

JP1 Version 11

**JP1/Data Highway - Server System Administrator
Guide**

3021-3-B43-20(E)

Notices

■ Relevant program products

For details about the applicable OS versions, and a service pack and patch that are prerequisites for JP1/Data Highway - Server, check the *Release Notes*.

P-2A41-9ABL JP1/Data Highway - Server version 11-50 (For Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016)

P-8141-9ABL JP1/Data Highway - Server version 11-50 (For Linux 6 (x64))

P-2A41-9BBL JP1/Data Highway - Server Starter Edition 11-50 (For Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016)

P-8141-9BBL JP1/Data Highway - Server Starter Edition 11-50 (For Linux 6 (x64))

P-2A41-9CBL JP1/Data Highway - Server Starter to Standard Upgrade 11-50 (For Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016)

P-8141-9CBL JP1/Data Highway - Server Starter to Standard Upgrade 11-50 (For Linux 6 (x64))

■ Trademarks

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

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

Intel is a trademark of Intel Corporation in the U.S. and/or other countries.

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

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.



This product includes RSA BSAFE Cryptographic software of EMC Corporation.



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 (ey@cryptsoft.com)
3. This product includes software written by Tim Hudson (tjh@cryptsoft.com)
4. This product includes the OpenSSL Toolkit software used under OpenSSL License and Original SSLeay License. OpenSSL License and Original SSLeay License are as follow:

LICENSE ISSUES

=====

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

```

-----
/* =====
* Copyright (c) 1998-2016 The OpenSSL Project. All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
* notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
* notice, this list of conditions and the following disclaimer in
* the documentation and/or other materials provided with the
* distribution.
*
* 3. All advertising materials mentioning features or use of this
* software must display the following acknowledgment:
* "This product includes software developed by the OpenSSL Project
* for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
* endorse or promote products derived from this software without
* prior written permission. For written permission, please contact
* openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
* nor may "OpenSSL" appear in their names without prior written
* permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
* acknowledgment:
* "This product includes software developed by the OpenSSL Project
* for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;

```

```

* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* =====
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com). This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/
Original SSLeay License
-----
/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
* All rights reserved.
*
* This package is an SSL implementation written
* by Eric Young (eay@cryptsoft.com).
* The implementation was written so as to conform with Netscapes SSL.
*
* This library is free for commercial and non-commercial use as long as
* the following conditions are aheared to. The following conditions
* apply to all code found in this distribution, be it the RC4, RSA,
* lhash, DES, etc., code; not just the SSL code. The SSL documentation
* included with this distribution is covered by the same copyright terms
* except that the holder is Tim Hudson (tjh@cryptsoft.com).
*
* Copyright remains Eric Young's, and as such any Copyright notices in
* the code are not to be removed.
* If this package is used in a product, Eric Young should be given
attribution
* as the author of the parts of the library used.
* This can be in the form of a textual message at program startup or
* in documentation (online or textual) provided with the package.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the copyright
* notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright

```

```

* notice, this list of conditions and the following disclaimer in the
* documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
* must display the following acknowledgement:
* "This product includes cryptographic software written by
* Eric Young (eay@cryptsoft.com)"
* The word 'cryptographic' can be left out if the routines from the library
* being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
* the apps directory (application code) you must include an acknowledgement:
* "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
*
* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed. i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]
*/

```

■ Microsoft product name abbreviations

This manual uses the following abbreviations for Microsoft product names.

Full name or meaning	Abbreviation	
Windows(R) Internet Explorer(R)	Internet Explorer	
Windows(R) 10 Home	Windows 10	Windows
Windows(R) 10 Pro		
Windows(R) 10 Enterprise		
Microsoft(R) Windows(R) 7 Professional	Windows 7	
Microsoft(R) Windows(R) 7 Enterprise		
Microsoft(R) Windows(R) 7 Ultimate		

Full name or meaning	Abbreviation	
Windows(R) 8.1	Windows 8.1	Windows
Windows(R) 8.1 Pro		
Windows(R) 8.1 Enterprise		
Microsoft(R) Windows Server(R) 2008 R2 Datacenter	Windows Server 2008 R2	
Microsoft(R) Windows Server(R) 2008 R2 Enterprise		
Microsoft(R) Windows Server(R) 2008 R2 Standard		
Microsoft(R) Windows Server(R) 2012 Standard	Windows Server 2012	
Microsoft(R) Windows Server(R) 2012 Datacenter		
Microsoft(R) Windows Server(R) 2012 R2 Standard	Windows Server 2012 R2	
Microsoft(R) Windows Server(R) 2012 R2 Datacenter		
Microsoft(R) Windows Server(R) 2016 Standard	Windows Server 2016	
Microsoft(R) Windows Server(R) 2016 Datacenter		

■ 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

Nov. 2017: 3021-3-B43-20(E)

■ Copyright

All Rights Reserved. Copyright (C) 2015, 2017, Hitachi, Ltd.

All Rights Reserved. Copyright (C) 2015, 2017, Hitachi Solutions, Ltd.

Summary of amendments

The following table lists changes in this manual (3021-3-B43-20(E)) and product changes related to this manual.

Changes	Location
The following web browsers are supported: <ul style="list-style-type: none">• Mozilla Firefox ESR 52• Safari 10	1.1.3(1) , 1.1.3(2)
The following OS are now supported: <ul style="list-style-type: none">• macOS 10.12 (Sierra)	1.1.3(2)
You can now create a new group by copying an existing group.	4.2.1
You can now sort the display order of groups in the Users & Groups window. In addition, you can narrow down a search and display only users matching a specific state (activated or inactivated) in search results.	ALL

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

Preface

This manual describes how to operate JP1/Data Highway - Server (hereinafter abbreviated as *JP1/DH - Server*).

■ Intended readers

This manual is intended for users who manage and operate the domains of JP1/DH - Server. Readers of this manual must have an understanding of:

- Basics of the OS to be used
- Basics related to networks

■ Conventions: Fonts and symbols

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

Text formatting	Convention
Bold	<p>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:</p> <ul style="list-style-type: none">• From the File menu, choose Open.• Click the Cancel button.• In the Enter name entry box, type your name.
<i>Italic</i>	<p>Italic characters indicate a placeholder for some actual text to be provided by the user or system. For example:</p> <ul style="list-style-type: none">• Write the command as follows: <code>copy source-file target-file</code>• The following message appears: A file was not found. (file = <i>file-name</i>) <p>Italic characters are also used for emphasis. For example:</p> <ul style="list-style-type: none">• Do <i>not</i> delete the configuration file.
Monospace	<p>Monospace characters indicate text that the user enters without change, or text (such as messages) output by the system. For example:</p> <ul style="list-style-type: none">• At the prompt, enter <code>dir</code>.• Use the <code>send</code> command to send mail.• The following message is displayed: <code>The password is incorrect.</code>

The following table explains the symbols used in this manual:

Symbol	Convention
	<p>In syntax explanations, a vertical bar separates multiple items, and has the meaning of OR. For example: <code>A B C</code> means A, or B, or C.</p>

Symbol	Convention
{ }	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.
x	Multiplication sign
/	Division sign

■ 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*.

■ Domain on a directory server

If the word *domain* refers to a domain on a directory server, it is explained that way in this manual.

If the word *domain* is used without such an explanation, it means the management unit of groups in JP1/DH - Server.

■ JP1/DH - Server notation

Where *JP1/DH - Server* is distinguished from *JP1/Data Highway - Server Starter Edition* in this manual, it is so described. Unless otherwise specified, the term *JP1/DH - Server* is used to also refer to *JP1/Data Highway - Server Starter Edition*.

Contents

Notices 2

Summary of amendments 8

Preface 9

1 Prerequisites 13

1.1 Prerequisites for installation 14

1.1.1 Required hardware 14

1.1.2 Recommended hardware 14

1.1.3 Required software 14

2 Common Specifications for Window 17

2.1 Window structure 18

2.1.1 Example of the window 18

2.1.2 Structure 18

2.2 Notes 19

3 Preparation for Operating JP1/DH - Server 20

3.1 General procedure for making preparation necessary to operate JP1/DH - Server 21

3.2 Logging in as a system administrator 22

3.3 Editing system administrator information 23

3.4 Registering the number of purchased users 25

3.5 Setting an authentication rule for the system administrator 26

3.5.1 Setting an authentication policy for the system administrator 26

3.5.2 Setting a network set for the system administrator 28

3.5.3 Setting an authentication rule for the system administrator 29

3.6 Editing the standard authentication policy 32

3.7 Editing the standard delivery policy 34

3.8 Setting a Bandwidth Limitation Rule 39

3.8.1 Creating a Bandwidth Limitation Rules 39

3.8.2 Editing the Bandwidth Limitation Rules 40

3.8.3 Activating or inactivating a Bandwidth Limitation Rules 41

3.8.4 Deleting a Bandwidth Limitation Rules 42

4 Operating the System 43

4.1 General operation procedure 44

4.2 Managing domains 45

4.2.1 Creating a domain 45

4.2.2	Editing the domain	47
4.2.3	Deleting the domain	48
4.3	Managing representative users	49
4.3.1	Creating a user	49
4.3.2	Designating an existing user as the representative user	50
4.3.3	Removing the representative user role	52
4.3.4	Editing the user	53
4.3.5	Deleting the user	54
4.4	Activating or inactivating the authentication rule	55
4.5	Viewing the System Monitor window	56

Appendixes 59

A	Version Changes	60
A.1	Changes in version 11-50	60
A.2	Changes in version 11-10	60
A.3	Changes in version 11-00	61
B	Reference Material for This Manual	62
B.1	Related publications	62
B.2	Conventions: Abbreviations for product names	62
B.3	Conventions: Acronyms	62
B.4	Default installation folder	62
B.5	Meaning of "Administrator permissions" in this manual	63
B.6	Conventions: KB, MB, GB, and TB	63
C	Glossary	64

Index 67

1

Prerequisites

This chapter describes the prerequisites for JP1/DH - Server.

1.1 Prerequisites for installation

This section describes the prerequisites for the client PC to be used with JP1/DH - Server.

1.1.1 Required hardware

- PC/AT compatible machine (An approximately 900 MB of available memory space is required to receive a 50-GB file.)
- There must be twice as much available hard disk space as the size of the file to be downloaded.

1.1.2 Recommended hardware

The following table describes the recommended hardware for the client PC.

Table 1–1: Recommended hardware for the client PC

Recommended hardware	
CPU	Intel Core 2 Duo or equivalent, running at 2.4 GHz or greater
Memory	3 GB or greater
Available disk space	At least twice as much as the file to be sent or received
Network card	100 Mbps or greater

1.1.3 Required software

This subsection describes the software requirements for the client PC.

(1) In Windows

The following table describes the OSs and browsers that can be used when the OS for the client PC is Windows.

Table 1–2: Required OS and browser for the client PC (in Windows)

Required OS ^{#1} or software	
OS	One of the following operating systems is required: <ul style="list-style-type: none">• Windows(R) 7 Professional (32-bit or 64-bit) (Service Pack 1 or later)• Windows(R) 7 Enterprise (32-bit or 64-bit) (Service Pack 1 or later)• Windows(R) 7 Ultimate (32-bit or 64-bit) (Service Pack 1 or later)• Windows(R) 8.1 (32-bit or 64-bit) (With or without Update)^{#2}• Windows(R) 8.1 Pro (32-bit or 64-bit) (With or without Update)^{#2}• Windows(R) 8.1 Enterprise (32-bit or 64-bit) (With or without Update)^{#2}• Windows(R) 10 Home (32-bit or 64-bit)• Windows(R) 10 Pro (32-bit or 64-bit)• Windows(R) 10 Enterprise (32-bit or 64-bit)
Browser	One of the following browsers is required:

Required OS ^{#1} or software	
Browser	<ul style="list-style-type: none"> • Internet Explorer 11^{#3#4} • Microsoft Edge • Mozilla Firefox ESR 45 • Mozilla Firefox ESR 52 • Google Chrome 52 or later

#1

Japanese, English, and simplified Chinese editions of each OS are supported. However, Asian fonts must be installed in a client PC to correctly display items registered in Japanese or simplified Chinese edition.

#2

Operations on Modern UI are not supported.

#3

You need to enable the following functions for Internet Explorer:

- Cookies
- JavaScript (including the Ajax function and the DOM function)
- Cascading style sheets (CSS)
- SSL
- Java applet

If the web pages are not displayed correctly or other page layout errors occur in Internet Explorer 8 or later, change the setting (on/off) for the Compatibility View function in addition to the above functions.

#4

If you use Internet Explorer, set by using either of the following procedures:

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

(2) In Mac OS

The following table describes the OSs and browsers that can be used when the OS for the client PC is Mac OS.

Table 1–3: Required OS and browser for the client PC (In Mac OS)

Required OS and software	
OS	<ul style="list-style-type: none"> • OS X 10.9 (Mavericks) • OS X 10.10 (Yosemite) • OS X 10.11 (El Capitan) • macOS 10.12 (Sierra)
Browser	<ul style="list-style-type: none"> • Safari 7 • Safari 8 • Safari 9[#] • Safari 10[#]

#

It is available in OS X 10.10.5 or later.

(3) Java software

The Java software that can be used with the client PC is described below.

One of the following Java software is required:

- Java Runtime Environment Version 6.0 (32-bit) (Update45 or later)
- Java Runtime Environment Version 6.0 (64bit) (Update45 or later)
- Java Runtime Environment Version 7.0 (32-bit) (Update51 or later)
- Java Runtime Environment Version 7.0 (64bit) (Update51 or later)[#]
- Java Runtime Environment Version 8.0 (32-bit) (Update 40 or later)
- Java Runtime Environment Version 8.0 (64-bit) (Update 40 or later)[#]

[#]

If the client PC is running on the Mac OS, use this version of the software.

2

Common Specifications for Window

This chapter describes the common specifications for the JP1/DH - Server windows.

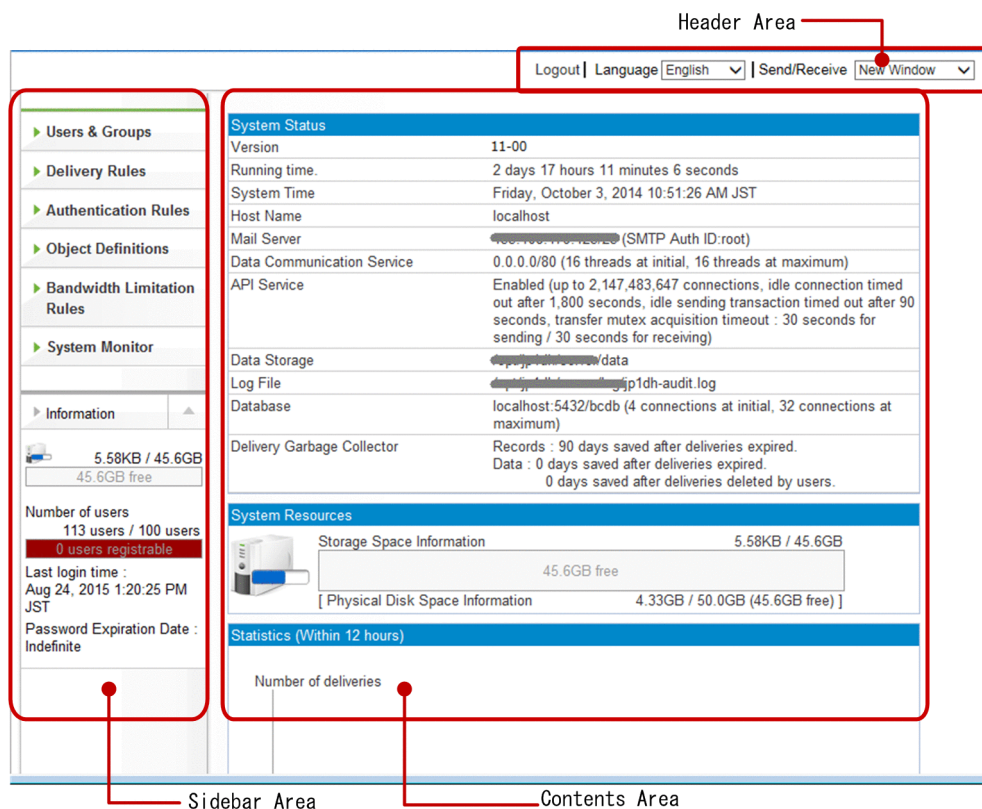
2.1 Window structure

This section describes the common specifications for the JP1/DH - Server windows.

2.1.1 Example of the window

The figure below shows an example of the main window of JP1/DH - Server.

Figure 2–1: JP1/DH - Server window structure



2.1.2 Structure

A window used by JP1/DH - Server consists of three areas as described in the following table.

Table 2–1: Areas comprising the JP1/DH - Server windows

Item	Description
Header area	Displays the name of the logged in user and a link to log out of the system etc. Depending on the system settings, the drop-down menu for switching the New Delivery window may not be displayed.
Sidebar area	This area displays the operation menu, data area information, and the number of users (registered users in the entire system/purchased users).
Content area	This area displays system information, and allows you to specify various settings.

2.2 Notes

Observe the following notes when using the JP1/DH - Server windows:

- If, after setting up JP1/DH - Server in the Windows environment, you want to continue creating domains, groups, and users on the server machine on which JP1/DH - Server is set up do not change the initial browser settings. Note that, under this circumstance, you cannot use the **Check Your Environment** function in the login window or issue an electronic certificate from the Edit User window.

If you have set up JP1/DH - Server in the Linux environment, you have to use a client PC with Windows OS to create domains, groups, and users.

- Use buttons and anchor texts in the windows for window operation. If you operate windows by using the **Back**, **Next**, and **Refresh** buttons or by browsing histories in the web browser, the windows for JP1/DH - Server might not appear properly.
- Do not click buttons repeatedly when you operate windows. If you do so, the windows for JP1/DH - Server might not appear properly.
- Do not operate a window while Loading . . . is displayed at the top of the window. If you do so, the windows for JP1/DH - Server might not appear properly.



- If a login authentication fails repeatedly (normally, five times), your account will be locked. In this case, you cannot log in to JP1/DH - Server for a certain period of time (normally 10 minutes) even if you enter the correct user ID and password. Wait a while before attempting to log in again. Your account becomes unlocked after a successful login.

The account lock occurs only after several failed log-in attempts made using the login ID and password. If a login attempt made using an electronic certificate fails, the system displays a message dialog box instead of locking the account.

- All the date and time information displayed by JP1/DH - Server is based on the time zone setting of the server on which JP1/DH - Server is located. This means that the saved date and time or delivery date and time might be inconsistent with the local time data on the client PC that uses JP1/DH - Server.
- Do not include a space character at the beginning or end of a character string you enter into input fields. If a space character is included at the beginning or end of a character string, the character string you enter might not be recognized correctly.
- If you change the language setting from the header area, the information you are entering in the currently displayed window will be cleared. Do not change the language setting while you are entering information in a window.

3

Preparation for Operating JP1/DH - Server

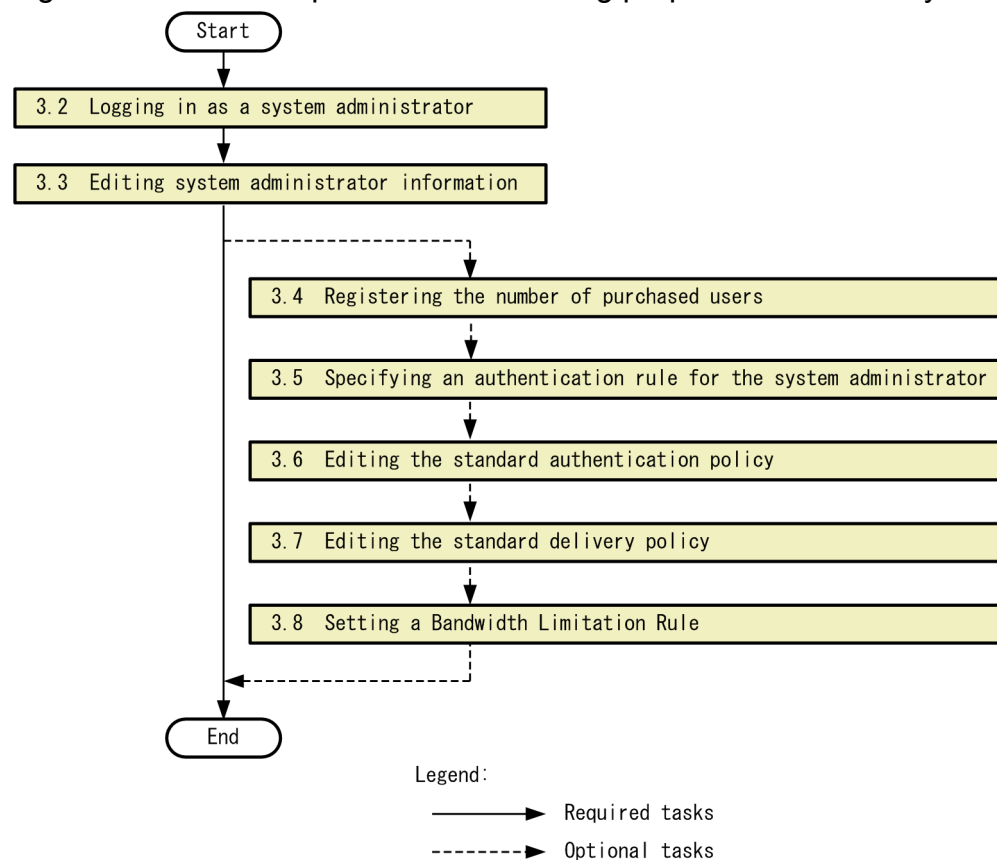
This chapter describes the preparation for operating JP1/DH - Server.

3.1 General procedure for making preparation necessary to operate JP1/DH - Server

The figure below shows the general procedure for making the preparation necessary to operate JP1/DH - Server.

This preparation involves editing system administrator information including the password, registering the number of purchased users, and editing the authentication rule for the system administrator.

Figure 3–1: General procedure for making preparation necessary to operate JP1/DH - Server

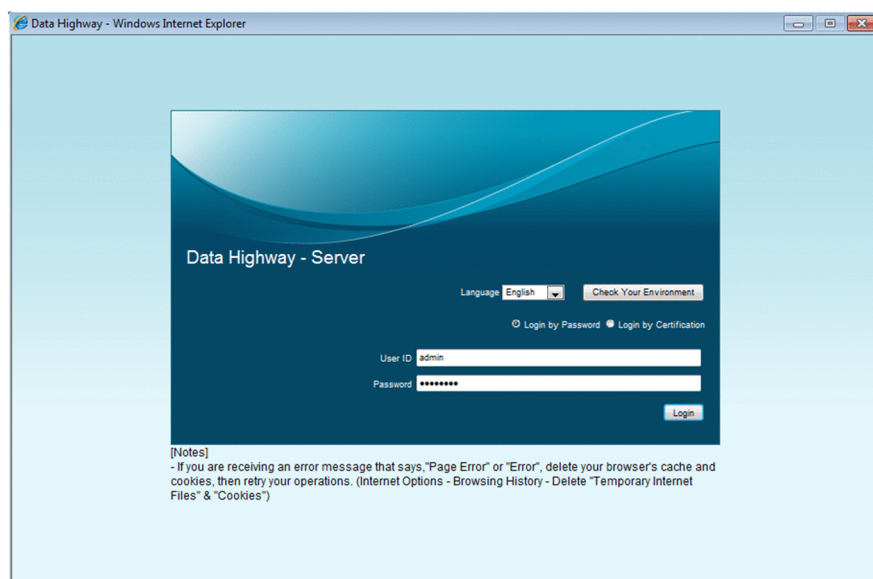


3.2 Logging in as a system administrator

This section describes how to log in to JP1/DH - Server as a system administrator.

1. Access the JP1/DH - Server URL (`https://server-host-name/`).

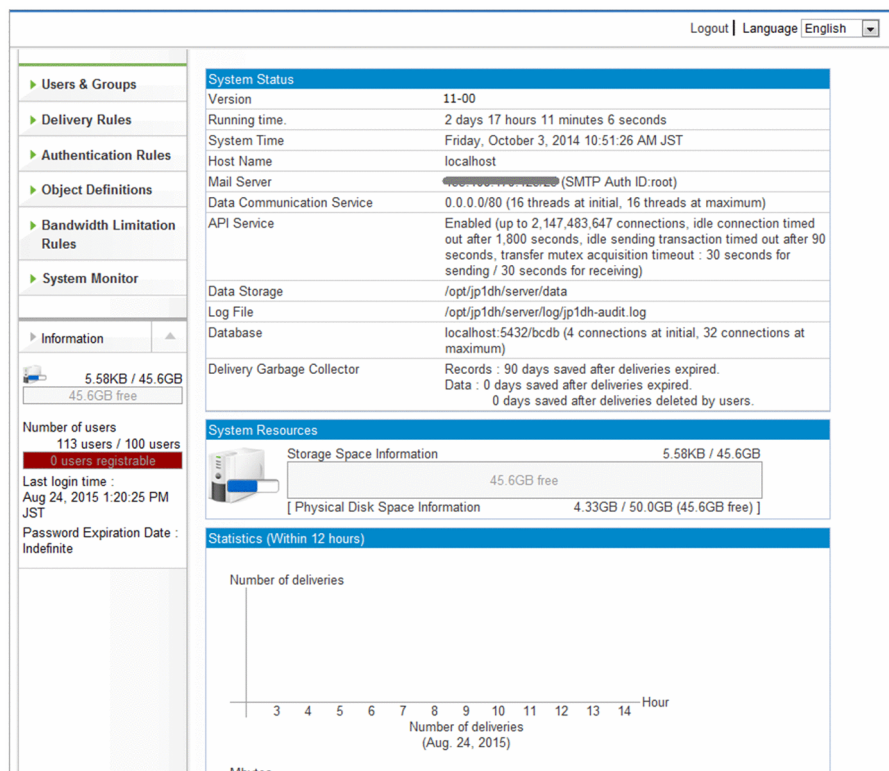
The User Authentication window appears.



2. Enter your user ID and password, and then click the **Login** button.

Log in to JP1/DH - Server as a system administrator. The user ID for a system administrator is fixed to `admin`. The initial password is `password`. After changing the password, use the new password.

The System Monitor window appears.



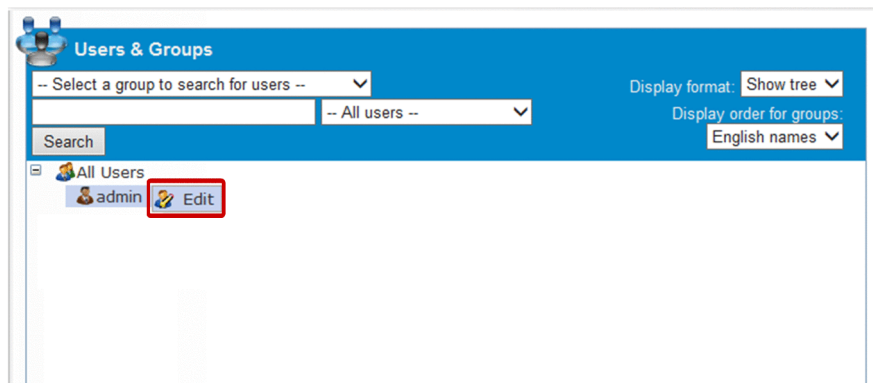
3. Preparation for Operating JP1/DH - Server

3.3 Editing system administrator information

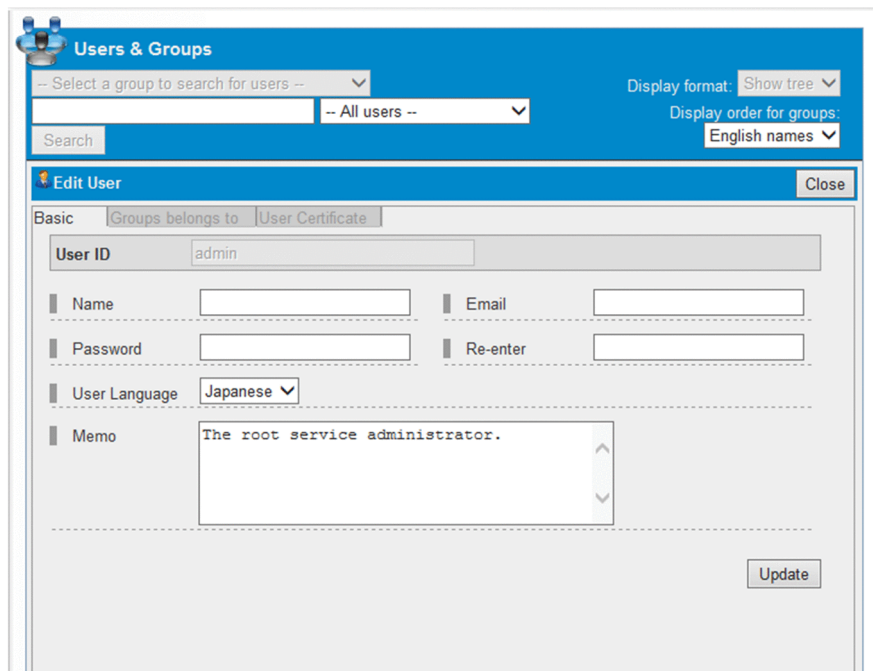
This section describes how to edit system administrator information.

The following steps are mainly for changing the password for system administrator.

1. Log in to JP1/DH - Server.
2. In the sidebar area, click **Users & Groups**.
The Users & Groups window appears in the content area.
3. Under **All Users**, click **admin**, and then select **Edit**.
The Edit User window appears.



4. Edit the settings.
For details about each setting items, see the *JP1/Data Highway - Server Administrator Guide*.
Note that you cannot edit the user ID or setting items in the **Groups belongs to** and **User Certificate** tabs.



5. Click the **Update** button.
A dialog box appears asking for your confirmation to update the system administrator information.

6. Click the **OK** button.

3.4 Registering the number of purchased users

This section describes how to register the number of purchased users.

You can register the number of purchased users, that is, the number of purchased user licenses, in the system. The number of purchased users you registered is displayed in the sidebar area of the window along with the number of registered users in the entire system. This function allows you to easily confirm that the number of registered users across the entire system does not exceed the number of purchased user licenses.

For details about how to register the number of purchased users, see the *JP1/Data Highway - Server Configuration and Administration Guide*.

3.5 Setting an authentication rule for the system administrator

This section describes how to create an authentication rule for the system administrator.

Set the authentication rule to limit the network environments to which the system administrator can log in.

An authentication rule is set up using a combination of an authentication policy and a network set.

For details about the authentication rule, the authentication policy, and the network set, see the *JP1/Data Highway - Server Administrator Guide*.

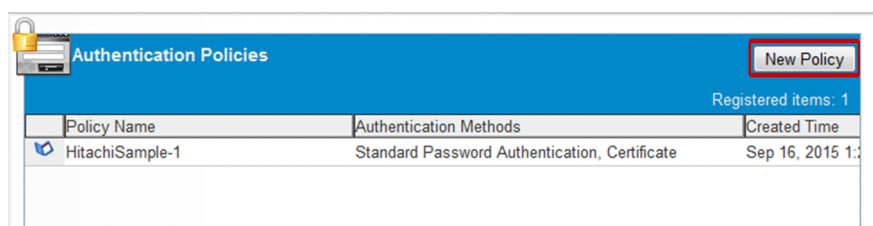
3.5.1 Setting an authentication policy for the system administrator

This subsection described how to set an authentication policy for the system administrator.

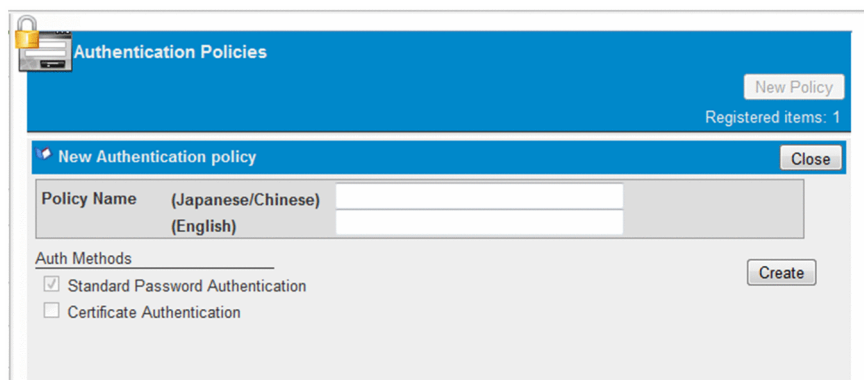
(1) Creating an authentication policy for the system administrator

To create an authentication policy for the system administrator:

1. Log in to JP1/DH - Server.
2. Click **Authentication Rules** in the sidebar area, and then **Authentication Policy Definitions**.
The Authentication Policies window appears in the content area.
3. Click the **New Policy** button.
The New Authentication policy window appears.



4. Create an authentication policy.



Enter the policy name in the **(Japanese/Chinese)** and **(English)** fields. For an authentication policy for the system administrator, the policy name is the only setting item to be specified.

For details about each setting items, see the *JP1/Data Highway - Server Administrator Guide*.

5. Click the **Create** button.

The authentication policy for the system administrator is now created. A dialog box appears, asking for your confirmation to register the authentication policy.

6. Click the **OK** button.

The Authentication Policies window appears.


(2) Editing the authentication policy for the system administrator

To edit the authentication policy for the system administrator:

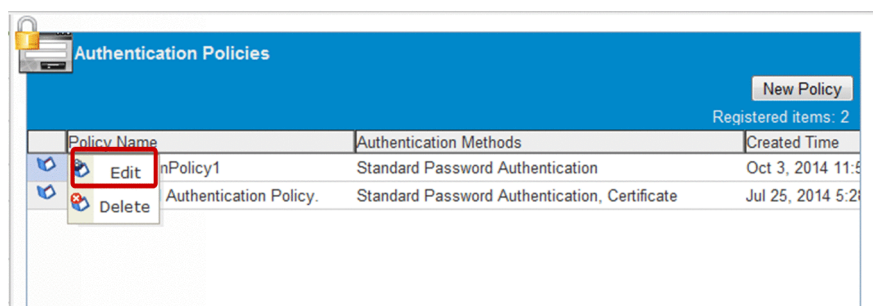
1. Log in to JP1/DH - Server.

2. Click **Authentication Rules** in the sidebar area, and then **Authentication Policy Definitions**.

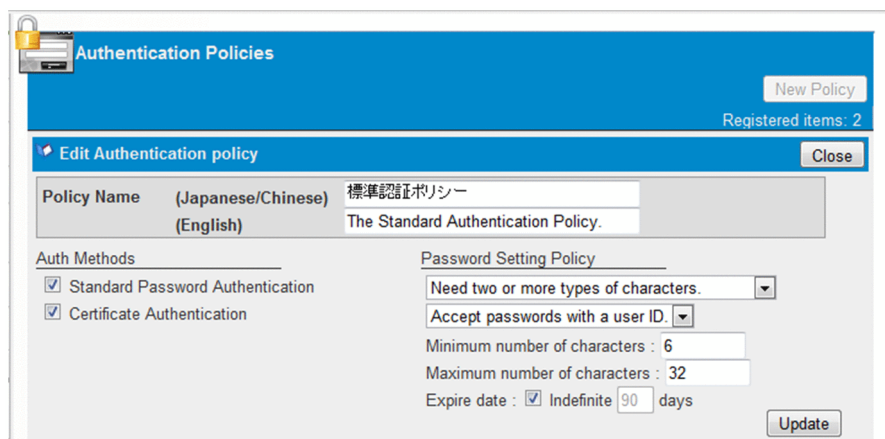
The Authentication Policies window appears in the content area.

3. Click the menu icon () beside the authentication policy you want to edit, and then select **Edit**.

The Edit Authentication policy window appears.



4. Edit the settings.



For details about each setting items, see the *JP1/Data Highway - Server Administrator Guide*.

5. Click the **Update** button.


The authentication policy for the system administrator is now updated. A dialog box appears, asking for your confirmation to update the authentication policy.

6. Click the **OK** button.

The Authentication Policies window appears.

(3) Deleting the authentication policy for the system administrator

To delete the authentication policy for the system administrator:

1. Log in to JP1/DH - Server.
2. Click **Authentication Rules** in the sidebar area, and then **Authentication Policy Definitions**.
The Authentication Policies window appears in the content area.
3. Click the menu icon () beside the authentication policy you want to delete, and then select **Delete**.
A dialog box appears, asking for your confirmation to delete the authentication policy.
4. Click the **OK** button.
The authentication policy for the system administrator is now deleted, and the Authentication Policies window appears.

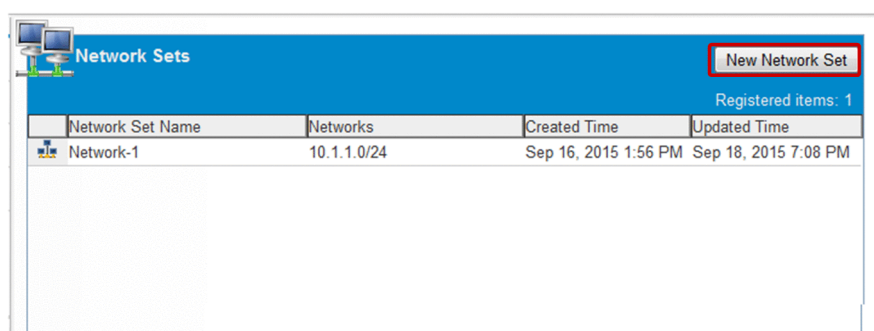
3.5.2 Setting a network set for the system administrator

This subsection describes how to set a network set for the system administrator.

(1) Creating a network set for the system administrator

To create a network set for the system administrator:

1. Log in to JP1/DH - Server.
2. In the sidebar area, click **Object Definitions**.
The Network Sets window appears in the content area.
3. Click the **New Network Set** button.
The New Network Set window appears.



For details about each setting items, see the *JP1/Data Highway - Server Administrator Guide*.

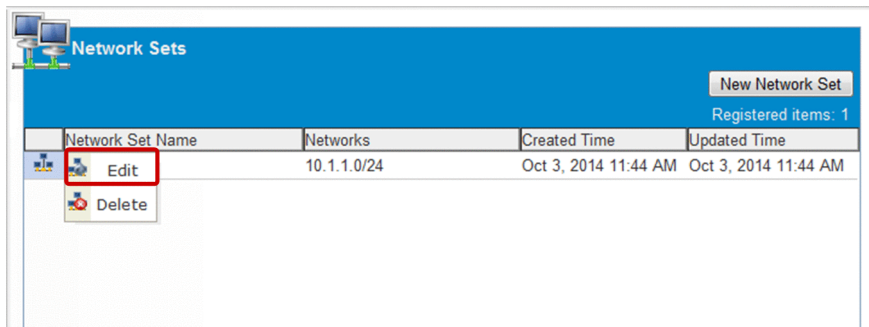
(2) Editing the network set for the system administrator

To edit the network set for the system administrator:

1. Log in to JP1/DH - Server.
2. In the sidebar area, click **Object Definitions**.
The Network Sets window appears in the content area.

3. Click the menu icon () beside the network set you want to edit, and then select **Edit**.


The Edit Network Set window appears.



For details about each setting items, see the *JP1/Data Highway - Server Administrator Guide*.

(3) Deleting the network set for the system administrator

To delete the network set for the system administrator:

1. Log in to JP1/DH - Server.
2. In the sidebar area, click **Object Definitions**.
The Network Sets window appears in the content area.
3. Click the menu icon () beside the network set you want to delete, and then select **Delete**.

3.5.3 Setting an authentication rule for the system administrator

This subsection describes how to set an authentication rule for the system administrator.[#]

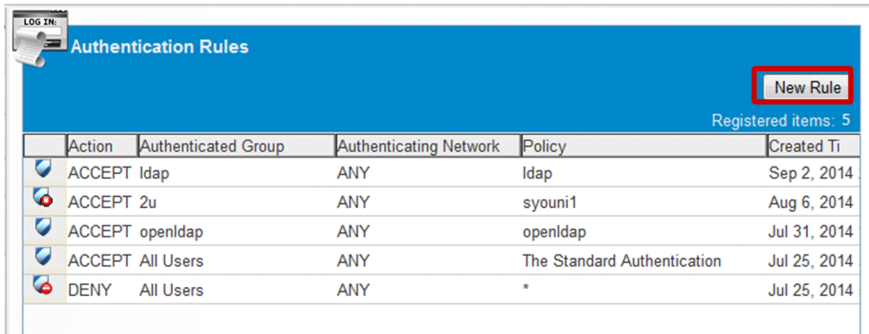
#

If you set an authentication rule for the system administrator incorrectly, you might become unable to log in to JP1/DH - Server as a system administrator. In this case, perform an emergency login to inactivate the authentication rule in question. For details about how to perform an emergency login, see the *JP1/Data Highway - Server Configuration and Administration Guide*.

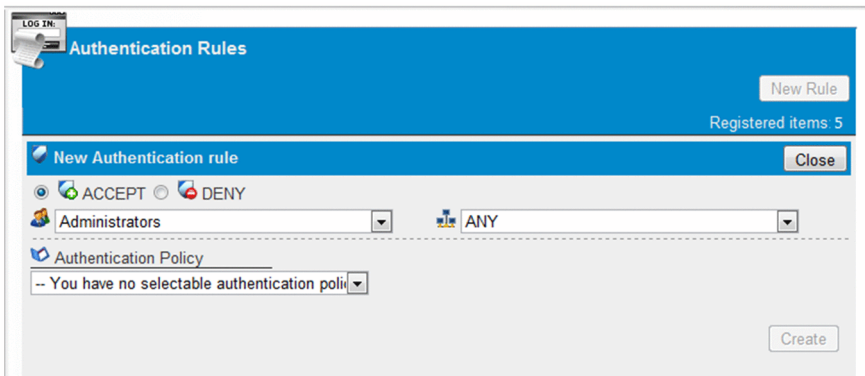
(1) Creating an authentication rule for the system administrator

To create an authentication rule for the system administrator:

1. Log in to JP1/DH - Server.
2. In the sidebar area, click **Authentication Rules**.
The Authentication Rules window appears in the content area.
3. Click the **New Rule** button.
The New Authentication rule window appears.



4. Create an authentication rule.



You can only select **Administrators** as the group. Select the network set and the authentication policy that you have created in advance, and then select **ACCEPT** to permit authentication or **DENY** to deny authentication.

5. Click the **Create** button.

The authentication rule is now created.

! Important

The **Create** button is disabled if no authentication policy is created.


(2) Editing the authentication rule for the system administrator

To edit the authentication rule for the system administrator:

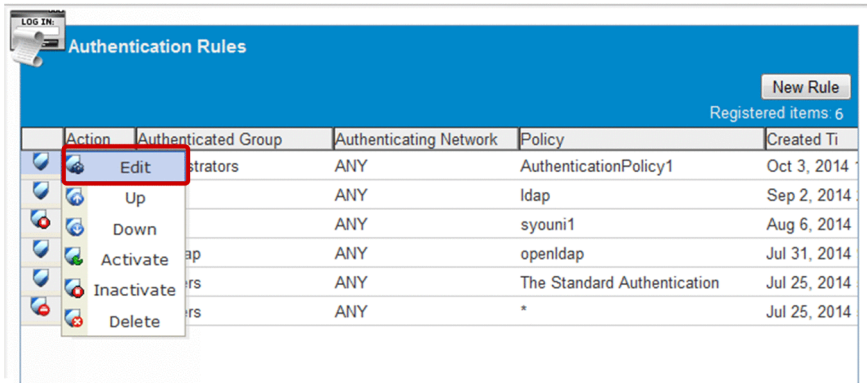
1. Log in to JP1/DH - Server.

2. In the sidebar area, click **Authentication Rules**.

The Authentication Rules window appears in the content area.

3. Click the menu icon () beside the authentication rule you want to edit, and then select **Edit**.

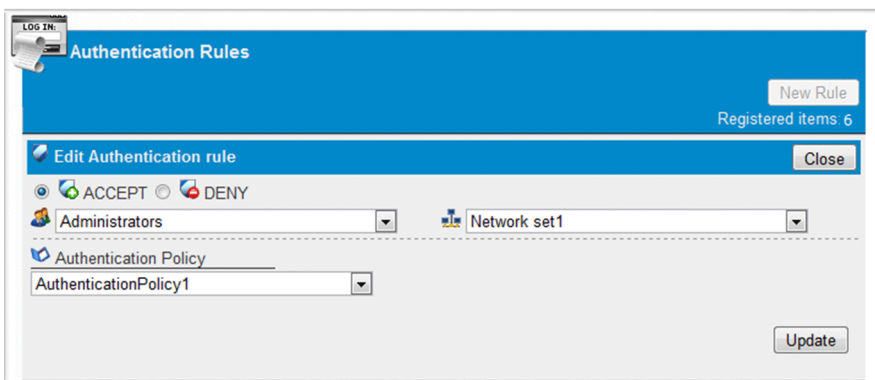
The Edit Authentication rule window appears.



Note 1: For details about the **Up**, **Down**, **Activate**, and **Inactivate** options, see the *JP1/Data Highway - Server Administrator Guide*.

Note 2: You cannot edit the following authentication rules: authentication rules created by a representative user and the two authentication rules that have been created in advance (with **All Users** selected as the authentication group).

4. Edit the settings.



5. Click the **Update** button.

The authentication rule for the system administrator is now updated.

(3) Deleting the authentication rule for the system administrator

To delete the authentication rule for the system administrator:

1. Log in to JP1/DH - Server.

2. In the sidebar area, click **Authentication Rules**.

The Authentication Rules window appears in the content area.

3. Click the menu icon () beside the authentication rule you want to delete, and then select **Delete**.

Important

You cannot delete the authentication rule created by a representative user.


3.6 Editing the standard authentication policy

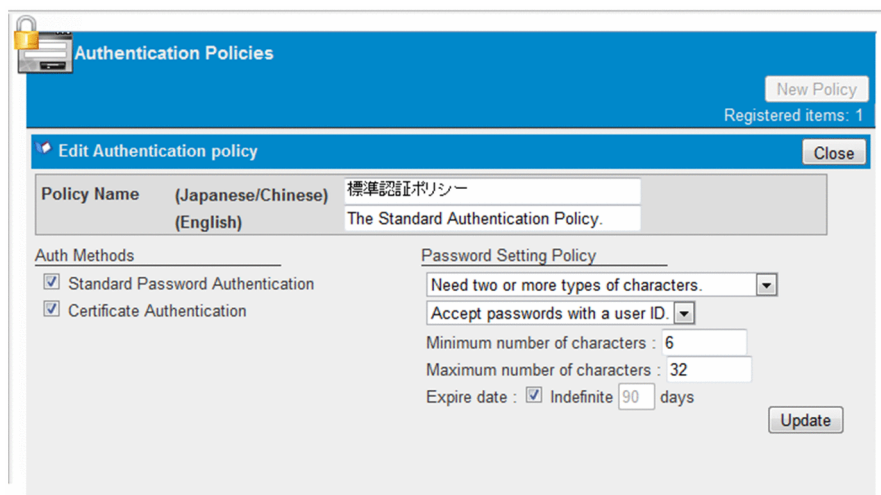
This section describes how to edit the standard authentication policy.

The standard authentication policy serves as the default authentication policy for the entire system.

Important

Caution is required when you are to edit the standard authentication policy after putting JP1/DH - Server into service. If there are any users using the standard authentication policy, changes made to the standard authentication policy will affect the authentication of these users.

1. Log in to JP1/DH - Server.
2. Click **Authentication Rules** in the sidebar area, and then **Authentication Policy Definitions**.
The Authentication Policies window appears in the content area.
3. Click the menu icon () beside the target policy name, and then select **Edit**.
The Edit Authentication policy window appears.



4. Edit the settings.
Specify the setting items described in the table below.

Table 3–1: Setting items for the standard authentication policy

Item	Description
Policy Name (Japanese/Chinese) text box ^{#1}	Enter the policy name. The value entered here is displayed in the Japanese and Chinese windows.
Policy Name (English) text box ^{#1}	Enter the policy name. The value entered here is displayed in the English window. You can only enter alphanumeric characters and symbols.
Auth Methods (authentication methods)	Select the authentication method. You can select both authentication methods. <ul style="list-style-type: none">• Standard Password Authentication: Select this option to use password authentication.• Certificate Authentication: Select this option to use authentication by using an electronic certificate issued for you.

Item	Description
Password Setting Policy	Set a policy concerning the types of password that can be used. <ul style="list-style-type: none"> • Need two or more types of characters. At least two of the following four types of characters must be included: numbers, lowercase alphanumeric characters, uppercase alphanumeric characters, and symbols. • Do not need two or more types of characters. Set whether to include a user ID in the password. <ul style="list-style-type: none"> • Accept passwords with a user ID. • Reject passwords with a user ID.
	Expire date ^{#2} By default, the Indefinite check box is selected. To set an expiration date, clear the Indefinite check box and then enter a value (the number of days) in the range from 1 to 365. By default, it is set to 90 days.

#1

- You cannot enter the following symbols: / \ ? * : | " < > @ ^ .
- You cannot enter a name consisting only of spaces or periods (.).
- You can enter no more than 256 alphanumeric characters and symbols.

#2

If you clear the **Indefinite** check box in the **Expire date** setting, the users who are currently using the applicable authentication policy must change their password the next time they log in to JP1/DH - Server.

5. Click the **Update** button.

The standard authentication policy is now updated. A dialog box appears, asking for your confirmation to update the standard authentication policy.

3.7 Editing the standard delivery policy

This section describes how to edit the standard delivery policy.

The standard delivery policy serves as the default delivery policy for the entire system.


Important

Caution is required when you are to edit the standard delivery policy after putting JP1/DH - Server into service. If there are any delivery policies that are using the standard delivery policy settings, changes made to the standard delivery policy will affect these delivery policies.

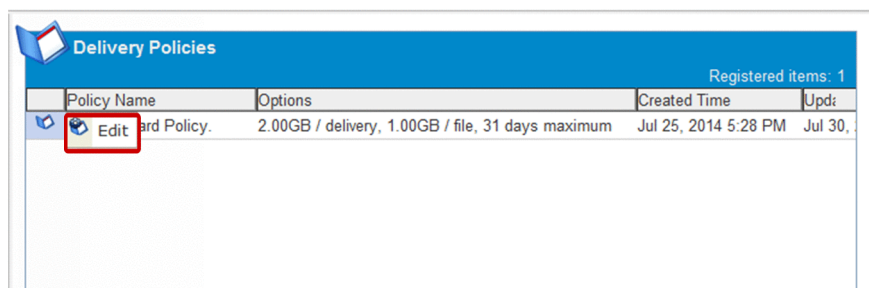
1. Log in to JP1/DH - Server.



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

The Delivery Policies window appears in the content area.

3. Click the menu icon () beside the target policy name, and then select **Edit**.

The Edit Delivery Policy window appears.



Delivery Policies				
				Registered items: 1
Policy Name	Options	Created Time	Upd:	
 Standard Policy.	2.00GB / delivery, 1.00GB / file, 31 days maximum	Jul 25, 2014 5:28 PM	Jul 30, 2014	

4. Edit the settings.

Specify the setting items described in the table below.

Table 3–2: Setting items for the standard delivery policy

Category	Item	Description
Policy Name^{#1}	Policy Name (Japanese/Chinese) text box	Enter the policy name. The value entered here is displayed in the Japanese and Chinese windows.
	Policy Name (English) text box	Enter the policy name. You can only enter alphanumeric characters and symbols. The value entered here is displayed in the English window.
Data Capacity	Data Capacity check boxes and text boxes	Enter the maximum volume of data that can be sent. The option corresponding to the selected check box becomes enabled. The maximum specifiable data delivery volume varies depending on the system setting. <ul style="list-style-type: none"> • MB/delivery This option specifies the maximum data volume that can be sent at a time. If you clear this check box, a maximum of 2048-MB data can be sent at a time. • MB/file This option specifies the maximum file size that can be sent at a time. If you clear this check box, a file not exceeding 2048 MB in size can be sent at a time. For the MB/file option, you cannot specify a value greater than the one that is specified for MB/delivery .
Storage period	Storage period check boxes and text boxes	Specify the maximum and initial values for the storage period that a user can set when sending a file. <ul style="list-style-type: none"> • Max. Enter the maximum storage period a user can specify when delivering data. • Set

Category	Item	Description
Storage period	Storage period check boxes and text boxes	Enter the default storage period that is applied when the user does not specify the storage period. If you clear this check box, the Max. setting is applied. The maximum specifiable value is 31 (days).
Security	Restriction of Download Once Field drop-down list box	You can use this function to allow the recipient to download the file just once. Select a desired option for this function.
	Automatic file deletion on download completion drop-down list box ^{#2}	This function deletes files automatically before the storage expiration date is reached, if all the users specified as the recipients download all the files. If this is selected, the system finds out that all the users specified as the recipients already downloaded all the files and then deletes the files automatically before the storage expiration date is reached. Note that the type of address to be checked (TO/CC/BCC) depends on the system configuration. Select how this function works.
e-Mail Notification	Notice of Delivery: drop-down list box	This function notifies both the sender and recipient when a file is uploaded or a message is sent. Select a desired option for this function.
	Notice of Opening: drop-down list box	This function notifies the sender when the sent file is opened. Select a desired option for this function.
	Notice on the Expiration Previous Day: drop-down list box	This function notifies the sender of the fact that the sent file was not opened by the day before the expiration of the storage period. Select a desired option for this function.
	Notice on the Expiration: drop-down list box	This function notifies the sender that the expiration date or the sent file has been reached. Select a desired option for this function.
	Detailed Message Option: drop-down list box	This function sets whether to include detailed information or other relevant information in the file delivery notification email. Select a desired option for this function.
	Notice if not Downloaded by Designated Date: drop-down list box	If the recipient has not downloaded the file by the date specified by the sender, this function sends an email notification to remind the recipient of the file that is pending download. Select a desired option for this function. Note that notification email is not sent for the deliveries sent from JP1/Data Highway - AJE version 10-00.
	Notice if not Approved by Designated Date: drop-down list box	If the approver has not approved or rejected the delivery by the date specified by the sender, this function sends an email notification to remind the approver of the file that is pending approval. Select a desired option for this function. This setting is ignored if no approval route is set in the delivery rule to which this delivery policy applies. Note that notification email is not sent for the deliveries sent from JP1/Data Highway - AJE version 10-00.
Compress	Compress Level: check boxes	Specify the compression levels that can be selected by the sender.

Category	Item	Description
Compress	Compress Level: check boxes	<p>If you clear all the check boxes, the system default setting is applied. (By default, the sender can only select the No compression option.)</p> <ul style="list-style-type: none"> • No compression: A file will not be compressed. • STRONG: A file is compressed using the highest compression rate. • MIDDLE: A file is compressed using a moderate compression rate. • WEAK: A file is compressed using the lowest compression rate.
	Compress Method ^{#3}	<p>Select the compression method.</p> <ul style="list-style-type: none"> • Standard: If a folder is sent or if STRONG, MIDDLE, or WEAK is selected as the compression level, a file or folder is sent in ZIP format. A file or folder to be sent in ZIP format must not exceed 3.96 GB (4,252,017,623 bytes) in size. • Extended: If a folder is sent or if STRONG, MIDDLE, or WEAK is selected as the compression level, a file or folder is sent using the extended compression method. Note in JP1/Data Highway - AJE version 10-00 the files are compressed in ZIP format to be sent. In addition, a file that is sent by using the extended compression method cannot be received by JP1/Data Highway - AJE version 10-00.
Other Options	Max. Addresses: check box	By selecting this check box, you can set the maximum number of addresses that can be specified for a single delivery.
	Max. Files and Folders: check box	By selecting this check box, you can set the maximum number of files that can be specified for a single delivery.
Connection	Max. TCP sessions per Connection: check box	<p>You can specify the maximum number of TCP sessions allowed for file transmission and reception.</p> <p>If you are using the standard delivery policy, do not clear this check box. The value specified by the standard delivery policy is set by default.</p>
	Always connect with Max. TCP sessions check box	<p>You can specify whether to always establish a connection using the maximum number of TCP sessions specified by the Max. TCP sessions per Connection setting. If you are using the standard delivery policy, do not clear this check box.</p> <ul style="list-style-type: none"> • Enabled: A connection is always established using the maximum number of TCP sessions. • Disabled: The number of TCP sessions is automatically determined according to the network distance. <p>The value specified by the standard delivery policy is set by default.</p>

#1

- You cannot enter the following symbols: / \ ? * : | " < > @ ^ .
- You cannot enter a name consisting only of spaces or periods (.).
- You can enter no more than 256 characters.

#2

- If the user sends multiple files in a single delivery, the files will be deleted together after all of them are downloaded. The system does not delete files one-by-one.
- A file will be deleted at the end of the day when all the recipient users download it. It is not deleted at the moment when the download is complete. Furthermore, the date of deletion is based on the system date of the server.

#3

In JP1/Data Highway - AJE version 10-00, if data sent using the extended compression method arrives, the reception of that data is skipped, and only the data sent by using other compression methods is received. If the data is to be received by JP1/Data Highway - AJE version 10-00, specify a delivery policy appropriate to that version.

5. Click the **Update** button.

The standard delivery policy is now updated. A dialog box appears, asking for your confirmation to update the standard delivery policy.

3.8 Setting a Bandwidth Limitation Rule

This section describes how to set a bandwidth limitation rule.

A bandwidth limitation rule stipulates the total maximum network bandwidth used for each group or network set. The maximum transmission speed for a user to which a bandwidth limitation rule applies is the network bandwidth set in the rule. The user shares the bandwidth with other users whose transmissions are simultaneously in progress. A bandwidth limitation rule is set up using a combination of a group, network set, and the maximum network bandwidth.

Note that you need to create a network set before creating a bandwidth limitation rule. For details about how to create a network set, see the *JP1/Data Highway - Server Administrator Guide*.

3.8.1 Creating a Bandwidth Limitation Rules

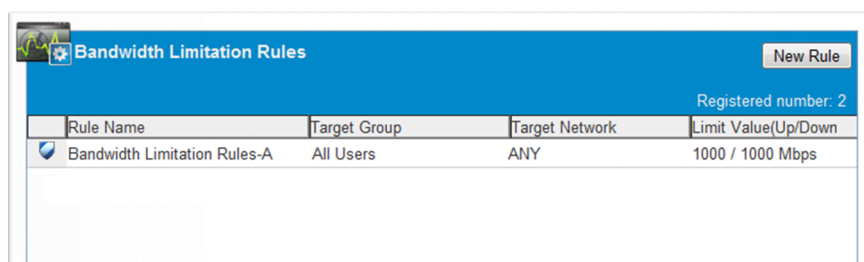
To create a bandwidth limitation rules:

1. Log in to JP1/DH - Server.
2. In the sidebar area, click **Bandwidth Limitation Rules**.

The bandwidth limitation rules window appears in the content area.

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

The **New Bandwidth Limitation rule** window appears.



4. Create a bandwidth limitation rules.

Specify the setting items described in the table below.

Table 3–3: Setting items for the bandwidth limitation rules

Item	Description
Rule Name text box	Enter a name of a bandwidth limitation rule. You cannot enter the following symbols: /, \, ?, *, :, , ", <, >, @, ^ . You cannot enter a name consisting only of spaces or periods (.). You can enter no more than 256 alphanumeric characters and symbols.
Limitation Group	This item indicates a group to which a bandwidth limitation rule applies. You can select All Users only.
Limitation Network drop-down list box	Select a network set to which a bandwidth limitation rule applies. Note that you need to create a network set before creating a bandwidth limitation rule.

Item	Description
Bandwidth limitation	Specify the maximum limitation of the network bandwidth for uploading and downloading in the range from 0 to 1000 (in Mbps). If 0 is specified, there is no limitation on the network bandwidth.

5. Click the **Create** button.

The bandwidth limitation rules is created, and the **Bandwidth Limitation Rules** window appears.

! Important

A maximum of 1,000 bandwidth limitation rules can be created in the system.

3.8.2 Editing the Bandwidth Limitation Rules

To edit a bandwidth limitation rules:

1. Log in to JP1/DH - Server.

2. In the sidebar area, click **Bandwidth Limitation Rules**.

The Bandwidth Limitation Rules window appears in the content area. A list of the registered bandwidth limitation rules is displayed in the window.

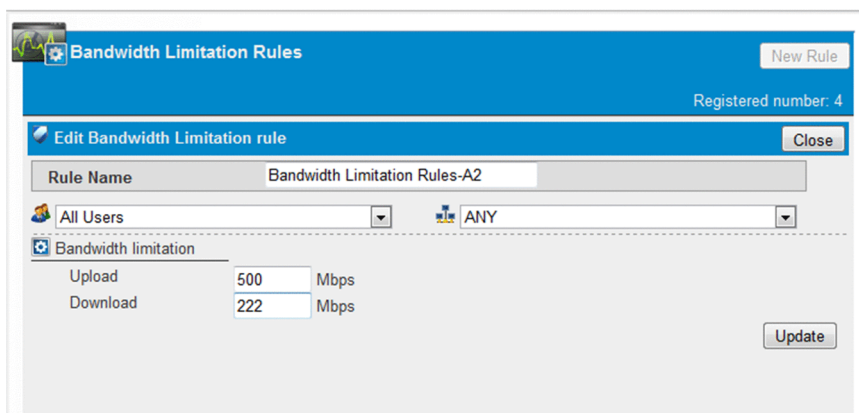
3. Click the menu icon of the bandwidth limitation rules you want to edit, and then select **Edit**.

The **Edit Bandwidth Limitation rule** window appears.

Rule Name	Target Group	Target Network	Limit Value(Up/Down)
ion Rules-A2	All Users	ANY	1000 / 1000 Mbps
	All Users	ANY	0 / 100 Mbps
ion Rules-A	All Users	ANY	1000 / 1000 Mbps
	All Users	ANY	222 / 222 Mbps

4. Change the settings. For details about each item, see *3.8.1 Creating a Bandwidth Limitation Rules*.

5. Click the **Update** button.



6. The settings of the bandwidth limitation rules are now updated.

3.8.3 Activating or inactivating a Bandwidth Limitation Rules

To activating or inactivating a bandwidth limitation rules:

1. Log in to JP1/DH - Server.
2. In the sidebar area, click **Bandwidth Limitation Rules**.
The Bandwidth Limitation Rules window appears in the content area.
3. Click the menu icon corresponding to the bandwidth limitation rule to be activated or inactivated, and then select a desired menu item.

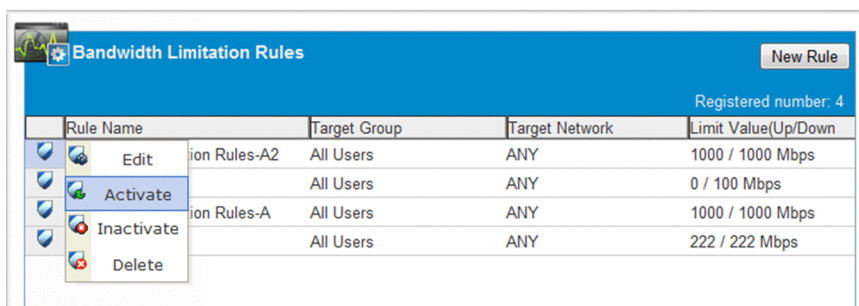


Table 3—4: Activating or inactivating a bandwidth limitation rules

Item	Description
Activate	Activates a bandwidth limitation rules.
Inactivate	Inactivates a bandwidth limitation rules. The inactivated bandwidth limitation rules becomes temporarily unavailable. To make the inactivated rule available, activate it again.

4. A confirmation dialog box appears depending on your choice. Click the **OK** button to activating or inactivating the action.

3.8.4 Deleting a Bandwidth Limitation Rules

To delete a bandwidth limitation rules:

1. Log in to JP1/DH - Server.
2. In the sidebar area, click **Bandwidth Limitation Rules**.
The Bandwidth Limitation Rules window appears in the content area.
3. Click the menu icon of the bandwidth limitation rules you want to delete, and then select **Delete**.
A dialog box appears asking you to confirm that you want to delete the rules.
4. Click the **OK** button.
The bandwidth limitation rules is deleted, and the **Bandwidth Limitation Rules** window appears.

4

Operating the System

This chapter describes the operation for JP1/DH - Server system.

4.1 General operation procedure

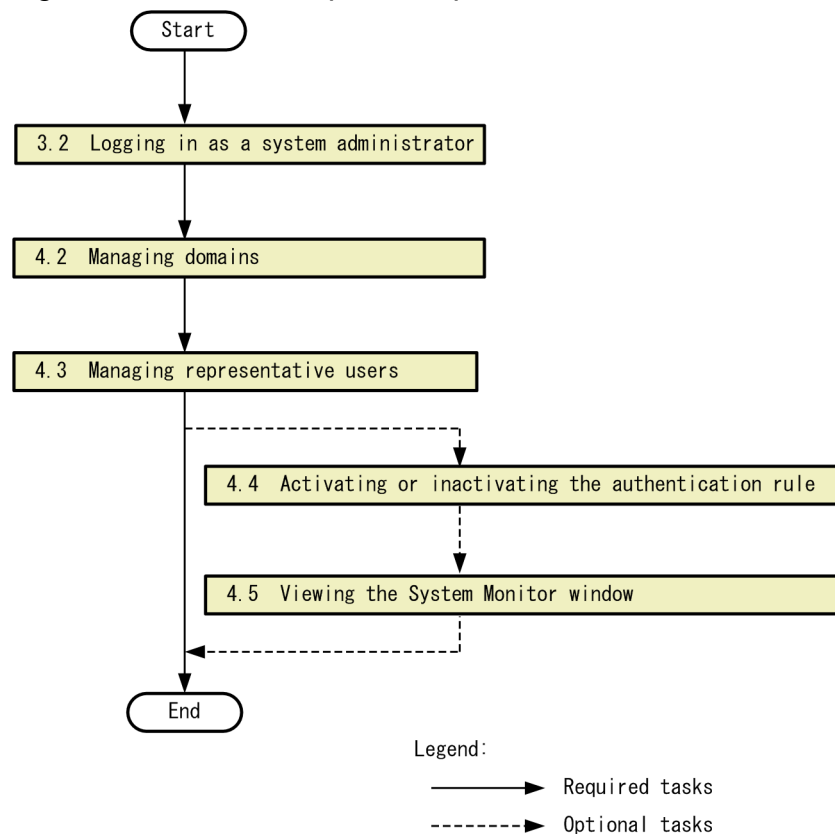
The figure below shows the general operation procedure for JP1/DH - Server.

The system administrator manages both domains and the representative users who manage the domains. The representative users manage which users can send and receive files and also the rules for sending and receiving files.

When a representative user sets an incorrect authentication rule and becomes unable to log in to JP1/DH - Server, the system administrator has to activate or inactivate the authentication rule.

Furthermore, the system administrator views the System Monitor window to keep track of system use and resource use.

Figure 4–1: General operation procedure



4.2 Managing domains

This section describes how to set a domain, one of the management units of JP1/DH - Server.

A domain refers to a group directly below the top-level group (**All Users** group).

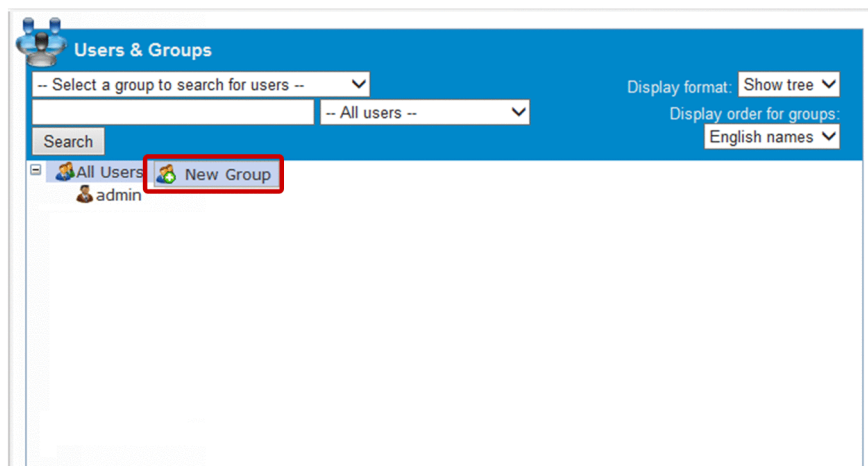
! Important

The system administrator must not create groups other than domains or users other than representative users (these must be created by representative users).

4.2.1 Creating a domain

To create a domain:

1. Log in to JP1/DH - Server.
2. In the sidebar area, click **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. Create a domain.

The table below describes the setting items in the **Basic** tab.

For details about each setting items in the **Properties** tab and the **Address Book Manager** tab, see the *JP1/Data Highway - Server Administrator Guide*.

Table 4–1: Settings items in the Basic tab


Item	Description
Group Name: (Japanese/Chinese) text box	<p>Enter a group name (domain name). The value entered here is displayed in the Japanese and Chinese windows. Once you create a group, you cannot change the group name.</p> <ul style="list-style-type: none"> You can enter no more than 200 characters. You cannot use the following symbols: / \ ? * : " < > # @ ^ [] \$. You cannot enter a name consisting only of spaces or periods (.).
Group Name: (English) text box	<p>Enter a group name (domain name). The value entered here is displayed in the English window. The lower-case version of the value entered here, with all the spaces removed, appears after the at mark (@) of the IDs assigned to the users under this domain. Once you create a group, you cannot change the group name.</p> <ul style="list-style-type: none"> You can enter no more than 50 alphanumeric characters and symbols. You cannot use a space character or the following symbols: / \ ? * : " < > # @ ^ [] \$. You cannot enter a name consisting only of periods (.) or ending with a period (.). You cannot use Windows reserved words (CON, PRN, AUX, CLOCK\$, NUL, COM0, COM1, COM2, COM3, COM4, COM5, COM6, COM7, COM8, COM9, LPT0, LPT1, LPT2, LPT3, LPT4, LPT5, LPT6, LPT7, LPT8, LPT9).
Parent Group drop-down list box	<p>Select a parent group to which the new group belongs. Select All Users.</p>
Type of Group drop-down list box	<p>You cannot change the group type.</p>

Item	Description
Create Guests check box	Set whether to permit or deny the use of the guest creation function. If this check box is cleared, the guest creation function cannot be used. A representative user can change this setting later.
Download limit text box	Enter the maximum amount of data that can be downloaded per month by the entire domain in the unit of MB. <ul style="list-style-type: none"> The minimum specifiable value is 0, and the maximum specifiable value is 8,796,093,022,207. A representative user can change this setting later.
Download limit resets at text box	Enter the date of the month on which the download limit count is reset. <ul style="list-style-type: none"> The minimum specifiable value is 1, and the maximum specifiable value is 31. If you enter 31 in this text box, the download limit count is reset at the end of each month.
Download limit changes by representative users text box	Set whether to permit or deny download limit changes by representative users. The default is accept . If you do not want to allow changes, clear this check box.
Total Disk Space text box	Enter the total disk space available to the entire domain in the unit of MB. <ul style="list-style-type: none"> The minimum specifiable value is 0, and the maximum specifiable value is 8,796,093,022,207.
Storage period check boxes	Specify the maximum values for the storage period that a user can set when sending a file. The default is the maximum storage period set on the system.
Limit Number Of Users text box	Set the maximum number of users that can be registered by the entire domain. <ul style="list-style-type: none"> The minimum specifiable value is 1, and the maximum specifiable value is 1,000,000.
Sending To Unregistered Addresses check box	Set whether to permit or deny the entire domain the use of the function that enables transmission of files to unregistered addresses. If you clear this check box, the entire domain is denied the use of this function.

5. Click the **Create** button.



Note

If you want to create a new domain group whose settings are identical to those of an existing one, click the menu icon () beside the group you want to copy, and then select **Copy Group**. The New Group window appears, in which the original domain group settings are specified as the default settings for the new group. This group copy function allows you to easily create a group, especially when you want to create a new group with a unique name but with settings that are identical to those of an existing one.

4.2.2 Editing the domain

To edit the domain:

1. Log in to JP1/DH - Server.
2. In the sidebar area, click **Users & Groups**.
The Users & Groups window appears in the content area.
3. Click the group (domain) you want to edit, and then select **Edit**.
The Edit Group window appears.
4. Edit the settings.

For details about each entry, see [4.2.1 Creating a domain](#).

5. Click the **update** button.

4.2.3 Deleting the domain

To delete the domain:

1. Log in to JP1/DH - Server.
2. In the sidebar area, click **Users & Groups**.
The Users & Groups window appears in the content area.
3. Click the group (domain) you want to delete, and then select **Delete**.

This deletes the domain as well as all the users and groups under the domain.

Note: If you want to disable the domain without deleting the groups and users under the domain, click **Inactivate**. Users belonging to the inactivated domain will not be able to log in to JP1/DH - Server.

4.3 Managing representative users

This section describes how to set a representative user who manages the domain.

For details about how to create a representative user, see [4.3.1 Creating a user](#). For details about how to designate an existing user as the representative user, see [4.3.2 Designating an existing user as the representative user](#).

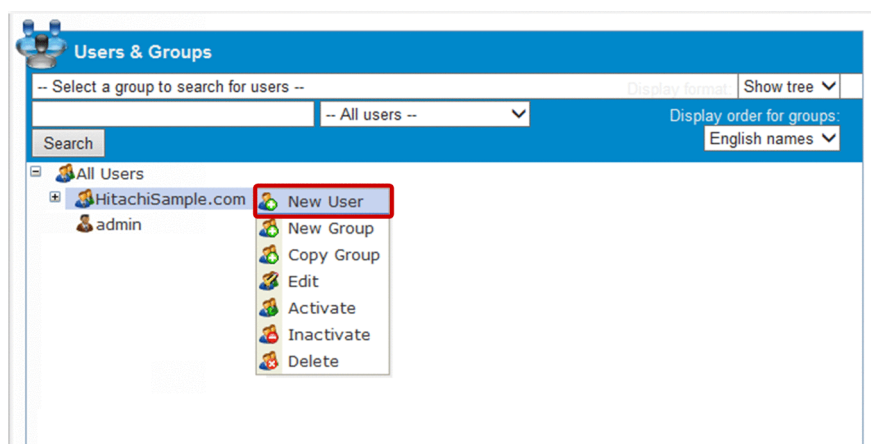
! Important

The system administrator must not create groups other than domains or users other than representative users. Creation of groups and users within a domain must be done by a representative user.

4.3.1 Creating a user

To create a user:

1. Log in to JP1/DH - Server.
2. In the sidebar area, click **Users & Groups**.
The Users & Groups window appears in the content area.
3. Click the domain you have created in [4.2.1 Creating a domain](#), and then select **New User**.
The New User window appears.



4. Create a user.

Users & Groups

-- Select a group to search for users --

Display format: Show tree

-- All users --

Display order for groups: English names

Search

New User Close

Basic Groups belongs to User Certificate

User ID @hitachisample.com

Name

Email

Password

Re-enter

User Language Japanese

Memo

Create

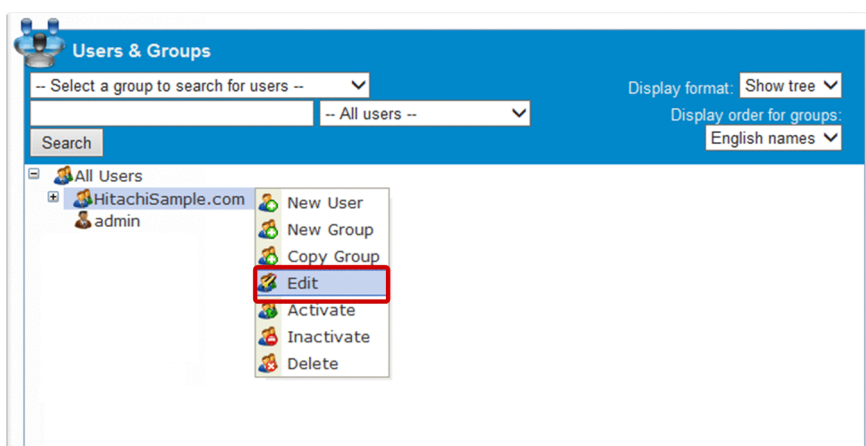
For details about each setting items, see the *JP1/Data Highway - Server Administrator Guide*.

5. Click the **Create** button.

4.3.2 Designating an existing user as the representative user

To designate an existing user as the representative user:

1. Log in to JP1/DH - Server.
2. In the sidebar area, click **Users & Groups**.
The Users & Groups window appears in the content area.
3. Click the domain you have created in [4.2.1 Creating a domain](#), and then select **Edit**.
The Edit Group window appears.



4. Click the **Group Administration** tab.

Users & Groups

-- Select a group to search for users --
 Search: -- All users --
 Display format: Show tree
 Display order for groups: English names

Edit Group [Close]

Basic | Properties | Address Book Manager | **Group Administration**

Group Name: (Japanese/Chinese) 日立Sample株式会社
 (English) HitachiSample.com

Parent Group: No parent groups

Type of Group: Group for Users
 Create Guests: ☒ accept

Download limit: 50 MB / month
 Download limit resets at: 31 every month.

Download limit changes by representative users: ☒ accept

Total Disk Space: 100000 MB

☐ Storage period: Max. 31 days

Limit Number Of Users: 10 users

Sending To Unregistered Addresses: ☒ accept

[update]

- Select the user you want to designate as the representative user, and then click the **V** button.
The user is added to the list of administrators.

Users & Groups

-- Select a group to search for users --
 Search: -- All users --
 Display format: Show tree
 Display order for groups: English names

Edit Group [Close]

Basic | Properties | Address Book Manager | **Group Administration**

Adding Group Administrators.

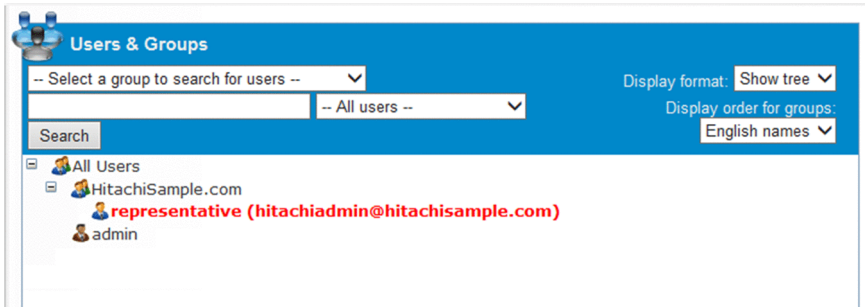
representative (hitachiadmin@hitachisample.com) ☒

V

representative (hitachiadmin@hitachisample.com)

[update]

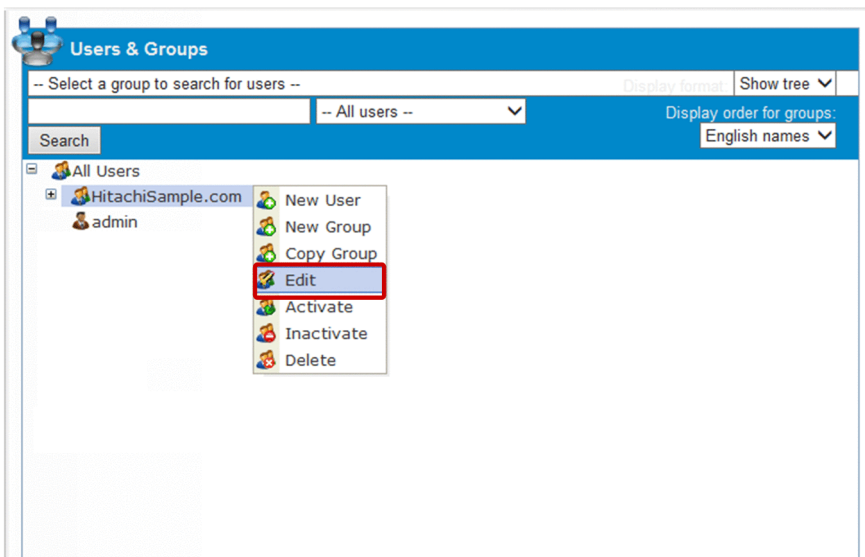
- Click the **update** button.
The name of the user designated as the representative user is highlighted in red.



4.3.3 Removing the representative user role

To remove the representative user role of the user:

1. Log in to JP1/DH - Server.
2. In the sidebar area, click **Users & Groups**.
The Users & Groups window appears in the content area.
3. Click the domain you have created in [4.2.1 Creating a domain](#), and then select **Edit**.
The Edit Group window appears.



4. Click the **Group Administration** tab.

Users & Groups

-- Select a group to search for users --

-- All users --

Display format: Show tree

Display order for groups: English names

Edit Group Close

Basic Properties Address Book Manager **Group Administration**

Group Name: (Japanese/Chinese) 日立Sample株式会社
(English) HitachiSample.com

Parent Group No parent groups

Type of Group Group for Users

Create Guests ☒ accept

Download limit 50 MB / month

Download limit resets at 31 every month.

Download limit changes by representative users ☒ accept

Total Disk Space 100000 MB

☐ **Storage period:** Max. 31 days

Limit Number Of Users 10 users

Sending To Unregistered Addresses ☒ accept

update

5. From the list of representative users, click the icon () beside the representative user whose representative user role you want to remove.

The user is removed from the list of administrators.

Users & Groups

-- Select a group to search for users --

-- All users --

Display format: Show tree

Display order for groups: English names

Edit Group Close

Basic Properties Address Book Manager Group Administration

Adding Group Administrators.

representative (hitachiadmin@hitachisample.com)

representative (hitachiadmin@hitachisample.com)

update

6. Click the **update** button.

4.3.4 Editing the user

See the *JP1/Data Highway - Server Administrator Guide*.

4.3.5 Deleting the user

See the *JP1/Data Highway - Server Administrator Guide*.


4.4 Activating or inactivating the authentication rule

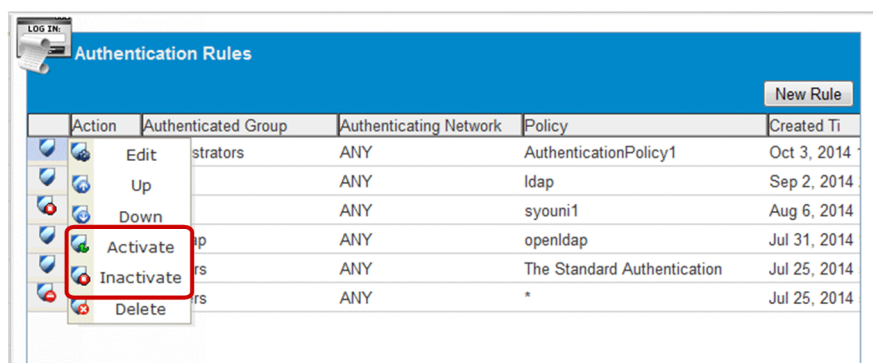
This section describes how to activate or inactivate the authentication rule.

If a representative user incorrectly sets an authentication rule and becomes unable to log in to JP1/DH - Server, the system administrator can use this procedure to activate or inactivate the authentication rule. The inactivated authentication rule will be ignored.

! Important

For details about the authentication rule, see the *JP1/Data Highway - Server Administrator Guide*.

1. Log in to JP1/DH - Server.
2. In the sidebar area, click **Authentication Rules**.
The Authentication Rules window appears in the content area.
3. Click the menu icon () beside the authentication rule you want to edit, and then select **Activate** or **Inactivate**.



! Important

You cannot activate or inactivate the two authentication rules (with **All Users** selected as the authentication group) that have been created in advance.

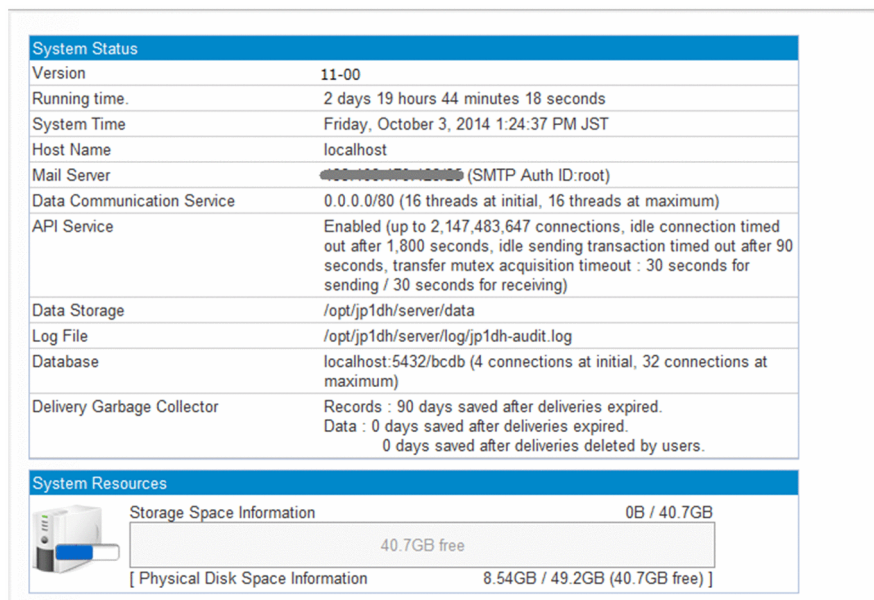
4.5 Viewing the System Monitor window

This section describes how to view the System Monitor window.

By viewing the System Monitor window, the system administrator can keep track of system use and resource status.

1. Log in to JP1/DH - Server.
2. In the sidebar area, click **System Monitor**.

The System Monitor window appears in the content area.



The screenshot displays the System Monitor window, which is divided into two main sections: System Status and System Resources.

System Status

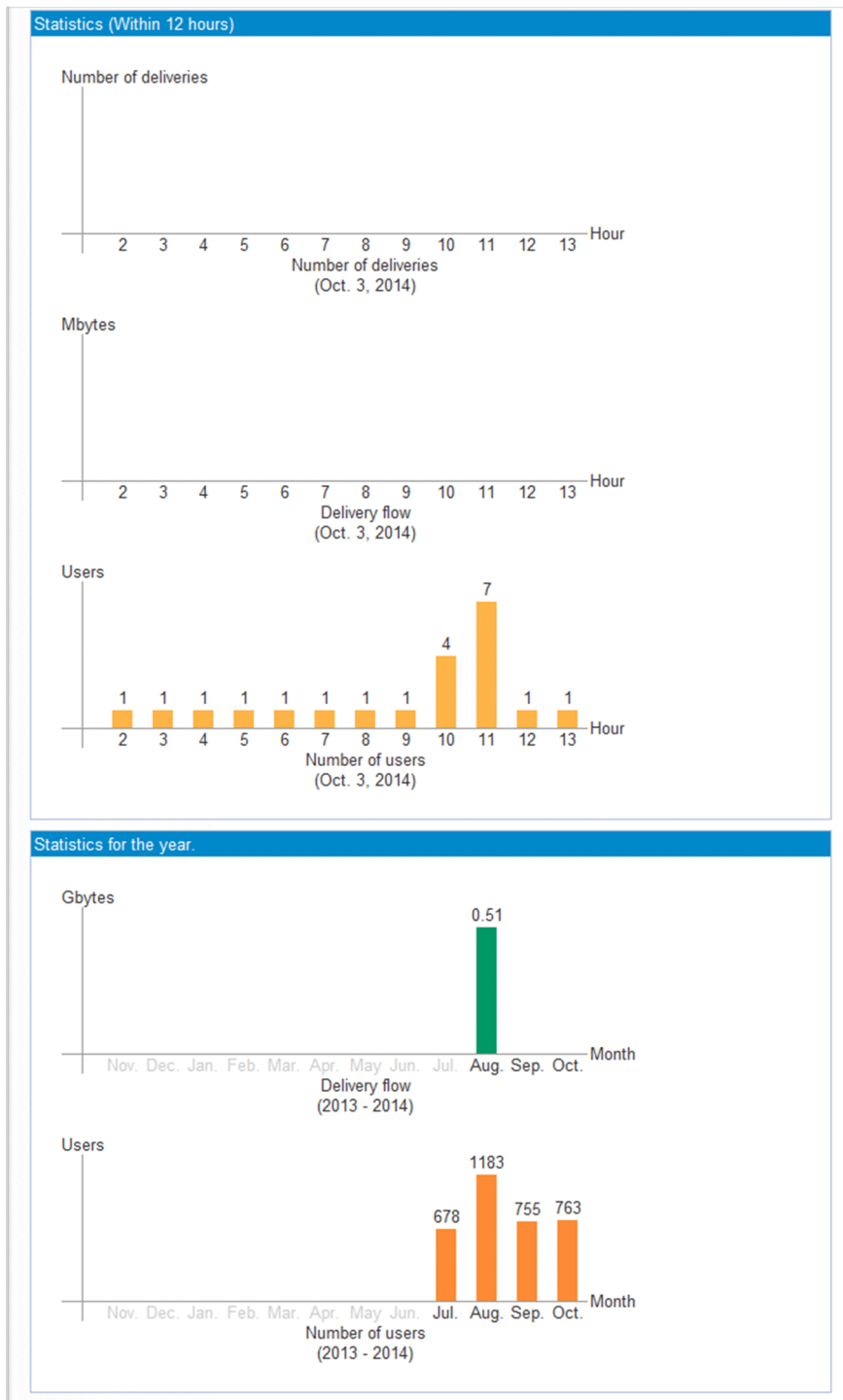
Version	11-00
Running time.	2 days 19 hours 44 minutes 18 seconds
System Time	Friday, October 3, 2014 1:24:37 PM JST
Host Name	localhost
Mail Server	***** (SMTP Auth ID:root)
Data Communication Service	0.0.0.0/80 (16 threads at initial, 16 threads at maximum)
API Service	Enabled (up to 2,147,483,647 connections, idle connection timed out after 1,800 seconds, idle sending transaction timed out after 90 seconds, transfer mutex acquisition timeout : 30 seconds for sending / 30 seconds for receiving)
Data Storage	/opt/jp1dh/server/data
Log File	/opt/jp1dh/server/log/jp1dh-audit.log
Database	localhost:5432/bcdb (4 connections at initial, 32 connections at maximum)
Delivery Garbage Collector	Records : 90 days saved after deliveries expired. Data : 0 days saved after deliveries expired. 0 days saved after deliveries deleted by users.

System Resources

Storage Space Information 0B / 40.7GB

40.7GB free

[Physical Disk Space Information 8.54GB / 49.2GB (40.7GB free)]



The table below describes each item in the System Monitor window.

Table 4–2: Items displayed in the System Monitor window

Category	Item	Description
System Status	Version	Displays the product version.
	Running time	Displays the system operating time.
	System Time	Displays the system time.
	Host Name	Displays the server host name.

Category	Item	Description
System Status	Mail Server	Displays the host name and port number of the mail server.
	Data Communication Service	Displays the initial number of threads and the maximum number of threads used by the communication engine.
	Data Storage	Displays the path to the destination to which the data sent and received is saved.
	Log File	Displays the path to the file to which the log file is saved.
	Database	Displays the following information regarding the database: host name, database name, and the number of threads.
	Delivery Garbage Collector	Displays the delivery garbage collector setting. This entry also provides information on the timing at which delivery data will be deleted from the database, as well as the timing at which files will be deleted from the file system.
System Resources	Storage Space Information	The status bar displays the free space on the physical disk as well as the disk space that is currently used by JP1/DH - Server.
	<i>XX GB free</i>	Displays the free space on the physical disk of the system.
	Physical Disk Space Information	Displays resource information for the physical disk.
Statistics (Within 12 hours)	Number of deliveries	The number of deliveries made over the last 12 hours is displayed in a graph.
	Delivery flow	The amount of data delivered (uploaded) over the last 12 hours is displayed in a graph.
	Number of users	The number of system users over the last 12 hours is displayed in a graph.
Statistics for the year	Delivery flow	The amount of data delivered (uploaded) over the past year is displayed in a graph.
	Number of users	The number of system users over the past year is displayed in a graph.

Appendixes

A. Version Changes

This appendix describes the changes in each version.

A.1 Changes in version 11-50

- The following web browsers are supported:
 - Mozilla Firefox ESR 52
 - Safari 10
- The following OS are now supported:
 - macOS 10.12 (Sierra)
- You can now create a new group by copying an existing group.
- You can now sort the display order of groups in the Users & Groups window. In addition, you can narrow down a search and display only users matching a specific state (activated or inactivated) in search results.

A.2 Changes in version 11-10

- The following OSs are no longer supported:
 - Windows 8
- The following web browsers are supported:
 - Microsoft Edge
 - Google Chrome
 - 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
- The following OS are now supported:
 - OS X 10.11 (El Capitan)
- The system can find out that all the users specified as the recipients already downloaded all the files, and then delete the files automatically before the storage expiration date is reached.
- The following settings can be configured when creating a domain:
 - Allowing representative users to change download limits
 - Changing the file storage period

A.3 Changes in version 11-00

- The following OS for the client PC are now supported: OS X 10.10 (Yosemite) and Windows 10
- The following browser are supported: Mozilla FireFox ESR 38 and Safari 8
- The following the Java software are supported:
 - Java Runtime Environment Version 8.0 (32-bit) (Update 45 or later)
 - Java Runtime Environment Version 8.0 (64-bit) (Update 45 or later)
- To be supported the rules that set the upper limit of the total bandwidth of the specified each group or network.
- The following OSs are no longer supported:
 - Microsoft(R) Windows(R) XP Professional Operating System
 - Microsoft(R) Windows(R) XP Professional x64 Edition
 - Microsoft(R) Windows Vista(R) Home Premium
 - Microsoft(R) Windows Vista(R) Business
 - Microsoft(R) Windows Vista(R) Ultimate
 - Microsoft(R) Windows Vista(R) Enterprise
- The following browser are no longer supported:
 - Internet Explorer 7

B. Reference Material for This Manual

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

B.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 11 JP1/Data Highway - Server Configuration and Administration Guide* (3021-3-B42(E))
- *JP1 Version 11 JP1/Data Highway - Server Administrator Guide* (3021-3-B43(E))
- *JP1 Version 11 JP1/Data Highway - Server User's Guide* (3021-3-B44(E))
- *JP1 Version 11 JP1/Data Highway - Automatic Job Executor* (3021-3-B46(E))

B.2 Conventions: Abbreviations for product names

This manual uses the abbreviations for product names listed below. However, when necessary, products names are written in full.

Full name or meaning	Abbreviation	
Java™ Runtime Environment	Java Runtime Environment	JRE
JP1/Data Highway - Automatic Job Executor	JP1/Data Highway - AJE	
JP1/Data Highway - Server	JP1/DH - Server	
Red Hat Enterprise Linux(R) Server 6 (64-bit x86_64)	Linux 6 (x64)	Linux

B.3 Conventions: Acronyms

This manual also uses the following acronyms:

Acronym	Full name or meaning
HTTPS	HyperText Transfer Protocol over Secure Socket Layer
ID	Identification Data
OS	Operating System
PC	Personal Computer
URL	Uniform Resource Locator
XML	Extensible Markup Language

B.4 Default installation folder

JP1/DH - Server is installed in the following folder by default:

Default installation folder

- In Windows
`system-drive:\Program Files\Hitachi\jpldh\server`
- In Linux
`/opt/jpldh/server`

B.5 Meaning of "Administrator permissions" in this manual

The term user with *Administrator permissions* in this manual refers to a user who is a member of the Administrators group on the local PC only.

B.6 Conventions: KB, MB, GB, and TB

This manual uses the following conventions:

- 1 KB (kilobyte) is 1,024 bytes.
- 1 MB (megabyte) is 1,024² bytes.
- 1 GB (gigabyte) is 1,024³ bytes.
- 1 TB (terabyte) is 1,024⁴ bytes.

C. Glossary

This appendix describes the terms used in JP1/DH - Server.

A

authentication policy

A policy that governs the authentication password set for users. It defines the complexity and length required for the password to be set.

An authentication policy is managed by the system administrator and the representative user.

authentication rule

A rule that defines the scope of application of the authentication policy. The scope of application is defined by the combination of a group and a network range. The authentication rule can permit or deny the authentication of users within the specified range.

An authentication rule is managed by the system administrator and the representative user.

B

bandwidth limitation rules

A bandwidth limitation rule stipulates the total maximum network bandwidth used for each group or network set. A bandwidth limitation rule is set up using a combination of a group, network set, and the maximum network bandwidth.

Bandwidth Limitation Rules is managed by the system administrator.

C

creating a guest user

An operation where a general user adds a user to JP1/DH - Server. A general user must be granted authority to create a guest user.

D

delivery rule

A rule that defines the scope of application of both the delivery policy and the approval route. The scope of application is defined by the combination of a sender group and the recipient group. This rule permits delivery within the specified range.

A delivery rule is managed by the representative user.

domain

One of the management units of JP1/DH - Server. A domain is a group that is directly below the top-level group.

A user ID assigned to users other than the system administrator always includes the domain name. Only the system administrator can view data across multiple domains. A domain is indicated as group in the window.

N

network set

A concept that defines the range of a network. A network set is used to create an authentication rule and a delivery rule.

A network set is managed by the system administrator and the representative user.

R

representative user

A user who manages a whole domain.

A representative user is managed by the system administrator.

S

standard authentication policy

A default authentication policy for the entire JP1/DH - Server system.

standard delivery policy

A default delivery policy for the entire JP1/DH - Server system.

system administrator

A user who manages the JP1/DH - Server domain and the representative users.

You cannot register an additional system administrator.

U

unregistered user

A user who is not registered in JP1/DH - Server.

An unregistered user can receive an email with an open password that is sent by a user who is allowed to send data to unregistered addresses in JP1/DH - Server.

An unregistered user can use only the function to receive files.

user

A person who uses JP1/DH - Server, including a system administrator, a representative user, group manager, general user, and unregistered user.

user disk space

Amount of storage space allocated to a user. A user cannot send files that exceed the amount of free user disk space.

Index

A

Activating or inactivating a Bandwidth Limitation Rules
 Activating 41
activating or inactivating authentication rule 55

C

common specifications for window 17
 notes 19
 window structure 18
conventions
 fonts and symbols 9
 version numbers 10
Creating a Bandwidth Limitation Rules
 Creating 39
creating domain 45
creating user 49

D

Deleting a Bandwidth Limitation Rules
 Deleting 42
deleting domain 48
deleting user 54
designating existing user as representative user 50

E

Edit Authentication policy window 27, 32
Edit Group window 47, 50, 52
editing domain 47
editing standard authentication policy 32
editing standard delivery policy 34
editing system administrator information 23
Editing the Bandwidth Limitation Rules
 Editing 40
editing user 53
example of window 18

F

font conventions 9

G

general operation procedure 44
general procedure for making preparation necessary to operate JP1/DH - Server 21

H

hardware
 recommended hardware 14
 required hardware 14

J

JP1/DH - Server
 preparation for operating 20

L

logging in as system administrator 22

M

managing domains 45
 creating domain 45
 deleting domain 48
managing representative users 49
 creating user 49
 deleting user 54
 designating existing user as representative user 50
 editing user 53
 removing representative user role 52

N

New Group window 45
New User window 49

O

operating system 43
 activating or inactivating authentication rule 55
 general operation procedure 44
 managing domains 45
 managing representative users 49
 viewing System Monitor window 56

P

preparation for operating JP1/DH - Server 20
 editing standard authentication policy 32
 editing standard delivery policy 34
 editing system administrator information 23
 general procedure 21
 logging in as system administrator 22

- registering number of purchased users 25
- setting authentication rule for system administrator 26
- prerequisites 13
- prerequisites for installation 14
 - recommended hardware 14
 - required hardware 14
 - required software 14

- Edit Authentication policy window 27, 32
- Edit Group window 47, 50, 52
- example 18
- New Group window 45
- New User window 49
- structure 18
- System Monitor window 56
- window structure 18

R

- recommended hardware 14
- registering number of purchased users 25
- removing representative user role 52
- required hardware 14
- required software 14

S

- Setting a Bandwidth Limitation Rule
 - Setting 39
- setting authentication policy for system administrator 26
- setting authentication rule for system administrator 26, 29
 - setting authentication policy 26
 - setting authentication rule 29
 - setting network set 28
- setting network set for system administrator 28
- software
 - required software 14
- symbol conventions 9
- system administrator
 - Bandwidth Limitation Rule 39
 - Bandwidth Limitation Rules 39, 40, 42
 - editing system administrator information 23
 - inactivating a Bandwidth Limitation Rules 41
 - logging 22
 - setting authentication policy 26
 - setting authentication rule 26, 29
 - setting network set 28

V

- version number conventions 10
- viewing System Monitor window 56

W

- window 18



6-6, Marunouchi 1-chome, Chiyoda-ku, Tokyo, 100-8280 Japan
