arguments:

`-rand` *file-name[:file-name…]*

Specify the name of any file to be used for generating a random number. You can specify only one file name. Specify a file of adequate size as the file for generating a random number.

The following is an example of how to specify a file name:

installation-folder`\misc\digikatsuwide\digikatsuwide\WEB-INF\digikatsuwide.xml`

`[-des|-des3]`

To encrypt a secret key, specify the encryption type.

This encryption type has nothing to do with the encryption type for SSL communication between the JP1/DH - Server and a Web browser.

`-des`

When -des is specified, DES (Data Encryption Standard) is selected for the encryption type.

`-des3`

When -des3 is specified, Triple DES is selected.

If you specify this operand, you are required to enter your password when you create a secret key, create a certificate signing request (CSR), or start the JP1/DH - Server.

If you want to enable automatic password# entry for starting the JP1/DH - Server, see the prerequisites in the *JP1/Data Highway - Server Configuration and Administration Guide*.

# You can enter a password from 4 to 64 characters. If you enter a password less than 4 characters, a message appears, prompting you to enter a password from 4 to 1,023 characters long. Even so, remember that your password must be from 4 to 64 characters long. Particular care must be exercised to ensure that your password does not exceed 64 characters because, even if it does, no error is output.

`-out` *key-file-name*

Specify the name of the file to which the created secret key is output.

`[512|1024|2048|4096]`

Specify the bit length of the secret key to be created.

If you omit this argument, `2048` is used.

Keys with a bit length of `1024` or lower are becoming more dangerous with decreased safety. Therefore, specify `2048` or higher for the bit length.

Operation result

The secret key file with the name specified for `-out` is created.

(2) Creating a certificate signing request (CSR) for the production environment

Create a certificate signing request (CSR) required to create a server certificate.

Prerequisites

- To perform this task, the system administrator logs in as the built-in Administrator user to the machine on which JP1/DH - Server is installed, and then starts the command prompt.
- A secret key must be created beforehand.

Procedure

1. Start the command prompt.

   Start the command prompt at the following location, in which the command for creating a CSR is stored:

   installation-folder`\uCPSB\httpsd\sbin`

2. Execute the `openssl.bat` command with the necessary arguments specified.

```
openssl.bat req -new [-md5|-sha1|-sha224|-sha256|-sha384|-sha512]
                  -key key-file-name
                  -out CSR-file-name
```

The following are details of the arguments:

`[-md5|-sha1|-sha224|-sha256|-sha384|-sha512]`

Specify the signature algorithm used for creating a CSR. If you omit this operand, the underlined signature algorithm is used.

`md5`: Use md5WithRSAEncryption.

`sha1`: Use sha1WithRSAEncryption.

`sha224`: Use sha224WithRSAEncryption.

`sha256`: Use sha256WithRSAEncryption.

`sha384`: Use sha384WithRSAEncryption.

`sha512`: Use sha512WithRSAEncryption.

> **Important**
>
> The signature algorithms `md5` and `sha1` are becoming more dangerous with decreased safety. Therefore, specify the signature algorithms value other than.

`-key` *key-file-name*

Specify the name of the secret key file that was created beforehand.

`-out` *CSR-file-name*

Specify the name of the file to which the created CSR is output.

Enter the values for the required items, in interactive mode.

```
C(Country Name) : two-letter-country-code (JP for Japan)
S(State or Province Name) : state-or-province-name
L(Locality Name) : city-or-area-name
O(Organization Name) : organization-name
OU(Organization Unit Name) : organization-unit-name
CN(Common Name) : server-host-name-(FQDN)
EA(Email Address) : email-address
```

The following is a specification example:

```
C(Country Name) : JP
S(State or Province Name) : Tokyo
```

```
L(Locality Name) : Shinagawa-ku
O(Organization Name) : Hitachi,Ltd.
OU(Organization Unit Name) : SoftwareDevelopment
CN(Common Name) : jp1dhserver.foo1.foo2.co.jp
EA(Email Address) : jp1dh-system@foo1.foo2.co.jp
```

Operation result

The certificate signing request (CSR) file with the name specified for `-out` is created.

(3) Obtaining a server certificate for the production environment

Obtain a server certificate before JP1/DH - Server starts in the production environment.

Procedure

1. After a certificate signing request (CSR) is created, request a certificate authority to issue a server certificate and conduct the procedures required to obtain a server certificate.
   These tasks must be complete before JP1/DH - Server starts in the production environment.

2. After you obtain a server certificate, store it in any location on the machine on which JP1/DH - Server is installed.

Postrequisites

Set the network configuration, and install the server certificate in JP1/DH - Server.

Related topics

- *1.6 Setting the network configuration*

1.6 Setting the network configuration

Edit the `httpsd.conf` file to install a server certificate for SSL (HTTPS) communication and enable access from client machines to JP1/DH - Server.

Prerequisites

- To perform this task, the system administrator logs in as the built-in Administrator user to the machine on which JP1/DH - Server is installed.
- A secret key and server certificate for the test or production environment must be prepared beforehand.

Procedure

1. Use a text editor to open the `httpsd.conf` file.

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

   installation-folder`\misc\httpsd\conf`

2. For `SSLCertificateFile`, specify the path of the server certificate.

   ```
   SSLCertificateFile "server certificate-file-path"
   ```

   Specify the path of the server certificate file for the test or production environment. Do not use multi-byte characters or Unicode supplementary characters in the file path.

3. For `SSLCertificateKeyFile`, specify the path of the secret key.

   ```
   SSLCertificateKeyFile "secret-key-file-path"
   ```

   Specify the path of the secret key file for the test or production environment. Do not use multi-byte characters or Unicode supplementary characters in the file path.

4. For `ProxyPass` and `ProxyPassReverse`, specify the server host name.

   ```
   ProxyPass / http://server-host-name-(FQDN)/
   ProxyPassReverse / http://server-host-name-(FQDN)/
   ```

   Specify the server host name in lower-case characters. If you specify it by using other characters, the server will not work correctly.

5. For `ThreadsPerChild`, specify the maximum number of concurrent sessions for transmitting data by JP1/DH - Server.

   ```
   ThreadsPerChild maximum-number-of-concurrent-sessions
   ```

   You can specify a maximum of 1,024 for the maximum number of concurrent sessions.

6. Close the `httpsd.conf` file.

7. Execute `deploy_websvr.bat` to apply the settings in the `httpsd.conf` file to JP1/DH - Server.

   `deploy_websvr.bat` is stored in the following location:

   installation-folder`\setup_util`

Operation result

A server certificate for SSL (HTTPS) communication is installed, and client machines can access JP1/DH - Server.

Postrequisites

Start JP1/DH - Server.

Related topics

- *1.7 Starting JP1/DH - Server*

1.7 Starting JP1/DH - Server

After the environment settings are configured, start JP1/DH - Server.

Prerequisites

To perform this task, the system administrator logs in as the built-in Administrator user to the machine on which JP1/DH - Server is installed.

Procedure

1. From the Windows start menu, select **Control Panel**, **Administrative Tools**, and then **Services.**
   The Services window appears.

2. Right-click **JP1_DH_DATABASE_SVR**, and then select **Start**.
   JP1_DH_DATABASE_SVR is a database service.
   The database service starts.

3. Right-click **JP1_DH_WEB CONTAINER**, and then select **Start**.
   JP1_DH_WEB CONTAINER is a JP1/DH - Server service.
   The JP1/DH - Server service starts.

4. Right-click **JP1_DH_WEB SVR**, and then select **Start**.
   JP1_DH_WEB SVR is the proxy server service that is built into JP1/DH - Server.
   The JP1/DH - Server proxy server service starts.

Postrequisites

If JP1/DH - Server can start, check the created environment.

Related topics

- *1.8.1 Verifying that the environment settings of the machine on which JP1/DH - Server is installed are correct*
- *1.8.2 Verifying that the network settings are correct*

1.8 Checking the created environment

After JP1/DH - Server is installed and the environment settings are configured, check whether the installation and the environment settings have been implemented correctly.

1.8.1 Verifying that the environment settings of the machine on which JP1/DH - Server is installed are correct

On the machine on which JP1/DH - Server is installed, verify that the environment settings for JP1/DH - Server are correct.

Prerequisites

The system administrator performs this task on the machine on which JP1/DH - Server is installed.

Procedure

1. Start the web browser, and then access `http://localhost/`#.

   The JP1/DH - Server login window appears.

   If the login window does not appear, the environment settings for JP1/DH - Server might not be correct. Review the settings.

   #

   Check whether HTTP instead of SSL (HTTPS) communication can be used to access the URL.

2. If the login window appears, check whether the following ID and password for the system administrator can be used to log in to JP1/DH - Server:

   User ID: `admin`

   Password: `password`

   This password is the default value.

   It takes a long time to display the window at the first access after JP1/DH - Server is installed.

   If you can use the ID and password for the system administrator to log in to JP1/DH - Server and the JP1/DH - Server window appears, JP1/DH - Server was installed correctly and the environment settings are configured correctly.

Postrequisites

If you can confirm that the login window appears and the JP1/DH - Server window appears after logging in to JP1/DH - Server, the tasks required on the machine on which JP1/DH - Server is installed are complete. Next, use a client machine to verify that the network settings are correct.

Related topics

- *1.4 Setting up the environment for JP1/DH - Server*
- *1.8.2 Verifying that the network settings are correct*

1.8.2 Verifying that the network settings are correct

Use a client machine accessing JP1/DH - Server to verify that the network configuration is set correctly.

Prerequisites

- The system administrator performs this task on a client machine such as his or her own PC.
- Verifying that the environment settings of the machine on which JP1/DH - Server is installed are correct must be completed beforehand.

Procedure

1. Start the web browser on a client machine.

2. Access `https://`*server-host-name-(FQDN)*`/`#.

   The JP1/DH - Server login window appears.

   If the login window does not appear, the network configuration might not be set correctly. Review the settings of the network configuration.

   #

   Access the URL via SSL (HTTPS) communication.

Postrequisites

If you can verify that the network settings are correct, the setup of JP1/DH - Server is complete. Next, change the system administrator's password from the initial password.

Related topics

- *1.6 Setting the network configuration*
- *1.8.1 Verifying that the environment settings of the machine on which JP1/DH - Server is installed are correct*
- *1.9 Changing the password of the system administrator*

1.9 Changing the password of the system administrator

After JP1/DH - Server is set up, the system administrator changes the password from the initial password.

Prerequisites

The system administrator performs this task on a client machine such as his or her own PC.

Procedure

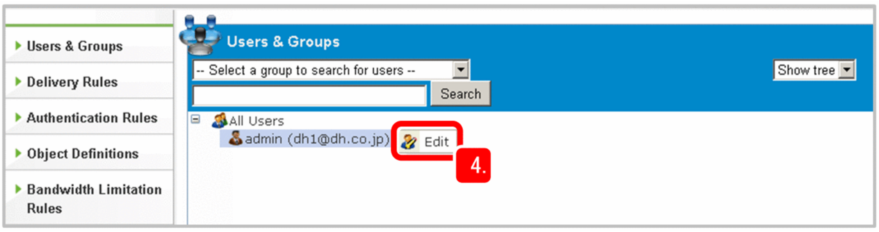
1. From a client machine, access and log in to JP1/DH - Server.

> **Important**
>
> At the first login to JP1/DH - Server, make sure that you read *2.2.1 Verifying that client machines meet prerequisites*, *2.2.2 Checking client environments and enabling the use of JP1/DH - Server (for Java applet)* and perform necessary operations.

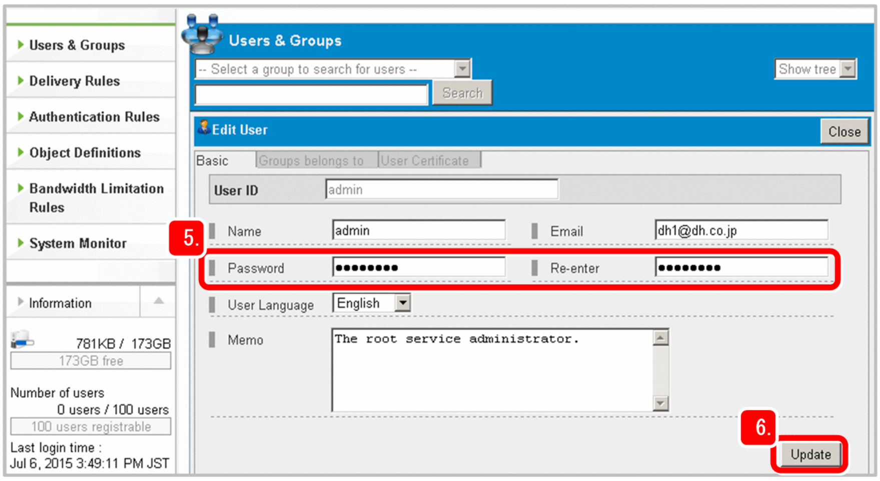
2. Log in to JP1/DH - Server with the user ID `admin` and the password `password`.
   The JP1/DH - Server window appears.

3. In the sidebar area, click **Users & Groups**.
   The Users & Groups window appears.

4. Click the admin user (👤), and then select **Edit**.
   The Edit User window appears.



5. Enter a new password.
   In the **Password** text box, enter a new password that contains alphanumeric characters and symbols (`!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~`). In the **Re-enter** text box, enter the same new password.



User ID: admin
Name: admin
Email: dh1@dh.co.jp
Password: ••••••••
Re-enter: ••••••••
User Language: English
Memo: The root service administrator.

781KB / 173GB
173GB free
Number of users
0 users / 100 users
100 users registrable
Last login time :
Jul 6, 2015 3:49:11 PM JST

6. Click the **Update** button.
   A dialog box indicating that the update is complete appears.

7. Click the **OK** button.
   The password is changed.

Postrequisites

In Chapter 2, access JP1/DH - Server from a client machine to prepare the operating environment.

Related topics

- *2. Preparation for JP1/DH - Server Operation*
- *2.2.1 Verifying that client machines meet prerequisites*
- *2.2.2 Checking client environments and enabling the use of JP1/DH - Server (for Java applet)*

2 Preparation for JP1/DH - Server Operation

This chapter describes how to prepare for JP1/DH - Server operation, such as by setting up JP1/DH - Server users and creating data delivery rules.

2.1 General procedure for JP1/DH - Server operation

The table below shows the tasks required to use JP1/DH - Server to deliver data.

Perform the tasks according to the order of the numbers shown in the table. For details about each task, see the applicable reference.

Order	Task overview	Worker	User authorities	Task details	Reference
1	Logging in to JP1/DH - Server for the first time	All	- - Administrators - - Representative user - - General user	Verify that client machines meet prerequisites.	*2.2.1*
				Check client environments and enable the use of JP1/DH - Server.	*2.2.2*
				Change passwords from the initial password.	*2.2.3*
				Using the Send and Receive App	*2.2.4*
2	Preparing groups (domains/domain content) used for JP1/DH - Server operation	System administrator	Administrators	Plan the domain content structure and management policy.	*2.3*
3				Create domains.	*2.4.1*
4				Set up representative users.	*2.4.2*
5				Define the password entry rules that apply to all domain content.	*2.5.1*
6				Define the data delivery policy to apply to all domain content.	*2.5.2*
7			Representative user	Prepare domain content.	*2.6*
8				Ask the domain-content manager to manage general users and groups.	*2.7*
9	Setting up JP1/DH - Server groups	Domain-content manager	Representative user	Plan the domain content structure and operation policy.	*2.8*
10				Create general users.	*2.9.1*
11				Set the address list to be displayed.	*2.9.2*
12				Determine the items related to data delivery, and create delivery policies.	*2.9.3*
13				Create approval routes.	*2.9.4*
14				Create delivery rules for groups by combining delivery policies and approval routes.	*2.9.5*
15				Notify general users of information required to use JP1/DH server.	*2.10*

2.2 Notes on logging in to JP1/DH - Server for the first time

At the first login to JP1/DH - Server, check the client environment and change the password. Similarly, at the first login to JP1/DH - Server with a new user ID or from a new client machine, check the client environment and change the password.

2.2.1 Verifying that client machines meet prerequisites

Verify that your client machine meets the prerequisites for using JP1/DH - Server.

Related topics

- *1.2.1 (2) Checking the environments of the client machines that will access JP1/DH - Server*
- *1.2.2 Checking required OSs*

2.2.2 Checking client environments and enabling the use of JP1/DH - Server (for Java applet)

> **Important**
>
> The procedure described in this section is required only if you use a Java applet to send and receive data. The default setting (where the App is used) does not require this procedure.

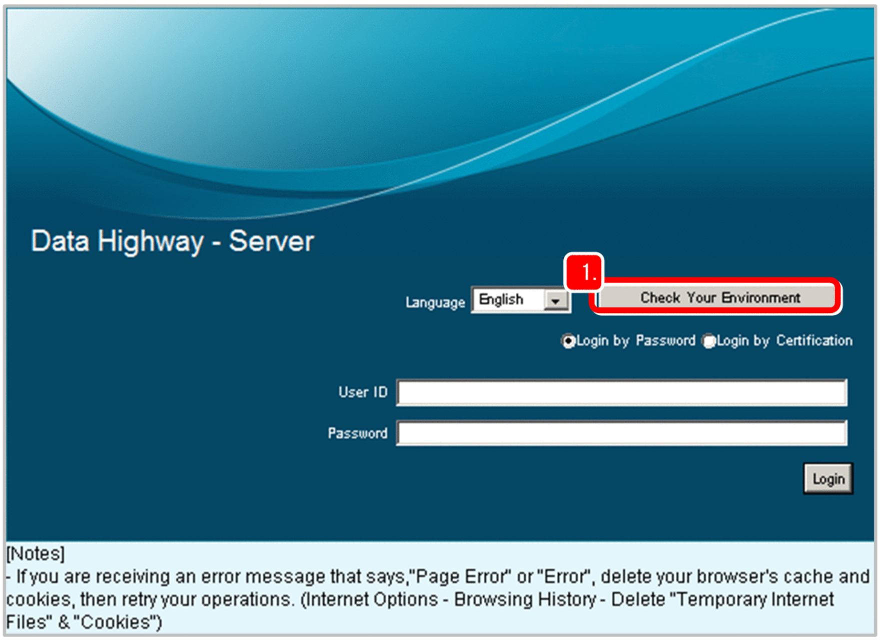
Follow the instructions given in the Check Your Environment window to set the environment of each client machine.

Prerequisites

- You must verify that your client machine meets the prerequisites for using JP1/DH - Server beforehand.

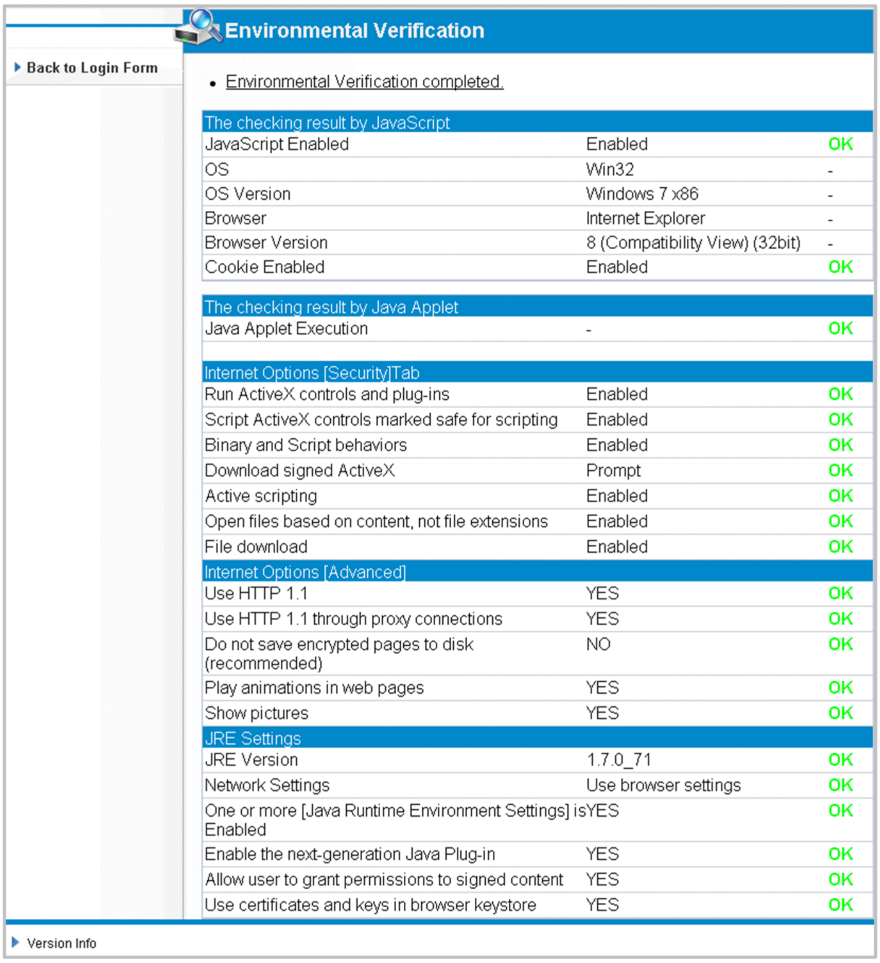
Procedure

1. Access the JP1/DH - Server URL, and then click the **Check Your Environment** button in the login window



[Notes]
- If you are receiving an error message that says,"Page Error" or "Error", delete your browser's cache and cookies, then retry your operations. (Internet Options - Browsing History - Delete "Temporary Internet Files" & "Cookies")

2. The Check Your Environment window appears. In this window, verify that the configured environment is correct. If items exist for which **NG** is displayed, review their settings. Repeat this step until **OK** is displayed for all check items.



- Environmental Verification completed.

The checking result by JavaScript		
JavaScript Enabled	Enabled	OK
OS	Win32	-
OS Version	Windows 7 x86	-
Browser	Internet Explorer	-
Browser Version	8 (Compatibility View) (32bit)	-
Cookie Enabled	Enabled	OK

The checking result by Java Applet		
Java Applet Execution	-	OK

Internet Options [Security]Tab		
Run ActiveX controls and plug-ins	Enabled	OK
Script ActiveX controls marked safe for scripting	Enabled	OK
Binary and Script behaviors	Enabled	OK
Download signed ActiveX	Prompt	OK
Active scripting	Enabled	OK
Open files based on content, not file extensions	Enabled	OK
File download	Enabled	OK
Internet Options [Advanced]		
Use HTTP 1.1	YES	OK
Use HTTP 1.1 through proxy connections	YES	OK
Do not save encrypted pages to disk (recommended)	NO	OK
Play animations in web pages	YES	OK
Show pictures	YES	OK
JRE Settings		
JRE Version	1.7.0_71	OK
Network Settings	Use browser settings	OK
One or more [Java Runtime Environment Settings] is Enabled	YES	OK
Enable the next-generation Java Plug-in	YES	OK
Allow user to grant permissions to signed content	YES	OK
Use certificates and keys in browser keystore	YES	OK

Postrequisites

- After you check the client environment, log in to JP1/DH - Server.
- Change the password from the initial password.

Related topics

- *1.2.1 (2) Checking the environments of the client machines that will access JP1/DH - Server*
- *1.2.2 Checking required OSs*
- *2.2.3 Changing passwords from the initial password*

2.2.3 Changing passwords from the initial password

When JP1/DH - Server starts, initial passwords are given to users. At the first login to JP1/DH - Server, users must immediately change their passwords from the initial password.

Procedure

1. Log in to JP1/DH - Server#. In the sidebar area, select **Options**. Then, select the **Authentication** tab

   The Change your password for the Standard Password Authentication window appears.

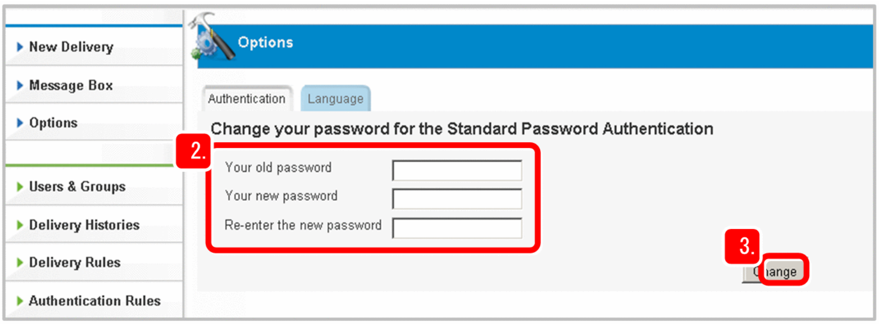
   #

   The system administrator who logs in as the `admin` user can omit this step because his or her password was already changed from the initial password in the previous process.

   However, if the system administrator has not changed his or her password from the initial password yet or logs in to JP1/DH - Server by using a user ID with the representative user authorities for the first time, the system administrator must change his or her password from the initial password.

2. In **Your old password**, enter the initial password. In **Your new password** and **Re-enter the new password**, enter a new password.

   Enter a new password that contains alphanumeric characters and symbols (`!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~`). In the **Re-enter the new password** text box, enter the same new password.



Change your password for the Standard Password Authentication

Your old password

Your new password

Re-enter the new password

3. Click the **Change** button.

   The password is changed.

2.2.4 Using the Send and Receive App

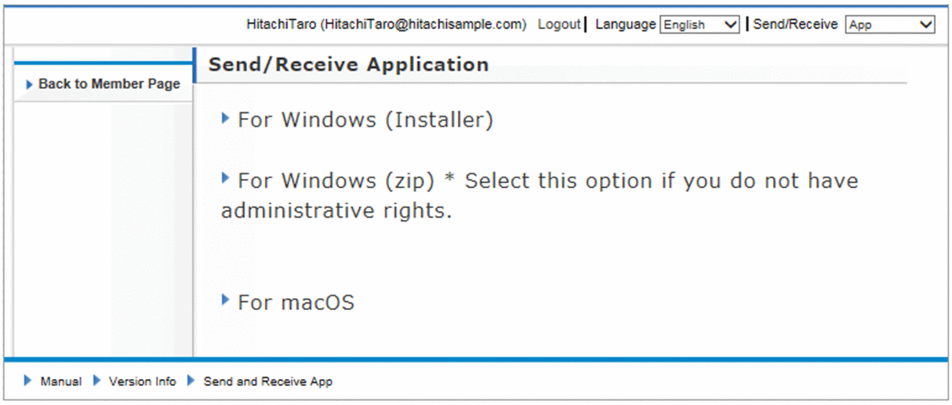
InJP1/DH - Server, you can download the Send and Receive App and use it to send and receive files and messages.

This section describes the steps required to use the App.

1. From the **Send/Receive** drop-down menu, select **App**.

2. Click **Send and Receive App** in the menu in the left side of the window.
   A window for downloading the Send and Receive App appears.
   The download window can also be displayed by clicking the **Send and Receive App** link at the footer.

3. Download the installer or zip file depending on the client OS.
   Save the downloaded file in a folder.



HitachiTaro (HitachiTaro@hitachisample.com) Logout | Language English | Send/Receive App

Back to Member Page

Send/Receive Application

- For Windows (Installer)
- For Windows (zip) * Select this option if you do not have administrative rights.
- For macOS

Manual Version Info Send and Receive App

4. Unzip the downloaded file and install the application.

   - For Windows (with the installer):
     Right-click `AFTClientInstaller.zip` to unzip it and click `aftsetup.exe`.
     Follow the steps in the installer to complete the setup.
     Select where to install the App. By default, the App is installed in the following folder:
     `C:\Program Files\ Data Highway Client`
     A folder for the application is created in the **Start** menu when the setup completes.

   - For Windows (with the zip file):
     Right-click the downloaded AFTClient.zip and select Expand All to unzip the file.
     Do one of the following:
     - Right-click the file 00_prepare.bat that is immediately under the folder into which the zip file was unzipped, and then run it with administrator rights.
     - Right-click the file config.aftxc that is immediately under the folder into which the zip file was unzipped, and then select Open with, Choose default program, and Browse. Click AFTClient.exe in the same folder.
     Close since the Send and Receive App setting screen opens.

   - For macOS
     Double-click `AFTClient.dmg` to expand it.
     Drag and drop the icon of Data Highway Client.app to the Applications icon.

5. If the server certificate was issued by a non-public authority, import it.

   - For Windows (with the installer):
     Run Import Certificate.bat in the Start menu as an administrator.The command prompt window appears.
     - Enter the path to the certificate in Input certificate file path:.
     - Enter a name (alphanumeric characters only) in Input certificate alias:.
     You will be asked if you trust the certificate. Enter y.When you see Completed, you are all set.

- For Windows (with the zip file):

  Unzip the zip file and run Import Certificate.bat in the resulting folder.The command prompt window appears.

  - Enter the path to the certificate in Input certificate file path:.

  - Enter a name (alphanumeric characters only) in Input certificate alias:.

  You will be asked if you trust the certificate. Enter y.When you see Completed, you are all set.

- For macOS

  Run the following command:

  ```
  /Applications/Data\ Highway\ Client.app/Contents/java/bin/keytool -import
  -file path-to-the-certificate -alias an-alphanumeric-only-string -keystore /Applications/
  Data\ Highway\ Client.app/Contents/java/lib/security/cacerts -storepass
  changeit -trustcacerts
  ```

  You will be asked if you trust the certificate. Enter `y`.

2.3 Planning the domain content structure and management policy (system administrator)

JP1/DH - Server users must be assigned to JP1/DH - Server groups. Therefore, the system administrator first prepares groups to manage JP1/DH - Server users.

Procedure

1. Prepare information about the users who use JP1/DH - Server to deliver data.

   This example assumes that the following users use JP1/DH - Server to deliver data.

Location	Department	User	User ID	Email address
Tokyo	-	Kobayashi Manabu#	`kobayashi`	`akaadmin@XXX.co.jp`
Tokyo	Design	Suzuki Tomoko	`suzuki`	`suzuki@XXX.co.jp`
Tokyo	Design	Sato Daisuke	`sato`	`sato@XXX.co.jp`
Tokyo	Design	Tanaka Kenta	`tanaka`	`tanaka@XXX.co.jp`
Overseas	Manufacturing	Watanabe Makoto	`watanabe`	`watanabe@XXX.co.jp`
Overseas	Manufacturing	Mia Wilson	`wilson`	`wilson@XXX.co.jp`
Overseas	Manufacturing	Li Jing	`li`	`li@XXX.co.jp`

   Legend -: Does not belong to a department defined in JP1/DH - Server.

   #:

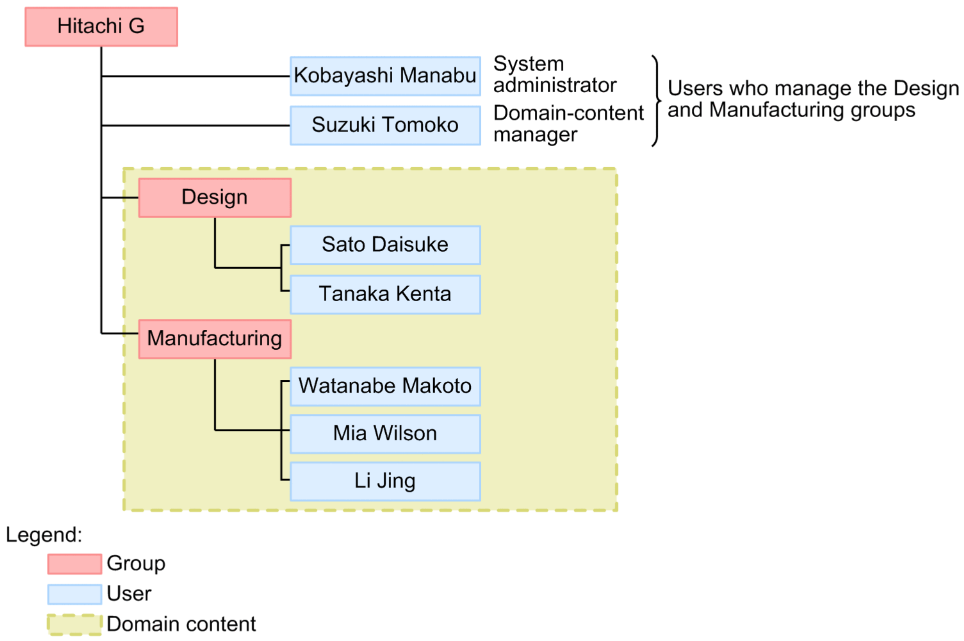
   In addition to a user with Administrator authority, the system administrator must prepare a user and user ID with the authority of a representative user. In the example above, the user Kobayashi Manabu with the user ID `kobayashi` is created for this purpose.

2. Create email accounts so that the users whose information was prepared in step 1 can send and receive email.

   Create accounts for these users on the mail server specified in the `digikatsuwide.xml` file. After the at mark (`@`) in the email address, specify a domain name that can be used in your environment. In this document, `XXX.co.jp` is used as an example domain name.

3. Design the layout on JP1/DH - Server for the users whose information was prepared in step 1.

   In JP1/DH - Server, data is delivered between users under the same group called a *domain*. This example assumes the following group configuration:



In this example, the group Hitachi G is a domain.

As shown in this example, a domain is a group that is created to aggregate subgroups and users.

By defining the Design and Manufacturing groups under the domain Hitachi G, users who belong to these groups and users defined directly under Hitachi G are able to deliver data to each other.

Note that in this scenario, the user Suzuki Tomoko is created directly under Hitachi G domain despite being affiliated with the Design department. This allows her to manage all domain content under the Hitachi G domain.

4. Select a domain-content manager, and determine the password he or she will use to log in to JP1/DH - Server.

   The groups such as Design and Manufacturing under a domain are collectively referred to as *domain content*.

   The system administrator selects the user (domain-content manager) who will manage this domain content.

   A domain-content manager is created by assigning the representative user authority to a user in JP1/DH - Server. When doing so, the system administrator also sets the initial password.

   In the example above, Kobayashi Manabu (the system administrator) and Suzuki Tomoko are nominated as domain-content managers.

   Tip

   When there are several domain-content managers, you can set the same character string as their initial password. This allows the system administrator to send the same email to each domain-content manager when notifying them in step 6.

5. Design the operational policies to apply to all domain content.

   Design the operational policies to be applied to the entire groups under the domain, including the groups Design and Manufacturing.

   - Password entry rules
   - Data delivery policies

6. Provide domain-content managers with the information they need.

   Send an email to domain-content managers that contains the JP1/DH - Server URL, their user IDs and passwords, and information about their responsibilities.

   The password contained in this email is the initial password. Ask the domain-content manager to change the password at the first login.

Postrequisites

Enter settings in JP1/DH - Server that implement the domain content structure and management policy that you designed in this procedure.

Related topics

- *2.4.1 Creating domains (system administrator)*
- *2.4.2 Setting up representative users (system administrator)*
- *2.5.1 Defining the password entry rules that apply to all domain content (system administrator)*
- *2.5.2 Defining data delivery policies that apply to all domain content (system administrator)*
- *2.6 Preparing domain content (system administrator)*
- *2.7 Asking the domain-content manager to manage general users and groups(system administrator)*

2.4 Preparing domains and representative users (system administrator)

In the Users & Groups window of JP1/DH - Server, create groups according to the domain content structure and management policy that you designed. First, create domains to manage groups.

2.4.1 Creating domains (system administrator)

To manage users and groups on JP1/DH - Server, first create domains. In this example, the domain *Hitachi G* will be created.

Prerequisites

- To perform this task, the system administrator logs in to JP1/DH - Server as `admin`.
- Client environments must be checked beforehand.

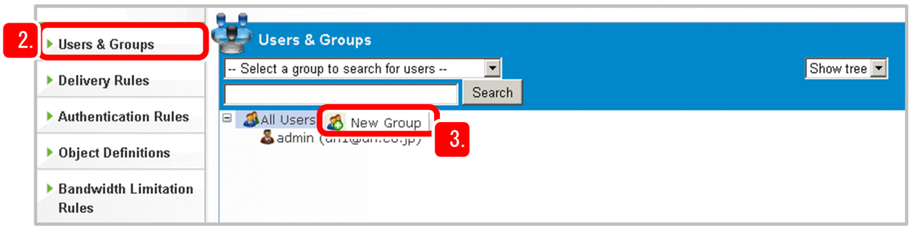
Procedure

1. Log in to JP1/DH - Server as `admin`.

   Important

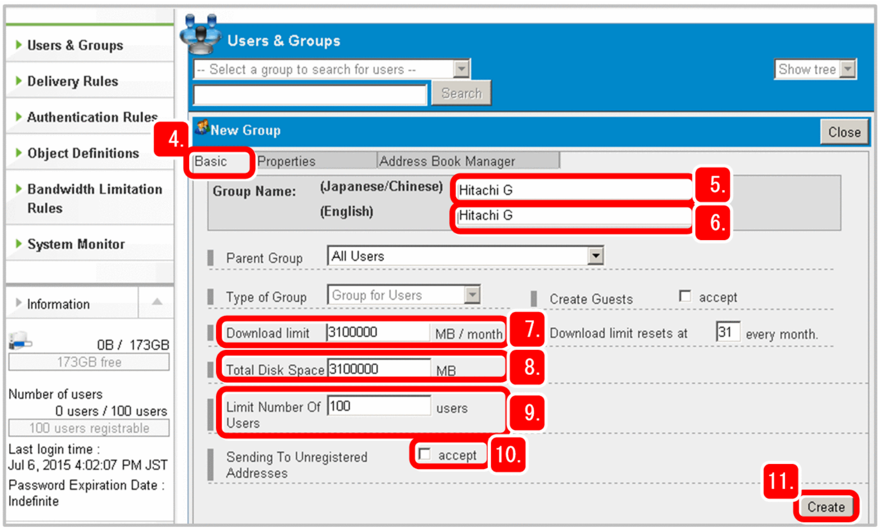
   If client environments have not been checked yet according to the descriptions in *2.2 Notes on logging in to JP1/DH - Server for the first time*, check the environments.

2. In the sidebar area, select **Users & Groups**.
   The Users & Groups window appears in the content area.



3. Click **All Users**, and then select **New Group**.
   The New Group window appears.

4. Select the **Basic** tab.



0B / 173GB
173GB free
Number of users
0 users / 100 users
100 users registrable
Last login time :
Jul 6, 2015 4:02:07 PM JST
Password Expiration Date :
Indefinite

Group Name: (Japanese/Chinese) Hitachi G
(English) Hitachi G
Parent Group: All Users
Type of Group: Group for Users
Create Guests: □ accept
Download limit: 3100000 MB / month
Download limit resets at 31 every month.
Total Disk Space: 3100000 MB
Limit Number Of Users: 100 users
Sending To Unregistered Addresses: □ accept

5. In **Group Name: (Japanese/Chinese)**, enter `Hitachi G`.

The group name specified here is displayed in the Japanese and Chinese windows. You cannot change the group name after the group is created.

6. In **Group Name: (English)**, enter `Hitachi G`.

The group name specified here is displayed in the English window. You cannot change a group name after the group is created.

Note

A domain ID is the value that is obtained by deleting spaces from the group name specified for **Group Name: (English)**, replacing uppercase characters with lowercase characters, and then adding an at mark (`@`) to the beginning. This domain ID is part of the user IDs for the users who are allocated under the domain. Users of JP1/DH - Server use these user IDs to log in to JP1/DH - Server.

Example of a user ID of a user who is allocated under a domain:

Domain name (English): Hitachi G
Hitachi Taro's user ID: HitachiTaro
Hitachi Taro's user ID for JP1/DH - Server: HitachiTaro@hitachig

7. In **Download limit**, specify a data size.

Enter the download limit for the entire domain per month, in MB.
This example assumes that the total size of delivery data per day is 100.0 GB.
In the **Download limit** text box, specify `3100000`.

8. Specify **Total Disk Space**.

Enter the disk space available for the entire domain, in MB.
This example assumes the following conditions: The number of deliveries that are generated per day by the users who are allocated under the domain is 100. The maximum delivery data file size is 1,000.0 MB. The storage period is 31 days.
In the **Total Disk Space** text box, specify `3100000`.

9. Specify the maximum number of JP1/DH - Server users.

Set the maximum number of users who can be registered for the entire domain.

In the **Limit Number Of Users** text box, specify `100`.

10. In **Sending To Unregistered Addresses**, verify that the **accept** check box is not selected.
    If this check box is selected, clear it.

11. Click the **Create** button.
    The domain is created.

Postrequisites

Set up the system administrator and domain-content managers as representative users in JP1/DH - Server.

Related topics

- *2.2 Notes on logging in to JP1/DH - Server for the first time*
- *2.3 Planning the domain content structure and management policy (system administrator)*
- *2.4.2 Setting up representative users (system administrator)*

2.4.2 Setting up representative users (system administrator)

In JP1/DH - Server, a user who has the authorities for managing a domain and the users under the domain is registered as a representative user. The system administrator registers representative users.

To register a representative user, create a user on JP1/DH - Server, first. Then, register the user as a representative user.

(1) Creating users

For system administrators and domain-content managers to serve as representative users, you need to create them under the domain Hitachi G.

The instructions below use the following user as an example:

Suzuki Tomoko (domain-content manager) User ID: `suzuki` Email address: `suzuki@XXX.co.jp`

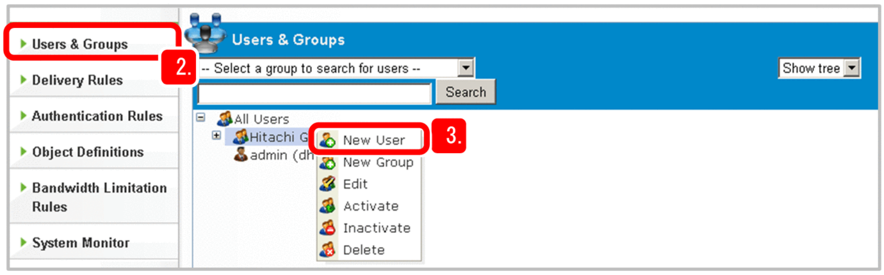
Prerequisites

- To perform this task, the system administrator logs in to JP1/DH - Server as `admin`.
- The system administrator must have a user ID other than `admin` prepared for a representative user, beforehand.
- The system administrator must decide in advance which users are to serve as domain-content managers, and have their names, user IDs, and email addresses on hand.

Procedure

1. Log in to JP1/DH - Server as `admin`.

2. In the sidebar area, select **Users & Groups**.
   The Users & Groups window appears in the content area.

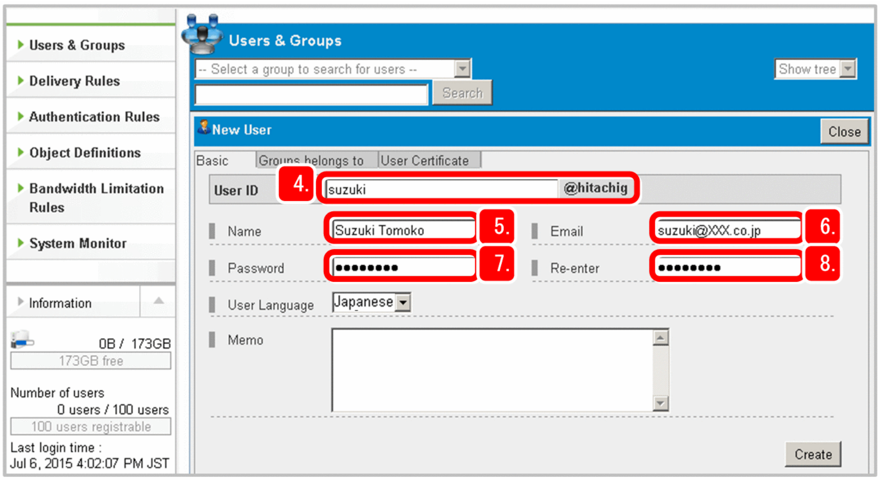


3. Click **Hitachi G**, and then select **New User**.

   The New User window appears.

4. In the **User ID** text box, enter `suzuki`.

   @hitachig, which is the domain ID for Hitachi G, is displayed. The user ID used to log in to JP1/DH - Server will be `suzuki@hitachig`, which is the user ID you entered (`suzuki`) with the domain ID `@hitachig` as the suffix.



User ID: suzuki @hitachig

Name: Suzuki Tomoko

Email: suzuki@XXX.co.jp

Password: ●●●●●●●●

Re-enter: ●●●●●●●●

User Language: Japanese

Memo:

0B / 173GB

173GB free

Number of users

0 users / 100 users

100 users registrable

Last login time :

Jul 6, 2015 4:02:07 PM JST

5. In the **Name** text box, enter `Suzuki Tomoko`.

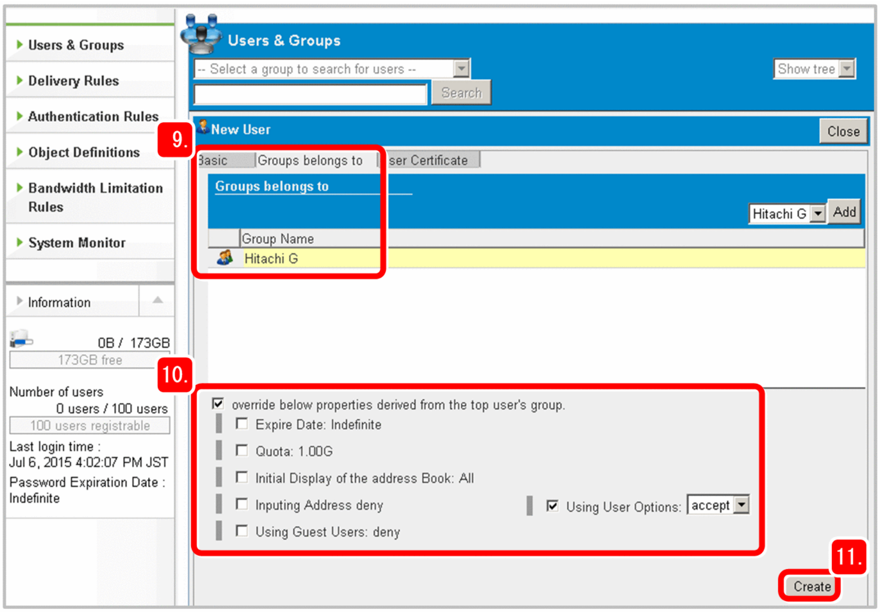
6. In the **Email** text box, enter `suzuki@XXX.co.jp`.

7. In the **Password** text box, enter any password.

   The password you enter serves as the initial password the domain-content manager uses to log in to JP1/DH - Server. Enter a character string of at least eight characters. The string can contain alphanumeric characters and symbols (`!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~`).

8. In the **Re-enter** text box, enter the same password as the password you entered in the **Password** text box.

9. Select the **Groups belongs to** tab, and then verify that **Hitachi G** is displayed.



0B / 173GB
173GB free
Number of users
0 users / 100 users
100 users registrable
Last login time :
Jul 6, 2015 4:02:07 PM JST
Password Expiration Date :
Indefinite

☑ override below properties derived from the top user's group.
□ Expire Date: Indefinite
□ Quota: 1.00G
□ Initial Display of the address Book: All
□ Inputting Address deny
☑ Using User Options: accept
□ Using Guest Users: deny

10. Enable the use of options.
    Select the **override below properties derived from the top user's group.** check box.
    Verify that a check box appears at the beginning of **Using User Options: accept**, and then select it.

11. Click the **Create** button.
    The user is created.

Postrequisites

- Also create an account for Kobayashi Manabu (the system administrator), with the user ID `kobayashi` and email address `akaadmin@XXX.co.jp`.
- After users are created, register the created users as representative users in JP1/DH - Server.

Related topics

- *2.4.2 (2) Registering users as representative users*

(2) Registering users as representative users

User accounts for the system administrator and domain-content manager have been created under the Hitachi G domain. You must now set up these users as representative users.

The instructions below use the following user as an example:

Suzuki Tomoko (domain-content manager) User ID: `suzuki` Email address: `suzuki@XXX.co.jp`

Prerequisites

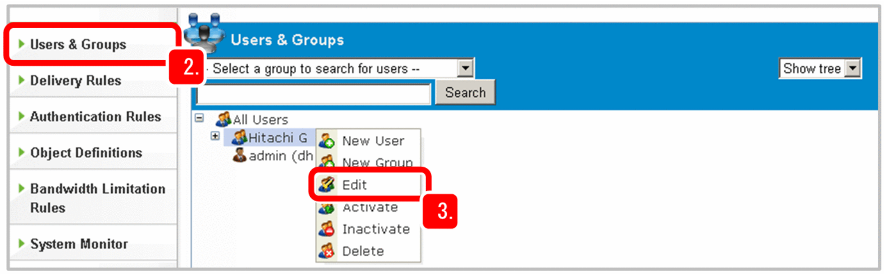
- To perform this task, the system administrator logs in to JP1/DH - Server as `admin`.
- The users to be registered as representative users must be created on JP1/DH - Server beforehand.

Procedure

1. Log in to JP1/DH - Server as `admin`.

2. In the sidebar area, click **Users & Groups**.

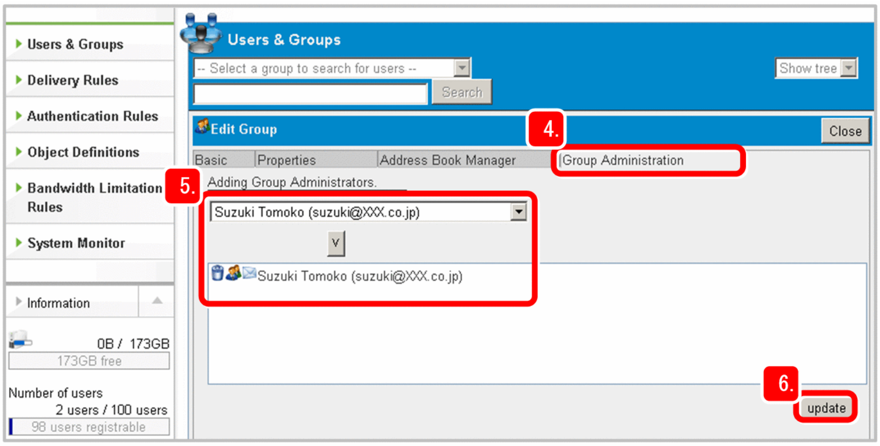
The Users & Groups window appears in the content area.



3. Click **Hitachi G**, and then select **Edit**.

   The Edit Group window appears.

4. Select the **Group Administration** tab.



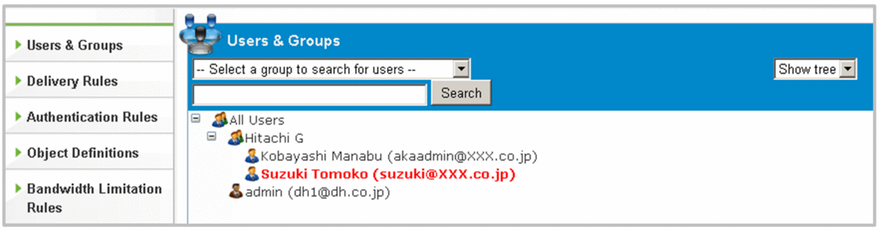
5. Select **Suzuki Tomoko** and click the **V** button.

   Suzuki Tomoko is added to the list of administrators.

6. Click the **Update** button.

   Suzuki Tomoko is set up as a representative user in JP1/DH - Server.

   In the Users & Groups window, representative users are displayed in red letters.


Users & Groups
Delivery Rules
Authentication Rules
Object Definitions
Bandwidth Limitation Rules
Users & Groups
-- Select a group to search for users --
Show tree
Search
All Users
Hitachi G
Kobayashi Manabu (akaadmin@XXX.co.jp)
Suzuki Tomoko (suzuki@XXX.co.jp)
admin (dh1@dh.co.jp)

Postrequisites

- Set Kobayashi Manabu (the system administrator) as a representative user for the domain Hitachi G in JP1/DH - Server.
- After setting up the representative users, define the operation policy that applies to all domain content.

Related topics

- *2.5 Setting operation policies for all domain content (system administrator)*

2.5 Setting operation policies for all domain content (system administrator)

2.5.1 Defining the password entry rules that apply to all domain content (system administrator)

Define the password entry rules for logging in to JP1/DH - Server.

The authentication rules for logging in to JP1/DH - Server are called *authentication policies*. An authentication policy that applies to all domain content for anyone who logs in to JP1/DH - Server is called the *standard authentication policy*. In this example, the standard authentication policy will be defined.

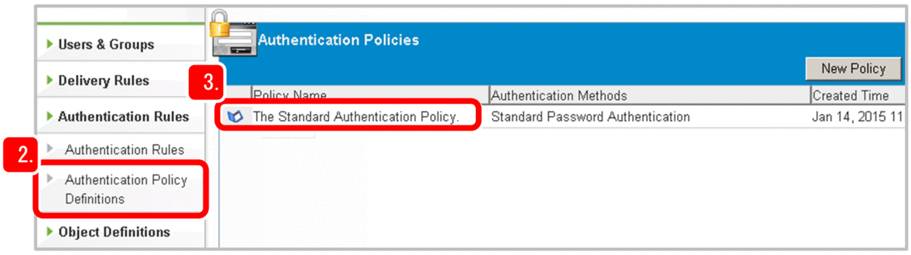
Prerequisites

- The system administrator logs in to JP1/DH - Server as `admin`.

Procedure

1. Log in to JP1/DH - Server as `admin`.

2. In the sidebar area, select **Authentication Rules** and **Authentication Policy Definitions**.
   The Authentication Policies window appears in the content area.

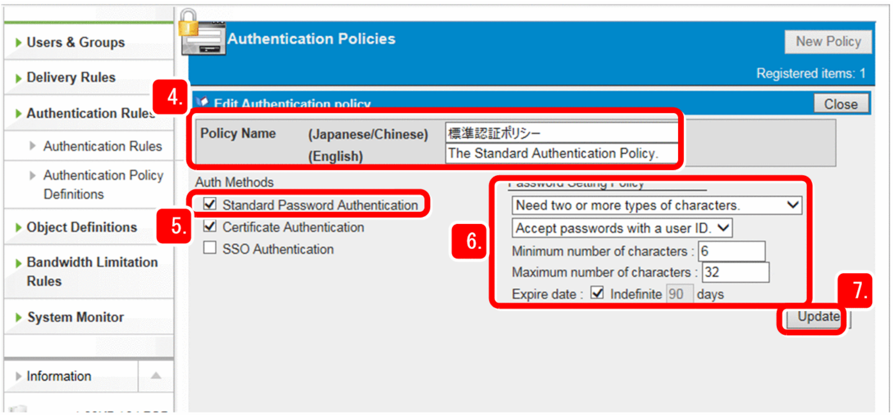


Policy Name	Authentication Methods	Created Time
The Standard Authentication Policy.	Standard Password Authentication	Jan 14, 2015 11

3. Click the menu icon ( ) for **The Standard Authentication Policy.**, and then select **Edit**.

   The Edit Authentication policy window appears.

4. Make sure that the name of the standard authentication policy appears in the **Policy Name (Japanese/Chinese)** and **Policy Name (English)** text boxes.
   Do not delete either of these names. If the text boxes are empty, you will be unable to update the policy.



Policy Name (Japanese/Chinese) 標準認証ポリシー
(English) The Standard Authentication Policy.

Auth Methods
☑ Standard Password Authentication
☑ Certificate Authentication
☐ SSO Authentication

Password Setting Policy
Need two or more types of characters.
Accept passwords with a user ID.
Minimum number of characters : 6
Maximum number of characters : 32
Expire date : ☑ Indefinite 90 days

5. In **Auth Methods**, check that only **Standard Password Authentication** is selected.

If **Standard Password Authentication** is not selected or if **Certificate Authentication** or **SSO Authentication** are selected, select only **Standard Password Authentication**.

6. Set **Password Setting Policy**.

   Set each items as follows:

   - Need two or more types of characters.
   - Reject passwords with a user ID.
   - Enter a value of 8 or more in **Minimum number of characters**.
   - Remove the **Expire date** check box, and then enter the expiration period.

7. Click the **Update** button.

   The standard authentication policy is updated, and the dialog box that indicates the completion of the update appears.

Postrequisites

Define the policies to apply to data delivery for all domain content.

Related topics

- *2.5.2 Defining data delivery policies that apply to all domain content (system administrator)*

2.5.2 Defining data delivery policies that apply to all domain content (system administrator)

Define the policies for using JP1/DH - Server to deliver data. The data delivery policies define the data size that can be delivered, the data storage period, and the email notification types that can be selected by senders when they deliver data. These policies are called *delivery policies*. A delivery policy that applies to data delivery for all domain content is called the *standard policy*. In this example, the standard policy will be defined.

Prerequisites

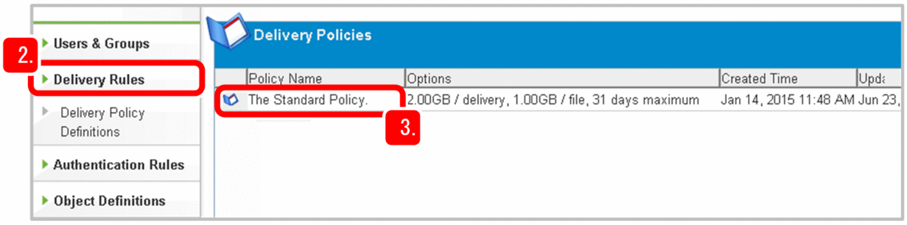
- To perform this task, the system administrator logs in to JP1/DH - Server as `admin`.

Procedure

1. Log in to JP1/DH - Server as `admin`.

2. In the sidebar area, select **Delivery Rules**.

   The Delivery Policies window appears in the content area.

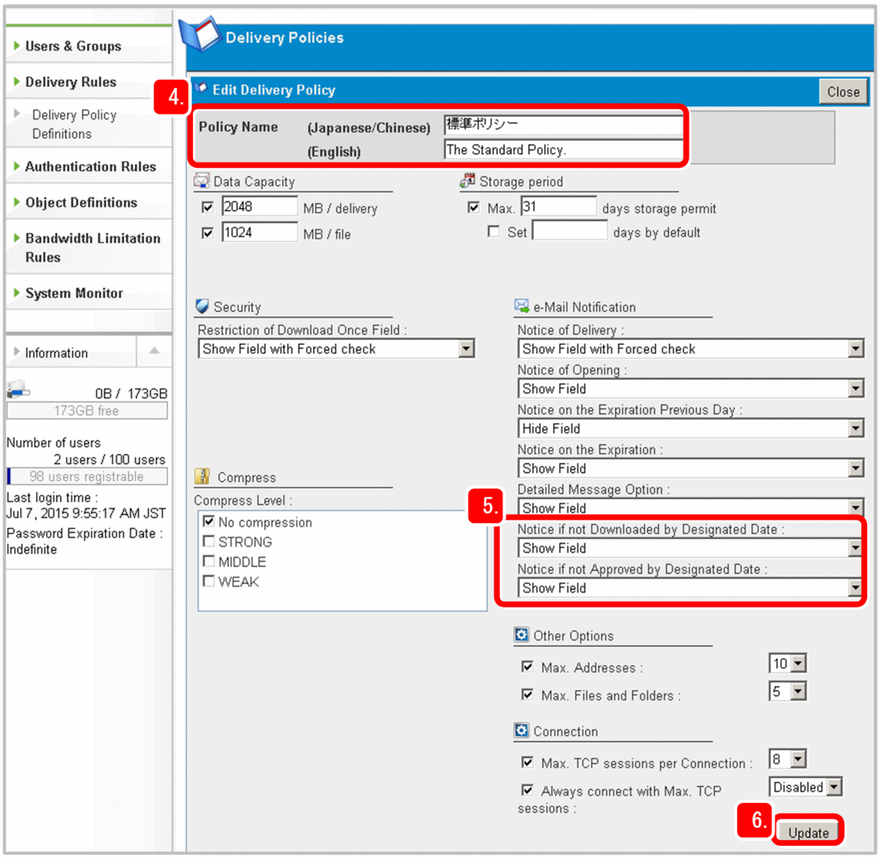


Policy Name	Options	Created Time	Upd:
The Standard Policy.	2.00GB / delivery, 1.00GB / file, 31 days maximum	Jan 14, 2015 11:48 AM	Jun 23,

3. Click the menu icon ( ) for **The Standard Policy.**, and then select **Edit**.

   The Edit Delivery Policy window appears.

4. Make sure that the name of the standard policy appears in the **Policy Name (Japanese/Chinese)** and **Policy Name (English)** text boxes.
   Do not delete either of these names. If the text boxes are empty, you will be unable to update the policy.



0B / 173GB
173GB free
Number of users
2 users / 100 users
98 users registrable
Last login time :
Jul 7, 2015 9:55:17 AM JST
Password Expiration Date :
Indefinite

Policy Name (Japanese/Chinese) 標準ポリシー
(English) The Standard Policy.

Data Capacity
☑ 2048 MB / delivery
☑ 1024 MB / file

Storage period
☑ Max. 31 days storage permit
☐ Set days by default

Security
Restriction of Download Once Field : Show Field with Forced check

e-Mail Notification
Notice of Delivery : Show Field with Forced check
Notice of Opening : Show Field
Notice on the Expiration Previous Day : Hide Field
Notice on the Expiration : Show Field
Detailed Message Option : Show Field
Notice if not Downloaded by Designated Date : Show Field
Notice if not Approved by Designated Date : Show Field

Compress
Compress Level :
☑ No compression
☐ STRONG
☐ MIDDLE
☐ WEAK

Other Options
☑ Max. Addresses : 10
☑ Max. Files and Folders : 5

Connection
☑ Max. TCP sessions per Connection : 8
☑ Always connect with Max. TCP sessions : Disabled

5. Verify that **e-Mail Notification** items are set as follows:
   - In the **Notice if not Downloaded by Designated Date** drop-down list box, **Show Field** is selected.
     If it is not selected, select it.
   - In the **Notice if not Approved by Designated Date** drop-down list box, **Show Field** is selected.
     If it is not selected, select it.

6. Click the **Update** button.
   The delivery standard policy is updated.

Postrequisites

Create the groups (domain content) under the domain.

Related topics

- *2.6 Preparing domain content (system administrator)*

2.6 Preparing domain content (system administrator)

Domain content is a term for the groups under a domain. The system administrator creates groups according to the group configuration that was designed beforehand.

In this example, the group *Design* will be created.

Prerequisites

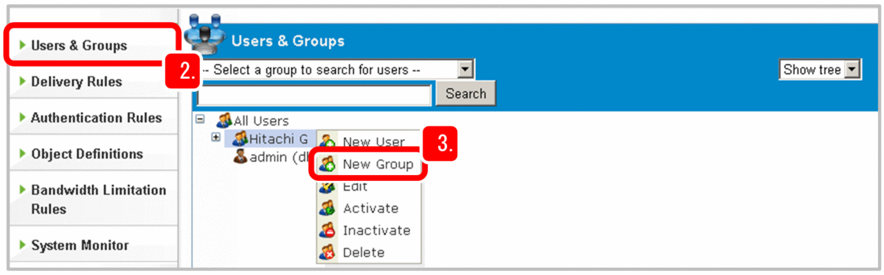
- To perform this task, the system administrator logs in to JP1/DH - Server with a representative user ID.
- The system administrator must be registered in JP1/DH - Server as a representative user beforehand.

Procedure

1. Log in to JP1/DH - Server with the representative user ID.

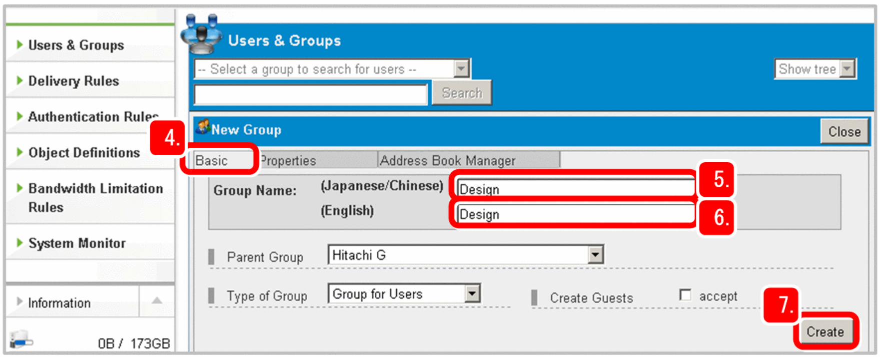
> **Important**
>
> At the first login to JP1/DH - Server with the representative user ID, make sure that you read *2.2 Notes on logging in to JP1/DH - Server for the first time* and perform necessary operations. If you use the same machine as the machine where you logged in as `admin`, perform only the operation to change your password from the initial password.

2. In the sidebar area, select **Users & Groups**.
   The Users & Groups window appears in the content area.



3. Click the domain **Hitachi G**, and then select **New Group**.
   The New Group window appears.

4. Select the **Basic** tab.



Group Name: (Japanese/Chinese) Design
(English) Design
Parent Group Hitachi G
Type of Group Group for Users
Create Guests □ accept

5. In **Group Name: (Japanese/Chinese)**, enter `Design`.

6. In **Group Name: (English)**, enter `Design`.

7. Click the **Create** button.

   The group is created.

   Create groups according to the group configuration that was designed beforehand.

> **Important**
>
> In this procedure, the system administrator just specifies group names. The domain-content manager is responsible for assigning users to groups.

Postrequisites

- Create the group Manufacturing according to the group configuration that was designed beforehand.
- After creating the domain content, request that the domain-content manager perform the subsequent tasks.

Related topics

- *2.2 Notes on logging in to JP1/DH - Server for the first time*
- *2.3 Planning the domain content structure and management policy (system administrator)*
- *2.7 Asking the domain-content manager to manage general users and groups(system administrator)*

2.7 Asking the domain-content manager to manage general users and groups (system administrator)

After setting up domain-content managers as representative users in JP1/DH - Server, the system administrator can provide those users with the information they need and ask them to perform additional tasks.

Procedure

1. Before asking a domain-content manager to perform additional tasks, the system administrator verifies the following:
    - All required domains and domain content have been created in JP1/DH - Server.
    - The domain-content user is set up as a representative user in JP1/DH - Server.
    - The **Using User Options: accept** check box on the **Groups belongs to** tab for the representative user is selected.

    > **Important**
    >
    > If the **Using User Options: accept** check box on the **Groups belongs to** tab for the representative user is not selected, options are not available.
    >
    > If options are not available, users cannot change their passwords from the initial password at the first login to JP1/DH - Server.

2. Send the following required information to the domain-content manager:
    - The user ID and initial password of the domain-content manager
    - JP1/DH - Server URL
    - Request to apply the standard policy
      Ask the groups under the domain to apply the standard policy as a data delivery policy.
    - Operation manual or documents equivalent to the operation manual
      For example: From section 2.8 in this manual

    > **Tip**
    >
    > Set the initial password with a character string common to domain-content managers. This allows you to send the same body text as a batch when notifying several domain-content managers.
    >
    > Ask the domain-content managers to change their passwords from the initial password at the first login.

Postrequisites

This concludes the system administrator's tasks.

Perform the following:

- If the server certificate for the production environment has not been obtained yet, obtain it.
- Before JP1/DH - Server starts in the production environment, make sure that you replace the server certificate for the test environment with the server certificate for the production environment.
- After JP1/DH - Server starts in the production environment, check and, if necessary, revise the network bandwidth, maximum size of files available for transfer, and Java heap memory.

Related topics

- *1.4.2 Using the file digikatsuwide.xml to set up the environment*
- *1.4.3 Setting Java heap memory sizes*
- *1.5.2 Creating a server certificate for the production environment*
- *2.4.2 (1) Creating users*

2.8 Planning the domain content structure and operation policy (domain-content manager)

The domain-content manager performs tasks in relation to the groups under the domain prepared by the system administrator. This includes setting up the users who will actually deliver data by using JP1/DH - Server, and defining the rules that apply to data delivery.

Procedure

1. Prepare information about the users who use JP1/DH - Server to deliver data.

   This example assumes that the following users use JP1/DH - Server to deliver data.

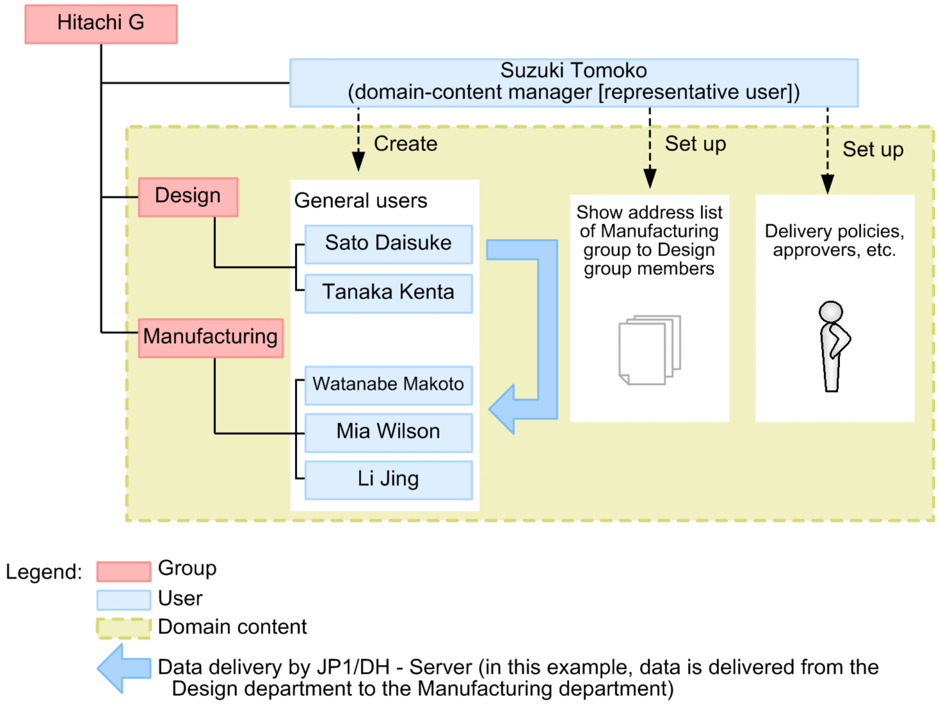
Location	Department	User	User authorities (role)	User ID	Email address	Language
Tokyo	Design	Suzuki Tomoko	Representative user (domain-content manager)	`suzuki`	`suzuki@XXX.co.jp`	Japanese
Tokyo	Design	Sato Daisuke	General user (approver)	`sato`	`sato@dXXX.co.jp`	Japanese
Tokyo	Design	Tanaka Kenta	General user	`tanaka`	`tanaka@XXX.co.jp`	Japanese
Overseas#	Manufacturing	Watanabe Makoto	General user	`watanabe`	`watanabe@XXX.co.jp`	Japanese
Overseas#	Manufacturing	Mia Wilson	General user	`wilson`	`wilson@XXX.co.jp`	English
Overseas#	Manufacturing	Li Jing	General user	`li`	`li@XXX.co.jp`	Chinese

   #:

   A domestic domain-content manager also sets up users who are located overseas.

2. Verify which groups will deliver data to each other based on the group structure, and plan which address list should be displayed to each group when delivering data.

   In this example, data will be delivered from Design to Manufacturing. Therefore, users in the Design group will be able to view the address list for the Manufacturing group.


Hitachi G
Suzuki Tomoko
(domain-content manager [representative user])
Create
Set up
Set up
Design
General users
Sato Daisuke
Tanaka Kenta
Manufacturing
Watanabe Makoto
Mia Wilson
Li Jing
Show address list of Manufacturing group to Design group members
Delivery policies, approvers, etc.
Legend:
Group
User
Domain content
Data delivery by JP1/DH - Server (in this example, data is delivered from the Design department to the Manufacturing department)

3. Check the language for each user.

4. Determine the password to be used when users log in to JP1/DH - Server.

> **Tip**
>
> Set the initial password with a character string common to users. By doing this, you can send, in a batch, an email that has the same content to multiple users.
>
> Ask users to change their passwords from the initial password at the first login.

5. Check the data delivery policies.

6. Determine the policies to be applied to the groups.

7. Determine data delivery approvers.

8. For each group, set a pair of a data delivery policy and an approver.

9. Notify each user of necessary information.
   Notify each user of the JP1/DH - Server URL, the user ID and password, and the operation method, by email.
   The password in this email is the initial password. Ask users to change their passwords from the initial password at the first login.

Postrequisites

Register the items that were designed here in JP1/DH - Server.

Related topics

- *2.9.1 Creating general users (domain-content manager)*
- *2.9.2 Setting address lists to be displayed (domain-content manager)*
- *2.9.3 Determining the items related to data delivery and creating delivery policies (domain-content manager)*

- *2.9.4 Creating approval routes (domain-content manager)*
- *2.9.5 Creating delivery rules for groups that combine delivery policies and approval routes (domain-content manager)*

2.9 Preparing domain-content groups and general users (domain-content manager)

The domain-content manager sets up the domain content structure and operation policy in JP1/DH - Server, in keeping with the design developed in previous steps.

2.9.1 Creating general users (domain-content manager)

In this example, the following general user will be created in the group Design.

Tanaka Kenta User ID: `tanaka` Email address: `tanaka@XXX.co.jp`

Prerequisites

- Client environments must be checked beforehand.
- These tasks are performed by the domain-content manager.
- The domain-content manager must be set up as a representative user in JP1/DH - Server, and possess the ID and password used to log in to JP1/DH - Server.
- The domain-content manager must acquire the names, user IDs, and email addresses of the users in advance.

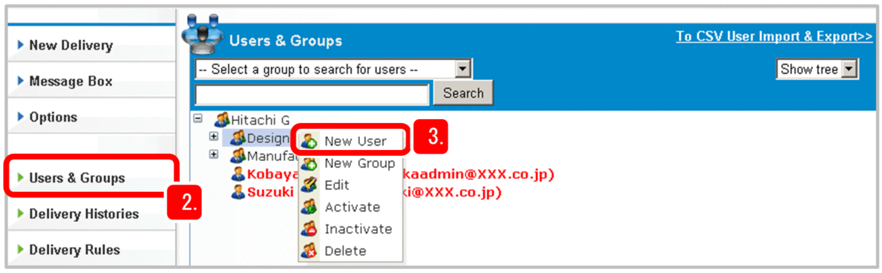
Procedure

1. Log in to JP1/DH - Server.
   Log in using the ID (`suzuki@hitachig`) and password of the domain-content manager.

   Important

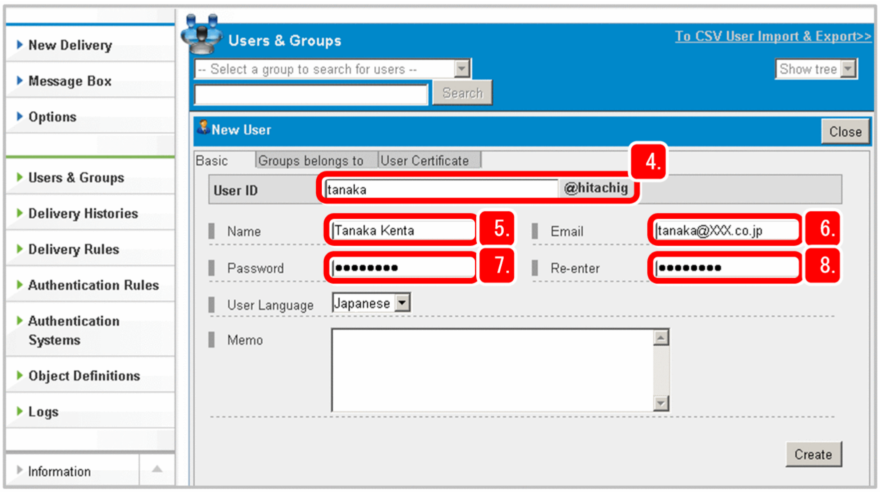
   At the first login to JP1/DH - Server, make sure that you read *2.2 Notes on logging in to JP1/DH - Server for the first time* and perform necessary operations.

2. In the sidebar area, select **Users & Groups**.
   The Users & Groups window appears in the content area.



3. Click **Design**, and then select **New User**.
   The New User window appears.

4. In the **User ID** text box, enter `tanaka`.
   @hitachig, which is the domain ID for Hitachi G, is displayed. The user ID used to log in to JP1/DH - Server will be `tanaka@hitachig`, which is the user ID you entered (`tanaka`) with the domain ID `@hitachig` as the suffix.



User ID: tanaka @hitachig

Name: Tanaka Kenta

Email: tanaka@XXX.co.jp

Password: ●●●●●●●●

Re-enter: ●●●●●●●●

User Language: Japanese

Memo

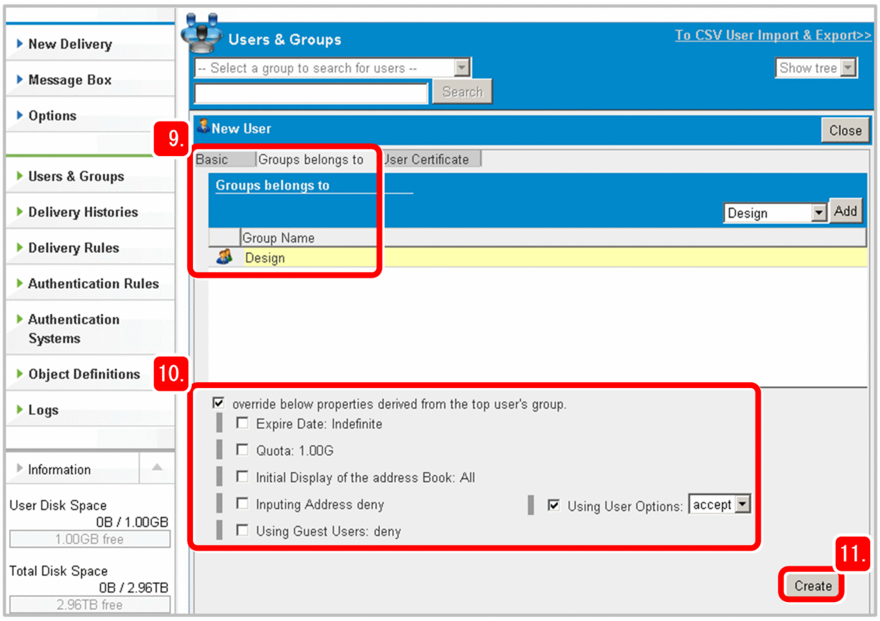
5. In the **Name** text box, enter `Tanaka Kenta`.

6. In the **Email** text box, enter `tanaka@XXX.co.jp`.

7. In the **Password** text box, enter any password.
   The password that is entered here is the initial password to be used for general users to log in to JP1/DH - Server. Enter a character string of at least eight characters. The string can contain alphanumeric characters and symbols (`!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~`).

8. In the **Re-enter** text box, enter the same password as the password entered in the **Password** text box.

9. Select the **Groups belongs to** tab, and then check that **Design** is displayed.



Groups belongs to: Design

Group Name
Design

☑ override below properties derived from the top user's group.

□ Expire Date: Indefinite

□ Quota: 1.00G

□ Initial Display of the address Book: All

□ Inputing Address deny

☑ Using User Options: accept

□ Using Guest Users: deny

User Disk Space
0B / 1.00GB
1.00GB free

Total Disk Space
0B / 2.96TB
2.96TB free

10. Enable the use of options.
    Select the **override below properties derived from the top user's group.** check box.
    Verify that a check box appears at the beginning of **Using User Options: accept**, and then select it.

11. Click the **Create** button.
    The user is created.

Postrequisites

- Create other general users.
- After all users are created, set the address lists to be displayed.

Related topics

- *2.2 Notes on logging in to JP1/DH - Server for the first time*
- *2.8 Planning the domain content structure and operation policy (domain-content manager)*
- *2.9.2 Setting address lists to be displayed (domain-content manager)*

2.9.2 Setting address lists to be displayed (domain-content manager)

The domain-content manager sets up JP1/DH -Server so that a group can view the address list of the group to which it delivers data. Set this information according to the domain content structure and operation policy that you set in advance. You perform this task in the Users & Groups window.

In this example, the address list for Manufacturing will be shown to Design.

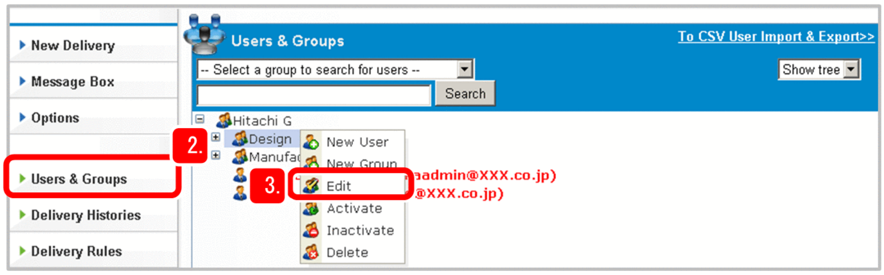
Prerequisites

- These tasks are performed by the domain-content manager.
- You must plan in advance which groups' addresses will be viewed by which groups.
- The groups whose address list is to be viewed must be created in JP1/DH - Server beforehand.

Procedure

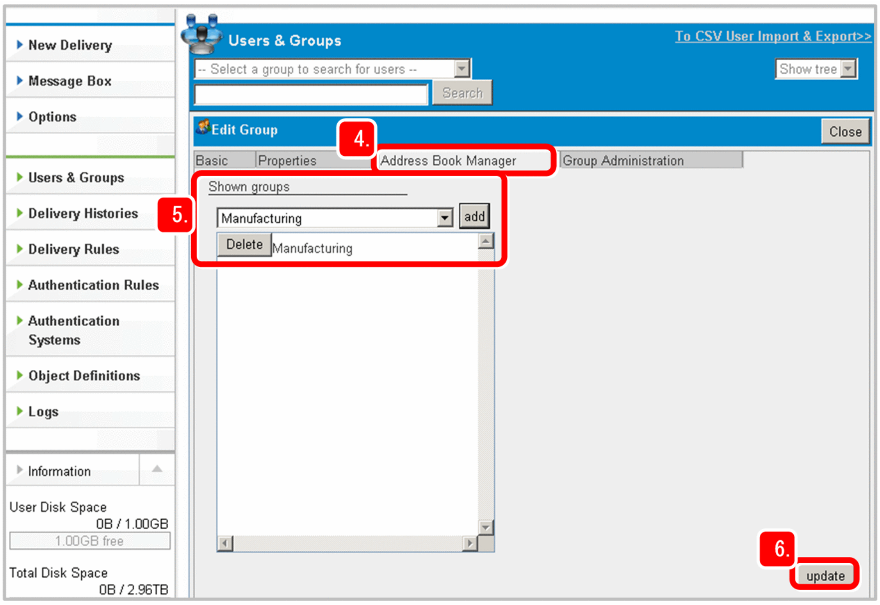
1. Log in to JP1/DH - Server.
   Log in by using the ID (`suzuki@hitachig`) and password of the domain-content manager.

2. In the sidebar area, select **Users & Groups**.
   The Users & Groups window appears in the content area.



3. Click **Design**, and then select **Edit**.
   The Edit Group window appears.

4. Select the **Address Book Manager** tab.



5. From the **Shown groups** drop-down list box, select **Design**. Then, click the **add** button.

6. Click the **Update** button.
   When a user in the Design group delivers data, he or she can now view the address list for users in the Manufacturing group.

Postrequisites

Create delivery policies

Related topics

- *2.8 Planning the domain content structure and operation policy (domain-content manager)*
- *2.9.3 Determining the items related to data delivery and creating delivery policies (domain-content manager)*

2.9.3 Determining the items related to data delivery and creating delivery policies (domain-content manager)

Delivery policies are usually created based on the standard policy that was created by the system administrator.

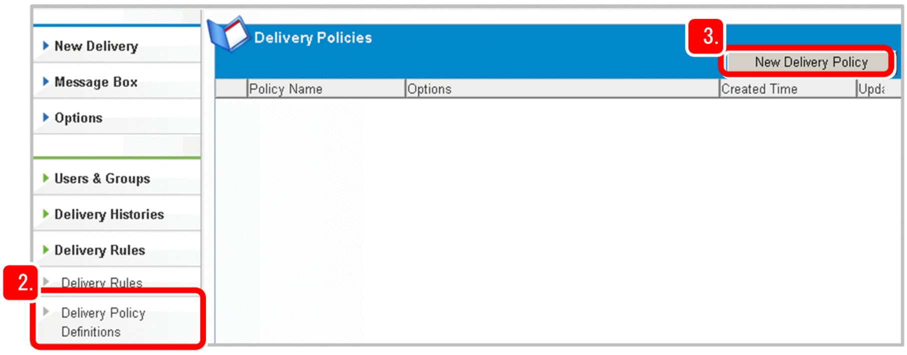
Prerequisites

- These tasks are performed by the domain-content manager.
- The system administrator must create the standard policy beforehand.

Procedure

1. Log in to JP1/DH - Server.
   Log in by using the ID (`suzuki@hitachig`) and password of the domain-content manager.

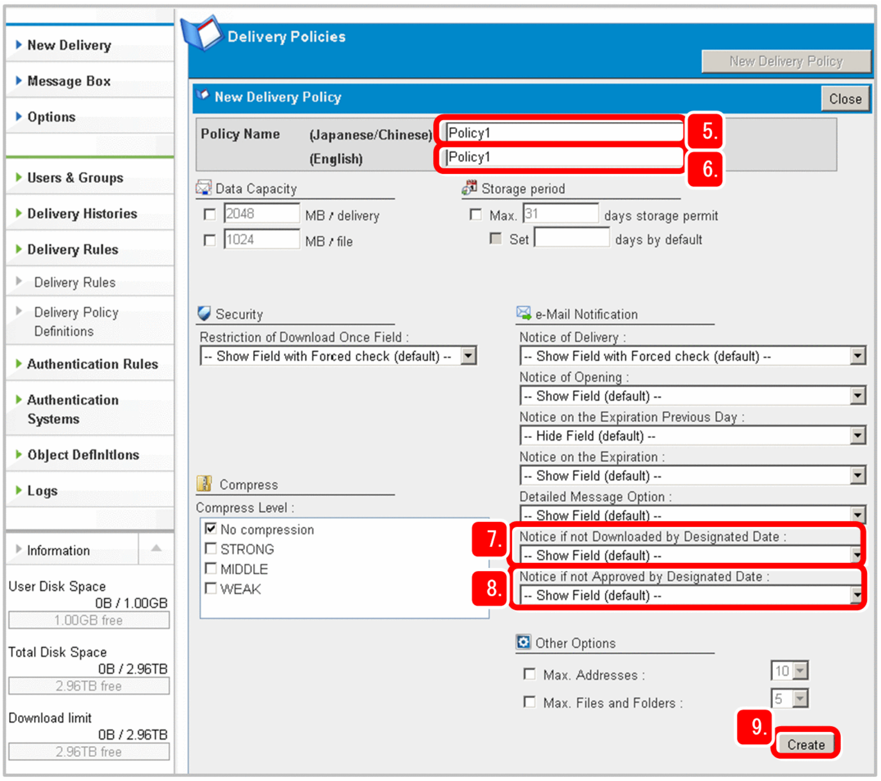
2. In the sidebar area, select **Delivery Rules** and **Delivery Policy Definitions**.
   The Delivery Policies window appears in the content area.



3. In the Delivery Policies window, click the **New Delivery Policy** button.
   The New Delivery Policy window appears.

4. Create a delivery policy.
   The initial display values of the New Delivery Policy window are the values that are set for the standard policy.

5. In the **Policy Name (Japanese/Chinese)** text box, enter `Policy1`.



Policy Name (Japanese/Chinese) Policy1
(English) Policy1

Data Capacity
☐ 2048 MB / delivery
☐ 1024 MB / file

Storage period
☐ Max. 31 days storage permit
☐ Set days by default

Security
Restriction of Download Once Field : -- Show Field with Forced check (default) --

e-Mail Notification
Notice of Delivery : -- Show Field with Forced check (default) --
Notice of Opening : -- Show Field (default) --
Notice on the Expiration Previous Day : -- Hide Field (default) --
Notice on the Expiration : -- Show Field (default) --
Detailed Message Option : -- Show Field (default) --
Notice if not Downloaded by Designated Date : -- Show Field (default) --
Notice if not Approved by Designated Date : -- Show Field (default) --

Compress
Compress Level :
☑ No compression
☐ STRONG
☐ MIDDLE
☐ WEAK

Other Options
☐ Max. Addresses : 10
☐ Max. Files and Folders : 5

User Disk Space
0B / 1.00GB
1.00GB free

Total Disk Space
0B / 2.96TB
2.96TB free

Download limit
0B / 2.96TB
2.96TB free

6. In the **Policy Name (English)** text box, enter `Policy1`.

7. In the **Notice if not Downloaded by Designated Date** drop-down list box, check that **Show Field** is specified.
   If it is not specified, select **Show Field**.

8. In the **Notice if not Approved by Designated Date** drop-down list box, check that **Show Field** is specified.
   If it is not specified, select **Show Field**.

9. Click the **Create** button.
   Policy1 is created.

Postrequisites

Create a data delivery approval route.

Related topics

- *2.9.4 Creating approval routes (domain-content manager)*

2.9.4 Creating approval routes (domain-content manager)

Set an operational policy to prohibit data delivery without a supervisor's approval.

In this example, Sato Daisuke will be set up as an approver.

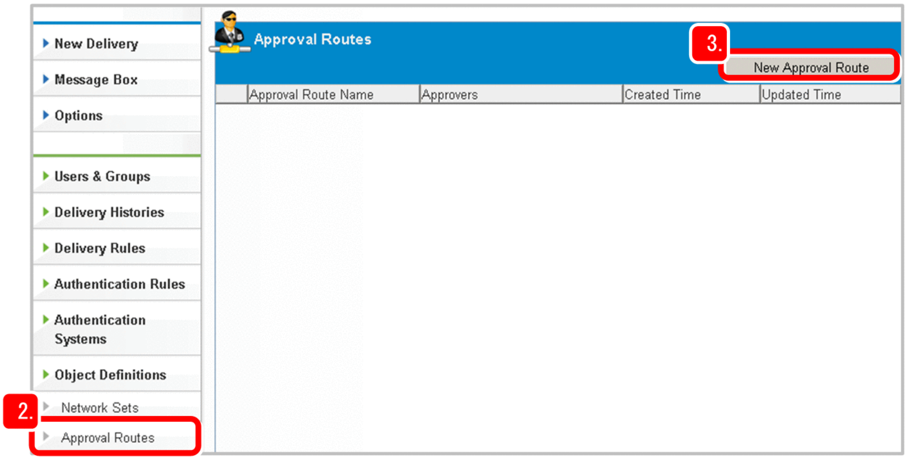
Prerequisites

- These tasks are performed by a domain-content manager.
- Users to be registered as approvers must be created in JP1/DH - Server beforehand.

Procedure

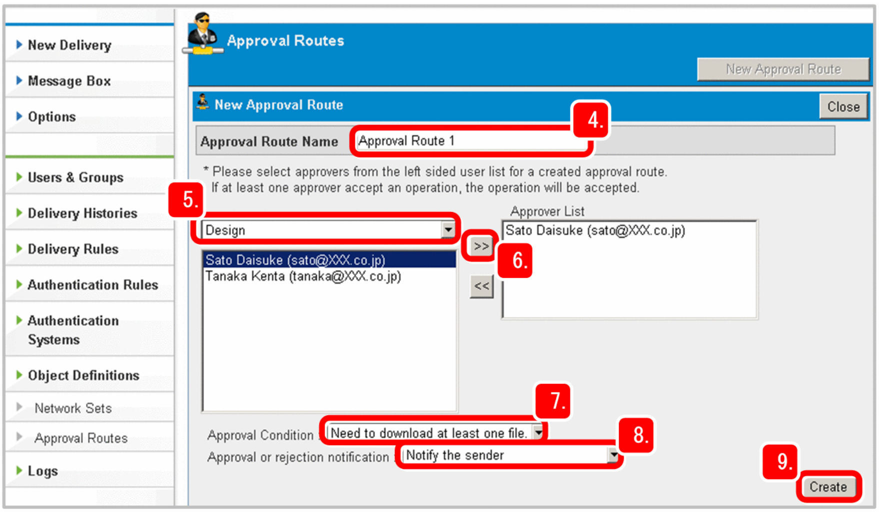
1. Log in to JP1/DH - Server.
   Log in by using the ID (`suzuki@hitachig`) and password of the domain-content manager.

2. In the sidebar area, select **Object Definitions** and **Approval Routes**.
   The Approval Routes window appears in the content area.



3. Click the **New Approval Route** button.
   The New Approval Route window appears.

4. In the **Approval Route Name** text box, enter `Approval Route 1`.



Approval Route Name: Approval Route 1

* Please select approvers from the left sided user list for a created approval route.
If at least one approver accept an operation, the operation will be accepted.

Design

Sato Daisuke (sato@XXX.co.jp)
Tanaka Kenta (tanaka@XXX.co.jp)

Approver List: Sato Daisuke (sato@XXX.co.jp)

Approval Condition: Need to download at least one file.

Approval or rejection notification: Notify the sender

5. From the drop-down list box, select **Design**.
   The list of the users who belong to the group Design is displayed.

6. Select `Sato Daisuke` and click the >> button.
   `Sato Daisuke` appears in the **Approver List** area.

7. From the **Approval Condition** drop-down list box, select **Need to download at least one file.**.
   An approval condition is set so that the approver must download and check at least one delivery data file to approve delivery data.

8. Verify that **Notify the sender** is selected in the **Approval or rejection notification** drop-down list box.
   If **Notify the sender** is not selected, select it now.

9. Click the **Create** button.
   Approval Route 1 is created.

Postrequisites

Create delivery rules.

Related topics

- *2.9.5 Creating delivery rules for groups that combine delivery policies and approval routes (domain-content manager)*

2.9.5 Creating delivery rules for groups that combine delivery policies and approval routes (domain-content manager)

Delivery rules define which delivery policies and approval routes that were created beforehand are applied to which groups.

In this example, Policy1 and Approval Route 1 are applied to the group Design.

Prerequisites

- These tasks are performed by the domain-content manager.
- The domain-content manager must have already created the delivery policies and approval routes.

- The groups to which delivery policies are to be applied must be created in JP1/DH - Server.

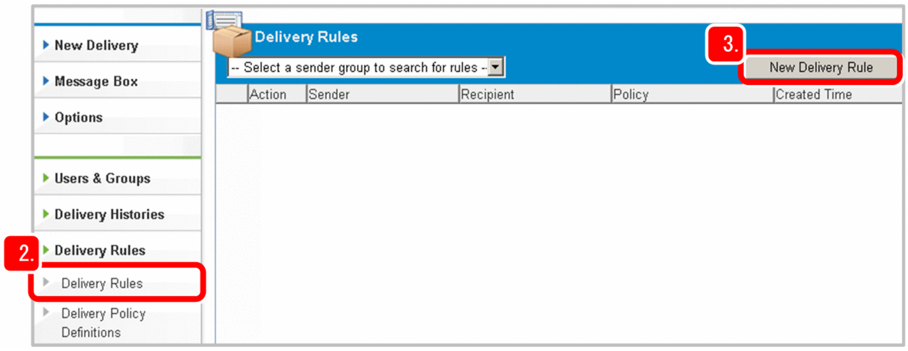
Procedure

1. Log in to JP1/DH - Server.

   Log in by using the ID (`suzuki@hitachig`) and password of the domain-content manager.

2. In the sidebar area, select **Delivery Rules** and **Delivery Rules**.

   The Delivery Rules window appears in the content area.

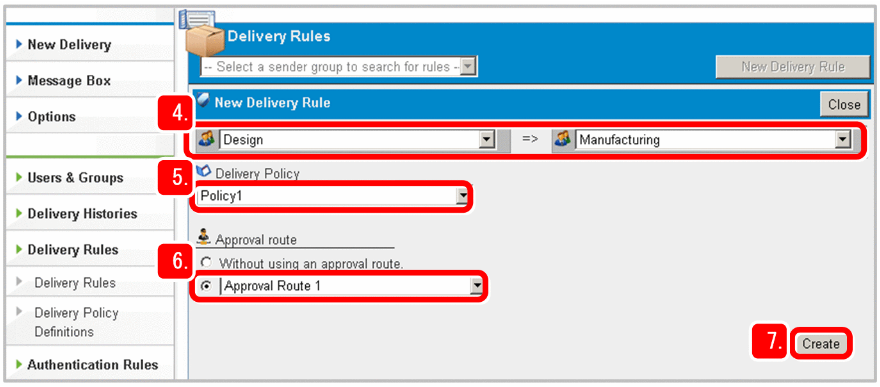


3. Click the **New Delivery Rule** button.

   The New Delivery Rule window appears.

4. From the drop-down list box on the left of the arrow (=>), select **Design**. From the drop-down list box on the right, select **Manufacturing**.

   The group on the left is the sender. The group on the right is the receiver.



5. From the **Delivery Policy** drop-down list box, select **Policy1**.

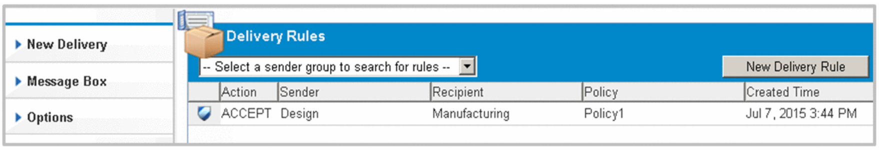
   Policy1 is applied when data is delivered from the group Design.

6. In **Approval route**, select the lower radio button. From the drop-down list box, select **Approval Route 1**.

   Delivery of data from the Design group will require the approval of Sato Daisuke who is assigned to Approval Route 1.

7. Click the **Create** button.

   The rule of applying Policy1 and Approval Route 1 when data is delivered from the group Design to the group Manufacturing is created.



	Action	Sender	Recipient	Policy	Created Time
🛡	ACCEPT	Design	Manufacturing	Policy1	Jul 7, 2015 3:44 PM

Tip

If multiple delivery rules are registered, the delivery rule at the top of the list in the Delivery Rules window is applied first. If you want to preferentially apply a delivery rule, click the icon (🛡) for the delivery rule and then select **Up** to move it to the top of the list.

Postrequisites

Notify the users who will use JP1/DH - Server to deliver data, of any necessary information.

Related topics

- *2.9.3 Determining the items related to data delivery and creating delivery policies (domain-content manager)*
- *2.9.4 Creating approval routes (domain-content manager)*
- *2.10 Notifying general users of information required to use JP1/DH server (domain-content manager)*

2.10 Notifying general users of information required to use JP1/DH server (domain-content manager)

The domain-content manager notifies general users of the information they need to use JP1/DH - Server.

Procedure

1. Before notifying general users, the domain-content manager verifies the following:
   - All JP1/DH - Server users are set.
   - JP1/DH - Server has been set up so that groups that deliver data can view the address list for destination groups.
   - Some users are registered in JP1/DH - Server as approvers.
   - Delivery rules that combine the appropriate delivery policies and approval routes have been created and assigned to the groups that will deliver data.
   - The **Using User Options: accept** check box on the **Groups belongs to** tab is selected.

   > **Important**
   >
   > If the **Using User Options: accept** check box on the **Groups belongs to** tab is not selected, options are not available.
   >
   > If options are not available, users cannot change their initial passwords at the first login.

2. Notify general users of the following necessary information:
   - User ID and initial password
   - JP1/DH - Server URL
   - Details of the tasks to be performed by the users who are registered as approvers
   - Operation manual or documents equivalent to the operation manual
     Example: Chapter 3 in this manual

   > **Tip**
   >
   > Set the initial password with a character string common to general users. By doing this, you can send, in a batch, an email that has the same content to multiple users.
   >
   > Ask the general users to change their passwords from the initial password at the first login.

Postrequisites

This concludes the preparation for JP1/DH - Server operation. Next, use JP1/DH - Server to deliver data.

3 Delivering Data Using JP1/DH - Server

This chapter describes how to access JP1/DH - Server from a web browser and deliver data.

3.1 General procedure for delivering data using JP1/DH - Server

The process of using JP1/DH - Server to deliver data includes the sending of the data, the approving of sent data, and the receiving of the data.

The table below shows the various tasks related to sending data. For details about each task, see the applicable reference.

Overview	Task	Reference
Sending data	Send data.	*3.2.1*
	Check the status and the delivery route of the sent data.	*3.2.2*
Approving sent data	Approve the data sent by using JP1/DH - Server	*3.3*
Receiving data	Receive data by using JP1/DH - Server	*3.4*

3.2 Sending data and checking the status of sent data using JP1/DH - Server

To send data in JP1/DH - Server, use the New Delivery window. To check the status of sent data, use the Out-box window.

> **Important**
>
> When logging into JP1/DH - Server for the first time, make sure that you read *2.2 Notes on logging in to JP1/DH - Server for the first time* and perform the described tasks.

Related topics

- *2.2 Notes on logging in to JP1/DH - Server for the first time*

3.2.1 Sending data

This section describes how to send data, using an example in which Tanaka Kenta in the Design group sends data to Watanabe Makoto in the Manufacturing group.

Prerequisites

- The user who will send the data must be defined in a group in JP1/DH - Server, and possess the ID and password used to log in to JP1/DH - Server.

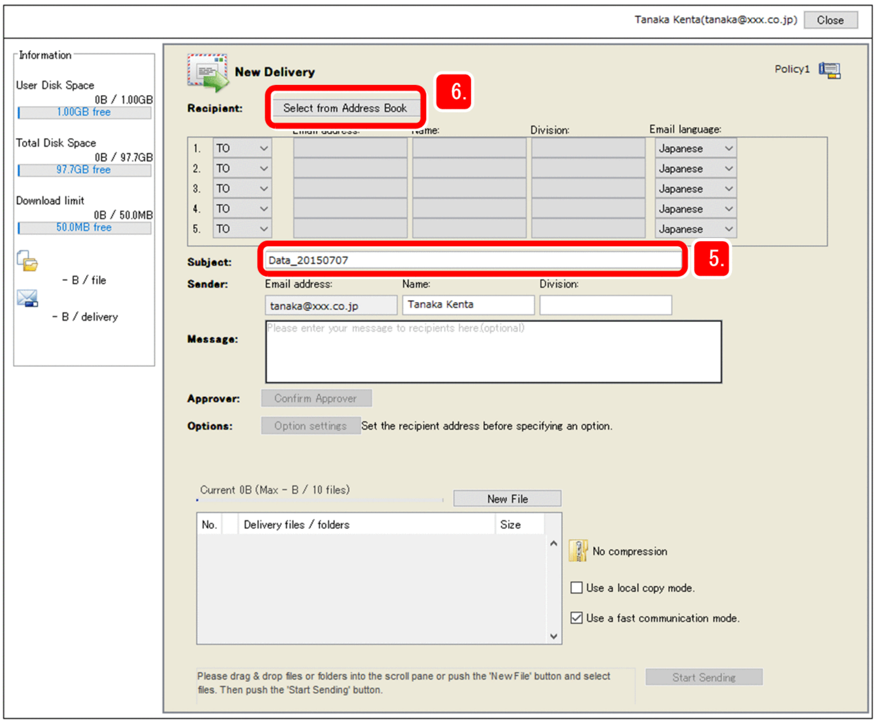
Procedure

1. Prepare the data to be sent, and place it in a local folder.

2. Log in to JP1/DH - Server, and in the sidebar area, select **New Delivery**.
   Log in by using Tanaka Kenta's ID (`tanaka@hitachig`) and password.

3. A dialog box for confirming the download of the `aftclient.dhxc` file appears.
   Click the **Save** button and open the downloaded `aftclient.dhxc`.

4. The New Delivery window appears in a separate window, with `Tanaka Kenta` displayed in the **Sender:** area.



Subject: Data_20150707

Sender: Email address: tanaka@xxx.co.jp Name: Tanaka Kenta Division:

Message: Please enter your message to recipients here(optional)

Options: Set the recipient address before specifying an option.

Current 0B (Max - B / 10 files)

□ Use a local copy mode.

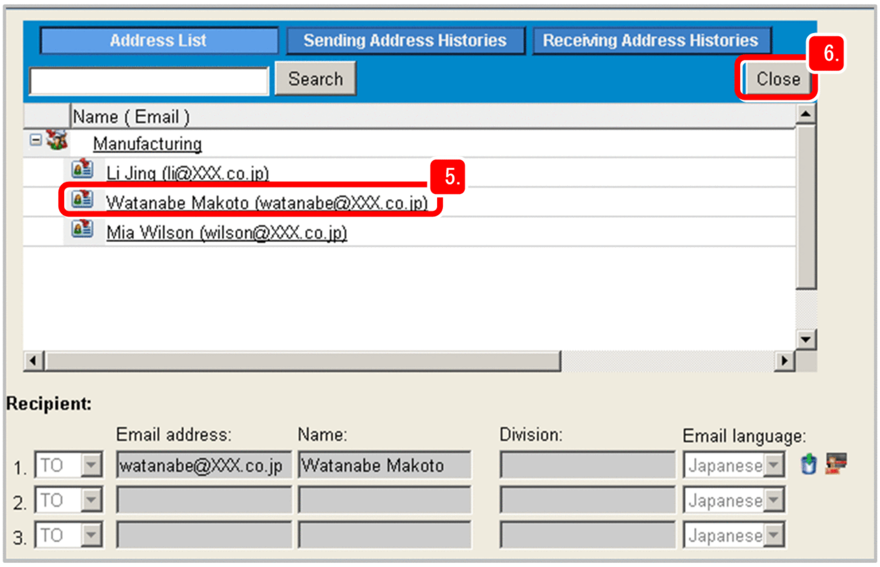
☑ Use a fast communication mode.

Please drag & drop files or folders into the scroll pane or push the 'New File' button and select files. Then push the 'Start Sending' button.

5. Enter the subject line of the email in the **Subject:** field.
   You can enter a maximum of 100 characters.

6. Click the **Select from Address Book** button, and verify that the address list for the Manufacturing group is displayed.

7. Select `Watanabe Makoto`.
   The name and email address of Watanabe Makoto appear in the **Recipient:** area.



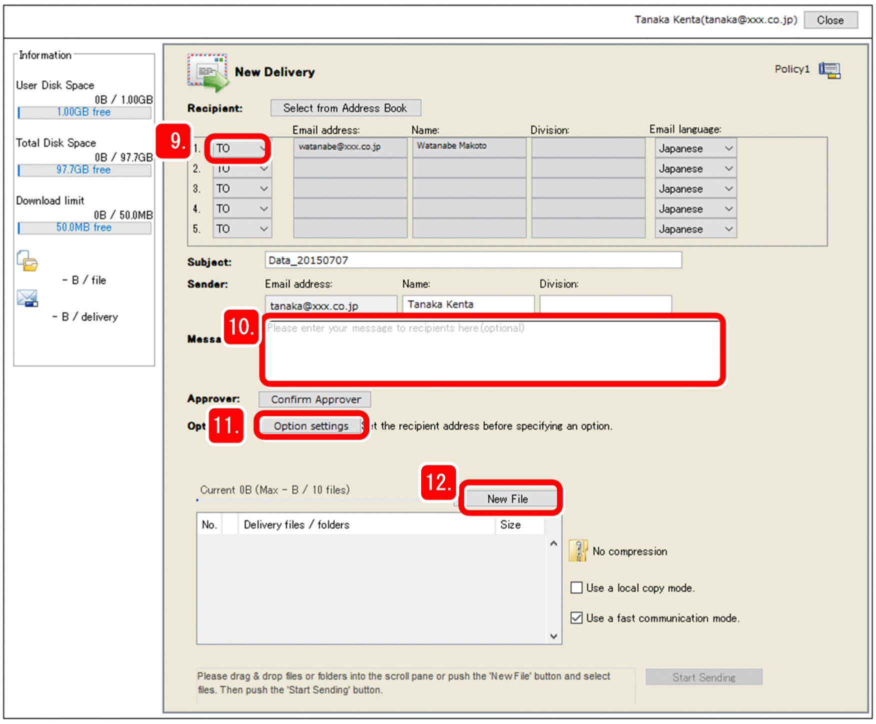
Manufacturing
- Li Jing (li@XXX.co.jp)
- Watanabe Makoto (watanabe@XXX.co.jp)
- Mia Wilson (wilson@XXX.co.jp)

	Email address:	Name:	Division:	Email language:
1. TO	watanabe@XXX.co.jp	Watanabe Makoto		Japanese
2. TO				Japanese
3. TO				Japanese

Important

You can specify a maximum of 100 recipients. This number includes the approver, who will approve the sent data, in addition to the users specified as recipients.

8. Click the **Close** button to close the address list.



Tanaka Kenta(tanaka@xxx.co.jp)

Information

User Disk Space 0B / 1.00GB 1.00GB free

Total Disk Space 0B / 97.7GB 97.7GB free

Download limit 0B / 50.0MB 50.0MB free

- B / file

- B / delivery

New Delivery

Policy1

Recipient:

		Email address:	Name:	Division:	Email language:
1.	TO	watanabe@xxx.co.jp	Watanabe Makoto		Japanese
2.	TO				Japanese
3.	TO				Japanese
4.	TO				Japanese
5.	TO				Japanese

Subject: Data_20150707

Sender: Email address: tanaka@xxx.co.jp Name: Tanaka Kenta Division:

Messa Please enter your message to recipients here.(optional)

Approver:

Opt ‌t the recipient address before specifying an option.

Current 0B (Max - B / 10 files)

No.		Delivery files / folders	Size

No compression

□ Use a local copy mode.

☑ Use a fast communication mode.

Please drag & drop files or folders into the scroll pane or push the 'NewFile' button and select files. Then push the 'Start Sending' button.

9. Select **TO**.

10. Enter a message.

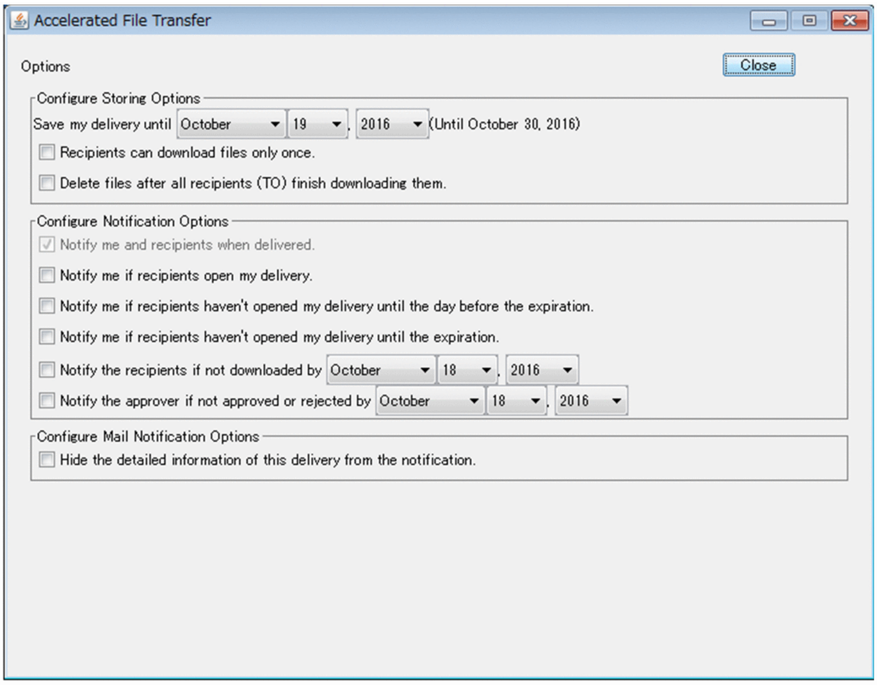
    The message you enter appears as the body text of the email that notifies the recipient when data has arrived. You can enter a maximum of 4,096 characters.

11. Click the **Options settings** button. Display the Options settings dialog notification options.

    Select the check boxes for the notification settings you want to enable.

    You can configure JP1/DH - Server to send notifications when the delivery has not been approved or a recipient has not downloaded the data by a certain date.

Notification option	Content
Notify the recipients if not downloaded by	Specify a date. Recipients are notified if they have not downloaded the data by this date.
Notify the approver if not approved or rejected by	Specify a date. The approver is notified if he or she has not accepted or rejected the delivery by this date.



Options

Configure Storing Options

Save my delivery until October ▾ 19 ▾, 2016 ▾ (Until October 30, 2016)

□ Recipients can download files only once.

□ Delete files after all recipients (TO) finish downloading them.

Configure Notification Options

☑ Notify me and recipients when delivered.

□ Notify me if recipients open my delivery.

□ Notify me if recipients haven't opened my delivery until the day before the expiration.

□ Notify me if recipients haven't opened my delivery until the expiration.

□ Notify the recipients if not downloaded by October ▾ 18 ▾, 2016 ▾

□ Notify the approver if not approved or rejected by October ▾ 18 ▾, 2016 ▾

Configure Mail Notification Options

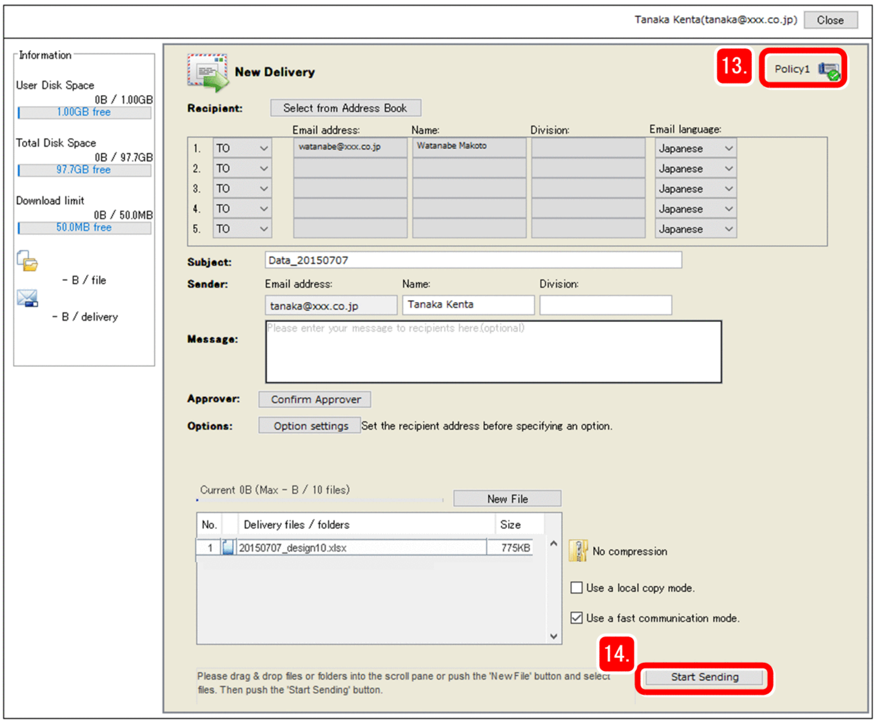
□ Hide the detailed information of this delivery from the notification.

12. Click the **New File** button and select the files and folders to send. Alternatively, you can use a drag-and-drop operation on the files or folders.

    When you click **New File**, the New File dialog box appears. Select the files and folders that you want to send, and then click **Open**.

    If you use a drag-and-drop operation on a drive, the word `Drive` appears in the **Delivery files / folders** field.

    > **Tip**
    >
    > If the drive that contains the files or folders you are sending is a network drive or a drive with a slow access speed, creating a local copy of the files or folders might reduce the transmission time.
    >
    > To do so, select the **Use a local copy mode** check box before selecting the file or folder.
    >
    > You can skip this step if the files and folders you are sending are already on a local drive.



Tanaka Kenta(tanaka@xxx.co.jp) Close

Information

User Disk Space 0B / 1.00GB 1.00GB free

Total Disk Space 0B / 97.7GB 97.7GB free

Download limit 0B / 50.0MB 50.0MB free

- B / file

- B / delivery

New Delivery

13. Policy1

Recipient: Select from Address Book

		Email address:	Name:	Division:	Email language:
1.	TO	watanabe@xxx.co.jp	Watanabe Makoto		Japanese
2.	TO				Japanese
3.	TO				Japanese
4.	TO				Japanese
5.	TO				Japanese

Subject: Data_20150707

Sender: Email address: tanaka@xxx.co.jp Name: Tanaka Kenta Division:

Message: Please enter your message to recipients here.(optional)

Approver: Confirm Approver

Options: Option settings Set the recipient address before specifying an option.

Current 0B (Max - B / 10 files) New File

No.	Delivery files / folders	Size
1	20150707_design10.xlsx	775KB

No compression

☐ Use a local copy mode.

☑ Use a fast communication mode.

14. Start Sending

Please drag & drop files or folders into the scroll pane or push the 'New File' button and select files. Then push the 'Start Sending' button.

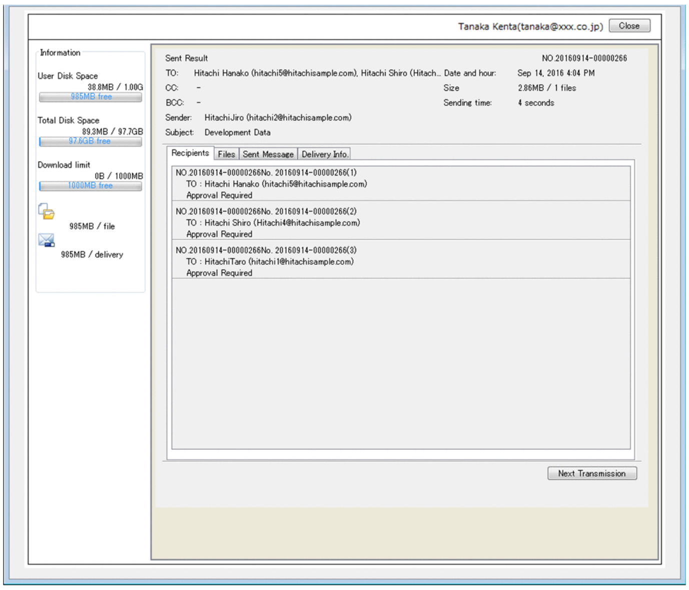
13. Verify that the delivery is ready.

The delivery is ready when the icon at the top right of the window has changed from 🖥 to 🖥✓ .

14. Click the **Start Sending** button.

JP1/DH - Server starts sending the data.

When the data has been sent, the Sent Result window appears with the notification message `Approval Required` displayed in the **Recipients** tab.



Tanaka Kenta(tanaka@xxx.co.jp) Close

Information

User Disk Space 38.8MB / 1.00G 985MB free

Total Disk Space 89.3MB / 97.7GB 97.6GB free

Download limit 0B / 1000MB 1000MB free

985MB / file

985MB / delivery

Sent Result NO.20160914-00000266

TO: Hitachi Hanako (hitachi5@hitachisample.com), Hitachi Shiro (Hitach... Date and hour: Sep 14, 2016 4:04 PM

CC: - Size 2.86MB / 1 files

BCC: - Sending time: 4 seconds

Sender: HitachiJiro (hitachi2@hitachisample.com)

Subject: Development Data

Recipients | Files | Sent Message | Delivery Info.

NO.20160914-00000266No. 20160914-00000266(1)
TO : Hitachi Hanako (hitachi5@hitachisample.com)
Approval Required

NO.20160914-00000266No. 20160914-00000266(2)
TO : Hitachi Shiro (Hitachi4@hitachisample.com)
Approval Required

NO.20160914-00000266No. 20160914-00000266(3)
TO : HitachiTaro (hitachi1@hitachisample.com)
Approval Required

Next Transmission

Postrequisites

- Verify that you have received a notification email from JP1/DH - Server indicating that the data has been sent.

Receiving this notification email does not mean that the data has been delivered to its recipients. It simply means that the process of sending the data was completed without any issues. Data for which delivery processing is complete will be delivered to the recipients after being approved by the approver.

- You can view the status and delivery route of sent data in the Out-box window.

Related topics

- *3.2.2 Checking the status and the delivery route of sent data*

3.2.2 Checking the status and the delivery route of sent data

By displaying detailed information of sent data, you can check who is approving the data you sent, or the current status of the data.

The following describes how to check the status of sent data, using an example of data sent from Tanaka Kenta in the Design group to Watanabe Makoto in the Manufacturing group.

Prerequisites

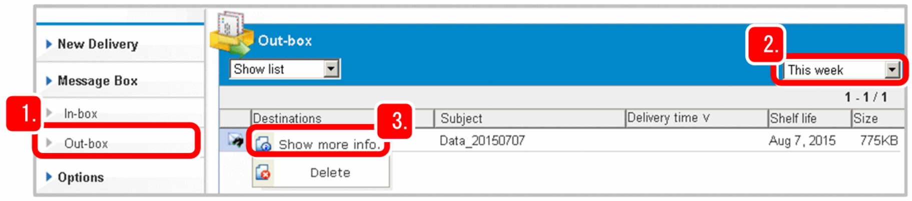
- You must check that the processing of data delivery has completed without problem by receiving notification such as an email from JP1/DH - Server in advance.

Procedure

1. Log in to JP1/DH - Server. Then, from the sidebar area, select **Message Box**, and then **Out-box**.

   Log in by using Tanaka Kenta's ID (`tanaka@hitachig`) and password.

   The Out-box window appears.



2. Select the period for which you want to view the history of sent data.

3. Click the icon ( ) at the beginning of the sent data and select **Show more info.**.

   Detailed information about the sent data is displayed.

4. Select the tab for the content you want to check.

   If you want to check the sent data, select the **Files** tab.

   Detailed information about the sent data is displayed.

   If you want to check whether approval is required to send data to Watanabe Makoto, select the **Recipients Info.** tab.

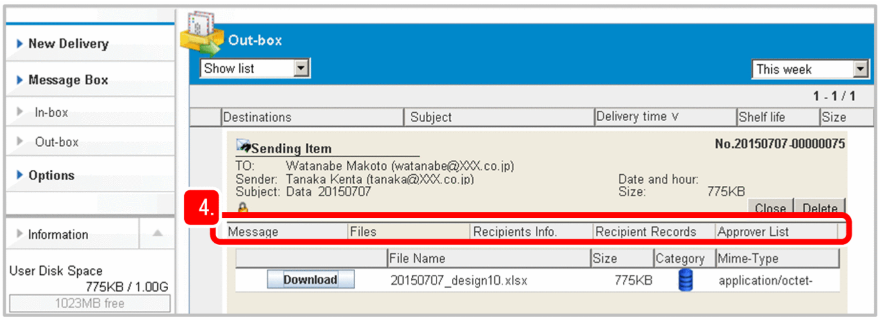
   The message `Approval Required` is displayed.

   If you want to check whether sent data has been received by the recipient, select the **Recipient Records** tab.

   Whether Watanabe Makoto has opened or downloaded the data is displayed.

   If you want to check who the approver is, select the **Approver List** tab.

   `Sato Daisuke` is displayed.



User Disk Space
775KB / 1.00G
1023MB free

1 - 1 / 1

Destinations	Subject	Delivery time ∨	Shelf life	Size

Sending Item No.20150707-00000075

TO: Watanabe Makoto (watanabe@XXX.co.jp)
Sender: Tanaka Kenta (tanaka@XXX.co.jp)
Subject: Data 20150707
Date and hour:
Size: 775KB

	File Name	Size	Category	Mime-Type
Download	20150707_design10.xlsx	775KB		application/octet-

3.3 Approving sent data in JP1/DH - Server

When data is sent from JP1/DH - Server, a notification email is sent from JP1/DH - Server to the approver according to the approval route. When the notification email is received, the approver needs to log into JP1/DH - Server to verify that the target data can be sent to the recipient.

In this example, Sato Daisuke will approve the data sent to Watanabe Makoto by Tanaka Kenta.

Prerequisites

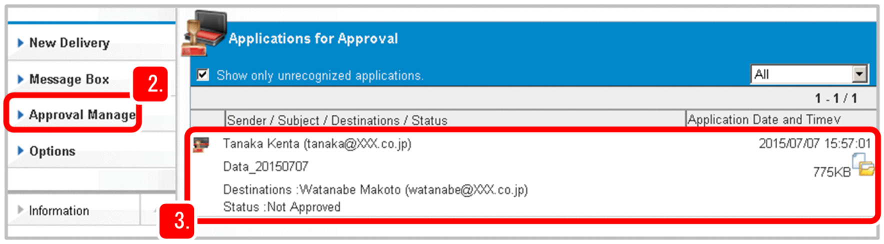
- The client environment must be checked and completed in advance.
- The user who approves the sending of data must be set as an approver in JP1/DH - Server, and must have an ID and a password to log into JP1/DH - Server.

Procedure

1. Log in to JP1/DH - Server.
   Log in by using Sato Daisuke's ID (`sato@hitachig`) and password.

> **Important**
>
> When logging into JP1/DH - Server for the first time, make sure that you read *2.2 Notes on logging in to JP1/DH - Server for the first time* and perform the described tasks.

2. From the sidebar area, select **Approval Manager**.
   The Applications for Approval window appears.

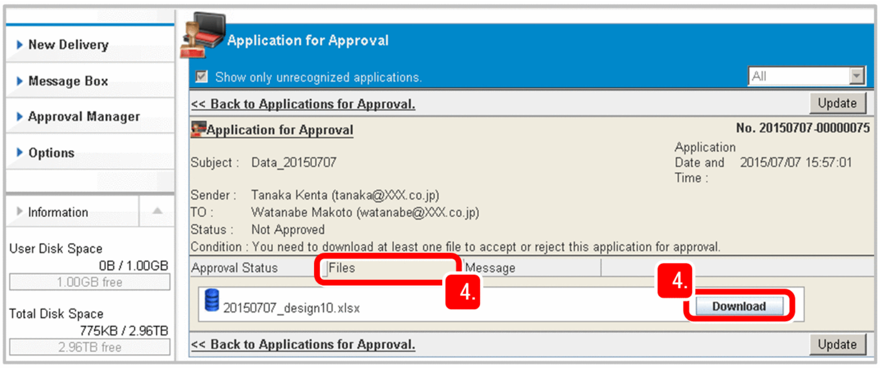

New Delivery
Message Box
Approval Manage
Options
Information
2.
3.
Applications for Approval
All
1 - 1 / 1
Sender / Subject / Destinations / Status
Application Date and Timev

☑ Show only unrecognized applications.

Tanaka Kenta (tanaka@XXX.co.jp) 2015/07/07 15:57:01
Data_20150707 775KB
Destinations :Watanabe Makoto (watanabe@XXX.co.jp)
Status :Not Approved

3. Select the application from Tanaka Kenta.
   The Application for Approval window appears.

4. Select the **Files** tab, and download the data file that needs to be approved.
   Check the content of the downloaded file.



☑ Show only unrecognized applications.

No. 20150707-00000075

Subject : Data_20150707
Application Date and Time : 2015/07/07 15:57:01
Sender : Tanaka Kenta (tanaka@XXX.co.jp)
TO : Watanabe Makoto (watanabe@XXX.co.jp)
Status : Not Approved
Condition : You need to download at least one file to accept or reject this application for approval.

20150707_design10.xlsx

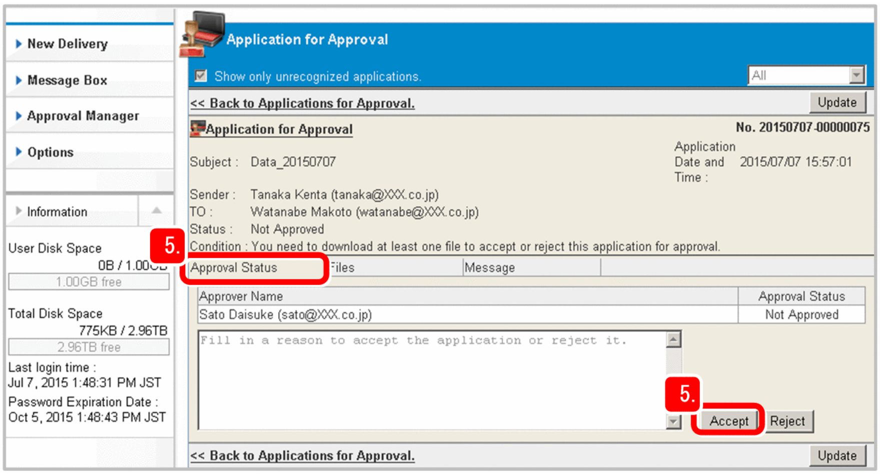
User Disk Space
0B / 1.00GB
1.00GB free

Total Disk Space
775KB / 2.96TB
2.96TB free

5. Select the **Approval Status** tab and click the **Accept** button.

A confirmation dialog box appears.

When the **OK** button is clicked, the application is approved.



☑ Show only unrecognized applications.

Application for Approval

No. 20150707-00000075

Subject : Data_20150707

Application Date and Time : 2015/07/07 15:57:01

Sender : Tanaka Kenta (tanaka@XXX.co.jp)

TO : Watanabe Makoto (watanabe@XXX.co.jp)

Status : Not Approved

Condition : You need to download at least one file to accept or reject this application for approval.

Approval Status

Approver Name	Approval Status
Sato Daisuke (sato@XXX.co.jp)	Not Approved

Fill in a reason to accept the application or reject it.

User Disk Space
0B / 1.00GB
1.00GB free

Total Disk Space
775KB / 2.96TB
2.96TB free

Last login time :
Jul 7, 2015 1:48:31 PM JST

Password Expiration Date :
Oct 5, 2015 1:48:43 PM JST

Operation result

When the application is approved, the recipient of the data from JP1/DH - Server, in this case Watanabe Makoto, is notified by email that the data has arrived.

Tanaka Kenta, who sent the data, is notified by email that the approval request has been accepted.

Tip

When data is sent from JP1/DH - Server, a notification email is sent from JP1/DH - Server to the approver according to the approval route. The email also contains a URL. By clicking the URL and logging into JP1/DH - Server from the displayed Login window, the approver can also download and approve the data.

Related topics

- *2.2 Notes on logging in to JP1/DH - Server for the first time*

3.4 Receiving data from JP1/DH - Server

When data is sent from JP1/DH - Server, a notification email is sent from JP1/DH - Server to the recipient user notifying him or her that the data has arrived. When the notification email is received, the recipient needs to log into JP1/DH - Server to download the target data.

In this example, Watanabe Makoto in the Manufacturing group receives the data sent by Tanaka Kenta in the Design group.

Prerequisites

- The client environment must be checked and completed in advance.
- The user who receives the data must be set in JP1/DH - Server group, and must have an ID and a password to log into JP1/DH - Server.

Procedure

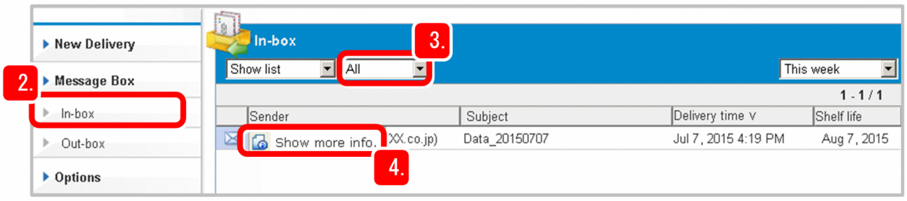
1. Log in to JP1/DH - Server.

   Log in by using Watanabe Makoto's ID (`watanabe@hitachig`) and password.

   > **Important**
   >
   > When logging into JP1/DH - Server for the first time, make sure that you read *2.2 Notes on logging in to JP1/DH - Server for the first time* and perform the described tasks.

2. From the sidebar area, select **Message Box**, and then **In-box**.

   The In-box window appears.



Sender	Subject	Delivery time ∨	Shelf life
XX.co.jp)	Data_20150707	Jul 7, 2015 4:19 PM	Aug 7, 2015

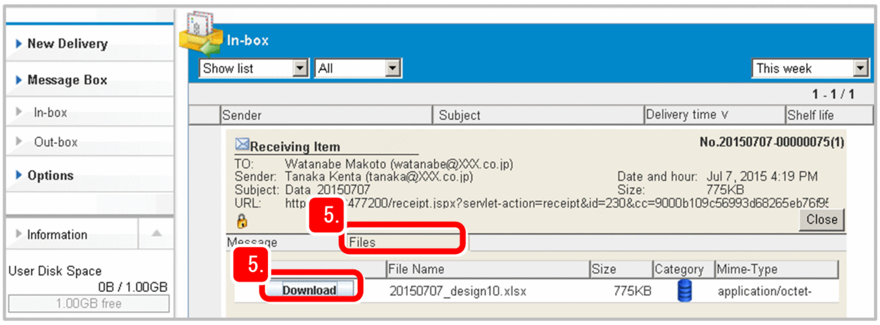
3. For the processing status to be displayed in the inbox, select **All**.

4. Click the icon (✉) for the message sent by `Tanaka Kenta`, and then select **Show more info.**.

   The contents of the delivery data is displayed in the Receiving Item window.

5. Select the **Files** tab, and click the **Download** button.

   A dialog box for downloading the `aftclient.dhxc` file appears. The Downloader window appears after you download the file and open it.



No.20150707-00000075(1)

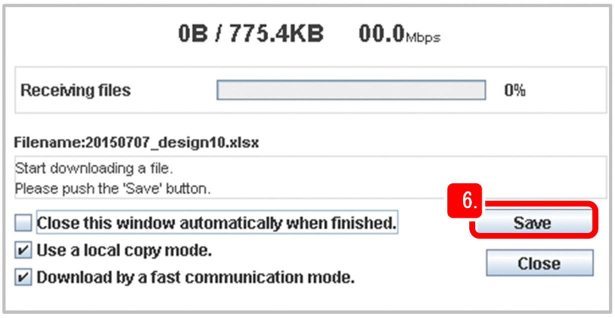
TO: Watanabe Makoto (watanabe@XXX.co.jp)
Sender: Tanaka Kenta (tanaka@XXX.co.jp)
Subject: Data 20150707
URL: http 477200/receipt.jspx?servlet-action=receipt&id=230&cc=9000b109c56993d68265eb76f9
Date and hour: Jul 7, 2015 4:19 PM
Size: 775KB

User Disk Space 0B / 1.00GB
1.00GB free

	File Name	Size	Category	Mime-Type
Download	20150707_design10.xlsx	775KB	🛢	application/octet-

6. Click the **Save** button and select the destination where the file is to be stored.

   If you want to specify a folder other than the local folder as the destination, select the **Use a local copy mode** check box. Selecting this check box can sometimes shorten the time to download the selected file or folder.

   0B / 775.4KB 00.0Mbps

   Receiving files 0%

   Filename:20150707_design10.xlsx

   Start downloading a file.
   Please push the 'Save' button.

   □ Close this window automatically when finished.
   ☑ Use a local copy mode.
   ☑ Download by a fast communication mode.

7. The Downloading Finished!! dialog box appears.

   The time taken to download the file is displayed in the download time.

8. Click the **OK** button.

   The download is complete.

Operation result

When the recipient (Watanabe Makoto) opens the email and downloads the data, the status of the message in the **Recipient Records** tab in the Out-box of the sender (Tanaka Kenta) changes to **Opened** and **Downloaded**.

Tip

When data is sent from JP1/DH - Server, a notification email is sent from JP1/DH - Server to the recipient user notifying him or her that the data has arrived. The email contains a URL for receiving the data. By clicking the URL and logging into JP1/DH - Server from the displayed Login window, the recipient can also download and open the data.

Related topics

- *2.2 Notes on logging in to JP1/DH - Server for the first time*

Appendixes

A. Advanced Use

This appendix describes additional functionality and operational methods that you can use to get the most out JP1/DH - Server. For details, see the manuals for the JP1/DH - Server series.

Purpose	Overview of functionality and operational method	Functionality to use	Reference
Batch registering users or groups	This functionality enables you to import a CSV file in which user information or group information has been defined, and register the file content into JP1/DH - Server in a batch operation. This enables you to efficiently register large numbers of users and groups.	User setup Import/Export (JP1/DH - Server)	*Users & Groups (batch management)* in the manual *JP1/Data Highway - Server Administrator Guide*
Delivering data automatically	This functionality enables you to build jobs for file delivery that uses JP1/DH Server, and register those jobs into the work managed by JP1/AJS3. The functionality enables you to execute data deliveries automatically, and helps to perform work efficiently.	n/a	Explanations related to JP1/DH - AJE in the manual *JP1/Data Highway - Server Configuration and Administration Guide*, and the *JP1/Data Highway - Automatic Job Executor Operation manual*
Linking multiple server systems and operating them as a single system, and enabling business work to continue when a problem occurs	This functionality enables use of logical IP addresses so that a client machine can access JP1/DH - Server in a cluster configuration. Operating the system in a cluster configuration can improve the availability of business systems.	n/a	Explanations related to *Configurations for Clustered System Operations* in the manual *JP1/Data Highway - Server Configuration and Administration Guide*

n/a: Not applicable

B. Version Changes

This appendix describes the changes in each version.

B.1 Changes in version 12-00

- The following OS are supported:
  - macOS 10.13 (High Sierra)
- The following web browser is change of supported version:
  - Mozilla Firefox ESR
- The following web browser are supported:
  - Safari 11
- The application (App) that is used to send and receive files and messages is now supported.
- The following OSs are no longer supported:
  - Windows Server 2008 R2

B.2 Changes in version 11-50

- The following OS are supported:
  - macOS 10.12 (Sierra)
- The following web browser are supported:
  - Microsoft Edge
  - Mozilla Firefox(R) ESR 52
  - Google Chrome 52 or later
  - Safari 10
- The default bit length for the creation of a secret key was changed.
- The subject name format specified for the certificate was changed.
- The default bit length for the creation of a self-signed server certificate was changed.
- The commands were changed to be used when creating a server certificate for the production environment.

B.3 Changes in version 11-10

- The following OSs are now supported:
  - Windows Server 2016
  - OS X 10.11 (El Capitan)
- The following OSs are no longer supported:
  - Windows 8
- The following web browser are supported:

    - Safari 9
- The following web browsers are no longer supported:
    - Internet Explorer 8
    - Internet Explorer 9
    - Internet Explorer 10
    - Mozilla Firefox ESR 31
    - Mozilla Firefox ESR 38

C. Reference Material for This Manual

This appendix provides reference information, including various conventions, for this manual.

C.1 Related publications

This manual is part of a related set of manuals. The manuals in the set are listed below (with the manual numbers):

- *JP1 Version 12 JP1/Data Highway - Server Configuration and Administration Guide* (3021-3-D41 (E))
- *JP1 Version 12 JP1/Data Highway - Server System Administrator Guide* (3021-3-D42(E))
- *JP1 Version 12 JP1/Data Highway - Server Administrator Guide* (3021-3-D43(E))
- *JP1 Version 12 JP1/Data Highway - Server User's Guide* (3021-3-D44(E))
- *JP1 Version 11 JP1/Data Highway - Automatic Job Executor Operation manual* (3021-3-B46(E))

C.2 Abbreviations for Microsoft product names

Full name or meaning	Abbreviation	
Microsoft(R) Windows Server(R) 2008 R2 Datacenter (Service Pack 1)	Windows Server 2008 R2	Windows
Microsoft(R) Windows Server(R) 2008 R2 Enterprise (Service Pack 1)		
Microsoft(R) Windows Server(R) 2008 R2 Standard (Service Pack 1)		
Microsoft(R) Windows Server(R) 2012 Datacenter	Windows Server 2012	
Microsoft(R) Windows Server(R) 2012 Standard		
Microsoft(R) Windows Server(R) 2012 R2 Datacenter (with update/without update)	Windows Server 2012 R2	
Microsoft(R) Windows Server(R) 2012 R2 Standard (with update/without update)		
Microsoft(R) Windows Server(R) 2016 Datacenter	Windows Server 2016	
Microsoft(R) Windows Server(R) 2016 Standard		
Microsoft(R) Windows(R) 7 Enterprise (Service Pack 1 or later)	Windows 7	
Microsoft(R) Windows(R) 7 Professional (Service Pack 1 or later)		
Microsoft(R) Windows(R) 7 Ultimate (Service Pack 1 or later)		
Windows(R) 8.1 (32 bit/64 bit) (with update/without update)#	Windows 8.1	
Windows(R) 8.1 Enterprise (32 bit/64 bit) (with update/without update)#		
Windows(R) 8.1 Pro (32 bit/64 bit) (with update/without update)#		
Windows(R) 10 Enterprise (32 bit/64 bit)#	Windows 10	
Windows(R) 10 Home (32 bit/64 bit)#		
Windows(R) 10 Pro (32 bit/64 bit)#		
Windows(R) Internet Explorer(R)	Internet Explorer	

#: Operation in the Modern UI is not supported.

C.3 Conventions: Installation folder for JP1/DH - Server

The default installation folder for JP1/DH - Server is as follows:

system-drive`:\Program Files\Hitachi\jp1dh\server`

C.4 Conventions: Abbreviations for product names

This manual uses the following abbreviations for product names. However, when necessary, the product names are written in full.

Full name or meaning	Abbreviation	
JP1/Automatic Job Management System 3	JP1/AJS3	
JP1/Data Highway - Automatic Job Executor	JP1/DH - AJE	
JP1/Data Highway - Server	JP1/DH - Server	
Red Hat Enterprise Linux(R) Server 6 (64-bit x86_64)	Linux 6 (x64)	Linux

C.5 Conventions: Acronyms

This manual also uses the following acronyms:

Acronym	Full name or meaning
Ajax	Asynchronous JavaScript + XML
CN	Common Name
CSS	Cascading Style Sheets
CSV	Comma Separated Values
DOM	Document Object Model
FQDN	Fully Qualified Domain Name
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol over Secure Socket Layer
ID	Identification Data
OS	Operating System
OU	Organization Unit
SSL	Secure Socket Layer
URL	Uniform Resource Locator
XML	Extensible Markup Language

C.6 Conventions: Units (such as KB, MB, GB, and TB)

This manual uses the following conventions:

- 1 KB (kilobyte) is 1,024 bytes.
- 1 MB (megabyte) is $1{,}024^2$ bytes
- 1 GB (gigabyte) is $1{,}024^3$ bytes.
- 1 TB (terabyte) is $1{,}024^4$ bytes.

D. Glossary

approval route

A rule that consists of the approvers of a delivery and the conditions for approval. An approval route is included in a delivery rule. An approval route is specified by a domain-content manager who has *representative user* authorities.

approver

A *general user* who has the role of approving applications for data deliveries. This role is specified by a domain-content manager who has *representative user* authorities.

authentication policy

The policy that governs the authentication passwords for users. This policy defines, for example, the complexity and length required for passwords. The authentication policy is managed by the *system administrator*.

delivery policy

A policy for data delivery by using JP1/DH - Server. This policy defines, for example, the size of files that can be delivered or the period that files are to be stored.

delivery rule

A rule that defines the scope of application of both a *delivery policy* and an *approval route*. A delivery rule is managed by a domain-content manager who has *representative user* authorities.

domain

One of the groups. A domain is a group for managing subordinate groups. A *system administrator* creates a domain directly under All Groups, which is the top-level group of JP1/DH - Server. A domain is managed by a domain-content manager who has *representative user* authorities.

In JP1/DH - Server, data is delivered between groups within the same domain. Only the *system administrator* can manage data of multiple domains

download limit

The total amount of data that can be downloaded in one month. The download limit is specified by the *system administrator*.

general user (authorities)

One of the user authorities of JP1/DH - Server. General user authorities are granted to a user who sends or receives data by using JP1/DH - Server. A general user is managed by a domain-content manager who has *representative user* authorities.

group

A unit for managing users. A group is managed by a domain-content manager who has *representative user* authorities.

representative user (authorities)

One of the user authorities of JP1/DH - Server. *Representative user* authorities are granted to a user who manages the domain.

standard authentication policy

The default authentication policy for the entire JP1/DH - Server system. The standard authentication policy is specified by the *system administrator*.

standard policy

The default delivery policy for the entire JP1/DH - Server system. The standard policy is specified by the *system administrator*.

system administrator

The user who installs and configures JP1/DH - Server. The system administrator also manages the JP1/DH - Server domain and *representative users*.

total disk space

The amount of disk storage allocated to a domain. A user cannot send files that exceed the amount of free disk space. The total disk space is specified by the *system administrator*.

user

A person who uses JP1/DH - Server. Users include the *system administrator*, *representative users*, and *general users*.

Index

Hitachi, Ltd.

6-6, Marunouchi 1-chome, Chiyoda-ku, Tokyo, 100–8280 Japan