

Job Management Partner 1 Version 10

**Job Management Partner 1/Data Highway - Server
Administrator Guide**

Description, User's Guide, Operator's Guide

3021-3-360(E)

JP1 *Version*
10

Notices

■ Relevant program products

For details about the applicable OS versions, and a service pack and patch that are prerequisites for Job Management Partner 1/Data Highway - Server, check the *Release Notes*.

R-1523P-1AAL Job Management Partner 1/Data Highway - Server version 10-50 (For Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2)

R-1S23P-1A8L Job Management Partner 1/Data Highway - Server version 10-50 (For Red Hat Enterprise Linux)

■ Trademarks

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

Firefox is a registered trademark of the Mozilla Foundation.

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

Internet Explorer is either a registered trademark or a 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.

OS X is a trademark of Apple Inc.

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

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

Safari is a trademark of Apple Inc.

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

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

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

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(R) software developed by EMC Corporation.



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.

■ Microsoft product name abbreviations

This manual uses the following abbreviations for Microsoft product names.

Full name or meaning	Abbreviation	
Microsoft(R) Internet Explorer(R)	Internet Explorer	
Microsoft(R) Windows Server(R) 2008 R2 Datacenter	Windows Server 2008 R2	Windows
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		

Full name or meaning	Abbreviation	
Microsoft(R) Windows(R) XP Professional Operating System	Windows XP Professional	Windows
Microsoft(R) Windows(R) XP Professional x64 Edition		
Microsoft(R) Windows Vista(R) Home Premium	Windows Vista	
Microsoft(R) Windows Vista(R) Business		
Microsoft(R) Windows Vista(R) Ultimate		
Microsoft(R) Windows Vista(R) Enterprise		
Microsoft(R) Windows(R) 7 Professional	Windows 7	
Microsoft(R) Windows(R) 7 Enterprise		
Microsoft(R) Windows(R) 7 Ultimate		
Windows(R) 8 Pro	Windows 8	
Windows(R) 8 Enterprise		
Windows(R) 8.1 Pro	Windows 8.1	
Windows(R) 8.1 Enterprise		

■ Related product

The following shows the product related to Job Management Partner 1/Data Highway - Server:

- Job Management Partner 1/Data Highway - Automatic Job Executor

This data transmission client allows users to automate the file transfer function of Job Management Partner 1/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

Dec. 2014: 3021-3-360(E)

■ Copyright

All Rights Reserved. Copyright (C) 2014, Hitachi, Ltd.

All Rights Reserved. Copyright (C) 2014, Hitachi Solutions, Ltd.

Preface

This manual describes how to use Job Management Partner 1/Data Highway - Server (hereinafter abbreviated as *JP1/DH - Server*).

In this manual, *Job Management Partner 1* is abbreviated as *JP1*.

■ Intended readers

This manual is intended for:

- Representative users or group managers responsible for managing and operating domains or groups

Readers of this manual must have:

- An understanding of basic operations of the OS to be used
- A basic knowledge of networking

■ Conventions: Text formatting used in explanation of Windows operation

The following table describes the text formatting conventions for Windows used in explaining operations:

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.

Screenshots in this manual are captured in an environment where the OS is Windows 7 and the browser is Internet Explorer 8. The windows displayed in your OS or browser might differ from the screenshots in this manual. For details, see Windows Help.

■ 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.

Contents

Notices	2
Preface	5

1 Overview of JP1/DH - Server 9

1.1	What is JP1/DH - Server?	10
1.2	Features of JP1/DH - Server	11
1.2.1	Features in terms of functionality	11
1.2.2	Features in terms of installation and operation	11
1.3	Functional overview of JP1/DH - Server	12
1.3.1	File send and receive function	12
1.3.2	User and group management function	13
1.3.3	Audit log function	14
1.4	Prerequisites for installation	16
1.4.1	Prerequisite hardware	16
1.4.2	Recommended hardware	16
1.4.3	Prerequisite software	16
1.4.4	Prerequisite products for a specific function or with conditions	18

2 Operating JP1/DH - Server 19

2.1	General operation procedure for JP1/DH - Server	20
2.1.1	Configuring the authentication system	20
2.1.2	Configuring the system	21
2.1.3	Managing users and groups	21
2.1.4	Setting a delivery rule	22
2.1.5	Creating a guest user	23
2.1.6	Sending and receiving files	23
2.1.7	Auditing histories	24
2.2	Authentication methods	25
2.2.1	Authentication using user management information in JP1/DH - Server	25
2.2.2	Authentication linked to a directory server	25
2.2.3	Setting	26
2.3	Audit logs	29
2.3.1	Output format of an audit log	29
2.3.2	Audit log output details	29
2.3.3	Audit log error messages	36
2.3.4	Example of the output audit log	38
2.4	User type and authority	39

3	Explanations of JP1/DH - Server Operations	40
3.1	Window common specifications	41
3.1.1	Window structure	41
3.1.2	List of icons	42
3.1.3	Notes	44
3.2	Basic operations	46
3.2.1	List of operations	46
3.2.2	Logging in to JP1/DH - Server by using the standard password authentication	46
3.2.3	Logging in to JP1/DH - Server by using the electronic certificate authentication	48
3.2.4	Logging in by using a directory server	49
3.2.5	Logging out of JP1/DH - Server	50
3.2.6	Changing the display language	50
3.3	General-user operations	52
3.3.1	List of operations	52
3.3.2	New Delivery	52
3.3.3	Receiving a file by accessing a URL in a delivery notification email	61
3.3.4	Receiving a file in the in-box	63
3.3.5	Viewing or deleting the user's own delivery history	65
3.3.6	Approval Manager	69
3.3.7	Guest user settings	72
3.3.8	Options	76
3.4	Group-manager operations	79
3.4.1	List of operations	79
3.4.2	Users & Groups	79
3.4.3	Delivery Histories	96
3.5	Representative-user operations	100
3.5.1	List of operations	100
3.5.2	Users & Groups (batch management)	101
3.5.3	Delivery Rules	120
3.5.4	Authentication Rules	128
3.5.5	Authentication Systems	134
3.5.6	Object Definitions	139
3.5.7	Logs	144
4	Troubleshooting	146
4.1	FAQs	147
4.1.1	FAQs related to operations performed by the group manager	147
4.1.2	FAQs related to operations performed by the representative user	147
4.2	Temporary restrictions	149
4.2.1	Restrictions related to operations performed by the group manager	149
4.2.2	Restrictions related to operations performed by the representative user	149

Appendixes 151

A	Delivery Rule	152
B	Authentication Rule	155
C	List of CSV Error Messages	157
D	List of Email Messages	162
E	Reference Material for This Manual	164
E.1	Related publications	164
E.2	Conventions: Abbreviations for product names	164
E.3	Conventions: Acronyms	164
E.4	Default installation folder	165
E.5	Meaning of "Administrator permissions" in this manual	165
E.6	Conventions: KB, MB, GB, and TB	165
F	Glossary	166

Index 170

1

Overview of JP1/DH - Server

This chapter provides an overview of JP1/DH - Server.

1.1 What is JP1/DH - Server?

JP1/DH - Server is a product that enables the transfer of large files at high speed between domestic and foreign offices.

By using JP1/DH - Server, in an environment in which an Internet connection is available, you can perform high-speed file transfer through multiplex communication technology to overseas areas that are behind Japan in developing communication infrastructure. In addition, you can also transfer a gigabyte-sized large file, which has to be split to be sent by email, without splitting it by using an existing Internet connection.

1.2 Features of JP1/DH - Server

The features of JP1/DH - Server are as follows:

Features in terms of functionality

- Capable of quick, reliable, and safe transfer of large data even in conditions such as long distance and low communication quality
- Multilingual support

Features in terms of installation and operation

- Easy installation and low operation cost
- Possible to check who used the system when

1.2.1 Features in terms of functionality

(1) Capable of quick, reliable, and safe transfer of large data even in conditions such as long distance and low communication quality

JP1/DH - Server achieves improved performance and reliability for file transfer through multiplex transfer technology[#]. Thanks to this, you can deliver a large amount of data in a quick, reliable, and safe manner to remote places including abroad, where the communication line can carry only a small amount of traffic and communication is likely to be disconnected frequently.

#: Technology for using multiple HTTP(S) sessions simultaneously

(2) Multilingual support

In addition to Japanese, the web window, a user interface of JP1/DH - Server, also supports English and simplified Chinese, so that even local users in overseas offices can use the web window smoothly.

1.2.2 Features in terms of installation and operation

(1) Easy installation and low operation cost

You do not need to arrange any dedicated line because an existing Internet connection is used for communication.

Users do not need to install dedicated software on their clients to use JP1/DH - Server. Only a web browser is required for operation.

(2) Possible to check who used the system when

You can view a record such as when, by whom, and what file was sent or received as an event. In addition, you can download other operation log files to audit the system usage.

1.3 Functional overview of JP1/DH - Server

JP1/DH - Server provides the following functions:

- File send and receive function
- User and group management function
- Audit log function

1.3.1 File send and receive function

JP1/DH - Server users can send and receive large files by using JP1/DH - Server. JP1/DH - Server provides the following functions to users when they send and receive files:

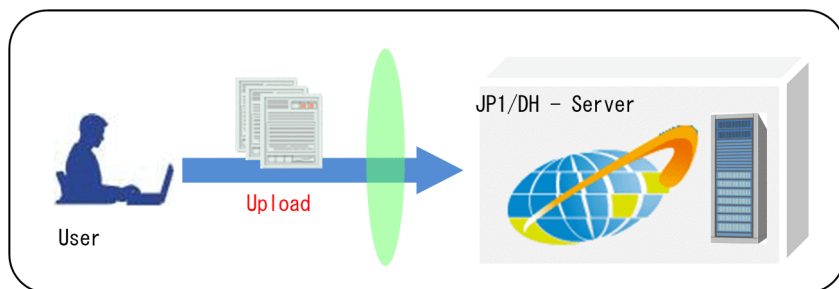
- File transmission
- File reception
- Delivery setting

(1) File transmission

You can send a large file by using JP1/DH - Server. In file transmission, you can also send a file to multiple users simultaneously or send multiple files at one time.

The sender of a file can check whether the recipient received the file.

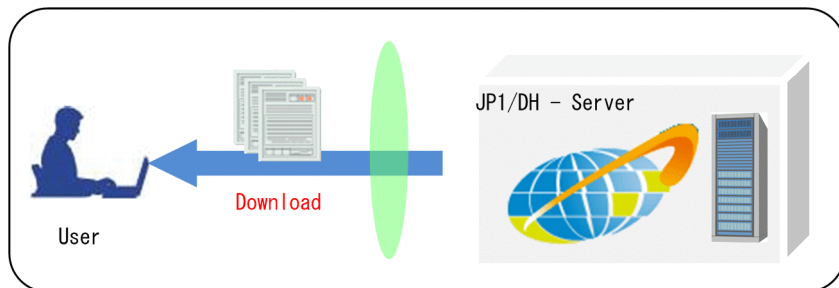
Figure 1–1: File transmission



(2) File reception

You can receive a large file by using JP1/DH - Server. The in-box provided in the web window of JP1/DH - Server or a notification email from JP1/DH - Server lets the recipient know that a file has been sent. You can download a file safely and at high speed based on the multiplex transfer technology of JP1/DH - Server.

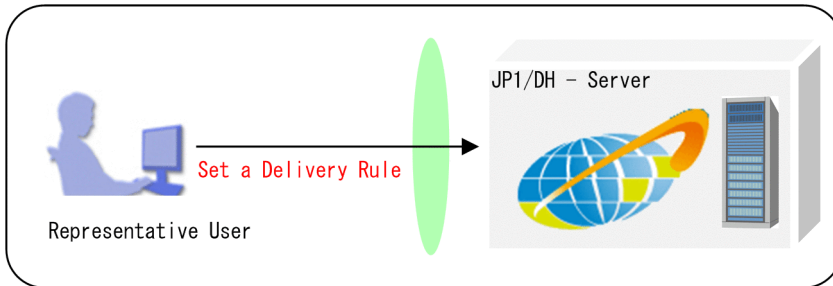
Figure 1–2: File reception



(3) Delivery setting

You can determine a rule related to file transmission such as limiting the maximum size for a file to be sent and setting a storage period on the server for a sent file. This rule is called a *delivery rule*. You can define a delivery rule by file transmission route.

Figure 1–3: Delivery rule setting



1.3.2 User and group management function

In JP1/DH - Server, the roles and authority of users are managed based on users and groups.

A representative user or group manager manages the users and groups he or she is related to. A representative user sets a rule for the users he or she manages.

The following table describes the user types in JP1/DH - Server.

Table 1–1: User types

Type	Description
Representative user	<p>A user who manages a domain created by the system administrator.</p> <p>The major roles of a representative user are shown below. Note that groups include guest groups and users include guest users.</p> <ul style="list-style-type: none">• Setting an authentication rule• Creating groups and users[#]• Managing (editing, deleting, activating, and inactivating) groups and users• Setting an environment• Delivery setting for file transmission and reception, network set configuration, and approval route setting• Auditing histories
Group manager	<p>A user who performs management inside a group created by a representative user. A group manager is created by a representative user or another group manager.</p> <p>A group manager can specify a user in a group in the Edit Group window to transfer the authority of the group manager to the specified user. The major roles of a group manager are shown below. Note that groups include guest groups and users include guest users.</p> <ul style="list-style-type: none">• Creating groups and users in the management target group[#]• Managing (editing, deleting, activating, and inactivating) the groups and users inside the management target group• Auditing sending and receiving histories of files within the management target group
General user	<p>A user who sends and receives files. A general user is created and managed by a representative user or group manager. The operations that a general user can perform are shown below. Note that depending on the authority that a general user has, the general user might be unable to use the Options function and the Guest Users function.</p> <ul style="list-style-type: none">• Sending and receiving files• Using the Guest Users function

Type	Description
General user	<ul style="list-style-type: none"> Using the Options function
Guest user	<p>A user who belongs to a guest group.</p> <p>A guest user is created by a representative user, group manager, or a user with the authority to create a guest user. A guest user cannot create another guest user.</p> <p>The operation that a guest user can perform is as follows:</p> <ul style="list-style-type: none"> Sending and receiving files
Unregistered user	<p>A user who is not registered in JP1/DH - Server.</p> <p>A user who is allowed to transmit data to an unregistered address in JP1/DH - Server can send a file to a user not registered in the system.</p> <p>An unregistered user can use only the function to receive files. In addition, an unregistered user can access JP1/DH - Server only when receiving a file from a user registered in the system.</p>

#

For the upper limit of the number of users that can be registered in each domain, contact the system administrator.

1.3.3 Audit log function

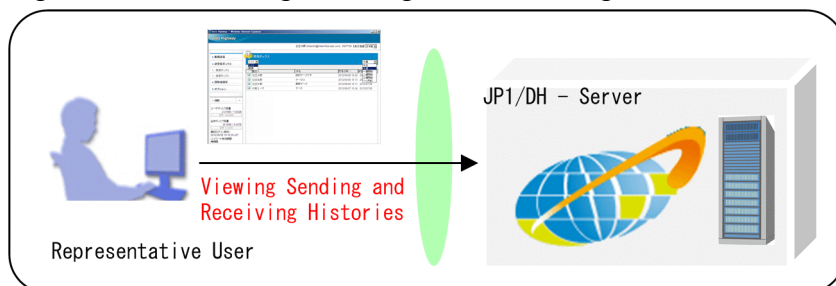
JP1/DH - Server keeps system usage logs. By using the web window for JP1/DH - Server, you can audit the system usage. For auditing, the following functions are provided:

- Viewing sending and receiving histories of files
- Downloading audit log files

(1) Viewing sending and receiving histories of files

You can check sending and receiving histories of files in the web window for JP1/DH - Server. A general user can check the sending and receiving histories of files that he or she sent. A group manager can check the sending and receiving histories of files within the management target group. A representative user can check the sending and receiving histories of files sent by all users in the domain. What files were sent and received by whom and when can be audited easily.

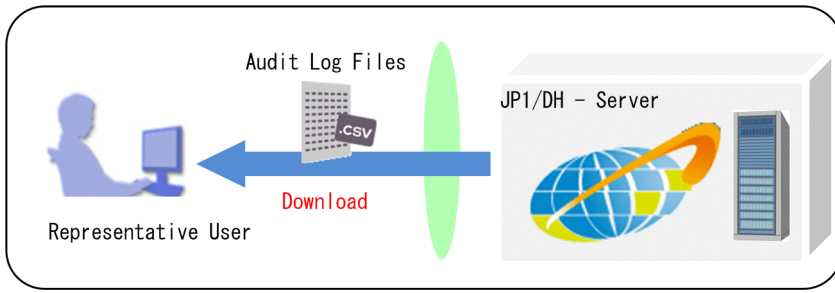
Figure 1–4: Viewing sending and receiving histories



(2) Downloading audit log files

A representative user can output usage histories for all users within the domain to a CSV text file. This file is called an *audit log file*. In an audit log file, not only sending and receiving histories of files but also histories of operations such as those performed in JP1/DH - Server to manage users and groups are recorded. Therefore, an audit log file helps a representative user audit the entire domain.

Figure 1–5: Downloading audit log files



1.4 Prerequisites for installation

The following subsections describe the prerequisites required for a client PC when you use JP1/DH - Server.

1.4.1 Prerequisite hardware

- PC/AT compatible machine
To receive files amounting to 50 GB in total on a PC/AT compatible machine, free memory space of approximately 900 MB is required.
- To download a file, free disk space twice the size of the file is required.

1.4.2 Recommended hardware

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

Table 1–2: Recommended hardware for a client PC

Recommended hardware	
CPU	Intel Core 2 Duo 2.4 GHz equivalent or higher
Memory	3 GB or more
Free disk space	Twice or larger than the size of a file to be sent or received
Network card	100 Mbps or more

1.4.3 Prerequisite software

The following subsections describe the prerequisite software for a client PC.

Note that we might not be able to respond to an inquiry about problems that occur due to software for which support has been discontinued by the manufacturer or provider of that software.

(1) In Windows

The following table describes the OSs and browsers that can be used when a client PC runs on a Windows OS.

Table 1–3: Prerequisite OSs and browsers for a client PC (in Windows)

Prerequisite OS and software	
OS	One of the following OSs is required: ^{# 1} <ul style="list-style-type: none">• Windows(R) XP Professional (32-bit) (Service Pack 3 or later)• Windows(R) XP Professional (64-bit) (Service Pack 2 or later)• Windows Vista(R) Home Premium (32-bit) (Service Pack 2 or later)• Windows Vista(R) Business (32-bit) (Service Pack 2 or later)• Windows Vista(R) Ultimate (32-bit) (Service Pack 2 or later)• Windows Vista(R) Enterprise (32-bit) (Service Pack 2 or later)• Windows(R) 7 Professional (32-bit or 64-bit) (Service Pack 1 or later)

1. Overview of JP1/DH - Server

Prerequisite OS and software	
OS	<ul style="list-style-type: none"> • 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 (32-bit or 64-bit)^{#2} • Windows(R) 8 Pro (32-bit or 64-bit)^{#2} • Windows(R) 8 Enterprise (32-bit or 64-bit)^{#2} • 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}
Browser	<p>One of the following browsers is required:</p> <ul style="list-style-type: none"> • Internet Explorer 7^{#3} • Internet Explorer 8^{#3} • Internet Explorer 9^{#3} • Internet Explorer 10^{#3#4} • Internet Explorer 11^{#3} • Mozilla Firefox ESR 24 • Mozilla Firefox ESR 31

#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

For Internet Explorer, you need to enable the following functions:

- 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 10, specify the browser's settings as follows:

- 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 OS and browser that can be used when a client PC runs on a Mac OS.

Table 1–4: Prerequisite OS and browser for a client PC (in Mac OS)

Prerequisite OS and software	
OS	OS X Mavericks

Prerequisite OS and software	
Browser	Safari 7

(3) Java software

The Java software that can be used for a client PC is shown below.

One of the following is required:

- Java Runtime Environment Version 6.0 (32-bit) (Update 24 or later)
- Java Runtime Environment Version 6.0 (64-bit) (Update 41 or later)
- Java Runtime Environment Version 7.0 (32-bit) (Update 51 or later)
- Java Runtime Environment Version 7.0 (64-bit) (Update 51 or later)#

#

If a client PC runs on a Mac OS, use this version of the software.

1.4.4 Prerequisite products for a specific function or with conditions

For authentication by using the directory server when a user attempts to log in to JP1/DH - Server, one of the following products is required as the prerequisite product on the system:

- Windows Server 2008 R2 Active Directory server
- Windows Server 2012 Active Directory server
- Windows Server 2012 R2 Active Directory server
- OpenLDAP V2.4

2

Operating JP1/DH - Server

This chapter describes operation procedures for JP1/DH - Server.

2.1 General operation procedure for JP1/DH - Server

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

Figure 2–1: General operation procedure for JP1/DH - Server



#1: Group managers cannot operate these items.

#2: Performed by users with approver authority.

Legend: Work performed by a representative user or group manager.
 Work performed by a general user.

Overviews of each operation described in the above figure are explained below. Note that a representative user can perform all the operations general users can perform.

2.1.1 Configuring the authentication system

Configure the authentication system that defines and manages information related to the authentication infrastructure to be used for logging in to JP1/DH - Server.

Two types of authentication system are available: *standard authentication system* and *LDAP authentication system*.

The standard authentication system is defined by default. The standard authentication system is used for authentication with user IDs and passwords that are defined and managed in JP1/DH - Server or for authentication by the electronic certificates.

An LDAP authentication system is used for authentication with a directory server. You can log in to JP1/DH - Server by using your user ID and password registered in the directory server. You do not need to manage passwords in JP1/DH - Server. However, because user information registered in JP1/DH - Server is used for managing the authentication rules and delivery rules for this product, the users whose user IDs are registered in the directory server must also be registered to JP1/DH - Server.

The LDAP authentication system is not defined by default. You must create a definition for LDAP authentication system for each linked directory server. In this system, you cannot log in by using the standard password authentication or electronic certificate authentication of JP1/DH - Server.

A representative user configures an authentication system. For details about window operations related to configuration of the authentication system, see the following table.

Table 2–1: Window operations related to configuration of the authentication system

Item	Description	Related subsection
Creating an authentication system	An authentication system is created.	3.5.5(1)
Editing an authentication system	An authentication system is edited.	3.5.5(2)
Deleting an authentication system	An authentication system is deleted.	3.5.5(3)

2.1.2 Configuring the system

Set the range of a network (network set) to be selected for the authentication rule or delivery rule. You can use JP1/DH - Server without setting a network set. However, by setting a network set, you can limit the use of JP1/DH - Server on a network basis.

A representative user configures the system. For details about window operations related to configuration of the system, see the following table.

Table 2–2: Window operations related to configuration of the system setting

Item	Description	Related subsection
Creating a network set	A network set is created.	3.5.6(1)
Editing a network set	A network set is edited.	3.5.6(2)
Deleting a network set	A network set is deleted.	3.5.6(3)

2.1.3 Managing users and groups

Set users who use JP1/DH - Server and groups, which are management units of users. Set a user under a group as a group manager to delegate authority to manage that group.

Also set a policy for setting user authentication passwords (authentication policy) and a rule that determines the applicable range of an authentication policy (authentication rule).

A representative user or group manager manages the users and groups he or she is related to. Note that only a representative user can use the batch management of users and groups by using CSV files.

For details about window operations related to user and group management, see the following table.

Table 2–3: Window operations related to user and group management

Item	Description	Related subsection
Creating a group	A new group is created.	3.4.2(8)
Editing a group	Group information is edited. A group manager is set.	3.4.2(9)
Activating, inactivating, or deleting a group	A group is activated, inactivated, or deleted.	3.4.2(10)
Creating a user	A new general user is created.	3.4.2(2)
Editing a user	General user information is edited.	3.4.2(3)
Activating, inactivating, or deleting a user	A general user is activated, inactivated, or deleted.	3.4.2(4)
Creating users and groups in a batch	Users and groups are created (imported) by using a CSV file.	3.5.2(2)
Viewing users and groups in a batch	Users and groups are viewed (exported) by using a CSV file.	3.5.2(3)
Deleting users in a batch	Users are deleted by using a CSV file.	3.5.2(4)
Creating an authentication policy	A new authentication policy is created.	3.5.4(4)
Editing an authentication policy	Authentication policy information is edited.	3.5.4(5)
Deleting an authentication policy	An authentication policy is deleted.	3.5.4(6)
Creating an authentication rule	A new authentication rule is created.	3.5.4(1)
Editing an authentication rule	Authentication rule information is edited.	3.5.4(2)
Activating, inactivating, or deleting an authentication rule	An authentication rule is activated, inactivated, or deleted.	3.5.4(3)

2.1.4 Setting a delivery rule

Set a delivery rule that determines the applicable range of a policy on file transmission and reception. For a delivery rule, set the following two policies and a delivery route, which defines their applicable range:

- A policy that defines an approver and conditions for approval (approval route)
- A policy on file delivery including the maximum size and storage period of a file to be sent and received (delivery policy definition).

A representative user sets a delivery rule.

For details about window operations related to the delivery rule setting, see the following table.

Table 2–4: Window operations related to the delivery rule setting

Item	Description	Related subsection
Creating an approval route	A new approval route is created.	3.5.6(4)

Item	Description	Related subsection
Editing an approval route	Approval route information is edited.	3.5.6(5)
Deleting an approval route	An approval route is deleted.	3.5.6(6)
Creating a delivery policy	A new delivery policy is created.	3.5.3(4)
Editing a delivery policy	Delivery policy information is edited.	3.5.3(5)
Deleting a delivery policy	A delivery policy is edited.	3.5.3(6)
Creating a delivery rule	A new delivery rule is created.	3.5.3(1)
Editing a delivery rule	Delivery rule information is edited.	3.5.3(2)
Activating, inactivating, or deleting a delivery rule	A delivery rule is activated, inactivated, or deleted.	3.5.3(3)

2.1.5 Creating a guest user

If a general user wants to set a user who uses JP1/DH - Server such as in the case of when temporarily adding a user who receives files, create a guest user.

A general user can create a guest user. Note that a general user must be granted authority to create a guest user by the representative user.

For details about window operations related to the creation of a guest user, see the following table.

Table 2–5: Window operations related to creation of a guest user

Item	Description	Related subsection
Creating a guest user	A new guest user is created.	3.3.7(1)
Editing a guest user	Guest user information is edited.	3.3.7(2)
Activating, inactivating, or deleting a guest user	A guest user is activated, inactivated, or deleted.	3.3.7(3)

2.1.6 Sending and receiving files

Send and receive files by using JP1/DH - Server. If an approver is set in the delivery rule, transmission of the file must be approved.

A general user sends and receives files.

For details about window operations related to sending and receiving files, see the following table.

Table 2–6: Window operations related to sending and receiving files

Item	Description	Related subsection
Sending files and messages	A file or message is sent by selecting an address from the address book.	3.3.2(1)

Item	Description	Related subsection
Sending files and messages	A file or message is sent by directly inputting an address not registered in the system.	3.3.2(2)
Receiving a file by accessing a URL in a delivery notification email	A user registered in the system can receive a file by accessing a URL written in a delivery notification email.	3.3.3(1)
	A user not registered in the system can receive a file by accessing a URL written in a delivery notification email.	3.3.2(2)
Receiving a file in the in-box	A file is received in the in-box.	3.3.4
Accepting or rejecting an application for approval by accessing a URL written in an email	An application for approval is accepted or rejected by accessing a URL written in an email received from JP1/DH - Server.	3.3.6(1)
Accepting or rejecting an application for approval from the list in the Applications for Approval window	An application for approval is accepted or rejected from the Applications for Approval window.	3.3.6(2)

2.1.7 Auditing histories

Audit operation histories by using JP1/DH - Server. You can check sending and receiving histories of files in the web window for JP1/DH - Server. You can also check other operation histories by downloading audit log files.

A representative user or group manager audits histories. A representative user can audit files sent and received by all users and obtain audit logs. A group manager can audit files sent and received in his or her management target group. Note that a general user can audit files sent by himself or herself.

For details about window operations related to history auditing, see the following table.

Table 2–7: Window operations related to history auditing

Item	Description	Related subsection
Viewing or deleting the user's own usage histories	The user's own file usage histories are viewed and deleted.	3.3.5
Viewing or deleting sending and receiving histories of files	The user's sending and receiving histories of files are viewed and deleted.	3.4.3(1)
Obtaining audit logs.	Audit logs are obtained.	3.5.7(1)

2.2 Authentication methods

The following two authentication methods are available to log in to JP1/DH - Server:

- Authentication using the user management information in JP1/DH - Server
- Authentication linked to a directory server

The following subsections describe the authentication methods.

2.2.1 Authentication using user management information in JP1/DH - Server

This authentication method uses user IDs and passwords registered in JP1/DH - Server for user authentication when a user logs in to the system. This is called the *standard authentication system*.

In the standard authentication system, user IDs and passwords are managed by JP1/DH - Server.

The standard authentication system has the following types of authentication:

- *Standard password authentication*: A user ID and password are used for authentication
- *Electronic certificate authentication*: An electronic certificate and password are used for authentication

2.2.2 Authentication linked to a directory server

This authentication method uses the directory server for user authentication when a user logs in to JP1/DH - Server.

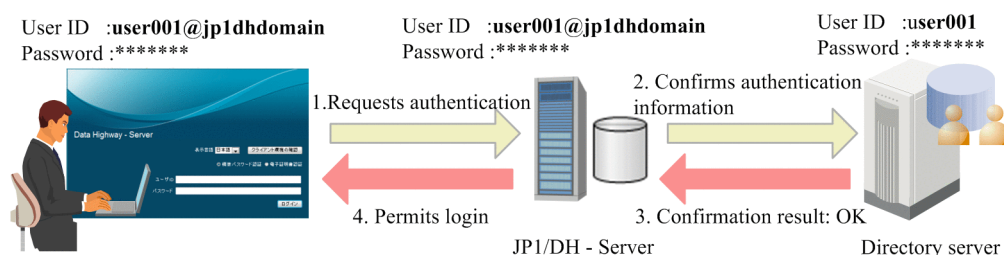
In this authentication method, the passwords of JP1/DH - Server users are managed by the directory server.

Users do not need to update their passwords in JP1/DH - Server because their passwords are managed by the directory server. Users can log in to JP1/DH - Server by using a password shared with another system linked to the directory server for authentication.

(1) General procedure for authentication

The following figure shows a general procedure for authentication when logging in to JP1/DH - Server by using the authentication linked to directory server.

Figure 2–2: General procedure for authentication



The description of the figure is as follows:

1. The user `user001@jp1dhdomain` logs in to JP1/DH - Server.

2. JP1/DH - Server checks that the user `user001@jp1dhdomain` is registered in the system. If the user is recognized as a user using the authentication linked to directory server, JP1/DH - Server checks authentication information through linkage with directory server.
3. JP1/DH - Server receives the result of the authentication linked to directory server.
4. When the directory server confirms the validity of the authentication information, the user is allowed to log in to the system.

(2) Notes on operation

If you use authentication linked to the directory server, note the following when operating the system.

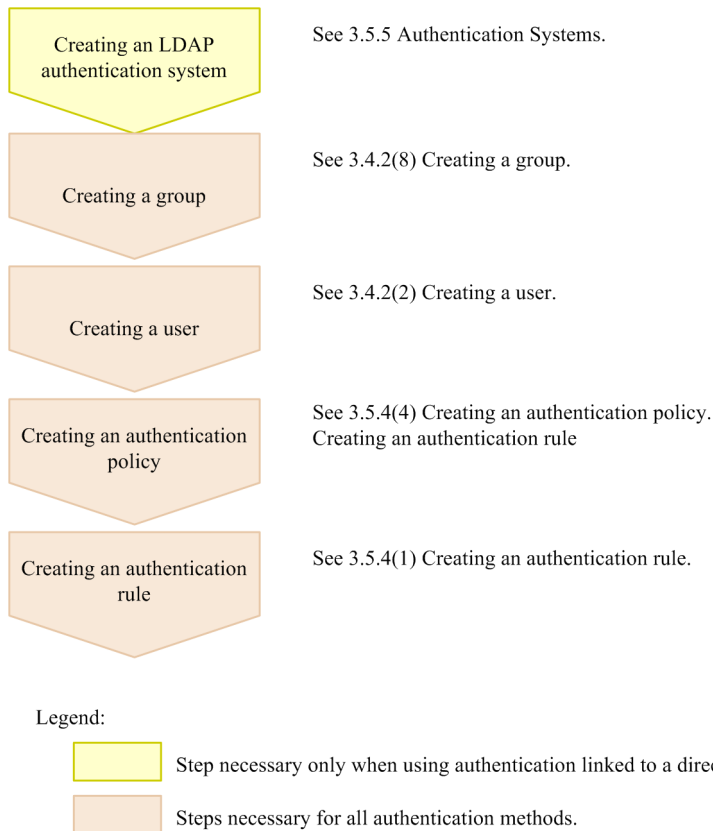
- Even when using authentication linked to directory server, you must create users in JP1/DH - Server in advance.
- Specify the same user IDs managed by directory server when creating users in JP1/DH - Server.
- When you create a user in JP1/DH - Server, specifying passwords is required as the user information managed by JP1/DH - Server. For this password, you can specify any password because the password is not used in authentication linked to directory server.
Note that you cannot change a password managed by the directory server by changing a password on JP1/DH - Server.
- The smallest unit for using authentication linked to directory server is a group.
- A login ID for JP1/DH - Server is *user-ID-managed-by-directory-server@domain-name-on-JP1/DH-Server-user-belongs-to*.
- When a user logs in to JP1/DH - Server, the system communicates with directory server. For that reason, it might take a while to log in when there is network traffic.

2.2.3 Setting

The authentication policy applied at the time of login determines the authentication method used for logging in to JP1/DH - Server.

Define an authentication method you want to use as the authentication policy, and also define the authentication rule to ensure that the authentication policy is applied properly. The following figure show general procedures for setting authentication.

Figure 2–3: General procedure for setting authentication



(1) Creating an LDAP authentication system

To use authentication linked to the directory server, create an LDAP authentication system that defines connection information such as the connection destination URL for the directory server. To link to multiple directory servers, create an LDAP authentication system for each linked directory server.

For authentication with the user management information in JP1/DH - Server, creation of an LDAP authentication system is not necessary, because the connection information is already defined in the standard authentication system to be used.

(2) Creating groups

Create groups.

An authentication policy is applied in units of domain and group. Create appropriate groups according to the types and quantities of authentication policies to be created later.

(3) Creating users

Create users belonging to a domain or group.

For the IDs of users using authentication linked to directory server, specify user IDs managed by the directory server.

(4) Creating an authentication policy

Create an authentication policy.

The type of authentication system selected in authentication policy creation determines the authentication method to be used when the authentication policy is applied.

If you want to use the authentication with the user management information in JP1/DH - Server, select the standard authentication system. If you want to use authentication linked to directory server, select an LDAP authentication system created in *(1) Creating an LDAP authentication system*.

(5) Creating an authentication rule

Create an authentication rule so that the authentication policy created in *(4) Creating an authentication policy* applied when the user who belongs to the group created in *(2) Creating groups* logs in to the system.

2.3 Audit logs

This section describes JP1/DH - Server audit logs.

2.3.1 Output format of an audit log

An audit log is output as a CSV file. The audit log output format is as follows:

```
"processed-date", "client-IP-address", "log-level", "identifier-for-operation-target-object",  
"operation-type-output-in-audit-log", "operation-details-output-in-audit-log"
```

2.3.2 Audit log output details

The following tables describe audit log output details.

Table 2–8: Audit log output details

No.	Item	Description
1	<i>processed-date</i>	<p>Date and time the log entry is written (server time). The data is output in the following format:</p> <pre>four-digit-year-two-digit-month-two-digit-dayTtwo-digit-hour:two-digit-minute:two-digit-second.three-digit-millisecond(+ -)UTC-time-offset-in-hours-and-minutesLdelay-time</pre> <p>The <i>delay-time</i> refers to a period of time from the event occurrence to the data to be written to a log. (in seconds)</p>
2	<i>client-IP-address</i>	<p>The IP address of the client that accessed the system is output. If access is made via a proxy server that hides the IP address of the client, the IP address of that proxy server is output.</p>
3	<i>log-level</i>	<p>A log level, which indicates the level of importance of the log, is output. One of the levels below is output. The levels are described in descending order of importance.</p> <ul style="list-style-type: none">• ERROR: A failure that cannot be recovered from by user operation or system operation• WARN: A failure that can be recovered from by user operation or system operation, or a failure that does not affect operational continuity• NOTICE: A user operation or system operation that has ended normally• INFO: Detailed information that complements the NOTICE level• DESC: Item or reference information that is not important in terms of management
4	<i>identifier-for-operation-target-object</i>	<p>The ID information of the object that has become an operation target is output. Multiple parameters might exist because different parameters are output depending on the operation type. Note that information might not be output depending on the operation condition. For output details, see Table 2-9 Details of the identifier for operation target object output in audit log.</p>
5	<i>operation-type-output-in-audit-log</i>	<p>A string indicating the operation type is output. For output details, see Table 2-10 Details of operation type output in audit log.</p>

No.	Item	Description
6	<i>operation-details-output-in-audit-log</i>	Various kinds of information related to the operation are output. Multiple parameters might exist because different parameters are output depending on the operation type. Note that information might not be output depending on the operation condition. For output data details, see <i>Table 2-11 Details of operation details output in audit log</i> .

Table 2–9: Details of the identifier for operation target object output in audit log

Identifier for operation target object	Parameter complemented by	Supplemental information
<code>uid=<No .serial-number#user-ID></code>	<i>serial-number</i> : A unique number assigned to a user	Indicates a user that logged in or out.
<code>fid=file-number</code>	<i>file-number</i> : A unique number assigned to a file	Indicates a file.
<code>did=delivery-number</code>	<i>delivery-number</i> : A unique number assigned to a file sending event	Indicates a file sending event.
<code>rid=reception-number</code>	A unique number assigned to a file receiving event	Indicates a file receiving event.
<code>user=<No .serial-number#user-ID></code>	<i>serial-number</i> : A unique number assigned to a user	Indicates a general user or guest user.
<code>group=<group-name></code>	--	Indicates a group.
<code>rsn=rule-number</code>	<i>rule-number</i> : A unique number assigned to a delivery rule or authentication rule	Indicates a delivery rule or authentication rule.
<code>accept=<(true false)></code>	true: Accept false: Deny	Indicates the <i>Accept</i> status or <i>Deny</i> status of the delivery rule or authentication rule.
<code>policy=<policy-name></code>	--	Indicates a delivery policy or authentication policy.
<code>from=<group-name></code>	--	For a delivery rule, indicates a sender group. For an authentication rule, indicates an applicable group.
<code>to=<group-name></code>	--	For a delivery rule, indicates a recipient group.
<code>from-net=<applicable-network></code>	<i>applicable-network</i> : ANY or a network set name	Indicates a network that the authentication rule is applied to.
<code>network-set=<network-set-name></code>	--	Indicates a network set.
<code>approval-route=<approval-route-name></code>	--	Indicates an approval route.
<code>src=<IP-address></code>	<i>IP-address</i> : IP address of an authenticated client	Indicates a client.
<code>system=<system-name></code>	--	Indicates the English name of an authentication system.

Table 2–10: Details of operation type output in audit log

Operation type	Operation type output in audit log	Description
Logging in	LOGIN	Recorded when a user logs in to JP1/DH - Server.
Logging out	LOGOUT	Recorded when a user logs out from JP1/DH - Server.
Sending a new delivery	SEND_DELIVERY	Recorded when a new file is sent.
Transmission failure	CONNECTION_ABORTED	Recorded when file transmission failed immediately after the file was transmitted.
Viewing details of a received file, or an attempt to open a file with password	OPEN_DELIVERY	Recorded in one of the following cases: <ul style="list-style-type: none"> The details of the file are viewed in the inbox. A file is opened by using the URL in the received email. A user whose address is not registered succeeded or failed in opening the file by using the open password.
Login	RECV_LOGIN	Recorded when a user logged in by using the URL in the received email.
Receiving or accessing the window	RECV_DELIVERY	Recorded in either of the following cases: <ul style="list-style-type: none"> A file is opened by using the URL in the received email. A user whose address is not registered accessed the JP1/DH - Server window.
Deleting a file	DELETE_DELIVERY	Recorded when a file is deleted.
Deleting an failure delivery file	DELETE_FAILURE_DELIVERY	Recorded when a file failed to be sent is deleted.
Downloading a received file	DOWNLOAD_FILE	Recorded when a file is downloaded.
Creating a guest user	CREATE_GUEST	Recorded when a guest user is created.
Updating guest user information	UPDATE_GUEST	Recorded when guest user information is updated.
Activating a guest user	ACTIVATE_GUEST	Recorded when a guest user is activated.
Inactivating a guest user	INACTIVATE_GUEST	Recorded when a guest user is inactivated.
Deleting a guest user	DELETE_GUEST	Recorded when a guest user is deleted.
Creating a general user	CREATE_USER	Recorded when a general user is created.
Updating general user information	UPDATE_USER	Recorded when general user information is updated.
Activating a general user	ACTIVATE_USER	Recorded when a general user is activated.
Inactivating a general user	INACTIVATE_USER	Recorded when a general user is inactivated.
Deleting a general user	DELETE_USER	Recorded when a general user is deleted.
Creating a group	CREATE_GROUP	Recorded when a group is created.
Updating group information	UPDATE_GROUP	Recorded when group information is updated.
Activating a group	ACTIVATE_GROUP	Recorded when a group is activated.
Inactivating a group	INACTIVATE_GROUP	Recorded when a group is inactivated.

Operation type	Operation type output in audit log	Description
Deleting a group	DELETE_GROUP	Recorded when a group is deleted.
Issuing an electronic certificate	CREATE_CERT	Recorded when an electronic certificate is issued.
Revoking an electronic certificate	REVOKE_CERT	Recorded when an electronic certificate is revoked.
Creating a delivery rule	CREATE_DELIVERY_RULE	Recorded when a delivery rule is created.
Updating a delivery rule	UPDATE_DELIVERY_RULE	Recorded when a delivery rule is updated.
Moving the delivery rule position downward	DOWN_DELIVERY_RULE	Recorded when the position of a delivery rule is moved downward in the delivery rule list.
Moving the delivery rule position upward	UP_DELIVERY_RULE	Recorded when the position of a delivery rule is moved upward in the delivery rule list.
Activating a delivery rule	ACTIVATE_DELIVERY_RULE	Recorded when a delivery rule is activated.
Inactivating a delivery rule	INACTIVATE_DELIVERY_RULE	Recorded when a delivery rule is inactivated.
Deleting a delivery rule	DELETE_DELIVERY_RULE	Recorded when a delivery rule is deleted.
Creating a delivery policy	CREATE_DELIVERY_POLICY	Recorded when a delivery policy is created.
Updating a delivery policy	UPDATE_DELIVERY_POLICY	Recorded when a delivery policy is updated.
Deleting a delivery policy	DELETE_DELIVERY_POLICY	Recorded when a delivery policy is deleted.
Creating an authentication rule	CREATE_AUTH_RULE	Recorded when an authentication rule is created.
Updating an authentication rule	UPDATE_AUTH_RULE	Recorded when an authentication rule is updated.
Moving the authentication rule position downward	DOWN_AUTH_RULE	Recorded when the position of an authentication rule is moved downward in the authentication rule list.
Moving the authentication rule position upward	UP_AUTH_RULE	Recorded when the position of an authentication rule is moved upward in the authentication rule list.
Activating an authentication rule	ACTIVATE_AUTH_RULE	Recorded when an authentication rule is activated.
Inactivating an authentication rule	INACTIVATE_AUTH_RULE	Recorded when an authentication rule is inactivated.
Deleting an authentication rule	DELETE_AUTH_RULE	Recorded when an authentication rule is deleted.
Creating an authentication policy	CREATE_AUTH_POLICY	Recorded when an authentication policy is created.
Updating an authentication policy	UPDATE_AUTH_POLICY	Recorded when an authentication policy is updated.
Deleting an authentication policy	DELETE_AUTH_POLICY	Recorded when an authentication policy is deleted.
Creating an authentication system	CREATE_AUTH_SYSTEM	Recorded when an authentication system is created.
Updating an authentication system	UPDATE_AUTH_SYSTEM	Recorded when an authentication system is updated.

Operation type	Operation type output in audit log	Description
Deleting an authentication system	DELETE_AUTH_SYSTEM	Recorded when an authentication system is deleted.
Failure in LDAP authentication system linkage	FAILED_LDAP_AUTHENTICATION	Recorded when authentication using an LDAP authentication system failed.
Multiple matching users are found in the authentication system	DUPLICATE_LDAP_USER_EXISTS	Recorded when multiple matching users are found in the searched directory server during an authentication process using an LDAP authentication system.
No matching user in the authentication system	LDAP_USER_DOES_NOT_EXISTS	Recorded when no matching user is found in the searched directory server during an authentication process using an LDAP authentication system.
Creating a network set	CREATE_NETWORK_SET	Recorded when a network set is created.
Updating a network set	UPDATE_NETWORK_SET	Recorded when a network set is updated.
Deleting a network set	DELETE_NETWORK_SET	Recorded when a network set is deleted.
Creating an approval route	CREATE_APPROVAL_ROUTE	Recorded when an approval route is created.
Updating an approval route	UPDATE_APPROVAL_ROUTE	Recorded when an approval route is updated.
Deleting an approval route	DELETE_APPROVAL_ROUTE	Recorded when an approval route is deleted.
Skipping an approval route	SKIP_DELIVERY_APPROVAL	Recorded if an approval process is skipped for a transmission by JP1/Data Highway - AJE.
Downloading an audit log file	DOWNLOAD_LOG	Recorded when an audit log file is downloaded.
Notification of delivery	NOTIFY_DELIVERY	Recorded when an email is sent to the recipient or approver to notify a new file delivery.
Notification of approval acceptance	NOTIFY_DELIVERY_ACCEPTED	Recorded when an email is sent to the sender to notify acceptance of file transmission approval.
Notification of approval rejection	NOTIFY_DELIVERY_REJECTED	Recorded when an email is sent to the sender to notify rejection of file transmission approval.
Notification of delivery opening	NOTIFY_OPEN_DELIVERY	Recorded when an email is sent to notify the opening of a file for which the notification for file opening is activated.
Changing a password	UPDATE_PASSWORD	Recorded when a user password is changed.
Expiration of password validity period	PASSWORD_EXPIRED	Recorded if the password validity period is expired when the user attempts to log in.
Changing user language	UPDATE_USER_LANG	Recorded when the user language setting is changed.
Client authentication acceptance	SERVER_ACCEPT_CLIENT	Recorded when the server of JP1/DH - Server accepted a Java applet authentication.
Unauthorized operation	ILLEGAL_INTERFACE_CALL	Recorded when an attempt is made to perform an unauthorized operation and the operation is aborted. Also recorded when data is sent to a user not displayed in the address book by using JP1/Data Highway - AJE.

Table 2–11: Details of operation details output in audit log

Operation details	Parameter complemented by	Supplemental information
application-type=(web command)	<ul style="list-style-type: none"> web: Log in by using the web window. command: Log in by using administrator commands or JP1/Data Highway - AJE. 	Indicates an interface at the time of login.
succeeded=(0 1)	<ul style="list-style-type: none"> 0: Failure 1: Success 	Indicates success or failure of operation.
token-type={password,local-stored-private-key}	<ul style="list-style-type: none"> password: standard password authentication local-stored-private-key: electronic certificate authentication 	Indicates an authentication type at the time of login.
auth-methods={std-pw-auth,cert-auth}	<ul style="list-style-type: none"> std-pw-auth: standard password authentication cert-auth: electronic certificate authentication 	Indicates the authentication method permitted in the authentication policy. If multiple authentication methods are permitted, they are output with each item separated by comma (,).
operator=<No..serial-number#user-ID>	<i>serial-number</i> : A unique number assigned to a user	Indicates the user who performed the operation.
operator=<user-ID>	--	Indicates the ID of the user who performed the operation.
account=(unlock lockout)	<ul style="list-style-type: none"> unlock: The account is unlocked. lockout: The account is locked. 	Indicates the account lock status at the time of login.
operator-group=<English-name-of-the-primary-group-for-the-operating-user>	--	Indicates the primary group an operating user belongs to.
filesize= <i>file-size</i>	--	Indicates the file size.
mime-type= <i>MIME-type</i>	--	Indicates the MIME type of a file.
compressed-by=(NONE ZIP/9 ZIP/5 ZIP/1)	<ul style="list-style-type: none"> NONE: Not compressed ZIP/9: STRONG is selected for standard compression method ZIP/5: MIDDLE is selected for standard compression method ZIP/1: WEAK is selected for standard compression method 	Indicates the compression level to be applied when the Standard compression method is selected for file transmission.
compressed-by=(NONE GCP/0 GCP/9 GCP/5 GCP/1)	<ul style="list-style-type: none"> NONE: Not compressed (for files) GCP/0: Not compressed (for folders) GCP/9: STRONG is selected for extended compression method GCP/5: MIDDLE is selected for extended compression method GCP/1: WEAK is selected for extended compression method 	Indicates the compression level to be applied when the Extended compression method is selected for transmission of a file or folder.
filename= <i>file-name</i>	--	Indicates a file name.
transferred= <i>number-of-bytes-that-are-sent</i>	--	Indicates the number of bytes that are sent.

Operation details	Parameter complemented by	Supplemental information
<code>received-time=reception-time</code>	--	Indicates the time it took to send or receive a file.
<code>start-time={start-date-and-time(JST)}</code>	--	Indicates the time of day (server time) the transmission or reception process started.
<code>end-time={end-date-and-time(JST)}</code>	--	Indicates the time of day (server time) the transmission or reception process ended. Reception-based charges are based on this time.
<code>throughput=throughput</code>	--	Indicates throughput in file transmission or reception.
<code>from=sender-email-address</code>	--	Indicates the sender of the file.
<code>to=recipient-email-address</code>	--	Indicates the recipient of the file.
<code>notify-opening-delivery=(0 1)</code>	<ul style="list-style-type: none"> 0: The notification for file opening is not sent. 1: The notification for file opening is sent. 	Indicates whether the notification for file opening is sent to the sender when the file is opened.
<code>end-time=end-time</code>	--	Indicates the date and time (server time) the operation is completed.
<code>email=<email-address></code>	--	Indicates an email address.
<code>delivery-policy=<No.serial-port-number#English-policy-name></code>	--	Indicates a delivery policy. Policies with the same name are distinguished based on their serial numbers.
<code>max-per-delivery=maximum-data-capacity-per-delivery</code>	--	Indicates the maximum amount of data to be delivered (per delivery) in the delivery policy. (In bytes)
<code>max-per-file=maximum-data-capacity-per-file</code>	--	Indicates the maximum amount of data to be delivered (per file) in a delivery policy. (In bytes)
<code>max-expire-date=maximum-storage-period</code>	--	Indicates the maximum storage period in a delivery policy. (In days)
<code>protocol=LDAP</code>	--	Indicates the communication protocol used for communication with the directory server when authentication with an LDAP authentication system is performed.
<code>server-type=(LDAP_V3 ACTIVE_DIRECTORY)</code>	<ul style="list-style-type: none"> LDAP_V3: Directory server except Active Directory ACTIVE_DIRECTORY: Active Directory 	Indicates the type of directory server to link with the system.
<code>directory-servers=<directory-server-host-name>:<port-number></code>	--	Indicates the server of the linked directory server.
<code>auth-methods=<<SIMPLE/finderDn=search-target-user-name>></code>	--	Indicates the user name searched for by the directory server.
<code>period=<start-day-end-day></code>	--	Indicates the period for the obtained audit log.
<code>code=error-type</code>	--	Indicates the error type when an error occurred.

2.3.3 Audit log error messages

The following table describes audit log error messages.

Table 2–12: Audit log error messages

No.	Item	Log type	Error code	Cause
1	Sending	SEND_DELIVERY	PERSISTENCE_ERROR	One of the following occurred during the file upload process: <ul style="list-style-type: none"> • The user aborted uploading. • The user exited the browser. • The network is disconnected. • The Java process is terminated. • A database failure occurred.
2			NETWORK_IO_ERROR	The sending process was canceled. <ul style="list-style-type: none"> • An error occurred during the preparation for sending a file. • An error occurred immediately before completion of sending a file. This error code is output for most of the errors that occur during transmission.
3			DELETE_FAILED	Sending the delivery failed and also deletion of the failed delivery failed (database failure).
4			SEND_REJECTED	Sending process was performed in an incorrect manner. This error does not occur in normal operation.
5			SEND_CANCELED	The user aborted uploading the file.
6	Receiving	DOWNLOAD_FILE	DATA_VERIFICATION_ERROR	The hash value for the downloaded file did not match the hash value at the time of transmission.
7			DOWNLOAD_LIMITS	The user attempted to download data exceeding the download limit.
8			PERSISTENCE_ERROR	One of the following occurred during the file download process: <ul style="list-style-type: none"> • The user aborted downloading. • The user exited the browser. • The network is disconnected. • The Java process is terminated. • A database failure occurred.
9			NETWORK_IO_ERROR	<ul style="list-style-type: none"> • Downloading of a compressed file was canceled. • A process was canceled during hash value calculation.
10			DOWNLOAD_REJECTED	Receiving process was performed in an incorrect manner. This error does not occur in normal operation.
11		DOWNLOAD_CANCELED	The user aborted downloading the file.	
12	Authentication policy	CREATE_AUTH_POLICY	POLICY_OPERATION_FAILED	Creation of the authentication policy failed.
13		UPDATE_AUTH_POLICY	POLICY_OPERATION_FAILED	Updating the authentication policy failed.

No.	Item	Log type	Error code	Cause
14	Authentication policy	DELETE_AUTH_POLICY	POLICY_OPERATION_FAILED	Deletion of the authentication policy failed.
15	Authentication rule	DELETE_AUTH_RULE	RULE_OPERATION_FAILED	Deletion of the authentication rule failed.
16		ACTIVATE_AUTH_RULE	RULE_OPERATION_FAILED	Activating the authentication rule failed.
17		INACTIVATE_AUTH_RULE	RULE_OPERATION_FAILED	Inactivating the authentication rule failed.
18		UP_AUTH_RULE	RULE_OPERATION_FAILED	Moving the authentication rule upward failed.
19		DOWN_AUTH_RULE	RULE_OPERATION_FAILED	Moving the authentication rule downward failed.
20	Delivery policy	CREATE_DELIVERY_POLICY	POLICY_OPERATION_FAILED	Creation of the delivery policy failed.
21		UPDATE_DELIVERY_POLICY	POLICY_OPERATION_FAILED	Updating the delivery policy failed.
22		DELETE_DELIVERY_POLICY	POLICY_OPERATION_FAILED	Deletion of the delivery policy failed.
23	Delivery rule	DELETE_DELIVERY_RULE	RULE_OPERATION_FAILED	Deletion of the delivery rule failed.
24		ACTIVATE_DELIVERY_RULE	RULE_OPERATION_FAILED	Activating the delivery rule failed.
25		INACTIVATE_DELIVERY_RULE	RULE_OPERATION_FAILED	Inactivating the delivery rule failed.
26		UP_DELIVERY_RULE	RULE_OPERATION_FAILED	Moving the delivery rule upward failed.
27		DOWN_DELIVERY_RULE	RULE_OPERATION_FAILED	Moving the delivery rule downward failed.
28	Network set	UPDATE_NETWORK_SET	OBJECT_OPERATION_FAILED	Updating the network set failed.
29		DELETE_NETWORK_SET	OBJECT_OPERATION_FAILED	Deleting the network set failed.
30		CREATE_NETWORK_SET	OBJECT_OPERATION_FAILED	Creating a network set failed.
31	Approval route	UPDATE_APPROVAL_ROUTE	OBJECT_OPERATION_FAILED	Updating the approval route.
32		DELETE_APPROVAL_ROUTE	OBJECT_OPERATION_FAILED	Deleting the approval route failed.
33		CREATE_APPROVAL_ROUTE	OBJECT_OPERATION_FAILED	Creating an approval route failed.
34	Delivery opening	OPEN_DELIVERY	PASSWORD_MISMATCH	A wrong open password was used in the delivery for an unregistered address.
35			DELIVERY_NOT_FOUND_OR_EXPIRED	Access to the URL in the message failed due to one of the following: <ul style="list-style-type: none"> The accessed URL is for a deleted delivery.

No.	Item	Log type	Error code	Cause
35	Delivery opening	OPEN_DELIVERY	DELIVERY_NOT_FOUND_OR_EXPIRED	<ul style="list-style-type: none"> The accessed URL is for an expired delivery.
36			NOTIFICATION_FAILED	Sending a notification email failed due to one of the following: <ul style="list-style-type: none"> The notified email address does not exist. The mail server is not set correctly. Other reasons
37	Notification email	NOTIFY_DELIVERY	APPROVAL_ROUTE_ILLEGAL_STATUS_DETECTED	The status of the approval route is incorrect at the time of new transmission. (verifyApprovalRouteStatus() is false.)
38			NOTIFICATION_FAILED	Email notification failed.
39			PERSISTENCE_FAILED	A database failure occurred.
40	Guest user setting	ACTIVATE_GUEST	ACTIVATE_FAILED	Activating the guest user failed.
41		INACTIVATE_GUEST	INACTIVATE_FAILED	Inactivating the guest user failed.
42		DELETE_GUEST	DELETE_FAILED	Deleting the guest user failed.
43	Options	UPDATE_PASSWORD	UPDATE_FAILED	Updating the standard password failed.
44		UPDATE_USER_LANG	UPDATE_FAILED	Changing the user language failed.

2.3.4 Example of the output audit log

An example of the output audit log is as follows:

```
"2010-09-22T19:25:41.674+09:00L0.131", "123.123.123.123", "NOTICE",
"uid=<No.1#admin@testdomain>", "LOGIN", "succeeded=1, token-type=local-stored-private-key, operator=<No.2496#admin@testdomain>, operator-group=</test>, application-type=web", "",
"2010-09-22T29:28:09.251+09:00L0.43", "123.123.123.123", "NOTICE",
"user=<No.2#testuser@testdomain>", "CREATE_USER", "operator=<No.1#admin@testdomain>, operator-group=</test>, email=<testuser@test.jp>"
"2010-09-22T19:33:43.681+09:00L0.44", "123.123.123.123", "NOTICE",
"", "DOWNLOAD_LOG", "operator=<No.1#admin@testdomain>, operator-group=</test>, period=<2010/1/1 - 2010/12/31>"
"2010-09-22T19:34:26.923+09:00L0.26", "123.123.123.123", "NOTICE",
"uid=<No.1#admin@testdomain>", "LOGOUT", "operator=<No.1#admin@testdomain>"
operator-group=</test>
"2010-09-23T11:13:35.200+09:00L0.609", "111.111.111.111", "NOTICE",
"did=123", "SEND_DELIVERY", succeeded=1, "operator=<No.2#testuser@testdomain>, operator-group=</test>, from=<admin@test.jp>, to=<admin@test.jp>"
```

2.4 User type and authority

The following table lists and describes the functions each user can use in JP1/DH - Server.

Table 2–13: List of available functions

Item	Representative user	Group manager	General user	Guest user ^{#1}	Unregistered user	Related subsection
Send ^{#2}	Y	Y	Y	Y	N	3.3.2
Receive	Y	Y	Y	Y	Y	3.3.3 3.3.4
Approval Manager	Y	Y	C	N	N	3.3.6
Guest Users	Y	Y	C	N	N	3.3.7
Options	Y	Y	C	C	N	3.3.8
Users & Groups	Y	Y	N	N	N	3.4.2
Users & Groups (batch management)	Y	N	N	N	N	3.5.2
Delivery Histories	Y	Y	N	N	N	3.4.3
Delivery Rules	Y	N	N	N	N	3.5.3
Authentication Rules	Y	N	N	N	N	3.5.4
Authentication Systems	Y	N	N	N	N	3.5.5
Object Definitions	Y	N	N	N	N	3.5.6
Logs	Y	N	N	N	N	3.5.7

Legend:

Y: Available

C: Available for a user who is allowed to use the function by a representative user or a group manager

N: Not available

#1
Restrictions are set to the granted account such as restrictions for a period and the number of transmissions.

#2
Some users can send data to an address that is not registered in the address book.

Important note

- A group manager can use the Users & Groups function and the Delivery Histories function for and under the group he or she belongs to. However, a group manager cannot change the group manager of the group he or she belongs to.
- A group manager must be positioned directly below the management target group.
- Note that you cannot specify one user as a manager in multiple groups. Even if a user belongs to multiple groups, set that user as the group manager for only one of those groups.

3

Explanations of JP1/DH - Server Operations

This chapter describes how to operate JP1/DH - Server.

3.1 Window common specifications

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

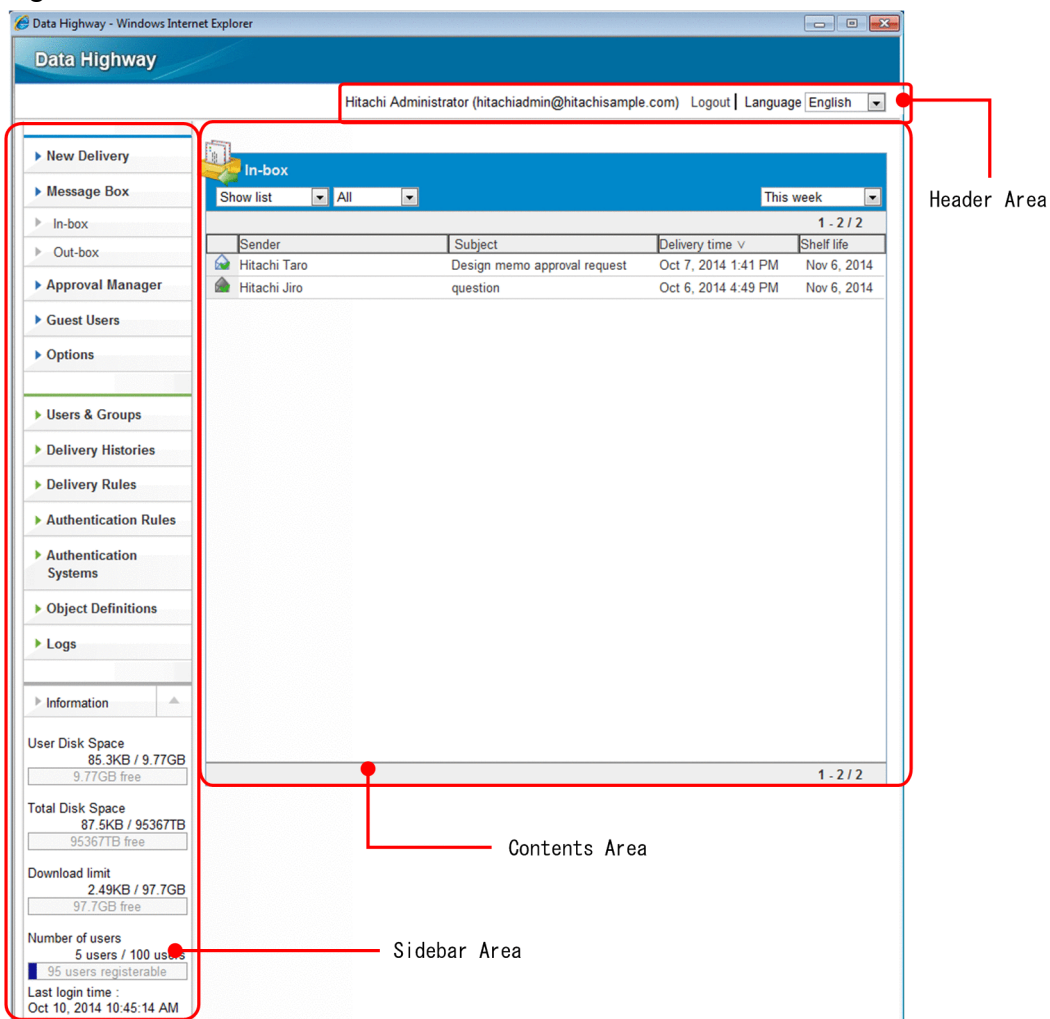
3.1.1 Window structure

This subsection describes the window structure of JP1/DH - Server.

(1) Window example

The figure below shows an example of the main window of JP1/DH - Server. The default display language depends on the language setting of each browser. If the browser language is set to Japanese, Chinese, or other languages, the windows are displayed in Japanese, Chinese, or English, respectively.

Figure 3–1: JP1/DH - Server window structure



(2) Structure

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


Table 3–1: Areas comprising the JP1/DH - Server windows



















Area	Description
Header area	Displays the name of the logged in user and a link to log out of the system.
Sidebar area	Displays the operation menu items, and user/total disk space. Note that a representative user can see the maximum number of available users, number of current users, and download limit.
Content area	Used to send and receive files and to configure various settings.










3.1.2 List of icons

The following table lists and describes icons displayed in a JP1/DH - Server window.

Table 3–2: List of icons displayed in a JP1/DH - Server window

Window	Icon	Description	
New Delivery window		Indicates all delivery settings have been specified. This icon appears when the delivery settings for a file and message are completely specified. You can send a file and message by clicking the Start Sending button.	
		Indicates that a mandatory field is incomplete in the delivery settings. This icon appears when a mandatory field is incomplete in the delivery settings.	
		Indicates there is an error in the delivery settings. This icon appears when there is an invalid delivery setting item.	
		Click this icon to delete the specified destination.	
		Indicates an approval is required to send a file and message to the specified destination.	
-- Address Book tab • Address List		Indicates a group.	
		Indicates a user.	
	Address Book tab • Sending Address Histories • Receiving Address Histories		Indicates a user.
			Click this icon to delete an address from the list.
Out-box window Outbound histories window In-box window Inbound histories window		Indicates the delivery has expired. Files contained in the delivery have not been deleted. A delivery marked by this icon is not included in the amounts of User Disk Space and Total Disk Space . In the Out-box or Outbound histories window, clicking this icon displays the Show more info. and Delete menu items. In the In-box or Inbound histories window, clicking this icon displays the Show more info. menu item.	
		Indicates the delivery has expired. Files contained in the delivery have been deleted. A delivery marked by this icon is not included in the amounts of User Disk Space and Total Disk Space . In the Out-box or Outbound histories window, clicking this icon displays the Show more info. and Delete menu items. In the In-box or Inbound	

Window	Icon	Description
Out-box window Outbound histories window In-box window Inbound histories window		histories window, clicking this icon displays the Show more info. menu item.
Out-box window Outbound histories window		Indicates the delivery is in process or waiting to be sent. Clicking this icon displays the Show more info. and Delete menu items.
		Indicates the delivery has failed. The delivery has not reached the destination user. Clicking this icon displays the Show more info. and Delete menu items.
		Indicates the delivery has been completed. Clicking this icon displays the Show more info. and Delete menu items.
		Indicates the delivery is rejected by the approver. The delivery has not reached the recipient. Clicking this icon displays the Show more info. and Delete menu items.
		Indicates the approver has not done the approval operation (accept or reject) of the delivery. The delivery has not reached the recipient. Clicking this icon displays the Show more info. and Delete menu items.
		Indicates that the system administrator temporarily stopped the delivery transmitted in JP1/Data Highway - AJE. The delivery has not reached the recipient. Clicking this icon displays the Show more info. and Delete menu items.
In-box window Inbound histories window		Indicates the delivery has not been opened yet. Clicking this icon displays the Show more info. menu item.
		Indicates the delivery has been opened. This icon appears when the delivery has been opened but no file has been downloaded or not all files have been downloaded. Clicking this icon displays the Show more info. menu item.
		Indicates all files contained in the delivery have been downloaded. This icon appears when the recipient has opened the delivery and downloaded all the files contained in it. Clicking this icon displays the Show more info. menu item.
Applications for Approval window [#]		Indicates a user who has applied for approval.
Users & Groups window		Indicates an activated user group.
		Indicates an activated guest group.
		Indicates an inactivated user group.
		Indicates an inactivated guest group.
		Indicates an activated general user.
		Indicates an inactivated general user.
		Indicates a general user whose account is locked.

Window	Icon	Description
List of guest users window [#]		Indicates an activated guest user.
		Indicates an inactivated guest user.
		Indicates a guest user whose account is locked.
Delivery Rules window Authentication Rules window		Indicates an activated rule in the approved delivery rules or authentication rules. Clicking this icon displays the Edit , Up , Down , Activate , Inactivate , and Delete menu items.
		Indicates an activated rule of the rejected delivery rules or authentication rules. Clicking this icon displays the Edit , Up , Down , Activate , Inactivate , and Delete menu items.
		Indicates an inactivated delivery rule or authentication rule. The system ignores the delivery rule or authentication rule marked by this icon. Clicking this icon displays the Edit , Up , Down , Activate , Inactivate , and Delete menu items.
Delivery Rules window Authentication Rules window		Indicates a delivery policy or authentication policy. Clicking this icon displays the Edit and Delete menu items.
Network Sets window		Indicates a network set. Clicking this icon displays the Edit and Delete menu items.
Approval Routes window		Indicates an approval route. Clicking this icon displays the Edit and Delete menu items.

#

This menu item is displayed only when you are allowed by a representative user or a group manager to use the function.

3.1.3 Notes

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

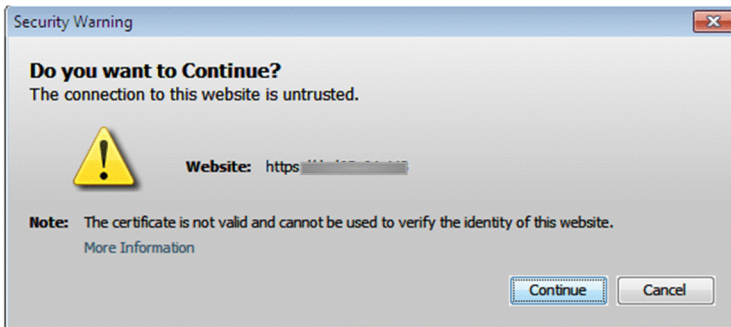
- Use buttons and anchor texts in the windows for window operation. If you operate windows by using the **Back**, **Next**, and **Refresh** buttons or by browsing histories in the web browser, the windows for JP1/DH - Server might not appear properly.
- Do not click buttons repeatedly when you operate windows. If you do so, 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, 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 login 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 the minor version of JRE 6 installed on your machine is Update 18 or earlier, a warning dialog box appears when you start using a Java applet. In this case, check the detailed information and then select **Yes** in the warning dialog box. Use JRE 6 Update 24 or later, which is a recommended environment.



- 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.

3.2 Basic operations

This section describes basic operations of JP1/DH - Server.

3.2.1 List of operations

The following table lists basic operations.

Table 3–3: List of basic operations

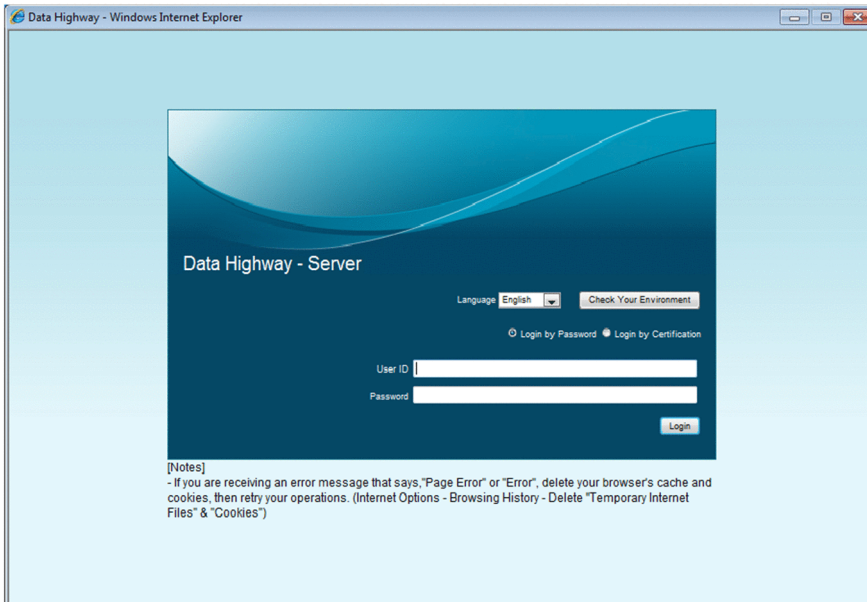
Operation	Related subsection
Logging in to JP1/DH - Server by using the standard password authentication	3.2.2
Logging in to JP1/DH - Server by using the electronic certificate authentication	3.2.3
Logging in by using LDAP authentication	3.2.4
Logging out of JP1/DH - Server	3.2.5
Changing the display language	3.2.6

Clicking the **Check Your Environment** button in the login window allows you to check whether your client environment meets the requirements. For details about the client environment, see the *Job Management Partner 1/Data Highway - Server User's Guide*.

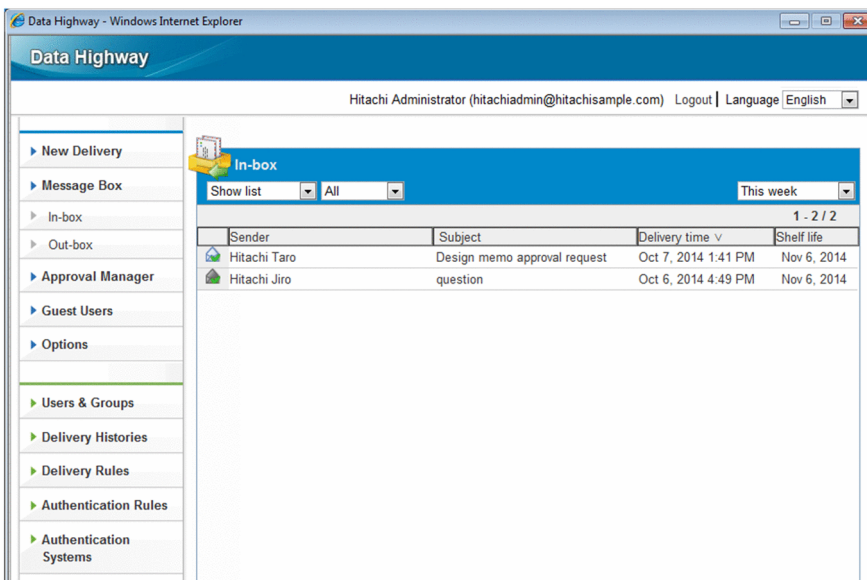
3.2.2 Logging in to JP1/DH - Server by using the standard password authentication

This subsection describes how to log in to JP1/DH - Server by selecting the **Login by Password** radio button with a user ID and password entered.

1. Access the JP1/DH - Server URL.
For your login page URL, contact your system administrator.
The User Authentication window appears.



2. Select the **Login by Password** radio button.
3. Enter your user ID and password, and then click the **Login** button.
You are now logged in to JP1/DH - Server. The main window appears.



Important note

Depending on the settings specified by the representative user, the Change Password window might appear when you attempt to log in. This window appears because you have not changed your password for a certain period of time since the last time you changed it. In this case, you cannot log in unless you change your password. For details about how to change the password, see [3.3.8 Options](#). Even if the Change Password window appears, you can log in by using an electronic certificate.

Reference note

For details about how to log in by using the electronic certificate, see [3.2.3 Logging in to JP1/DH - Server by using the electronic certificate authentication](#).

3.2.3 Logging in to JP1/DH - Server by using the electronic certificate authentication

This subsection describes how to log in to JP1/DH - Server by using an electronic certificate. Note that you cannot change your password when you are logged in with the electronic certificate.

Important note

- Before users can log in to JP1/DH - Server by using an electronic certificate, a representative user or group manager must issue the certificate. Also, the users must have received the issued certificate file and a password for the electronic certificate. A guest user cannot log in by using an electronic certificate.
- When a user enters an incorrect password for the electronic certificate, the system does not output failed-login information to the audit log. However, the system outputs this information if the user enters the correct password when authentication is disabled due to an expired account or authentication rule setting.

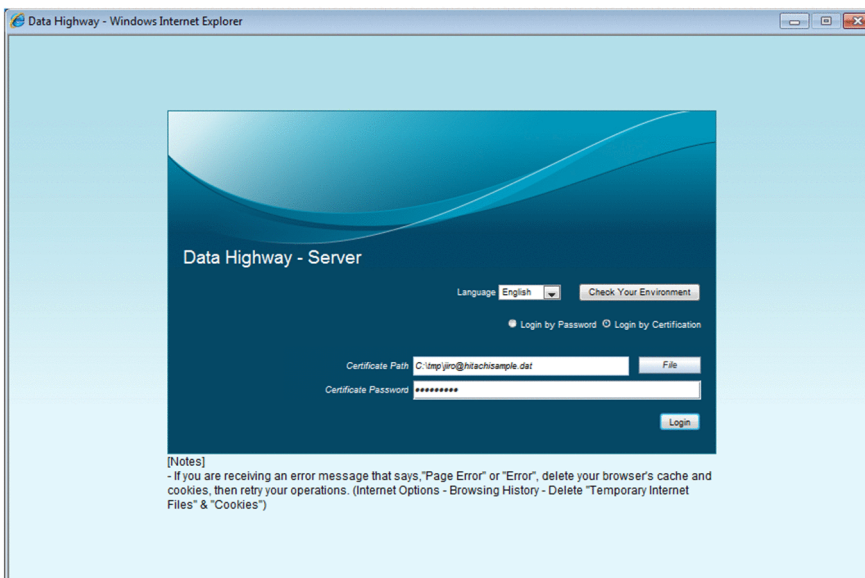
1. Access the JP1/DH - Server URL.

For your login page URL, contact your system administrator. The User Authentication window appears.

2. Select the **Login by Certification** radio button.

3. Click the **File** button to specify the path to the electronic certificate.

4. Enter the password for protecting the electronic certificate in the **Certificate Password** field.



5. Click the **Login** button.

You are now logged in to JP1/DH - Server.

Important note

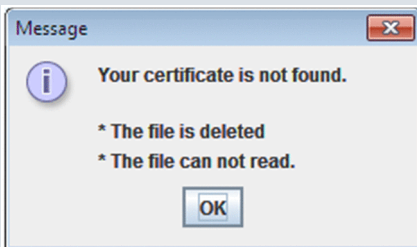
If the login fails, the dialog box below appears.

Click the **OK** button to go back to the User Authentication window.



If the certificate file does not exist on the specified path, the dialog box below appears.


Click the **OK** button to go back to the User Authentication window.



If you cannot resolve the above errors, contact your system administrator.

Reference note

If you log in by using an electronic certificate, the following icon appears in your user information:

 Hitachi Jiro (jiro@hitachisample.com) Logout

3.2.4 Logging in by using a directory server

If a directory server is used to authenticate users who attempt to log in to JP1/DH - Server, a user must specify the user ID in the following format when logging in:

user-ID-defined-in-the-directory-server@domain-name-in-the-JP1/DH-Server-system

If an authentication fails, an error message appears.

3.2.5 Logging out of JP1/DH - Server

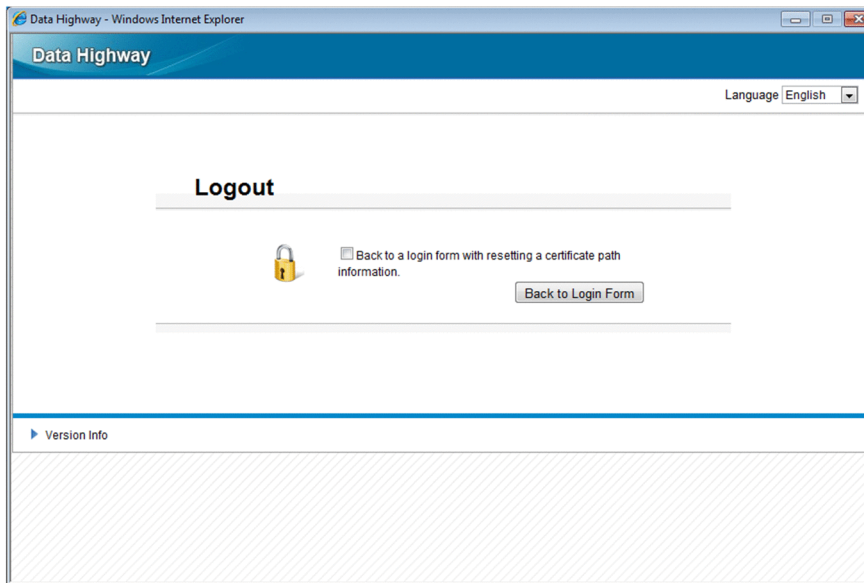
To log out of JP1/DH - Server:

1. In the header area, click the **Logout** anchor.

You are logged out of JP1/DH - Server, and the User Authentication window appears.

Reference note

If a user logs in to JP1/DH - Server by using an electronic certificate, the following window appears after the user is logged out:



Selecting the **Back to a login form with resetting a certificate path information.** check box and then clicking the **Back to Login Form** button resets the electronic certificate information used for login. If the information is reset, the user who is logging in must specify the path to the electronic certificate on the next login.

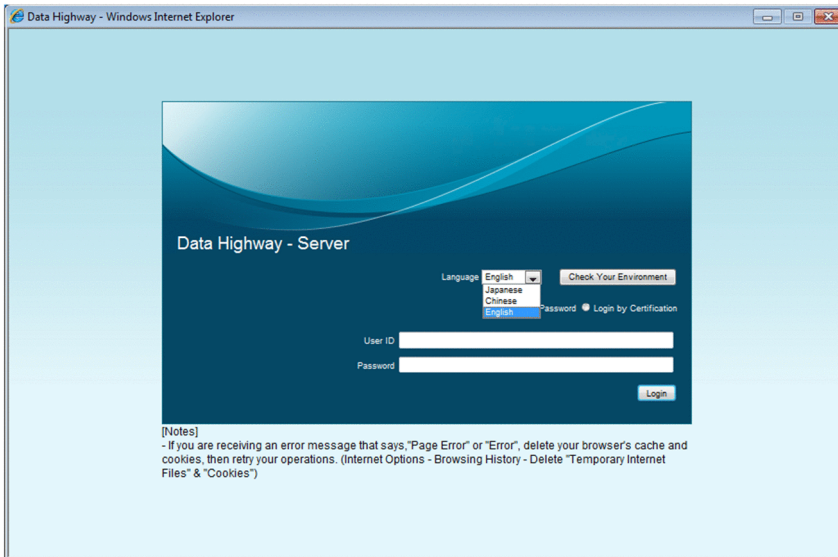
If it is not reset, the window to enter the password for the electronic certificate appears.

3.2.6 Changing the display language

This subsection describes how to change the language that JP1/DH - Server uses to display text in windows.

JP1/DH - Server windows can use one of the Japanese, English, or Chinese languages.

1. In the login window, from the **Language** drop-down list box, select the language you want to use.
2. When you log in, the window appears in the selected language.



3.3 General-user operations

This section describes what operations general users can perform. Group managers and representative users can also perform them.

3.3.1 List of operations

The following table lists operations performed by general users.

Table 3–4: List of general user operations

Menu item	Operation	Related subsection
New Delivery	Sending files and messages	3.3.2(1)
	Sending a file and message by specifying an unregistered recipient address	3.3.2(2)
Message Box	Receiving a file by a registered user	3.3.3(1)
	Receiving a file by an unregistered user	3.3.3(2)
	Receiving a file in the in-box	3.3.4
	Viewing or deleting sending and receiving history	3.3.5
Approval Manager [#]	Accepting or rejecting an application for approval by accessing a URL written in an email	3.3.6(1)
	Accepting or rejecting applications for approval	3.3.6(2)
Guest Users [#]	Creating a guest user	3.3.7(1)
	Editing a guest user	3.3.7(2)
	Activating, inactivating, or deleting a guest user	3.3.7(3)
Options	Changing a password	3.3.8(1)
	Changing the language used in email	3.3.8(2)

#

This menu item is displayed only when you are allowed by a representative user or a group manager to use the function.

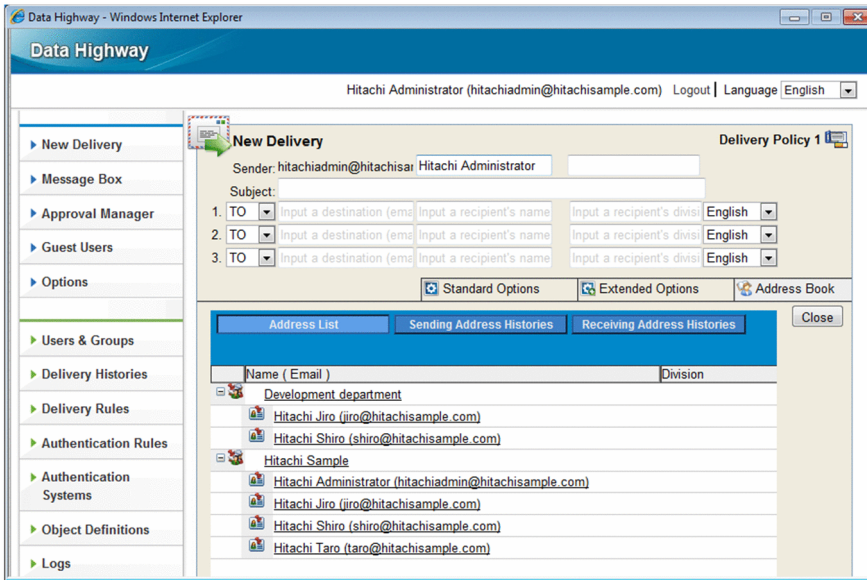
3.3.2 New Delivery

This subsection describes operations that users can perform in the New Delivery window.

(1) Sending files and messages

To send files and messages:

1. In the sidebar area, click **New Delivery**.
The New Delivery window appears in the content area.



2. Enter sender information, including the name and division of the sender. The following table lists items to be specified.

Table 3–5: Setting items for sender information

Item	Description
Sender text box (name)	Enter the name of the sender. The value entered here is displayed in the sender information field of delivery notification email. If the text box is left blank, the JP1/DH - Server system uses the registered name in it as a sender name.
Sender text box (division)	Enter the division that the sender belongs to. The value entered here is displayed in the sender information field of delivery notification email. However, nothing is displayed in this text box if the Sender text box (name) is left blank. You can enter no more than 1,024 characters.
Subject text box	Enter the subject for a delivery email message. You can enter no more than 100 characters.

3. From **Address List**, select one or more recipient addresses for the files and messages.

Clicking the anchor for a recipient user or group in **Address List** adds the user or group to one of the destination fields. Select **TO**, **CC**, or **BCC** for each address.

If you click the anchor for the recipient user, the email address and name of the selected user are displayed in the text boxes for a recipient. If you click the anchor for the recipient group, the name of the selected group is displayed in the text box for a recipient.

If you leave the recipient's name field blank, the name registered in the JP1/DH - Server system is used as the recipient of the delivery.

Important note

A user who is allowed by a representative user or group manager to enter any destination can directly fill in the destination fields. For details about how to enter the destination fields directly, see [3.3.2\(2\) Sending files and messages by entering an unregistered recipient address](#).

Note that to allow a user to specify any destination address, the **Inputting Address** check box must be selected in the settings of the group that the user belongs to. For details, see [3.4.2\(8\) Creating a group](#).

4. Enter a division and select the language for the delivery email, if necessary.


Table 3–6: Setting items for recipient information

Item	Description
Division text box	Enter the division of the recipient user. The value entered here is displayed in the destination information field of delivery notification email. However, nothing is displayed in this text box if the field for the name is left blank for some reason, such as an unregistered user. You can enter no more than 1,024 characters.
Language drop-down list box	Select the language to be used in the delivery email. The email uses the language selected here.

Tip

Data entered in the name and division entry fields is handled differently in Japanese or Chinese and in English. The data entered in the entry fields in Japanese or Chinese is not applied to the entry fields in English.

The following are initially displayed in the name and division entry fields: registered user information when you select an address in the **Address List**, data entered at the time of sending or receiving when you select an address in histories, and a blank when you enter an address in the field directly.

5. To delete the destination already specified, click the trash icon () displayed to the right of the destination fields.

Important note

You can send data to the limited number of addresses at a time, which is configured by the system administrator. If you use an approval route, this maximum number is the total number of the number of users specified in the destination fields plus the number of approvers in the approval route.

6. The Address List window is displayed in the New Delivery window by default. To select a recipient user from the sending or receiving address history, click the **Sending Address Histories** or **Receiving Address Histories** button, and then select the user you want to send a file and message to in the displayed window.

Tip

- The Sending Address Histories window displays a history of recipient addresses in the past. The Receiving Address Histories window displays a history of sender addresses in the past. Each window displays a maximum of 10 history records, from the newest last-used-date-and-time to the oldest.
- History records contain addresses of general and unregistered users, but do not contain any group addresses. Also, the name and email address at the time of delivery are displayed. For this reason, if a registered user edits and changes the name or email address in the registered information, those displayed in the history will remain the same.
- Only a user who is allowed by a representative user or group manager to enter any destination can select an unregistered user from the history.
- A user who is not allowed to enter any destination cannot select any unregistered user. This is because the unregistered user is inactivated in the lists even when that user is in the list of **Sending Address Histories** or **Receiving Address Histories**. If a user whose account has expired is selected, a transmission error occurs.

7. Select the **Standard Options** tab and specify the settings in it.

Clicking the tab displays the setting window shown below. If no destination is specified, you cannot specify the settings in this tab.

- **Standard Options** tab

Table 3–7: Items in the Standard Options tab

Category	Item name	Description
Configure Storing Options	Save my delivery until <i>month day, year</i>	You can specify the storage expiration date of the delivery. The maximum storage expiration date is set to the value defined by your system administrator. The date is based on the server date.

Category	Item name	Description
Configure Storing Options	Recipients can download files only once. check box	If you select this check box, recipients and approvers (if an approval route is specified) can download files only once.
Configure Notification Options [#]	Notify me and recipients when delivered. check box	If you select this check box, a notification email is sent to a sender and recipients when a file is uploaded or a message is sent.
	Notify me if recipients open my delivery. check box	If you select this check box, a notification email is sent to a sender when recipients open the delivery.
	Notify me if recipients haven't opened my delivery until the day before the expiration. check box	If you select this check box, a notification email is sent to a sender when recipients have not opened the delivery by the day before the expiration.
	Notify me if recipients haven't opened my delivery until the expiration. check box	If you select this check box, a notification email is sent to a sender when recipients have not opened the delivery by the expiration.
	Notify the recipients if not downloaded by <i>month day, year</i> check box	If you select this check box, a notification email is sent to recipients when recipients have not downloaded the file contained in the delivery by a designated date. If two or more files are contained in the delivery, a notification email is sent when any of the files is not downloaded by the designated date. By default, the day before the storage expiration date specified in the Configure Storing Options section is displayed in the drop-down list boxes. A notification email is sent on the day after the designated date. However, a notification email is not sent after the storage expiration date.
	Notify the approver if not approved or rejected by <i>month day, year</i> check box	If you select this check box, a notification email is sent to the approver when the delivery has not been approved or rejected by a designated date. By default, the day before the storage expiration date specified in the Configure Storing Options section is displayed in the drop-down list boxes. A notification email is sent on the day after the designated date. However, a notification email is not sent after the storage expiration date.

#

Depending on the setting specified by the representative user, displayed items are different.

8. Select the **Extended Options** tab and specify the settings in it.

Clicking the tab displays the setting window shown below. If no destination is specified, you cannot specify the settings in this tab.

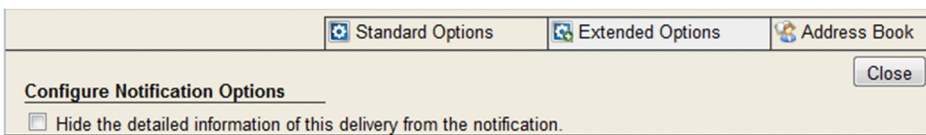
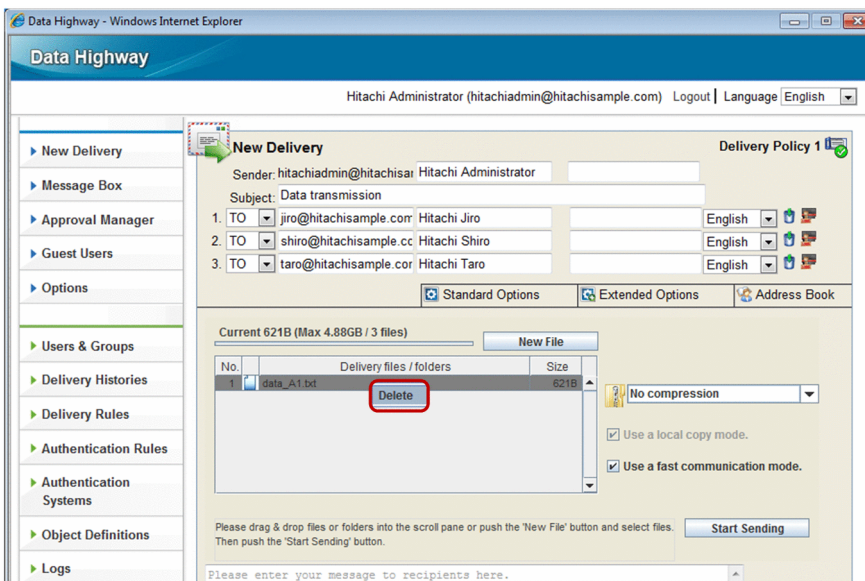


Table 3–8: Item in the Extended Options tab

Category	Item	Description
Configure Notification Options	Hide the detailed information of this delivery from the notification. check box	If you select this check box, the sender information, storage expiration date, file list, and other information are not written in a delivery notification email or an approval request email.

9. Specify one or more files or folders to be sent.

Click the **New File** button and select a file, or drag and drop files or folders to the area inside the list box. If you drag and drop a drive to the area, Drive is displayed in the **Delivery files / folders** column.



Tip

If you want to delete a file in the list box, select the file and then press the **Delete** key on the keyboard, or right-click the file and then select the **Delete** menu item.

Important note

- The total number of files and folders in a folder must be 65,534 or less for the **Standard** compression method in the delivery policy, or 262,144 or less for **Extended** compression method.
- The size of files that can be sent is restricted by delivery rules and the amount of free user disk space for a sender.
- After you select a file or folder, do not refer to the file or folder or change data or name of the file or folder until sending the file or folder is completed. If you want to refer to or change the file or folder, remove the file or folder from the sending target list and then select the file or folder again.
Note that when the file or folder increases or decreases in size due to a change of its data after selection, it cannot be sent. Moreover, if the selected file or folder is changed, regardless of data size, a verification error occurs at the time of reception.
- Depending on the file access method, referring to the file might change the data of the file. In such a case, an error occurs at the time of transmission and reception in the same manner as in the case of data change.

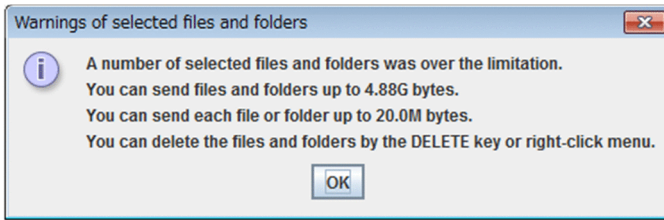
10. Select a compression level from the drop-down list box. Depending on the delivery policy definition specified by the representative user, you might not be able to select a compression level.

You can select one of the following:

- **No compression**: The file or files are not compressed.
- **STRONG**: The file or files are compressed with a method that provides the best compression ratio.
- **MIDDLE**: The file or files are compressed with a method that provides a moderate compression ratio.

- **WEAK:** The file or files are compressed with a method that provides the lowest compression ratio.

With the delivery policy that uses the **Standard** compression method, a file that exceeds 3.96 GB (4,252,017,623 bytes) cannot be compressed and sent. If the limit is exceeded, the dialog box below appears. If you want to send a file that exceeds 3.96 GB, use the **No compression** option.

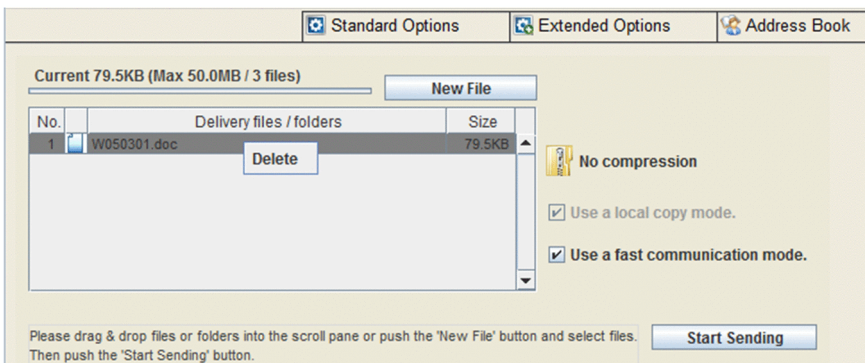


Important note

- If the total size of files in a sending target folder exceeds 3.96 GB (4,252,017,623 bytes), use the delivery policy for which the **Extended** compression method is selected. If the delivery policy for which the **Standard** compression method is selected is used, a folder that exceeds 3.96 GB cannot be sent. For details about the compression method set in a delivery policy, see [3.5.3\(4\) Creating a delivery policy](#).
- If this function is used to compress and send a file, the size of the file before compression is output to the log as a download size.
- If a compressed-file transmission fails and the file is downloaded from the Out-box window while the incomplete file remains on the server, the size of the original file is output to the log as the download size. An incomplete file is automatically removed in about three minutes. Do not download the incomplete file in the Out-box window of the sender before the file is automatically removed. If an incomplete file is not automatically removed, delete the delivery corresponding to the file from the Out-box window.

11. If you specify a file or folder in a non-local folder or on a drive with a slow access speed (such as an SD card), select the **Use a local copy mode.** check box before selecting a file or folder.

Selecting this check box could reduce the time required to display the target in the delivery window and to send it.



Important note

- If a sending target contains files or folders in both local and non-local folders together, you can select the **Use a local copy mode.** check box. However, you cannot select this check box only for a file or folder in a non-local folder or on a drive with a slow access speed.
- If you select the **Use a local copy mode.** check box and then specify a file or folder in a non-local folder, the target file or folder is copied in the local environment. The message `Copying files` is displayed during the copy. You cannot perform any other operations.

- You cannot select or clear the **Use a local copy mode**. check box after selecting a sending target file or folder. To change the check box status, delete all the sending target files and folders.
- When you select the **Use a local copy mode**. check box, there must be enough free space to copy the sending target file or folder to the local environment. Before selecting this check box, make sure that there is enough free space in the folder that is specified by the TEMP environment variable. If there is not enough free space, an error occurs. You must specify an existing folder by the TEMP environment variable. To check the location of the folder specified by the TEMP environment variable, open your machine's System Properties dialog box.

12. Select the **Use a fast communication mode**. check box according to the amount of data transmission. This check box is selected by default.

Tip

If your proxy server or firewall settings lead to a file transmission failure, you can solve this problem by clearing this check box.

13. In the **Message** text area, enter a message to be sent. You can enter no more than 4,096 characters.

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

You can only operate the **Cancel** button during transmission.

The file is sent and then the Sent Result window appears. The time taken for transmission is displayed in **Sending time**.

Important note

When the cursor is in the email address entry area, you cannot click the **Start Sending** button.

15. Click a tab in the Sent Result window to switch information to be displayed.

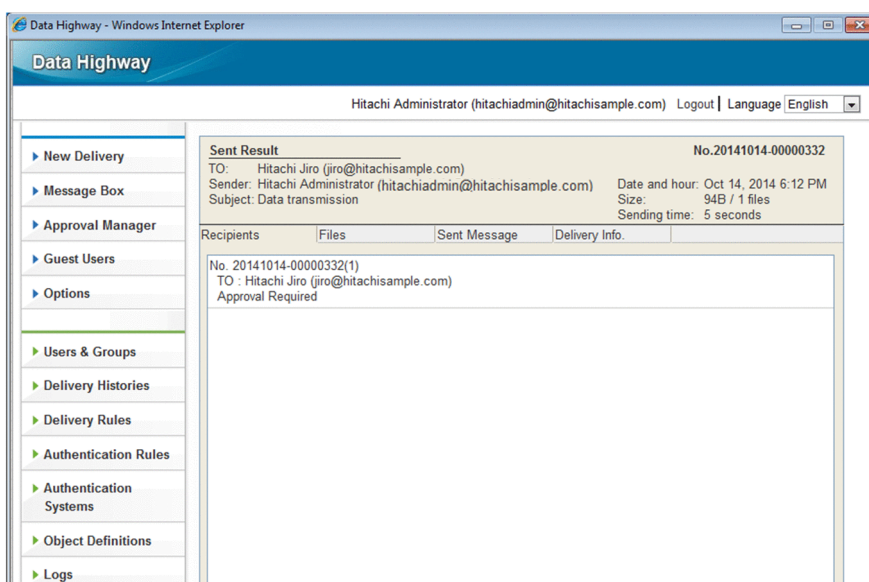


Table 3–9: Tabs in the Sent Result window

Tab	Description
Recipients tab	Displays the recipient-related information. If an approval is required, it is shown.
Files tab	Displays the information on the file that was sent.
Sent Message tab	Displays the message sent to the recipient users.
Delivery Info. tab	Displays options you specified when you sent the file. The options you did not specify when you sent the file are dimmed.

(2) Sending files and messages by entering an unregistered recipient address

A user who is allowed by a representative user or group manager to enter any destination can directly enter an email address in the email field to send a file and message, even if the recipient is not registered in the JP1/DH - Server system. An existing user on the address book can also be specified together.

To send a file and message to an unregistered recipient:

1. Log in to JP1/DH - Server.
For details about how to log in to the system, see [3.2 Basic operations](#).
2. In the sidebar area, click **New Delivery**.
The New Delivery window appears in the content area.
3. Enter the sender information.
You can enter this information in the same way you enter it by using the existing addresses. For details, see [\(1\) Sending files and messages](#).
4. Enter one or more recipient addresses of the files and messages in the text boxes for the email and name.
For details about the rules such as the number of available characters, see [3.4.2\(2\) Creating a user](#).
5. Enter a division and select the language for the delivery email, if necessary.
For details about these fields, see [\(1\) Sending files and messages](#).
6. Click the **Standard Options** tab to specify the open password.
The password must contain two or more different types of characters and consist of a string from 6 to 32 characters.

Important note

You also need to specify the open password if you send data to both a registered address and an unregistered address.

7. Specify one or more files or folders to be sent, and select a compression method.

For details, see *(1) Sending files and messages*.

8. In the **Message** text area, enter a message to be sent.

You can enter no more than 4,096 characters.

9. Click the **Start Sending** button.

The file is sent and then the Sent Result window appears.

For details about the Sent Result window, see *(1) Sending files and messages*.

Important note

- The unregistered user needs the specified open password to open a delivery. Notify the unregistered user of the open password by means other than JP1/DH - Server.
Note that you need to notify only the unregistered user of the open password if you send data to both a registered user and an unregistered user. You do not need to notify the registered user of the open password.
- If the delivery policy for the unregistered address is not defined, users cannot send data to any recipient address even if they are allowed to do so.

3.3.3 Receiving a file by accessing a URL in a delivery notification email

This section describes how to receive a file by accessing a URL written in a delivery notification email.

(1) When a registered user receives a file

To receive a file by accessing a URL written in a delivery notification email (for a registered user):

1. Access the URL written in the delivery notification email.

The Receipt Authentication window appears.

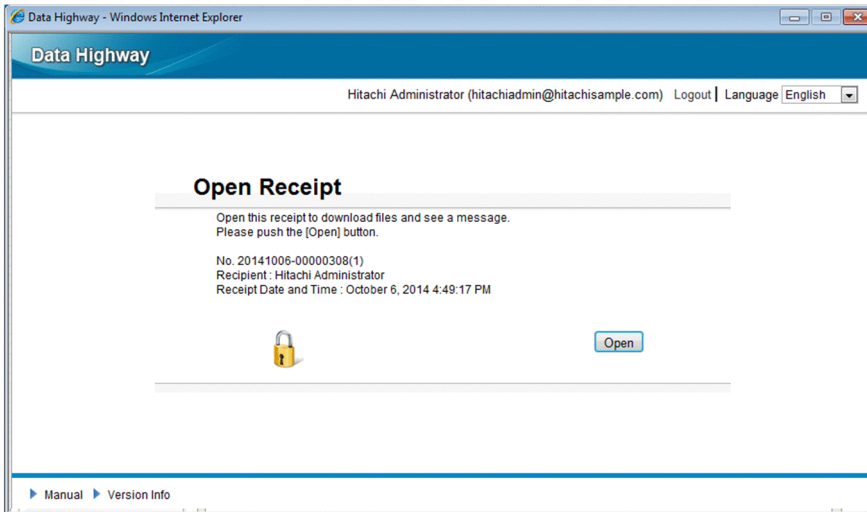
2. Log in to JP1/DH - Server.

For details about how to log in to the system, see *3.2 Basic operations*.

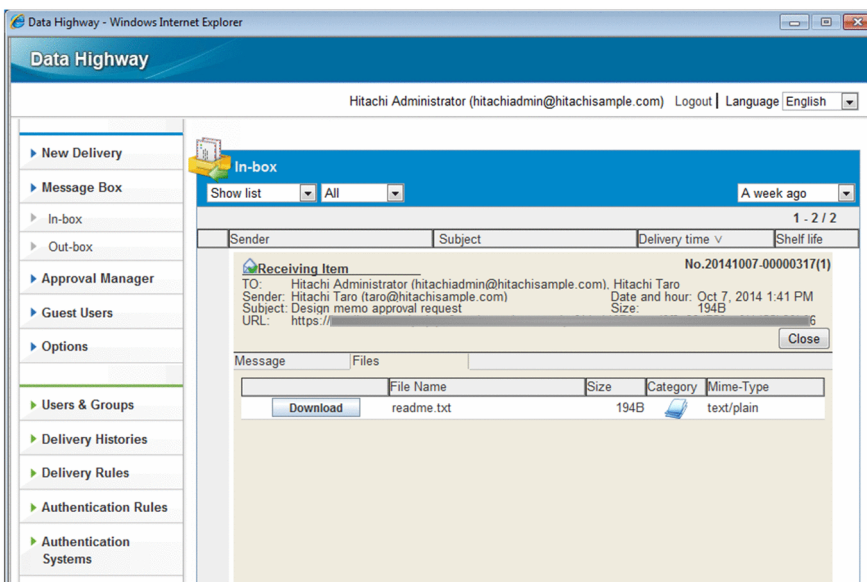
3. When you are logged in, the Open Receipt window appears.

4. Click the **Open** button.

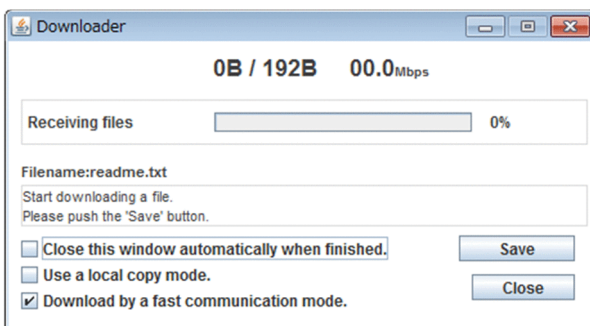
The Received Items window appears.



5. Click the **Download** button.
The Downloader window appears.



6. Click the **Save** button, and then select a destination where the file is saved.
If you specify a non-local folder as a destination, select the **Use a local copy mode**. check box. Selecting this check box could reduce the time required to download the selected file or folder.



Important note

- When you select the **Use a local copy mode.** check box, there must be enough free space to receive the target file or folder in the local environment. Before selecting this check box, make sure that there is enough free space in the folder that is specified by the TEMP environment variable. If there is not enough free space, an error occurs. You must specify an existing folder by the TEMP environment variable. To check the location of the folder specified by the TEMP environment variable, open your machine's System Properties dialog box.
- If a timeout occurs during the download, the file download fails. If you have specified a non-local folder as a destination, specify a local folder as a destination and then download the file again.
- If you select the **Use a local copy mode.** check box, the total reception time to the local folder is output to the audit log (`received-time`).

7. The Downloading Finished!! dialog box appears.

The time required for download is displayed in **Download time**.

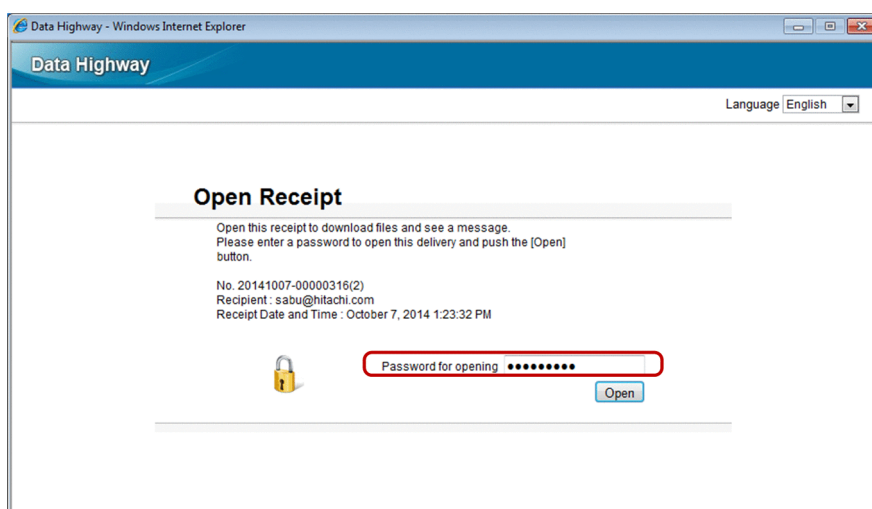
8. Click the **OK** button.

The download is now complete.

(2) When an unregistered user receives a file

When an unregistered user accesses a URL written in a delivery notification email, the Open Receipt window appears.

The user can then receive the file by entering the open password that has already been notified of by the sender and clicking the **Open** button.



3.3.4 Receiving a file in the in-box

To receive a file in the in-box:

1. In the sidebar area, click **Message Box** and then **In-box**.

The In-box window appears in the content area.

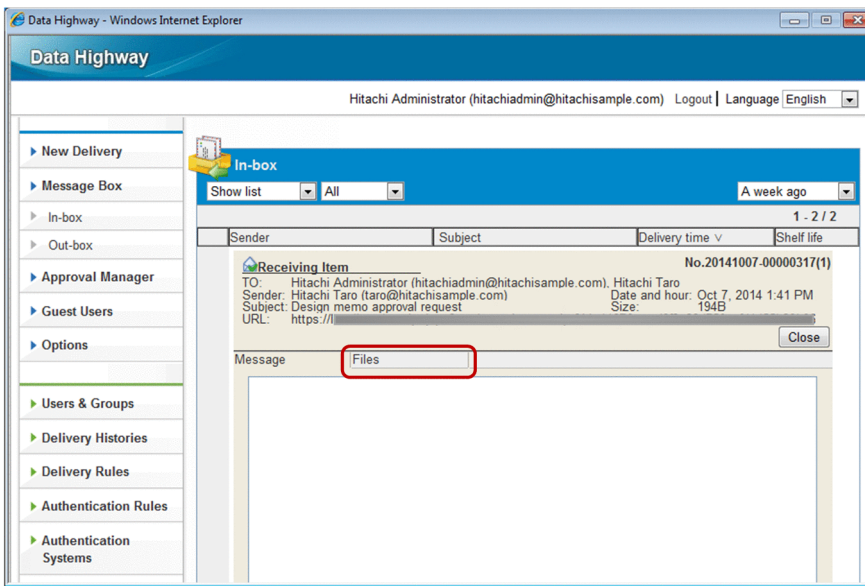
2. Select the processing status of delivery data displayed in the in-box from **Not opened**, **Opened**, or **All**.

3. Click the menu icon of the delivery data you want to receive, and then select **Show more info.**

The Receiving Item window appears.

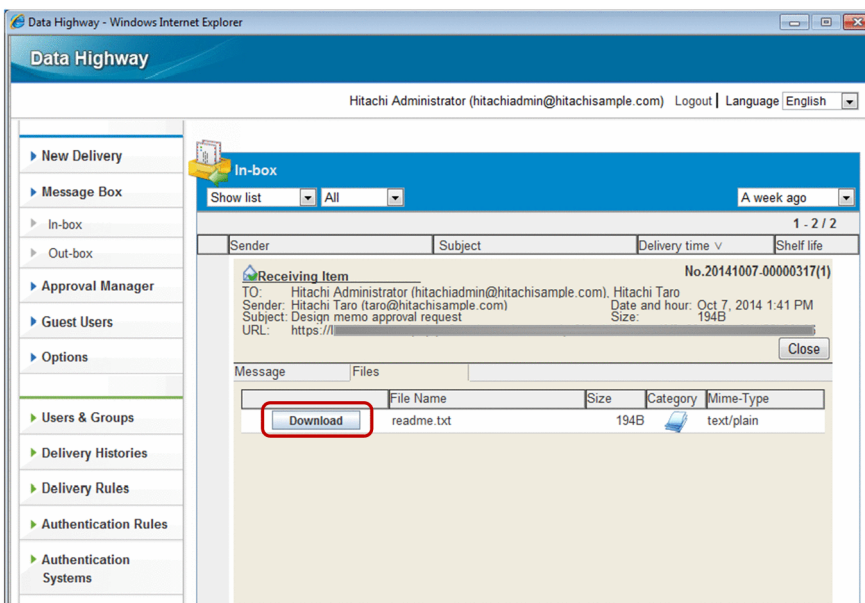
4. Click the **Files** tab.

The details of the received file are displayed.



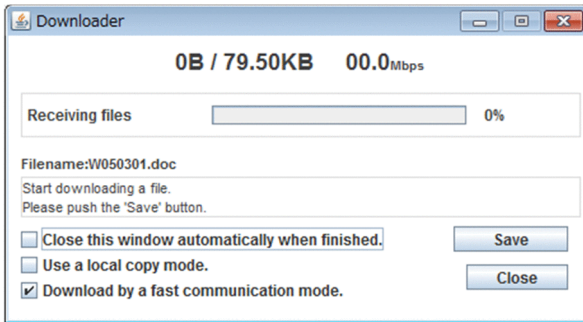
5. Click the **Download** button.

The Downloader window appears.



6. Click the **Save** button, and then select a destination where the file is saved.

If you specify a non-local folder as a destination, select the **Use a local copy mode.** check box. Selecting this check box could reduce the time required to download the selected file or folder.



Important note

- You cannot operate the In-box window while the Downloader window is displayed.
- When you select the **Use a local copy mode.** check box, there must be enough free space to receive the target file or folder in the local environment. Before selecting this check box, make sure that there is enough free space in the folder that is specified by the TEMP environment variable. If there is not enough free space, an error occurs. You must specify an existing folder by the TEMP environment variable. To check the location of the folder specified by the TEMP environment variable, open your machine's System Properties dialog box.
- If a timeout occurs during the download, the file download fails. If you have specified a non-local folder as a destination, specify a local folder as a destination and then download the file again.
- If you select the **Use a local copy mode.** check box, the total time is output to the audit log (received-time). This output time also include a time to copy the file or folder located in the local folder to the final destination.

7. The Downloading Finished!! dialog box appears.

The time required for download is displayed in **Download time.**

8. Click the **OK** button.

The download is now complete.

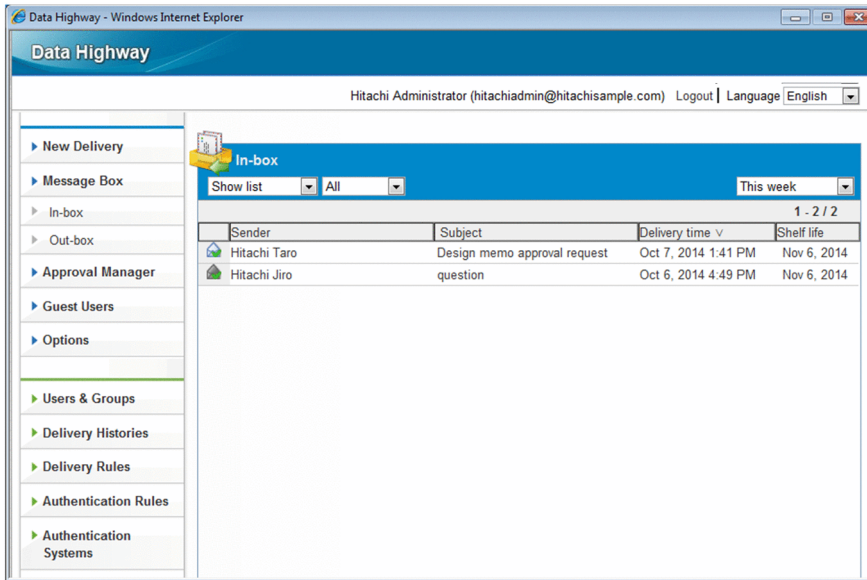
3.3.5 Viewing or deleting the user's own delivery history

To view or delete your delivery history:

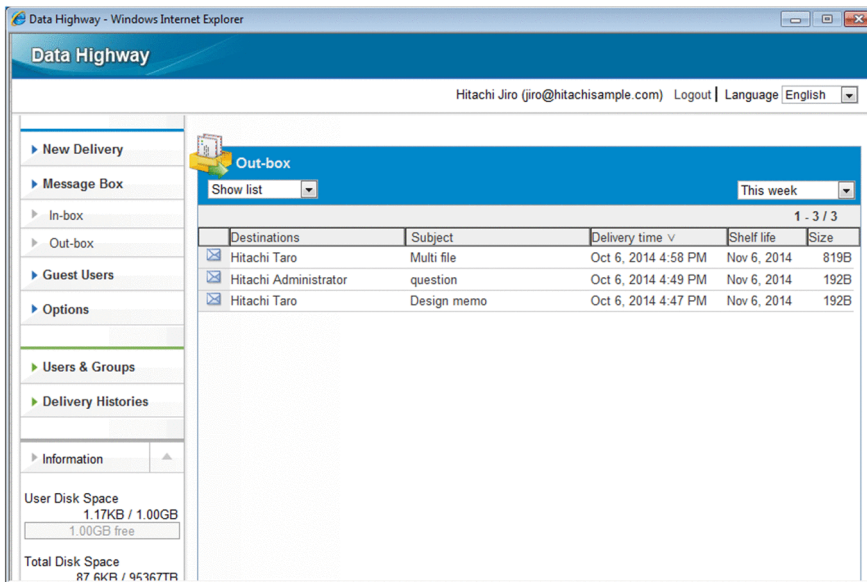
1. In the sidebar area, click **Message Box** and then **In-box** or **Out-box**.

The In-box or Out-box window appears in the content area.

- In-box window



- Out-box window



You can use the drop-down list box to change what is displayed in the window.

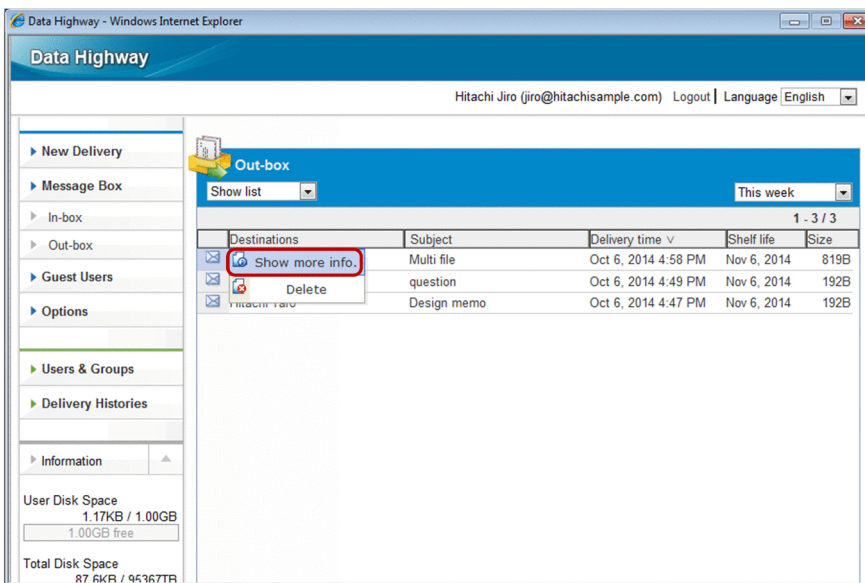
Table 3–10: Setting items in the In-box or Out-box window

Item	Description
Display style drop-down list box	You can select either of the following display styles: <ul style="list-style-type: none"> • List • Abstract style
Processing status drop-down list box	This is only displayed in the In-box window. You can filter delivery data by processing status. <ul style="list-style-type: none"> • All • Not opened • Opened
Display period drop-down list box	You can filter the list by time period. Filtering criteria depends on the date and time of the existing history records. The display periods for each option are as follows: <ul style="list-style-type: none"> • Today: The present day

Item	Description
Display period drop-down list box	<ul style="list-style-type: none"> • This week: From last Sunday to today • A week ago: From two Sundays ago to today • Two weeks ago: From three Sundays ago to today • Three weeks ago: From four Sundays ago to today • A month ago: From the first day of the last month to today <p>If the period specified by This week includes days of the previous month, the history to be displayed is that from the first day of the current month. The history of the days of the previous month is not displayed.</p> <p>If there are history records over the past one month or more, the list items you can select are displayed in the form of <i>MM YYYY</i>.</p>

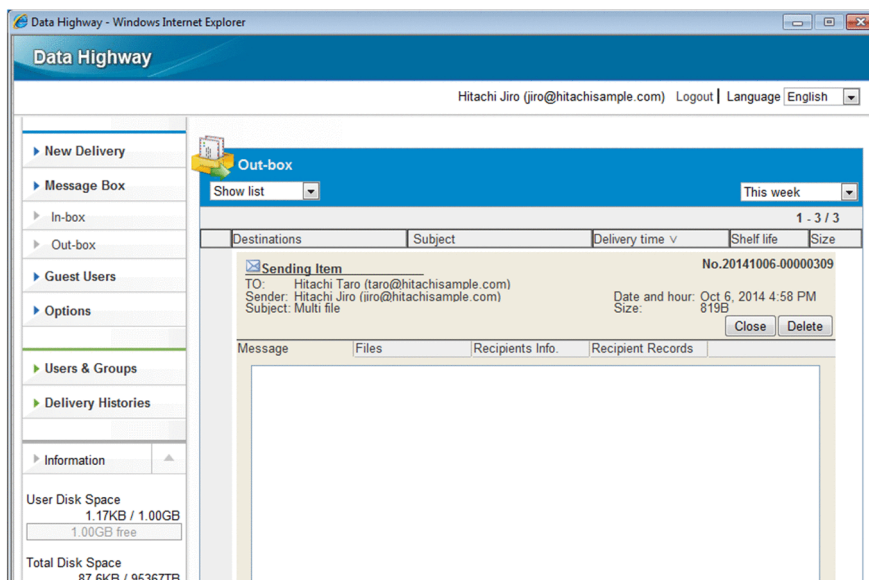
2. Click the menu icon and then select **Show more info.** to view the detailed history information.

The history detailed information window appears. If the sender is deleted or inactivated, you cannot view the detailed information.



3. Select one of the tabs in the history detailed information window. The content displayed on each tab is described below. Note that the **Recipients Info.**, **Recipient Records**, and **Approver List** tabs are displayed only when you select **Show more info.** to display the detailed information in the Out-box window.

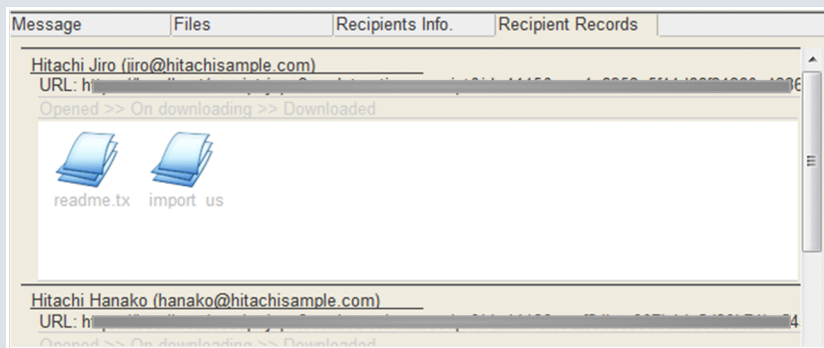
- **Message** tab: Displays the message you sent or received.
- **Files** tab: Displays the file name, size, and other detailed file information. Click the **Download** button to download files.
- **Recipients Info.** tab: Displays the recipient-related information.
- **Recipient Records** tab: Displays the receiving status of the recipients.
- **Approver List** tab: Displayed when the delivery requires approval. You can view the list of approvers. However, if all the approvers are deleted, the **Approver List** tab is not displayed.



Tip

- If you select **Show more info.** in the Out-box window to display the detailed information, clicking the **Delete** button can delete the sent file. If you delete a sent file, the recipient of the file delivery cannot download the file anymore.
- When you send two and more files at once, you can check which files are downloaded by the recipient on the **Recipient Records** tab. If the files have not been downloaded, the names of the files are displayed in gray.

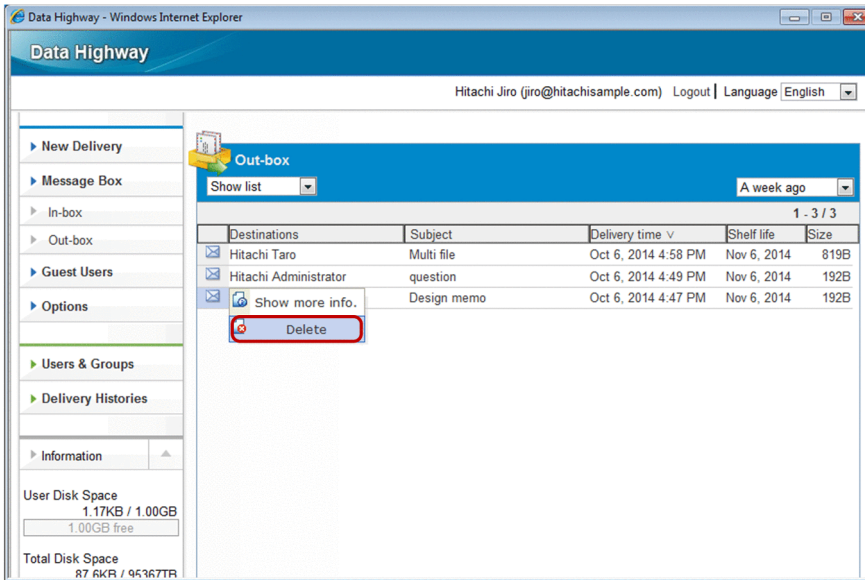
However, if a user receives a file without using the In-box window, or without accessing the URL written in a delivery notification email, the file is not marked as downloaded.



4. Click the **Close** button to return to the In-box or Out-box window.

5. To remove a record of history and the sent file in the Out-box window, click the menu icon of the history record you want to remove, and then select **Delete**.

A confirmation dialog box appears. Click the **OK** button to delete the history record.



3.3.6 Approval Manager

This subsection describes operations that users can perform in the Approval Manager window.

If an approval route is not defined in the delivery rule by a representative user, the **Approval Manager** menu item is not displayed in the sidebar area.

(1) Accepting or rejecting an application for approval by accessing a URL written in an email

To accept or reject an application for approval by accessing a URL written in an approval request notification:

1. Access the URL written in the approval request notification.

The User Authentication window appears.

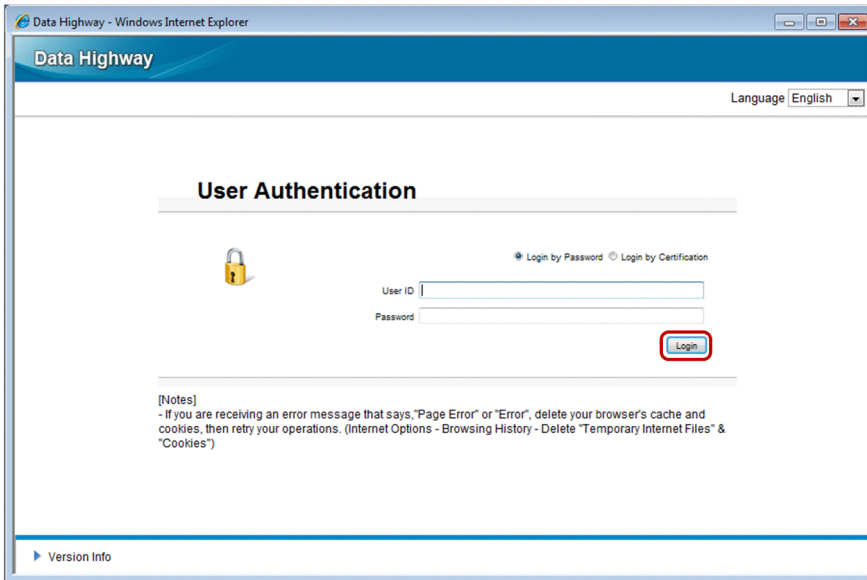
Important note

If JP1/DH - Server is configured to use an electronic certificate for a user to log in to, the Receipt Authentication window appears when you access the URL written in the delivery email. In this case, use the electronic certificate issued by the representative user to log in to the system. For details about how to log in by using the electronic certificate, see [3.2.3 Logging in to JP1/DH - Server by using the electronic certificate authentication](#).

2. Log in to JP1/DH - Server.

For details about how to log in to the system, see [3.2 Basic operations](#).

The Sending Approval window appears.



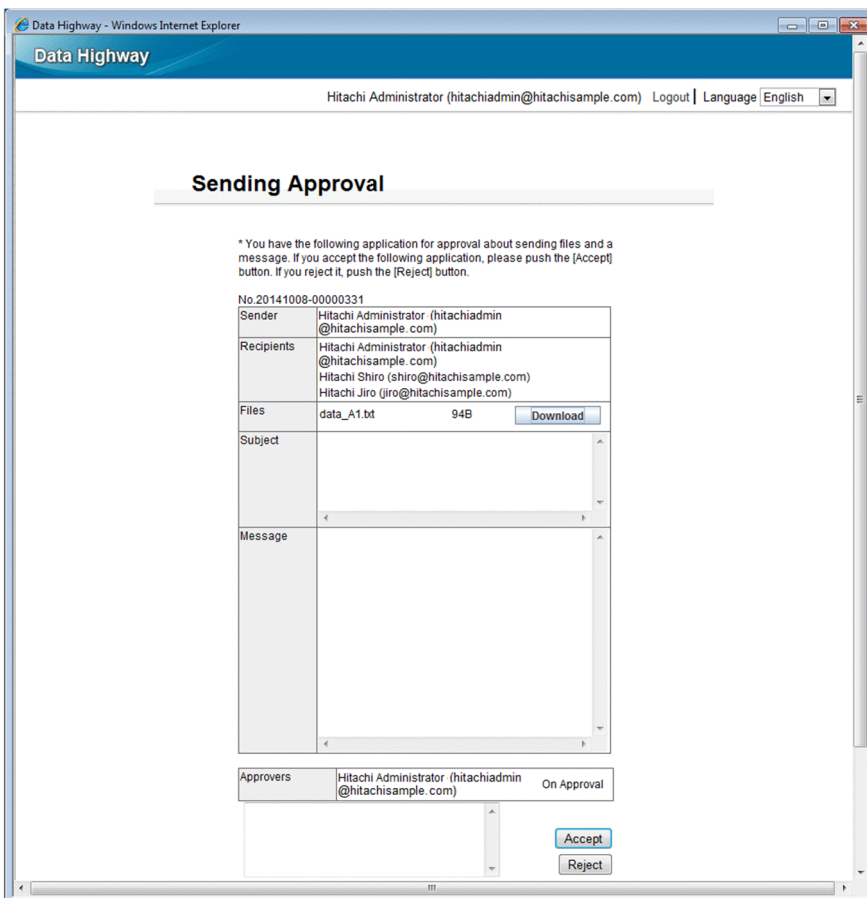
3. Enter the reason why you accept or reject the application.

If you reject the application, you need to enter the rejection reason in no more than 4,096 characters. If you accept the application, you can enter the reason if you want to.

4. Click the **Accept** button to accept the application, or click the **Reject** button to reject.

A confirmation dialog box appears.

Click the **OK** button in the dialog box to complete the approval operation (accept or reject).



Important note

To continue to use JP1/DH - Server after the approval operation, restart the browser.

(2) Accepting or rejecting applications for approval in the Applications for Approval window

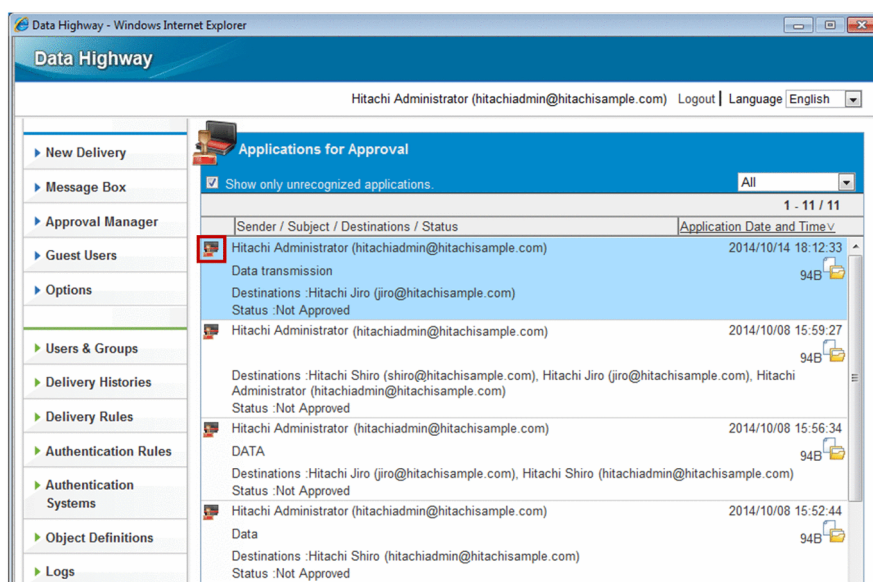
To accept or reject an application for approval in the Applications for Approval window:

1. In the sidebar area, click **Approval Manager**.
2. The Applications for Approval window appears in the content area.
3. To display only applications that have not been processed, select the **Show only unrecognized applications.** check box. Clearing the check box displays all applications in the list.

To filter data by time period, select a desired time period from the display period drop-down list box.

4. Select the application you want to operate.

The Application for Approval window appears.

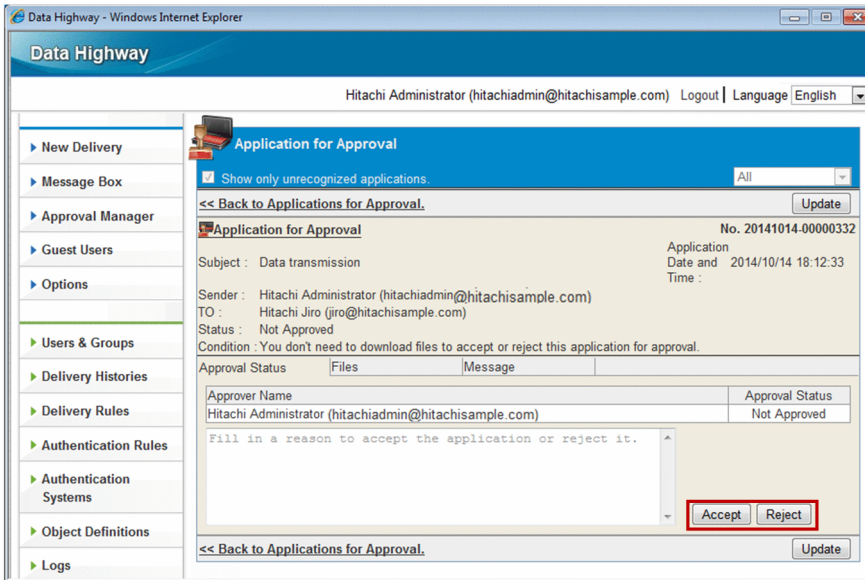


5. Enter the reason why you accept or reject the application.

If you reject the application, you need to enter the rejection reason in no more than 4,096 characters. If you accept the application, you can enter the reason if you want to.

6. Click the **Accept** button to accept the application, or click the **Reject** button to reject.

A confirmation dialog box appears. Click the **OK** button in the dialog box to complete the approval operation (accept or reject).



Important note

If you click the **OK** button but nothing happens, another approver might have already accepted or rejected the application. In this case, click the **Update** button to check the latest approval status.

3.3.7 Guest user settings

This subsection describes operations that users can perform in the Guest Users window.

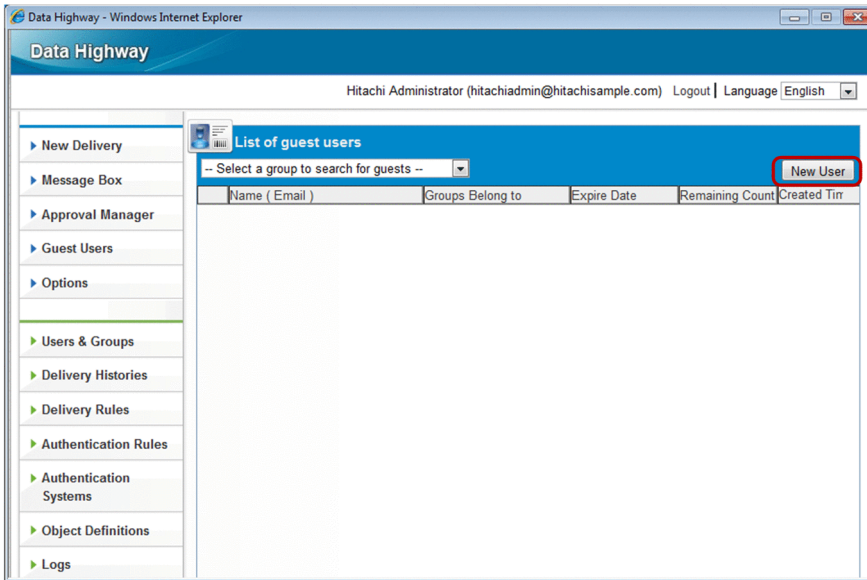
If you are not allowed to use the Guest Users function, the **Guest Users** menu item does not appear in the sidebar area. Even if you are allowed to use the Guest Users function, you cannot use the function when there is no guest group.

For details about how to allow a user to use the Guest Users function, see [3.4.2\(3\) Editing a user](#). For details about how to create a guest group, see [3.4.2\(8\) Creating a group](#).

(1) Creating a guest user

To create a guest user:

1. In the sidebar area, click **Guest Users**.
The List of guest users window appears.
2. Select a group in the group selection drop-down list box to display only the guest users belonging to the group.
3. Click the **New User** button.
The New User window appears.



4. In the New User window, specify the following items.

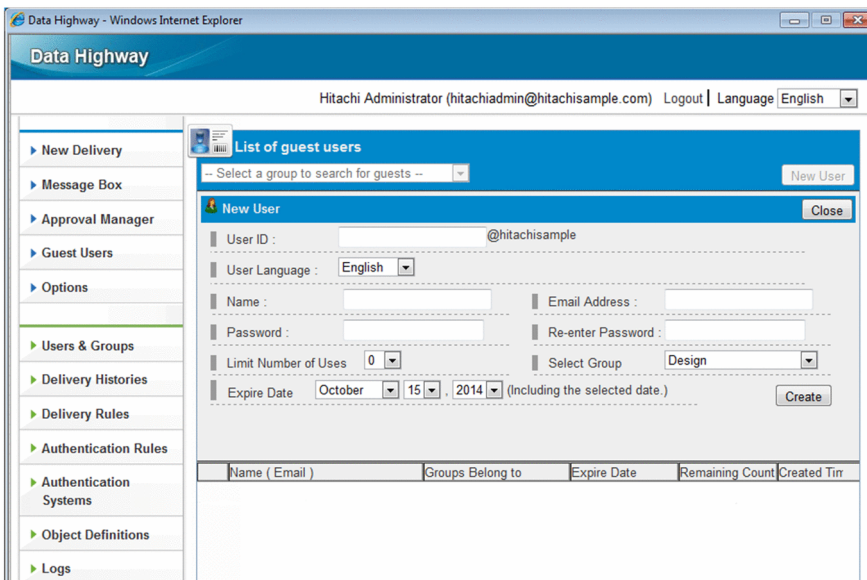


Table 3–11: Setting items in the New User window

Item	Description
User ID text box	<p>Enter a user ID of a guest user.</p> <p>The user ID entered in this text box is postfixed with an ID assigned to the domain. The ID assigned to the domain starting with an at mark (@) is shown on the right of the text box. The user ID must be unique within a domain.</p> <ul style="list-style-type: none"> You can enter no more than 100 (for Windows) or 256 (for Linux) alphanumeric characters and symbols, including the ID assigned to the domain. Some symbols (/ \ ? * : " < > # @ ^ [] \$) and space characters are not available. A user ID consisting of only a period or periods (.) are not available. Reserved words in Windows[#] are not available.
User Language drop-down list box	<p>Select the language the guest user uses.</p> <p>You can choose one of the following: Japanese, English, or Chinese.</p>
Name text box	<p>Enter the name of the guest user.</p> <ul style="list-style-type: none"> You can enter no more than 256 characters.

Item	Description
Name text box	<ul style="list-style-type: none"> Some symbols (/ \ ? * : " < > @ ^) are not available. A name consisting of only spaces or periods (.) is not available.
Email Address text box	Enter an email address for the guest user. Notification emails for delivery and approval are sent to the email address specified in this text box. <ul style="list-style-type: none"> You can enter no more than 256 alphanumeric characters and symbols. Some symbols (/ \ ? * : " < > ^) and space characters are not available.
Password text box	Enter a password for the guest user.
Re-enter Password text box	<ul style="list-style-type: none"> You can use alphanumeric characters and symbols in a given length and type as defined by authentication rules. The symbols of ! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { } ~ are available.
Limit Number of Uses drop-down list box	Specify the number of times the guest user can send files and messages in the range from 1 to 10. After sending files for the specified number of times, the guest user cannot send files anymore. Even in this case, the guest user can log in to JP1/DH - Server and receive files.
Select Group drop-down list box	Guest groups are displayed in the list. Select a guest group to which the guest user belongs.
Expire Date drop-down list box	Specify the expiration date of the account set for the guest user. After the expiration date, the guest user cannot log in to JP1/DH - Server. This list box can be browsed in the List of guest users window and the Users & Groups window. Changing the expiration date allows the guest user to log in again.

#: The following words are reserved in Windows:

- A word beginning with a space or period
- A word ending with a space or period
- Characters in the range from 0x00 to 0x31
- The following words and those with an extension:
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
- The following file and directory names cannot be used for the root directory name (immediately below the drive name):
\$AttrDef, \$BadClus, \$Bitmap, \$Boot, \$LogFile, \$MFT, \$MFTMirr, pagefile.sys, \$Secure, \$UpCase, \$Volume, \$Extend, \$Extend\ \$ObjId, \$Extend\ \$Quota, \$Extend\ \$Reparse (\$Extend is a directory)

5. Click the **Create** button.

The guest user is now created.

You need to notify the guest user of the user ID and password and ask the guest user to change the password.

(2) Editing a guest user

To edit a guest user:

1. In the sidebar area, click **Guest Users**.

The List of guest users window appears.

For details about the List of guest users window, see *(1) Creating a guest user*.

2. Click the menu icon () of the guest user you want to edit, and then select **Edit**.

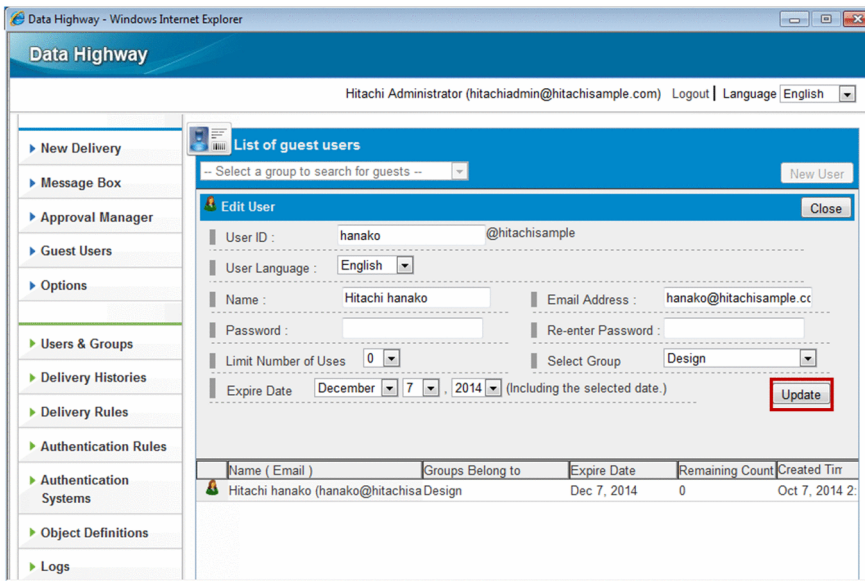
The Edit User window appears.

3. Change the settings.

For details about each item, see *(1) Creating a guest user*.

4. Click the **Update** button.

The setting of the guest user is updated.



Tip

The guest user you are editing is sometimes a new guest user who was originally a member of the non-guest group and who has an electronic certificate issued for the user. In this case, editing the user ID (including any case change) invalidates the electronic certificate. For this reason, the user will no longer be able to log in by using the issued electronic certificate after the user becomes a member of the non-guest group from the guest group.

(3) Activating, inactivating, or deleting a guest user

To activate, inactivate, or delete a guest user:

1. In the sidebar area, click **Guest Users**.

The List of guest users window appears. For details about the List of guest users window, see (1) *Creating a guest user*.

2. Click the target guest user of your action, and then select the menu item for it.

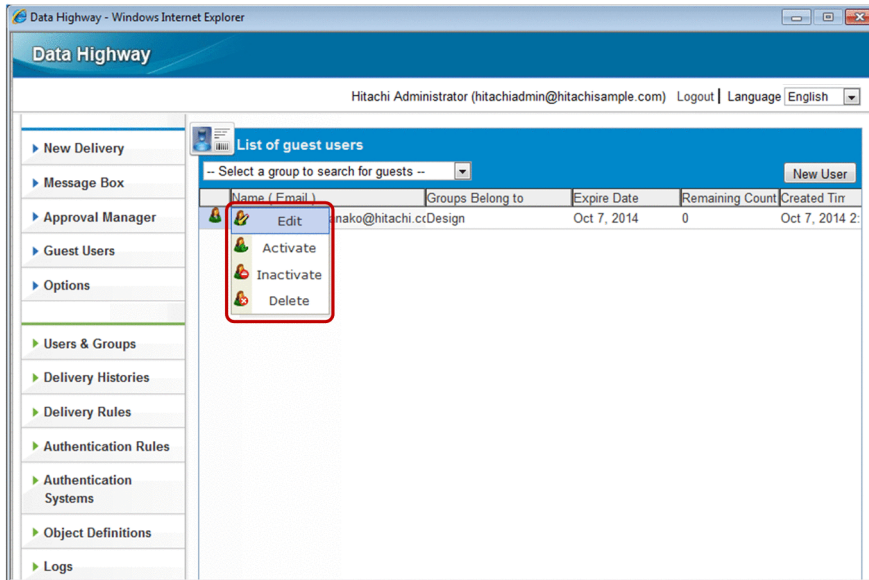


Table 3–12: Activating, inactivating, or deleting a guest user

Item	Description
Activate	Activates a guest user. For a guest user whose account is locked, the account is unlocked.
Inactivate[#]	Inactivates a guest user. The inactivated guest user cannot use JP1/DH - Server. To allow the guest user to use the system again, activate the guest user.
Delete[#]	Deletes a guest user. The deleted guest user cannot be restored.

Inactivating or deleting an approver user assigned to an approval route might cause the approval route to have no approver. No approval is required if a file is delivered by using a delivery rule that has the approval route with no approver.

3. A confirmation dialog box appears depending on your choice. Click the **OK** button to perform the action.

3.3.8 Options

This subsection describes the operation of the Options window. If your system administrator does not allow you to use the Options function, you cannot use the Options function.

(1) Changing a password

This subsection describes how to change a password. The current password is required to change the password. Note that you cannot change your password when you are logged in with the electronic certificate.

1. In the sidebar area, click **Options**, and then select the **Authentication** tab.

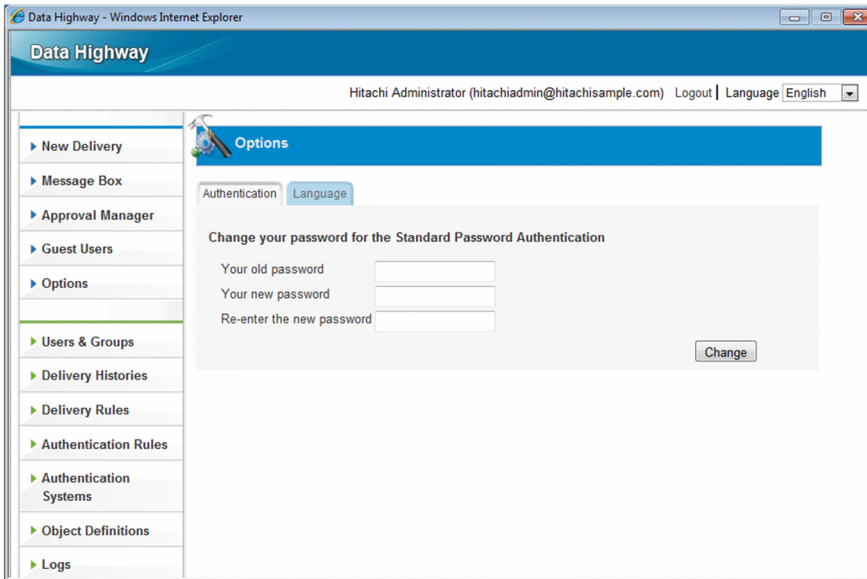
The "Change your password for the Standard Password Authentication" window appears in the content area.

2. Enter your current password in the **Your old password**, and a new password in the **Your new password** and **Re-enter the new password** fields.

You can use alphanumeric characters and symbols in a given length and type for a password as defined by authentication rules. The symbols of !"#%&'()*+,-./:;<=>?@[\\]^_`{|}~ are available.

3. Click the **Change** button.

The password is changed. A dialog box appears indicating the change took place.



4. Click the **OK** button.

(2) Changing the language used in email

This subsection describes how to change the language used in emails sent to users. Note that the language used in a delivery notification email is specified by the sender.

1. In the sidebar area, click **Options**, and then select the **Language** tab.

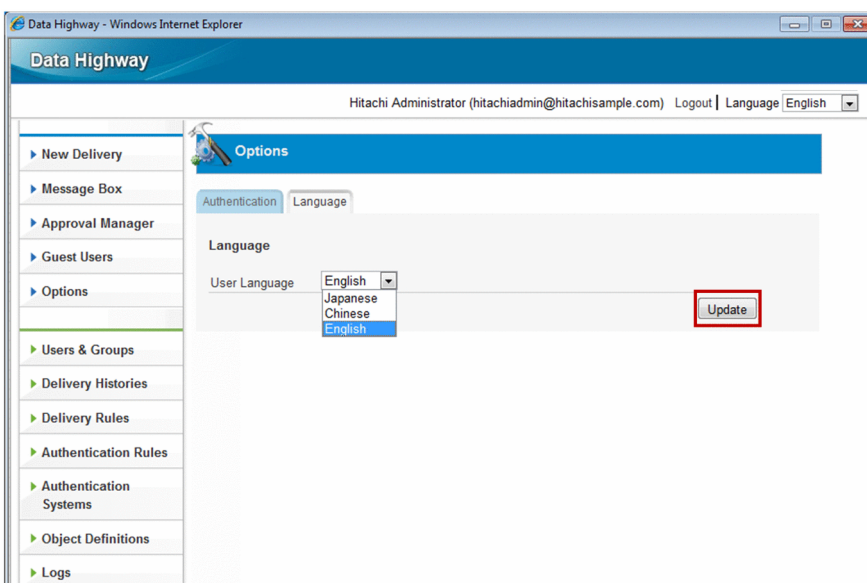
The Language window appears in the content area.

2. Select the language used in emails in the **User Language** drop-down list box.

You can select **Japanese**, **English**, or **Chinese** as a user language.

3. Click the **Update** button.

The user language is changed. A dialog box appears indicating the change took place.



4. Click the **OK** button.

3.4 Group-manager operations

This section describes what operations group managers can perform. Representative users can also perform them.

3.4.1 List of operations

The following table describes and lists operations performed by group managers.

Table 3–13: List of group manager operations

Function or category	Operation	Related subsection
Users & Groups	Searching for a user and group	3.4.2(1)
	Creating a user	3.4.2(2)
	Editing a user	3.4.2(3)
	Activating, inactivating, or deleting a user	3.4.2(4)
	Issuing an electronic certificate	3.4.2(5)
	Invalidating an electronic certificate	3.4.2(6)
	Re-issuing an electronic certificate	3.4.2(7)
	Creating a group	3.4.2(8)
	Editing a group or assigning a group manager	3.4.2(9)
	Activating, inactivating, or deleting a group	3.4.2(10)
Delivery Histories	Viewing or deleting delivery history	3.4.3(1)

3.4.2 Users & Groups

This subsection describes how to manage users and groups.

In JP1/DH - Server, different users appear in different colors. The following table describes the relationship between colors and user types.

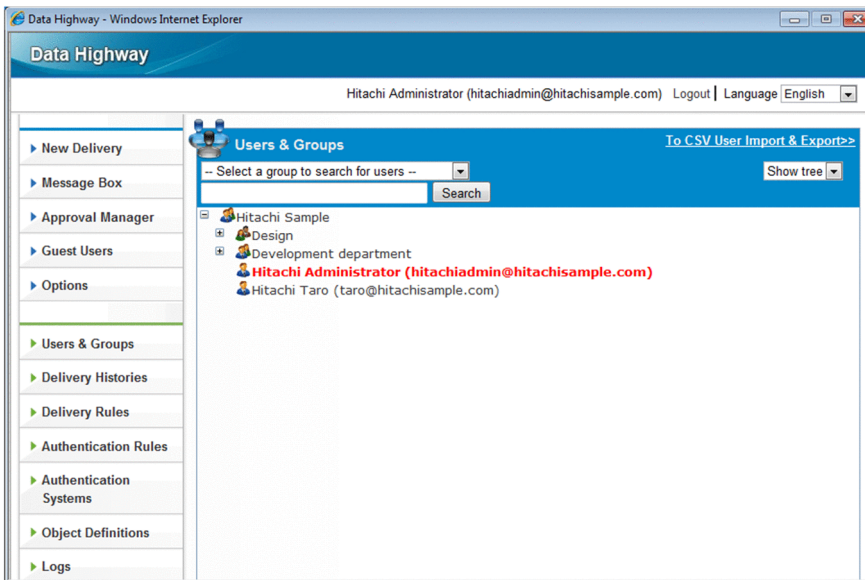
Table 3–14: Relationship between colors and user types

Color	User type
Red (in bold)	Representative user
Blue	Group manager
Black	General user or guest user
Light blue	Read-only group manager
Gray	Read-only general user

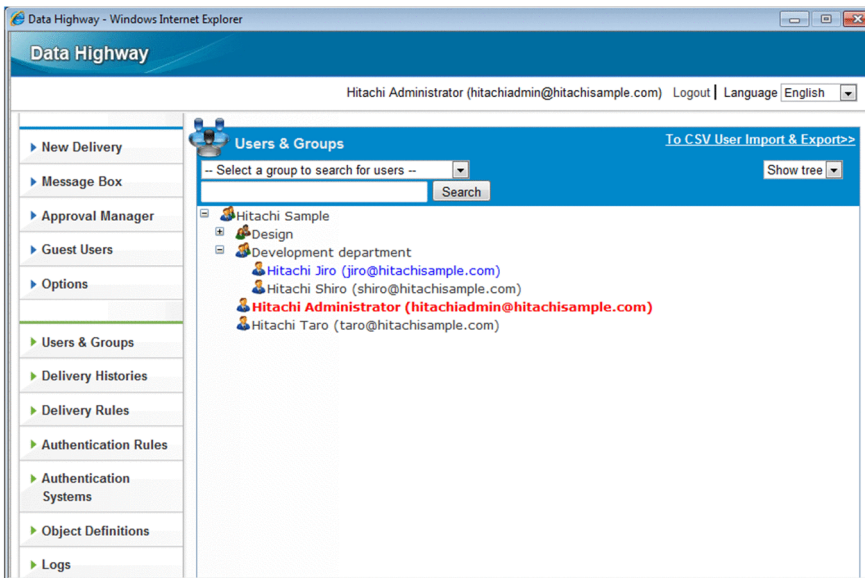
The figures below illustrate the Users & Groups windows for representative users and group managers.

You can use the display style drop-down list box to display users and groups in tree or list view.

- Representative user: All groups are displayed.



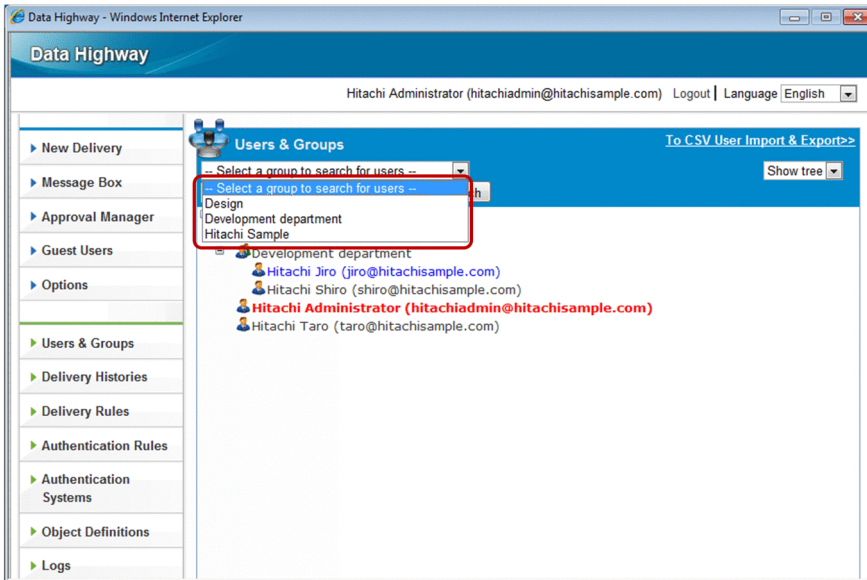
- Group manager: The group managed by the group manager and any group within it are displayed.



(1) Searching for a user and group

To search for a user or group in the Users & Groups window:

1. In the sidebar area, click **Users & Groups**.
The Users & Groups window appears in the content area.
2. Click the group selection drop-down list box to see groups filtered by your authority in the list box. Select a group to display the corresponding group in the window.



3. To search for a user or group by entering a user name or group name, type your keyword in the text box.

The following items are to be searched:

User ID, Name, Email, Group Name (Japanese/Chinese), Group Name (English)

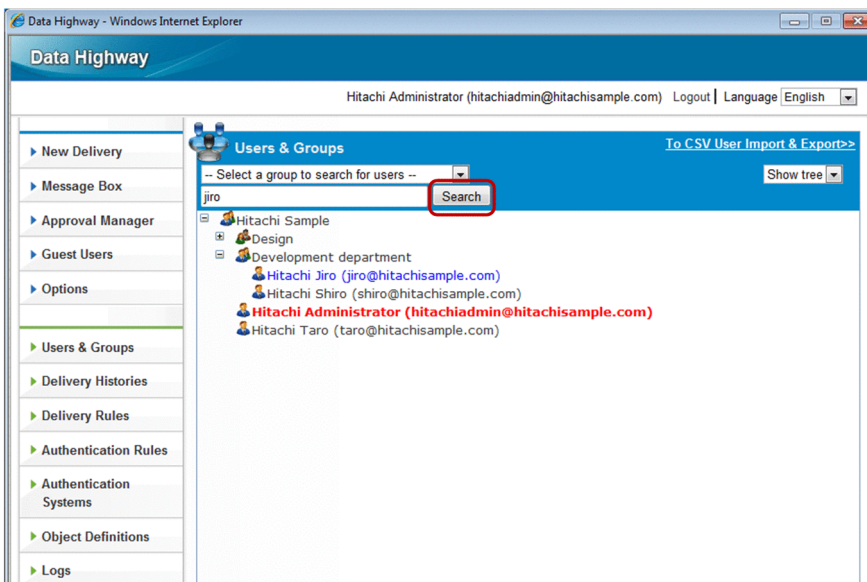
The search criteria are case-insensitive. Wild cards (for example, * and ?) are not available. Any wild card symbol is interpreted as just a character.

4. Click the **Search** button.

Search results are displayed in current display style.

If the display style is the list view and your search produces 25 or more results, the results are displayed in multiple pages. If the display style is the tree view and your search produces 100 or more results, an error message appears.

If your search results contain a user belonging to multiple groups, multiple records are displayed based on the number of groups the user belongs to.



The following table lists and describes the items displayed in the search results window. If the display style is the tree view, only the **Name (Email)** and **Groups belongs to** are displayed.

Table 3–15: Items displayed in the search results window

Item	Description
Name (Email)	The name of the searched user or group, and email address are displayed.
Groups belongs to	The groups to which the searched user or group belongs are displayed.
Created Time	The creation date and time of the searched user or group is displayed.
Updated Time	The update date and time of the searched user or group is displayed.
Count	The number of search results. If your search results contain a user belonging to multiple groups, the count is based on the number of groups the user belongs to.
<< First	This is visible if you are on the third page or later in the search results window. Clicking this will bring you to the first page.
< Previous	This is visible if you are on the second page or later in the search results window. Clicking this will bring you to the previous page.
Next >	This is visible if your search results have two or more pages. This is not visible on the last page.
Last >>	This is visible if your search results have three or more pages. This is not visible on the last page.

5. View or edit the user or group in the search results, if necessary.

For details about how to edit the user or group, see (3) *Editing a user* or (9) *Editing a group*.

6. In the sidebar area, click **Users & Groups** to reset your search.

(2) Creating a user

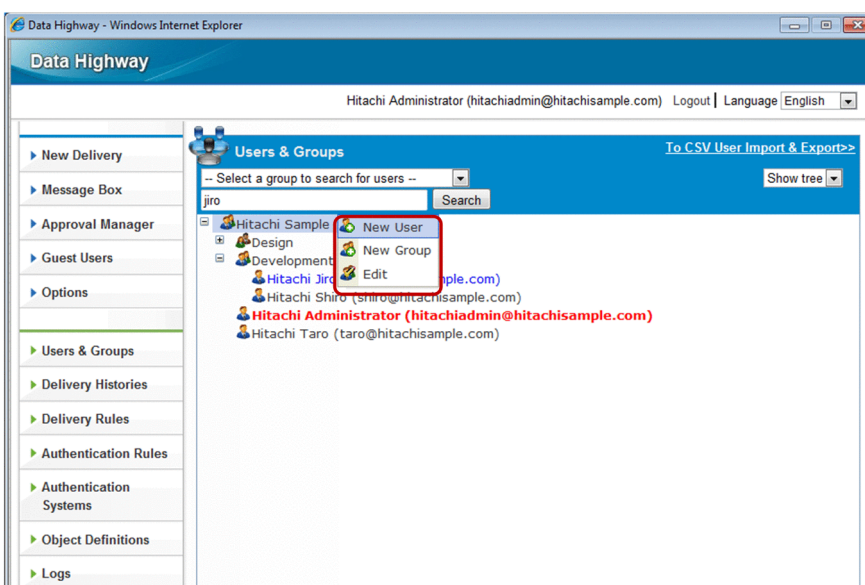
To create a user:

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

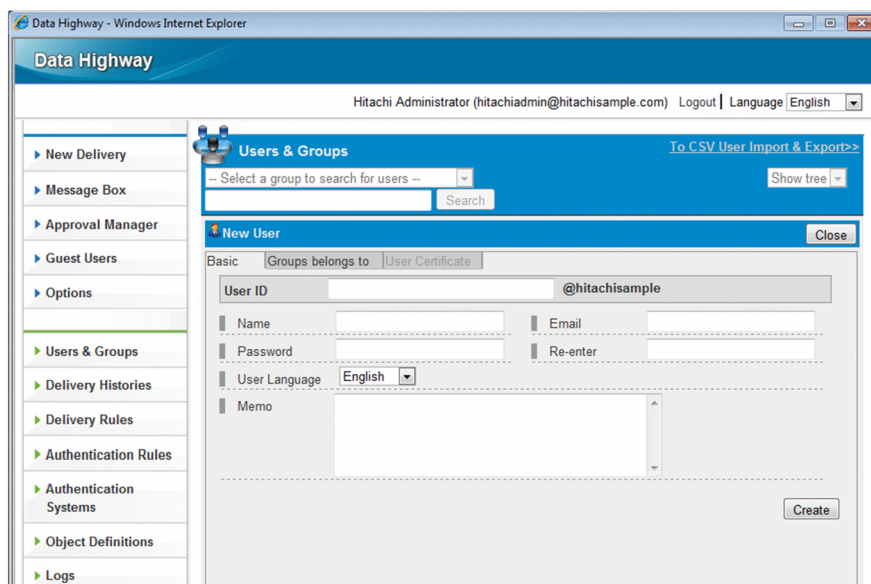
The Users & Groups window appears in the content area.

2. Click the group to which the new user will belong, and then select **New User**.

The New User window appears.



3. Configure the settings in the **Basic** tab.



The following table describes the items you specify.

Table 3–16: Setting items in the Basic tab

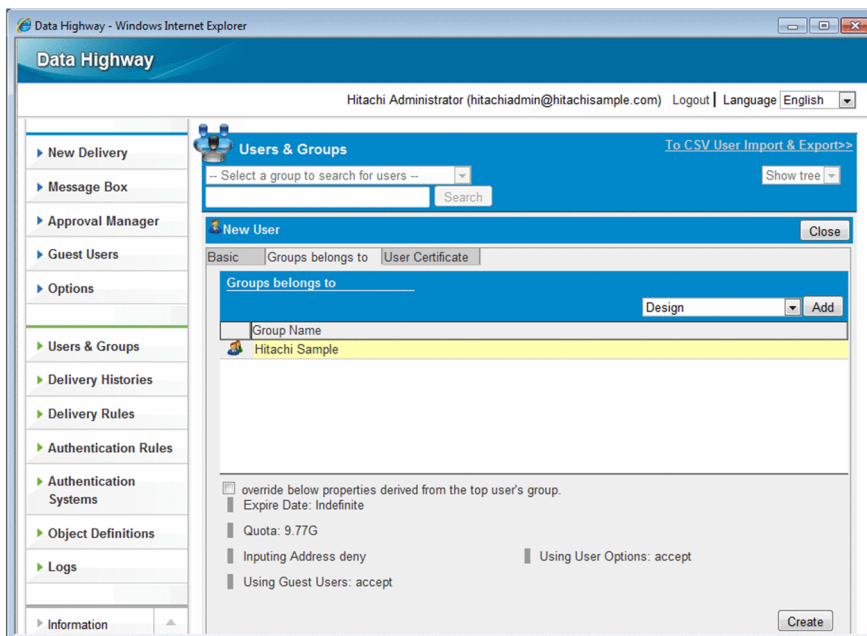
Item	Description
User ID text box	<p>Enter the user ID.</p> <p>The user ID entered in this text box is postfixed with an ID assigned to the domain. The ID assigned to the domain starting with an at mark (@) is shown on the right of the text box.</p> <p>The user ID must be unique within a domain.</p> <ul style="list-style-type: none"> You can enter no more than 100 (for Windows) or 256 (for Linux) alphanumeric characters and symbols, including the ID assigned to the domain. Some symbols (/ \ ? * : " < > # @ ^ [] \$) and space characters are not available. A user ID consisting of only a period or periods (.) is not available. Reserved words in Windows# are not available.
Name text box	<p>Enter the name of the user in English.</p> <p>The name you enter here is displayed in the Common Name text box in the User Certificate tab.</p> <ul style="list-style-type: none"> You can enter no more than 100 (for Windows) or 256 (for Linux) alphanumeric characters and symbols. Some symbols (/ \ ? * : " < > @ ^) are not available. A name consisting of only spaces or periods (.) is not available.
Email text box	<p>Enter the email address of the user.</p> <p>Notification emails for delivery and approval are sent to the specified email address. The email address you enter here is displayed in the Email Address text box in the User Certificate tab.</p> <ul style="list-style-type: none"> You can enter no more than 256 alphanumeric characters and symbols. Some symbols (/ \ ? * : " < > ^) and space characters are not available.
Password text box	<p>Enter a password.</p>
Re-enter text box	<p>A representative user can specify any password that does not follow the authentication rule.</p> <ul style="list-style-type: none"> You can use alphanumeric characters and symbols in a given length and type as defined by authentication rules. The symbols of ! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { } ~ are available. <p>JP1/DH - Server manages the password specified here. If a directory server is used to authenticate users, specify the JP1/DH - Server password, instead of using the password managed by the directory server. You cannot change the password managed by the directory server here.</p>
User Language drop-down list box	<p>Select the language that the user uses.</p>

Item	Description
User Language drop-down list box	You can choose one of the following: Japanese , English , or Chinese .
Memo text area	Enter a note on this user. You can enter no more than 4,096 characters.

#: The following words are reserved in Windows:

- A word beginning with a space or period
- A word ending with a space or period
- Characters in the range from 0x00 to 0x31
- The following words and those with an extension:
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
- The following file and directory names cannot be used for the root directory name (immediately below the drive name):
\$AttrDef, \$BadClus, \$Bitmap, \$Boot, \$LogFile, \$MFT, \$MFTMirr, pagefile.sys, \$Secure, \$UpCase, \$Volume, \$Extend, \$Extend\ObjId, \$Extend\Quota, \$Extend\Reparse (\$Extend is a directory)

4. Configure the settings in the **Groups belongs to** tab.



The following table describes the items you specify.

Table 3–17: Setting items in the Groups belongs to tab

Item	Description
Group selection drop-down list box	You can use it to add the user to a group. Click the Add button to add the group in the list. A user can be a member of a maximum of 10 groups.
Groups belongs to	<p>Selecting a group icon shows the following shortcut menu items:</p> <ul style="list-style-type: none"> • Up: Moves the selected group up one place in the list. • Down: Moves the selected group down one place in the list. • Delete: Deletes the selected group from the list. <p>The group at the top of the list is called the <i>primary group</i>. Managers of the primary group, or of parent groups of the primary group, can manage this user. A guest user can belong to only one group.</p>

Item	Description
override below properties derived from the top user's group. check box ^{#1}	Selecting this check box can change the settings below from those of the user's group. If not selected, the setting of the primary group is used. <ul style="list-style-type: none"> • Expire Date • Quota • Inputing Address^{#2} • Using User Options • Using Guest Users • Limit Number of Uses
--	
Expire Date check box ^{#2}	If selected, the account is no longer expired, or the expiration date can be specified in month, day, and year format. If not selected, it inherits the property value from the primary group. If the Indefinite check box is selected, the account never expires. The expiration date of a guest group cannot be changed.
Quota check box	Selecting this check box sets the storage quota to the value specified in the text box. If not selected, the setting of the primary group is used.
Inputing Address check box ^{#3}	This setting specifies whether a sender can enter any recipient address before sending a file.
Using User Options check box	If selected, the Options (changing the password and language) function becomes available. Clearing the check box disables the function. If the user is not allowed to use the function, the Options menu item does not appear in the sidebar area.
Using Guest Users check box	If selected, the Guest Users function becomes available. Clearing the check box disables the function. If the user is not allowed to use the function, the Guest Users menu item does not appear in the sidebar area.
Limit Number of Uses check box	If selected, you can specify how many times a guest user can use JP1/DH - Server. This setting is only visible for guest groups.

#1

If a user is created as a member of the guest group, this check box appears dimmed. However, you can change the settings in the **Expire Date**, **Quota**, **Inputing Address**, **Limit Number of Uses**, and **Using User Options** fields.

#2

If an electronic certificate is used, it will expire on December 31, 2037. When an account created in this window expires before that date, the user with that account will no longer be able to log in to JP1/DH - Server.

#3

This check box might not appear depending on the setting.

5. Configure the settings in the **User Certificate** tab.

If JP1/DH - Server uses electronic certificates to authenticate users, the **Use Certification** check box must be selected in this tab. The check box is not selected by default.

If the user is created as a member of the guest group, this tab appears dimmed.

The **Common Name** and **Email Address** text boxes show the values specified in the **Name** and **Email** text boxes of the **Basic** tab, respectively.

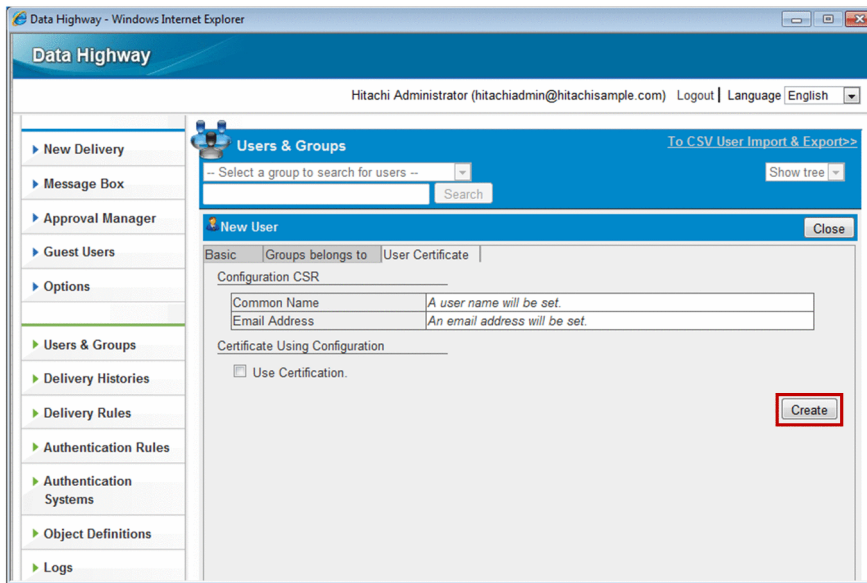
Important note

If the created user uses an electronic certificate, you must issue it after creating the user. For details, see [\(5\) Issuing an electronic certificate](#). Also, an authentication policy that authenticates users with an electronic certificate must be specified as the user's authentication rule. For details, see [3.5.4 Authentication Rules](#).

6. Click the **Create** button.

The user is now created.

You need to notify the user of the user ID and password and ask the user to change the password.



(3) Editing a user

To edit a user:

Important note

- If a user ID is changed (including any case change), the user's electronic certificate is automatically invalidated.
- If the type of a user's group is changed to the guest group, the user's electronic certificate remains valid. However, the user will no longer be able to log in to JP1/DH - Server by using the electronic certificate.

1. In the sidebar area, click **Users & Groups**.
The Users & Groups window appears in the content area.
2. Click the user you want to edit, and then select **Edit**.
The Edit User window appears.
3. Change the settings.
For details about each item on each tab, see (2) *Creating a user*.
If the password is not entered, it is not changed.
4. Click the **Update** button.
A dialog box appears indicating the information is updated.
5. Click the **OK** button.

(4) Activating, inactivating, or deleting a user

To activate, inactivate, or delete a user:

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

The Users & Groups window appears in the content area.

2. Click the target user of your action, and then select the menu item for it.

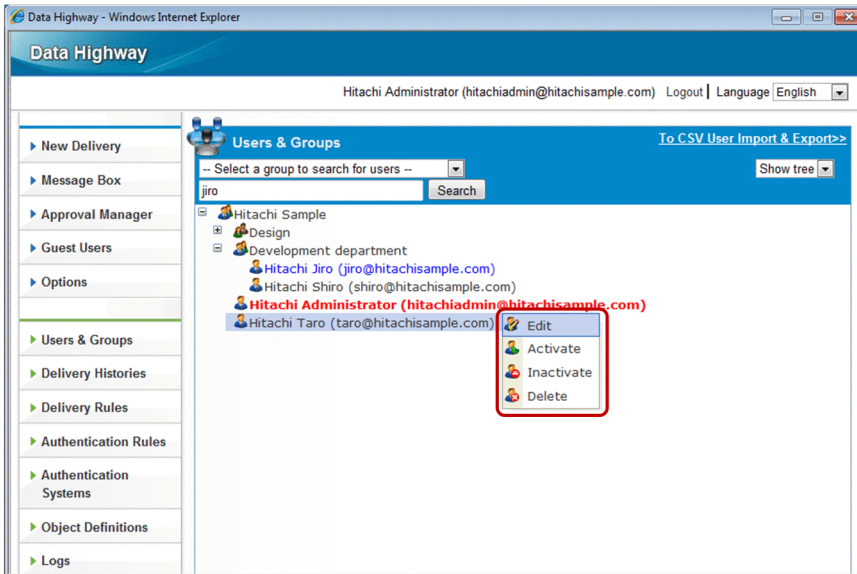


Table 3–18: Activating, inactivating, or deleting a user

Item	Description
Activate	Activates a user. For the user whose account is locked, the account is unlocked. You cannot activate a user if all groups to which the user belongs are inactivated.
Inactivate[#]	Inactivates a user. The inactivated user is no longer able to use JP1/DH - Server. To allow the user to use the system again, activate the user.
Delete[#]	Deletes a user. The deleted user cannot be restored.

- #
- Before you inactivate or delete a user, make sure that the user does not have data currently in delivery.
 - Inactivating or deleting an approver user assigned to an approval route might cause the approval route to have no approver. No approval is required if a file is delivered by using a delivery rule that has the approval route with no approver.

3. A confirmation dialog box appears depending on your choice. Click the **OK** button to perform the action.

(5) Issuing an electronic certificate

You can issue an electronic certificate for a user if the **Use Certification** check box is selected when the user is created or updated.

Important note

The issued electronic certificate expires on December 31, 2037. However, when an account expires before this date, the user with this account is no longer able to log in to JP1/DH - Server.

To issue an electronic certificate:

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

The Users & Groups window appears in the content area.

2. Click the user you want to issue an electronic certificate for, and then select **Edit**.

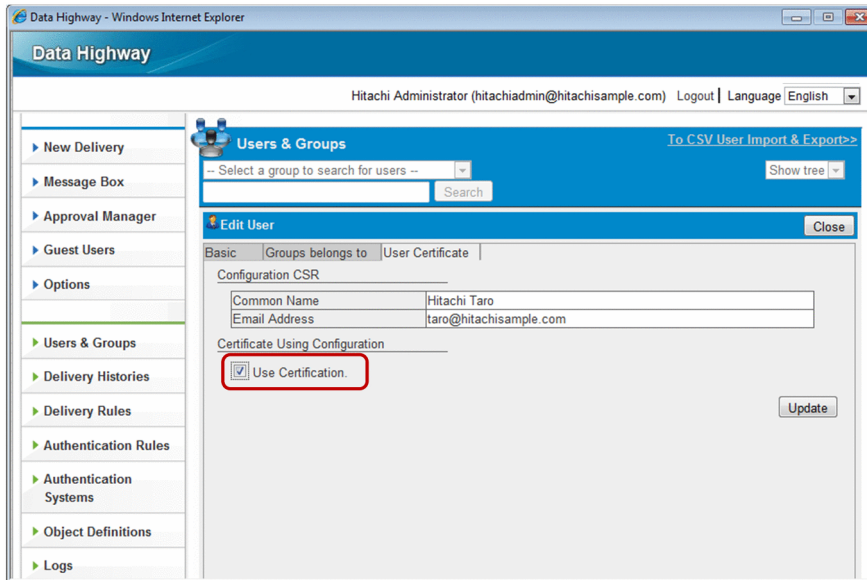
The Edit User window appears.

3. Click the **User Certificate** tab.

The Configuration CSR window appears.

4. Click the **To Issuing Screen** button.

The Issue Certificate window appears.



Tip

If the **Use Certification** check box is not selected in the **User Certificate** tab during user creation, the **To Issuing Screen** button does not appear. In this case, you need to select the **Use Certification** check box, click the **Update** button, and then edit the user again.

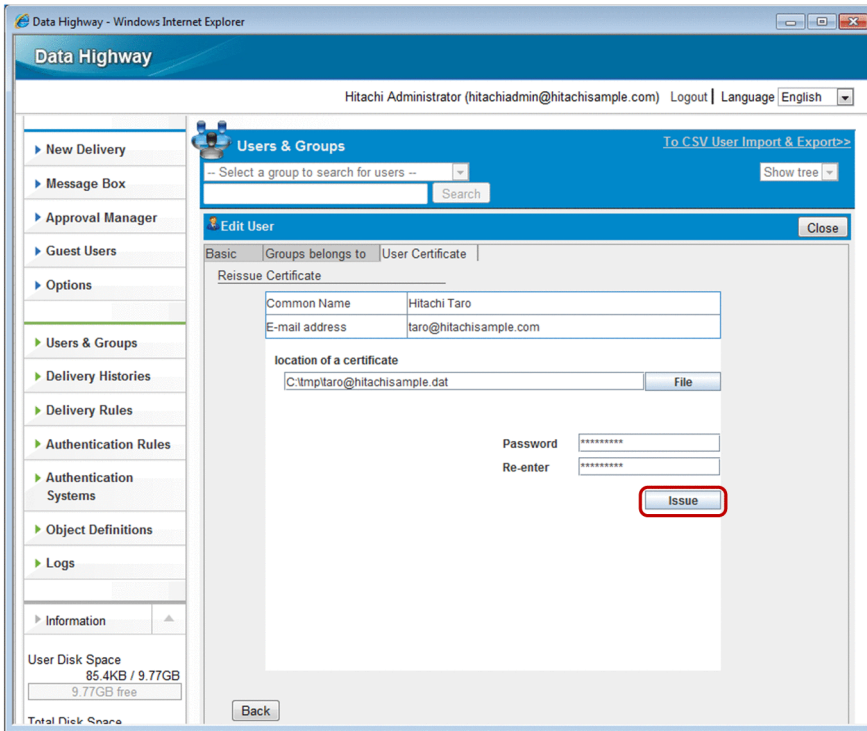
5. Click the **File** button, and then select a destination where the electronic certificate is saved. You can also directly enter the path to the file.

6. In the **Password** and **Re-enter** text areas, enter the password for protecting the electronic certificate.

The password must contain two or more different types of characters and consist of a string from 6 to 32 characters.

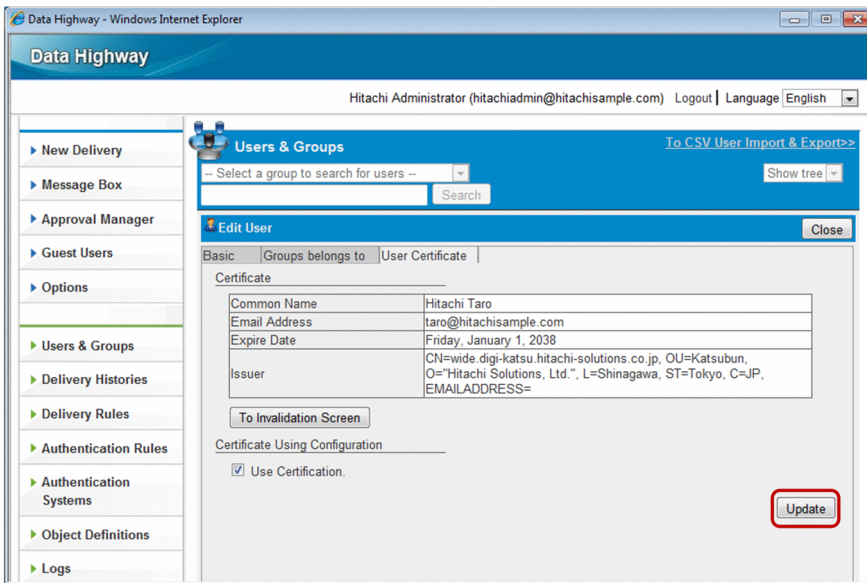
7. Click the **Issue** button.

A dialog box appears asking you to confirm that you want to issue the certificate.



8. Click the **OK** button.

The Certificate window appears. When you click the **Update** button, a dialog box appears indicating the information is updated.



9. Click the **OK** button.

The Users & Groups window appears.

Important note

An authentication rule for a user must use the authentication policy that authenticates the user with the electronic certificate, so that the user can use the issued electronic certificate. For details, see [3.5.4 Authentication Rules](#).

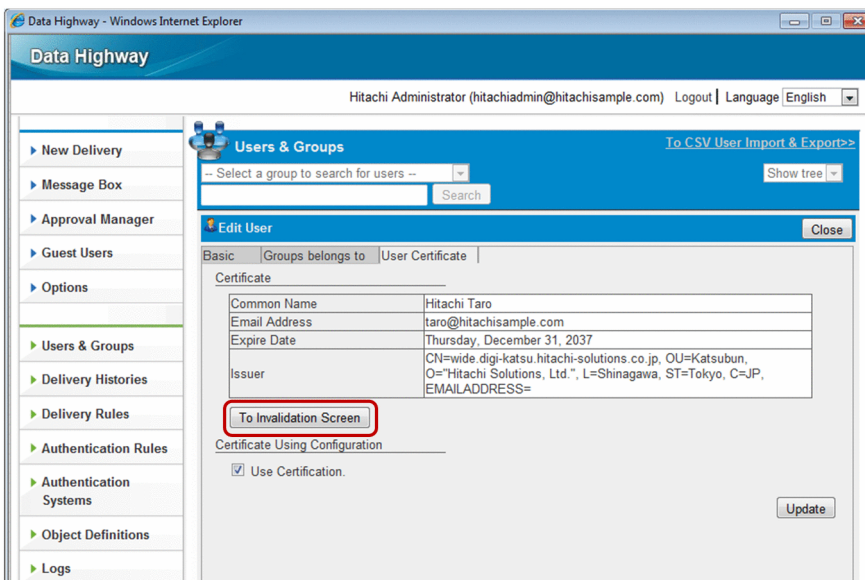
(6) Invalidating an electronic certificate

To invalidate an issued electronic certificate:

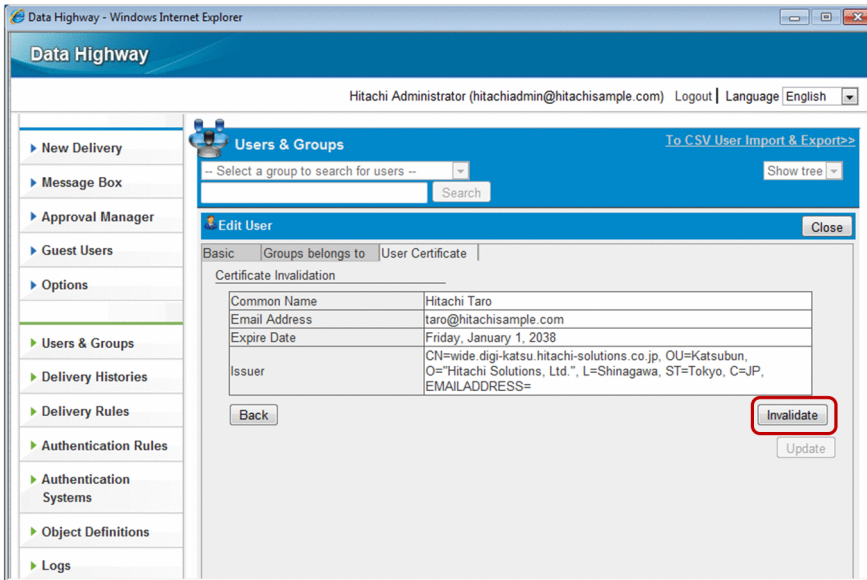
Important note

Invalidating an electronic certificate disables the use of it for login.

1. In the sidebar area, click **Users & Groups**.
The Users & Groups window appears in the content area.
2. Click the user you want to update or invalidate the electronic certificate for, and then select **Edit**.
The Edit User window appears.
3. Click the **User Certificate** tab.
The Certificate window appears.
4. Click the **To Invalidation Screen** button.
The Certificate Invalidation window appears.



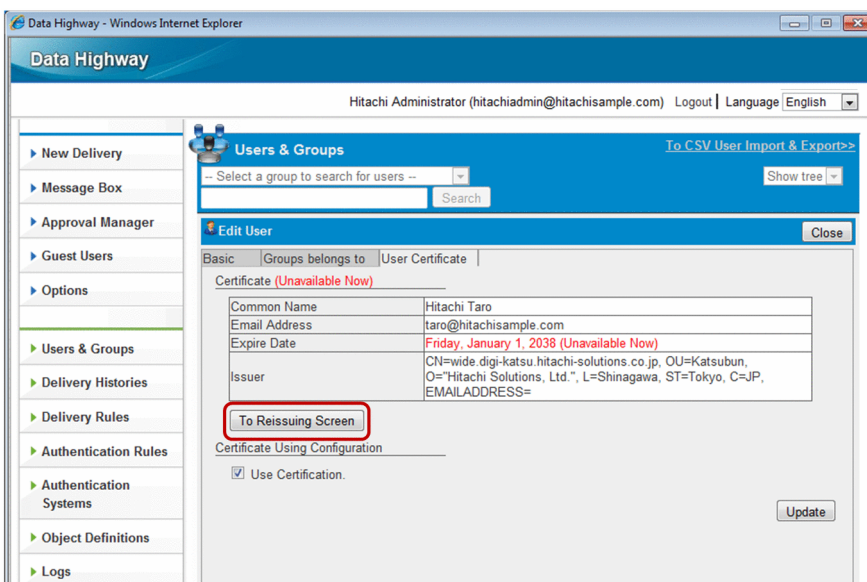
5. Click the **Invalidate** button.
The Certificate (Unavailable Now) window appears, indicating the certificate is invalidated.



(7) Re-issuing an electronic certificate

To re-issue an electronic certificate:

1. In the sidebar area, click **Users & Groups**.
The Users & Groups window appears in the content area.
2. Click the user you want to re-issue the electronic certificate for, and then select **Edit**.
The Edit User window appears.
3. Click the **User Certificate** tab.
The Certificate (Unavailable Now) window appears.
4. Click the **To Reissuing Screen** button.
The Reissue Certificate window appears.

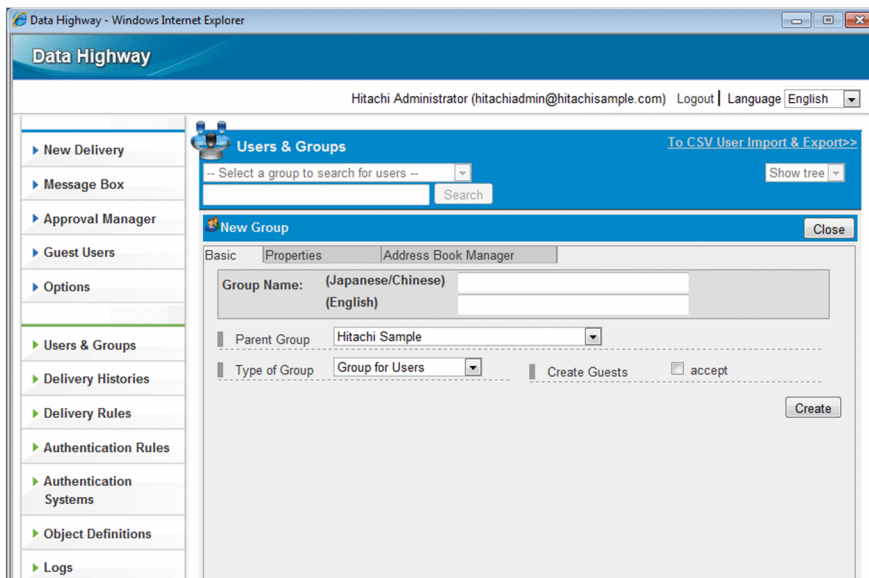


5. Follow the same steps as those in issuing an electronic certificate. See step 6 and later in (5) *Issuing an electronic certificate*.

(8) Creating a group

To create a group:

1. In the sidebar area, click **Users & Groups**.
The Users & Groups window appears in the content area.
2. Click the group to which the new group will belong, and then select **New Group**.
The New Group window appears.
3. Configure the settings in the **Basic** tab.



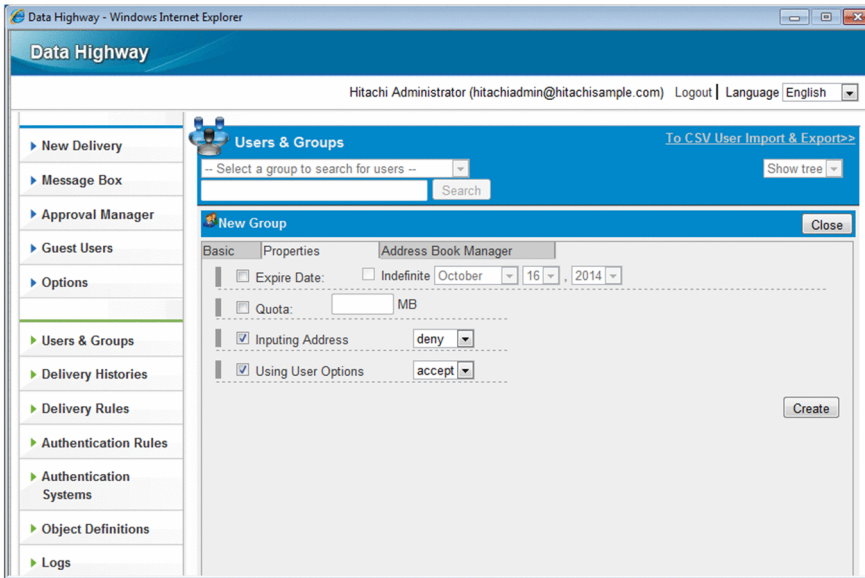
The following table describes the items you specify.

Table 3–19: Setting items in the Basic tab

Item	Description
Group Name: (Japanese/Chinese) text box	Enter the name of the group. The value you enter here is displayed in windows that use Japanese and Chinese. <ul style="list-style-type: none"> You can enter no more than 200 characters. Some symbols (/ \ ? * : " < > @ ^) are not available. A name consisting of only spaces or periods (.) is not available.
Group Name: (English) text box	Enter the name of the group. The value you enter here is displayed in windows that use English. <ul style="list-style-type: none"> You can enter no more than 200 alphanumeric characters and symbols. Some symbols (/ \ ? * : " < > @ ^) are not available. A name consisting of only spaces or periods (.) is not available.
Parent Group drop-down list box	Select a parent group of the group you create. Groups can be nested to a maximum of 10 levels, and the top-level group in the hierarchy is the first level. They cannot be nested to 11 levels or more. You need to select a parent group at the 9 th level or less.
Type of Group drop-down list box	Select either type of the groups below. The type of the group cannot be changed after it is created. <ul style="list-style-type: none"> Group for Users: Non-guest users and groups can be members of this type of group. Group for Guest Users: Guest users can be members of this type of group.

Item	Description
Create Guests check box	If selected, a user in this group can create a guest user. If the Type of Group drop-down list box is set to Group for Guest Users , this check box is disabled.

4. Configure the settings in the **Properties** tab.



The following table describes the items you specify.

Table 3–20: Setting items in the Properties tab

Item	Description
Expire Date check box ^{#1}	If selected, the group account is no longer expired, or the expiration date can be specified in month, day, and year format. If not selected, it inherits the property value from the primary group. This item is not visible for guest groups.
Quota check box	If you select the check box, you can specify the storage space amount for users in this group. The possible amount is defined by the system administrator. Clearing the check box sets the value to 1 GB.
Inputting Address check box ^{#2}	Specifies whether a sender can enter an unregistered recipient address before sending a file. The check box is not selected by default. If you select the Inputting Address check box, you can choose either of the following: <ul style="list-style-type: none"> accept: A user is allowed to enter an unregistered recipient address. The user can enter the email address in the email address field and send an email message to the unregistered user. deny: A user is not allowed to enter an unregistered recipient address in the email address field. However, the user can choose the recipient address from the user's address book and send an email message.
Using User Options check box	Specifies whether users are allowed to use the Options function. If they are not, the Options menu item does not appear in the sidebar area.

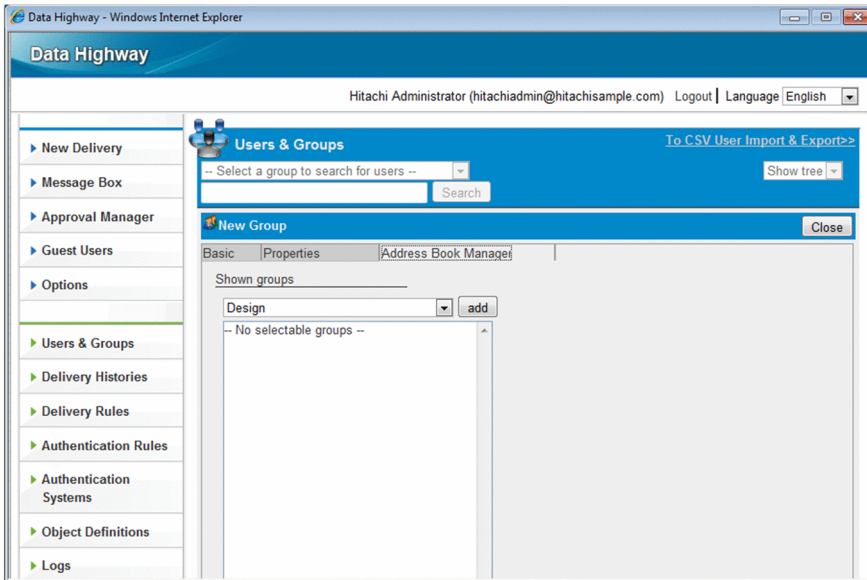
#1

If an electronic certificate is used, it will expire on December 31, 2037. When an account created in this window expires before that date, the user with that account will no longer be able to log in to JP1/DH - Server.

#2

The check box might not appear depending on the setting.

5. Configure the settings in the **Address Book Manager** tab.



The following table describes the items in this tab.

Table 3–21: Setting items in the Address Book Manager tab

Item	Description
Shown groups list box	Specifies groups that are listed in the address book. You can select a group in the group selection drop-down list box and then click the add button. The drop-down list box lists all groups in the domain. The groups you specify here, together with all users in those groups, are listed in the address book.

- Click the **Create** button.
The group is now created.

(9) Editing a group

To edit a group:

- In the sidebar area, click **Users & Groups**.
The Users & Groups window appears in the content area.
- Click the group you want to edit, and then select **Edit**.
The Edit Group window appears.
- Change the settings.
For details about items in the **Basic**, **Properties**, and **Address Book Manager** tabs, see (8) *Creating a group*.
- Edit the **Group Administration** tab.
In the **Group Administration** tab, you can add or delete group managers. The **Group Administration** tab is not visible for the top-level group.

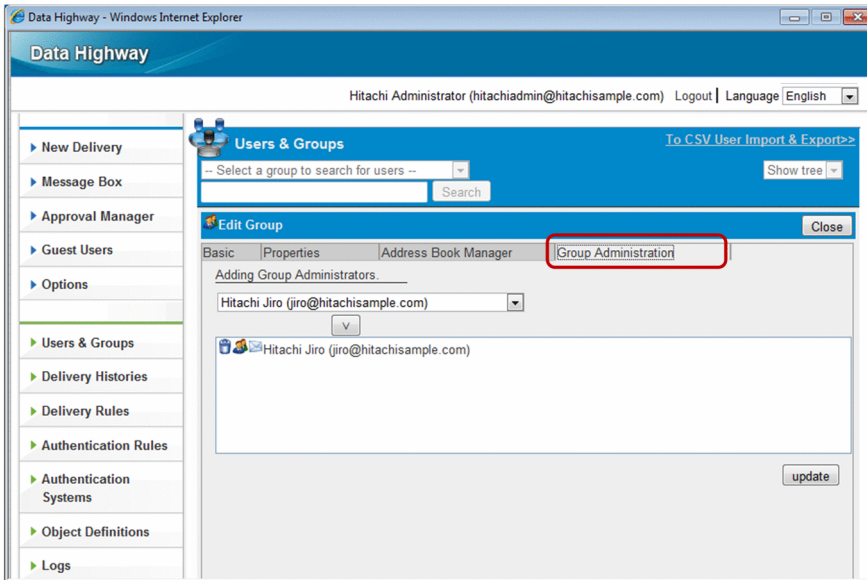



Table 3–22: Items in the Group Administration tab

Item	Description
Users list box	Lists all users in the group you are currently editing. Clicking the v button adds the selected user to the group manager list.
Group managers list box	Lists all group managers. To delete a group manager in the list, click the  icon to the left of the group manager you want to delete.

5. Click the **update** button.

The group settings are updated.

(10) Activating, inactivating, or deleting a group

To activate, inactivate, or delete a group:

1. In the sidebar area, click **Users & Groups**.
The Users & Groups window appears in the content area.
2. Click the target group of your action, and then select the menu item for it.

Table 3–23: Activating, inactivating, or deleting a group

Item	Description
Activate	Activates a group. This action does not change the state of users in the group.
Inactivate[#]	Inactivates a group. Users in the inactivated group are no longer able to use JP1/DH - Server. If an inactivated group is activated, it becomes available again, but the users in that group remain inactivated. You need to activate the users separately.
Delete[#]	Deletes a group. This action also deletes users in the group and related delivery rules and authentication rules. The deleted group cannot be restored.

#

A user who belongs to multiple groups is not inactivated or deleted.

3. A confirmation dialog box appears depending on your choice. Click the **OK** button to perform the action.

3.4.3 Delivery Histories

This subsection describes how to operate delivery history.

(1) Viewing or deleting delivery history

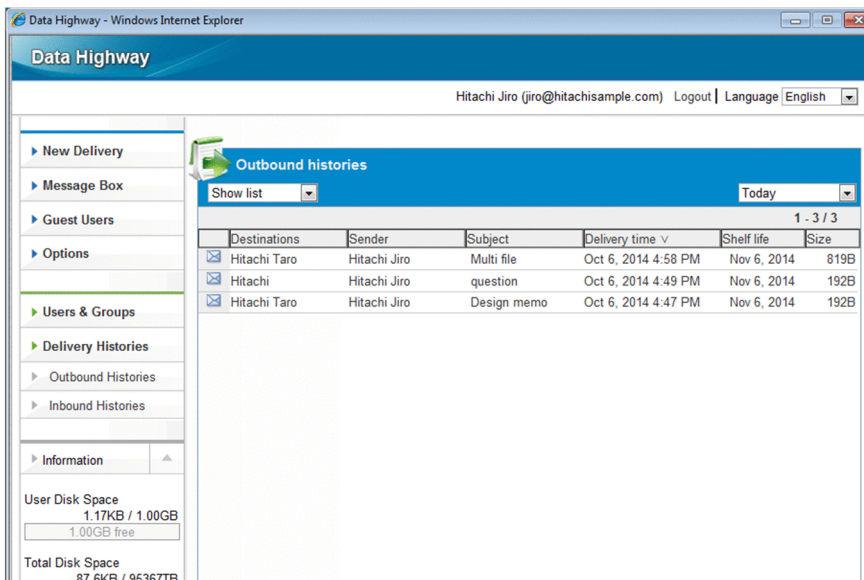
To view or delete delivery history:

1. In the sidebar area, click **Delivery Histories** and then **Outbound Histories** or **Inbound Histories**.

If you click **Outbound Histories**, the Outbound histories window appears, and if you click **Inbound Histories**, then the Inbound histories window appears in the content area.

Group managers can see delivery history records of users in the groups that they manage. Representative users can see all delivery history records.

- Outbound histories window



- Inbound histories window

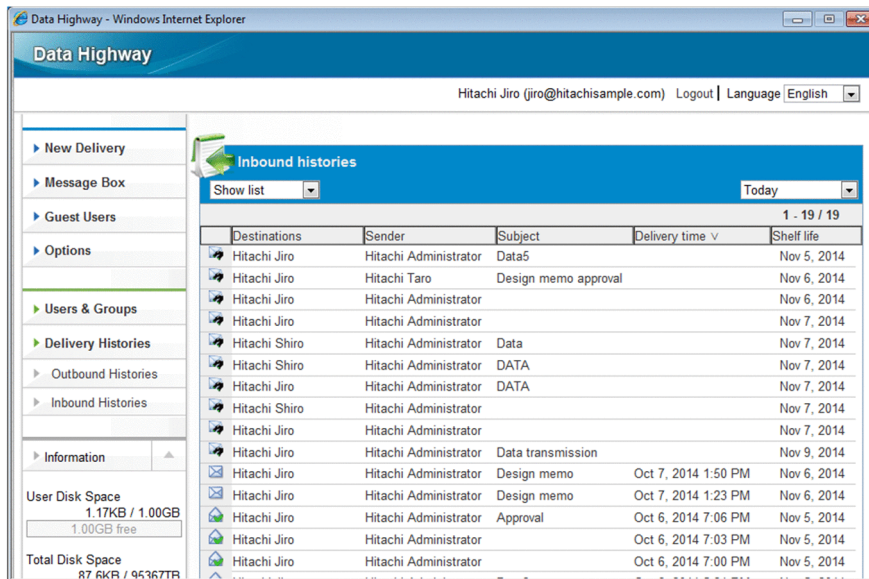


Table 3–24: Setting items in the Outbound histories and Inbound histories windows

Item	Description
Display style drop-down list box	You can select either of the following display styles: <ul style="list-style-type: none"> • List • Abstract
Display period drop-down list box	You can filter the list by time period. Filtering criteria depends on the date and time of the existing history records. The display periods for each option are as follows: <ul style="list-style-type: none"> • Today: The present day • This week: From last Sunday to today • A week ago: From two Sundays ago to today • Two weeks ago: From three Sundays ago to today • Three weeks ago: From four Sundays ago to today • A month ago: From the first day of the last month to today <p>If the specified time period includes a day or days of the previous month, the period starts from the first day of the current month.</p> <p>If there are history records over the past one month or more, the list items you can select are displayed in the form of <i>MM YYYY</i>.</p>

2. Click the menu icon and then select **Show more info.** to view the detailed history information.

The outbound histories detailed information or inbound histories detailed information window appears. A deleted or inactivated sender cannot view the detailed information.

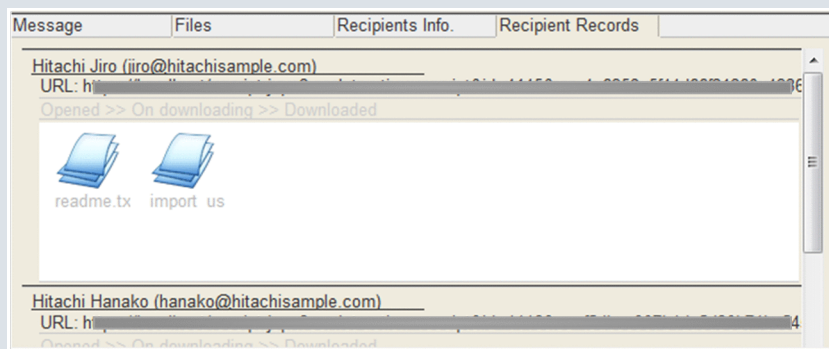
3. Check the information in the outbound histories detailed information or inbound histories detailed information window. Each tab of these windows shows the following:

- **Message** tab: Displays messages that the user sent or received.
- **Files** tab: Displays the file name, size, and other detailed file information. Click the **Download** button to download the file.
- **Recipients Info.** tab: Displays the recipient-related information.
- **Recipient Records** tab: Displays the receiving status of the recipients.
- **Approver List** tab: Displayed only if the delivery requires approval, in the outbound histories detailed information window. You can view the list of approvers. However, if all the approvers are deleted, the **Approver List** tab is not displayed.

Tip

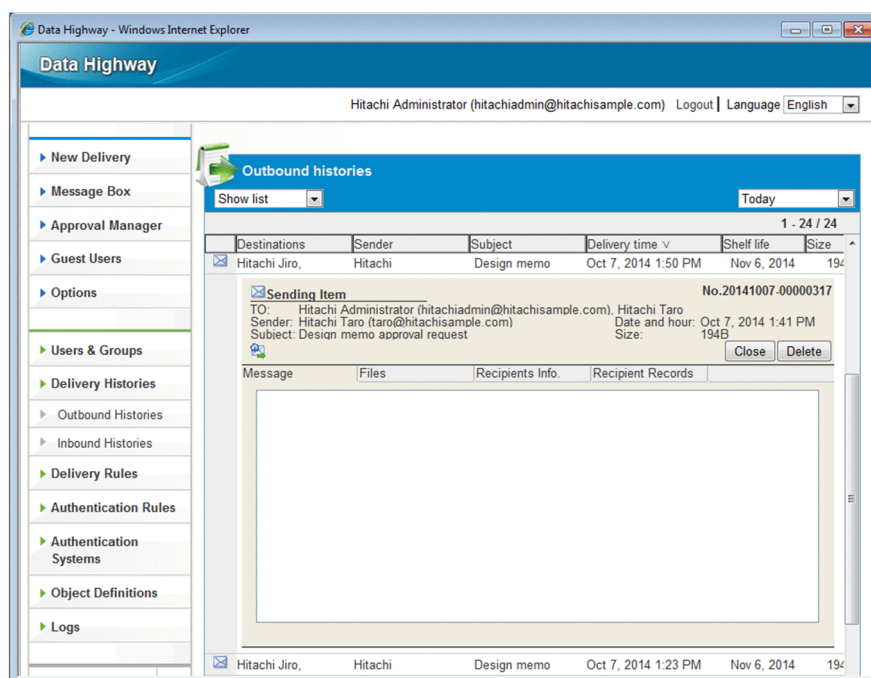
If a user sent two and more files at once, the user can check which files are downloaded by the recipient in the **Recipient Records** tab. If the files have not been downloaded, the names of the files are displayed in gray.

However, if a user receives a file without using the In-box window, or without accessing the URL written in a delivery notification email, the file is not marked as downloaded.

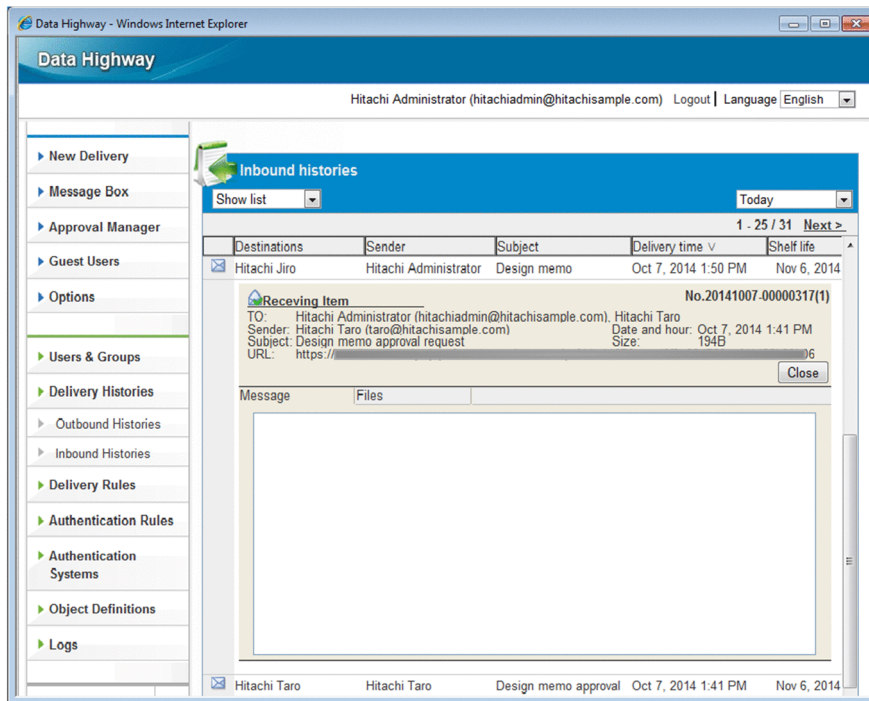


4. Click the **Close** button to return back to the Outbound histories or Inbound histories window.

- Outbound histories detailed information window



- Inbound histories detailed information window



5. To delete a history record in the Outbound histories window, click the menu icon of the history record you want to delete, and then select **Delete**.

The **Delete** button only appears in the outbound histories detailed information window.

6. Click the **OK** button to delete the history record.

3.5 Representative-user operations

This section describes what operations representative users can perform.

3.5.1 List of operations

The following table describes and lists operations performed by representative users.

Table 3–25: List of representative-user operations

Function or category	Operation	Related subsection
Users & Groups (batch management)	Creating multiple users and groups at a time	3.5.2(2)
	Viewing multiple users and groups at a time	3.5.2(3)
	Deleting multiple users at a time	3.5.2(4)
Delivery Rules	Creating a delivery rule	3.5.3(1)
	Editing a delivery rule	3.5.3(2)
	Activating, inactivating, or deleting a delivery rule	3.5.3(3)
	Creating a delivery policy	3.5.3(4)
	Editing a delivery policy	3.5.3(5)
	Deleting a delivery policy	3.5.3(6)
Authentication Rules	Creating an authentication rule	3.5.4(1)
	Editing an authentication rule	3.5.4(2)
	Activating, inactivating, or deleting an authentication rule	3.5.4(3)
	Creating an authentication policy	3.5.4(4)
	Editing an authentication policy	3.5.4(5)
	Deleting an authentication policy	3.5.4(6)
Authentication Systems	Creating an authentication system	3.5.5(1)
	Editing an authentication system	3.5.5(2)
	Deleting an authentication system	3.5.5(3)
Object Definitions	Creating a network set	3.5.6(2)
	Editing a network set	3.5.6(2)
	Deleting a network set	3.5.6(3)
	Creating an approval route	3.5.6(4)
	Editing an approval route	3.5.6(5)
	Deleting an approval route	3.5.6(6)
Logs	Downloading audit log files	3.5.7(1)

3.5.2 Users & Groups (batch management)

(1) Notes on creating the CSV file used for batch management

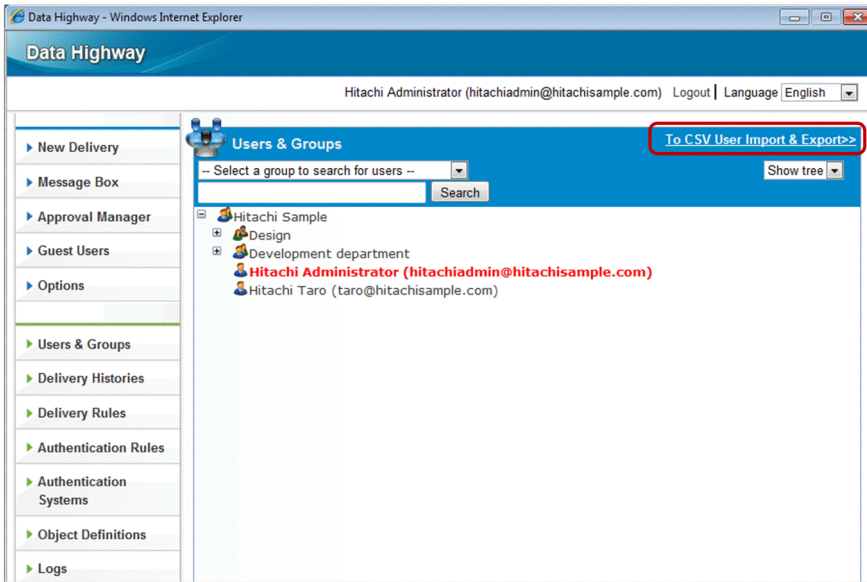
In Users & Groups (batch management), you create a CSV file and use it to create, view, or delete multiple users at a time. When you create a CSV file, be careful regarding the following:

- The first line of the CSV file must be empty.
- The CSV file must use the UTF-8 encoding. Importing a CSV file encoded in any other character encoding, such as S-JIS, might result in corrupted characters of registered users and groups. In addition, an attempt to delete users by using a file in other character encoding might delete unintended users because some users in the file are not properly identified.
- An entry containing a comma (,) and line feed must be enclosed in double quotation marks (").
- An entry containing a double quotation mark (") must be escaped with another double quotation mark (which means ""), and the entry itself must also be enclosed in double quotation marks. If the entry is not enclosed, an empty or truncated value might be stored in the system.
- The CSV file must use CRLF as a line feed code. If CR or LF is used, the file might not be read properly.
- If any surrogate pair is in an entry, less characters can be entered than the default length in the entry.
- Do not modify the identifier or the header row.
- No empty line must be between records. However, an empty line is required to separate major sections ([users], [groups], [binders], and [managers] definition sections).
- While CSV file importing is in progress, you might have to wait for importing to complete before you can perform any action against the user who imported the file and users and groups that are in the CSV file. In this case, the action will resume after the CSV file is imported.
- If a failure occurs on the server during a CSV file import, data to be imported is not stored on the server. However, if an error occurs on a client and the client cannot show the result of the import processing performed on the server, the processing itself is completed successfully when the server processed the data properly. You can see the result of the processing performed on the server in the audit log.
- When a CSV file is exported, a password is output as a password digest, which is the same value as the password digest used in standard authentication.

(2) Creating multiple users and groups at a time

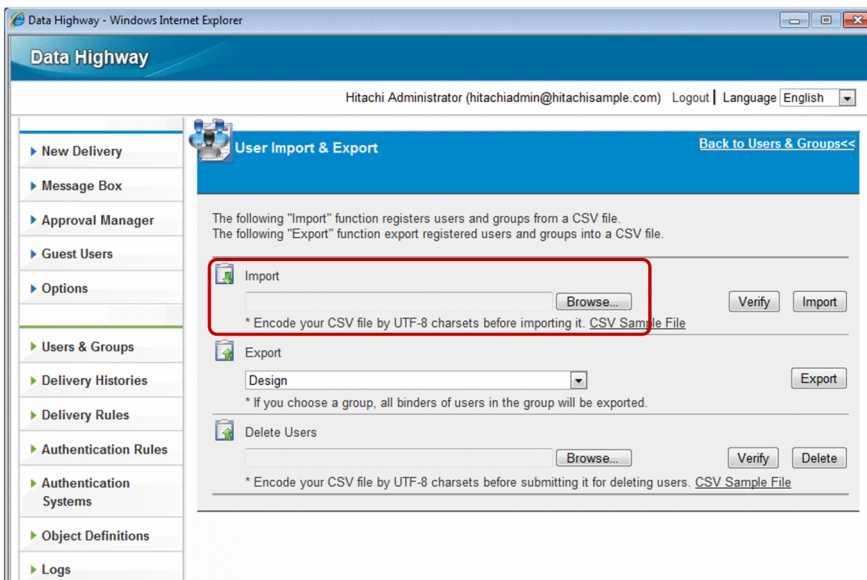
To create multiples users and groups at a time:

1. In the sidebar area, click **Users & Groups**.
The Users & Groups window appears in the content area.
2. In the upper right corner of the content area, click **To CSV User Import & Export**.
The User Import & Export window appears in the content area.



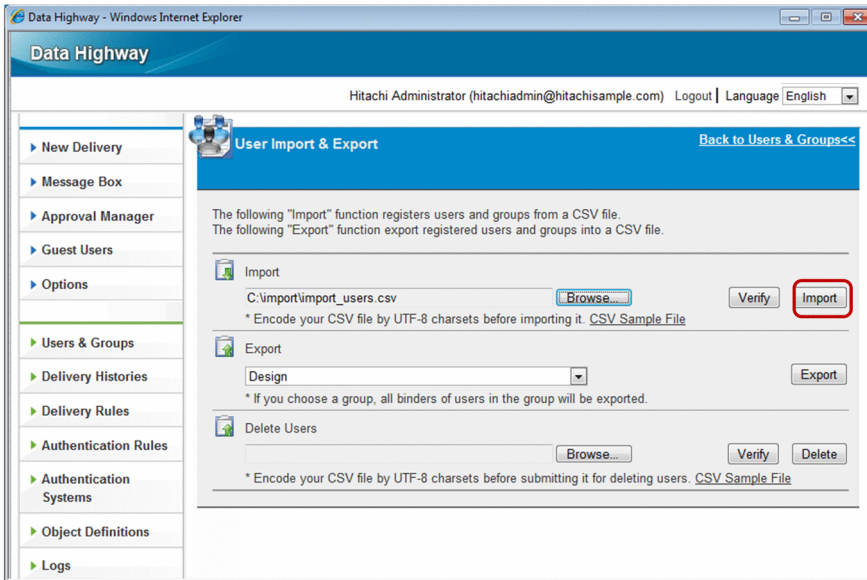
3. Specify the CSV file for import. You can directly enter the full path to the CSV file for import in the **Import** field, or click the **Browse...** button to select the file.

See (a) *Format of a CSV file for import* and create the CSV file for import beforehand.



4. Click the **Verify** button to check whether your CSV file for import is in the valid format.

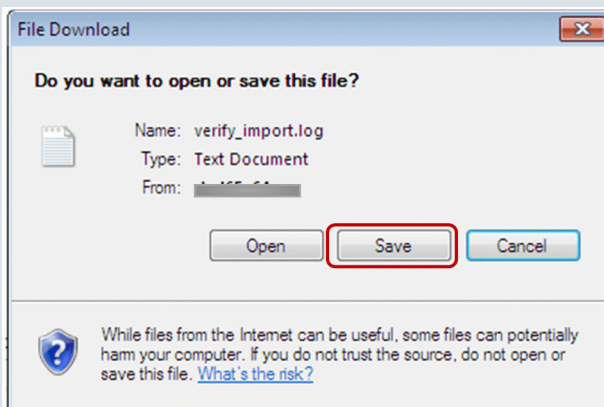
For details about what is checked by clicking the **Verify** button, see (b) *What is verified when the Verify button is clicked*.



5. After the File Download dialog box opens for downloading the file `verify_import.log`, click the **Save** button.

Important note

If nothing happens except for the window being refreshed, the file might not exist in the specified file path. In this case, specify the correct file path and click the **Verify** button again.



6. Open the saved file `verify_import.log` in UTF-8 encoding, and check the last line of the file. If you see the word OK in the last line, your CSV file for import is in the valid format. Make sure that the characters in each record (discussed later) are not corrupted.

Important note

If they are corrupted, the CSV file for import might not be encoded in UTF-8.

If you allow the import processing to proceed, users and groups might be stored in the system, with corrupted characters.

```

import_users.csv - Notepad
File Edit Format View Help

[users]
USER_ID,EMAIL,PASSWORD,NAME,NAME_EN,NAME_KANA,LANG,MEMO,EXPIRE_DATE,QUOTA,USE_USER_OPTION,USE
hanako@hitachisample.com,hanako@hitachi.com,text:HEX:5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8,,Hi
hitachiadmin@hitachisample.com,hitachiadmin@hitachisample.com,text:HEX:5baa61e4c9b93f3f0682250b6c
jiro@hitachisample.com,jiro@hitachisample.com,text:HEX:5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8,,
taro@hitachisample.com,taro@hitachisample.com,text:HEX:5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8,,

[groups]
NAME_EN,NAME_JA,PARENT_NAME_EN,FOR_GUEST,EXPIRE_DATE,QUOTA,USE_USER_OPTION,USER_REGISTERABLE,I
Design,設計部,Hitachi Sample,TRUE,,100,TRUE,FALSE,TRUE
Development department,開発部,Hitachi Sample,FALSE,,TRUE,TRUE,FALSE

[binders]
USER_ID,GROUP_NAME_EN,FLAG_DELETE
hanako@hitachisample.com,Design,FALSE
hitachiadmin@hitachisample.com,Hitachi Sample,FALSE
jiro@hitachisample.com,Development department,FALSE
taro@hitachisample.com,Hitachi Sample,FALSE

[managers]
USER_ID,GROUP_NAME_EN
jiro@hitachisample.com,Development department

```

If you see the word NG in the last line, your CSV file for import is not in the valid format. A verification result and an error description (for an error) are appended to each record (discussed later).

In this case, fix the cause of the error and then click the **Verify** button again.

```

verify_import[1].log - Notepad
File Edit Format View Help

[groups]
NAME_EN,NAME_JA,PARENT_NAME_EN,FOR_GUEST,EXPIRE_DATE,QUOTA,USE_USER_OPTION,USER_REGISTERABLE,I
NPUT_ANY_ADDRESS
General,総務部,Hitachi Sample,TRUE,,100,TRUE,FALSE,TRUE,SKIPPED
Development department,開発部,Hitachi Sample,FALSE,,TRUE,TRUE,FALSE NG,The group (Development
department) already exists. (NAME_EN) "Users, groups, binders or managers cannot be parsed
(usersParsed=false,groupsParsed=true,bindersParsed=true,managersParsed=true)."

[binders]
USER_ID,GROUP_NAME_EN,FLAG_DELETE
hanako@hitachisample.com,Design,FALSE NG,This user already belongs to this group (Design)
(USER_ID). "Users, groups, binders or managers cannot be parsed
(usersParsed=false,groupsParsed=true,bindersParsed=true,managersParsed=true)."
saboro@hitachisample.com,Hitachi Sample,FALSE,NG,A user ID (saboro@hitachisample) was not found in
the input csv data and the database. "Users, groups, binders or managers cannot be parsed
(usersParsed=false,groupsParsed=true,bindersParsed=true,managersParsed=true)."

[managers]
USER_ID,GROUP_NAME_EN
saboro@hitachisample.com,Development department,SKIPPED

NG

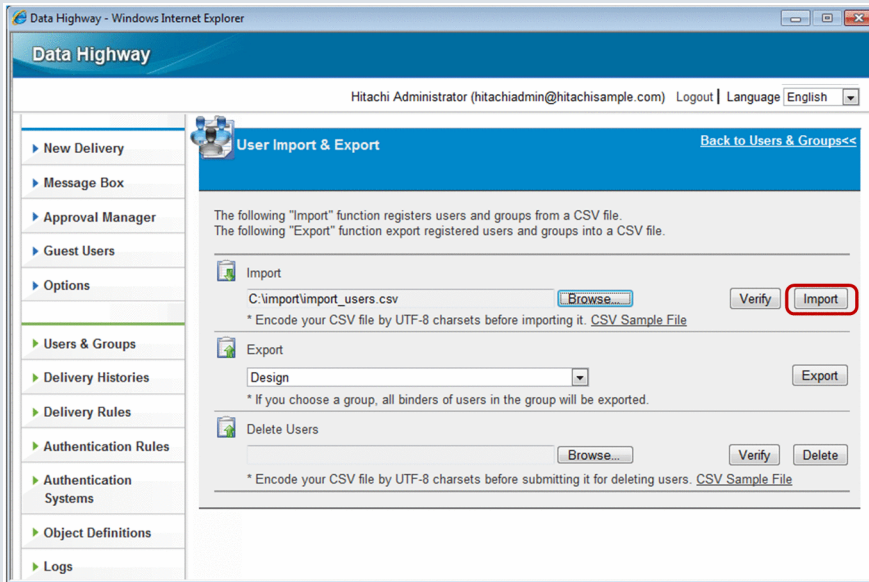
```

7. After you verify that your CSV file for import is correctly formatted, click the **Import** button to import it.

If a great number of users and groups are imported, it can take about five minutes for the import.

Important note

After clicking the **Import** button, do not do anything on the window until downloading `verify_import.log` starts. If you work with the window, the server keeps processing the import of the file, but you might not be able to obtain the file `verify_import.log` and might receive an unknown result.



8. After a dialog box opens for downloading the file `verify_import.log` in the same way as when you click the **Verify** button, click the **Save** button.

Important note

If nothing happens except for the window being refreshed, the file might not exist in the file path specified in the **Import** field. In this case, specify the correct file path and click the **Import** button again.

9. Open the saved file `verify_import.log` and check the last line of the file. If you see the word **OK** there, your batch creation of users and groups was successful.

If you see the word **NG**, a verification result and an error description (for an error) are appended to each record (discussed later). In this case, fix the cause of the error and then click the **Import** button again.

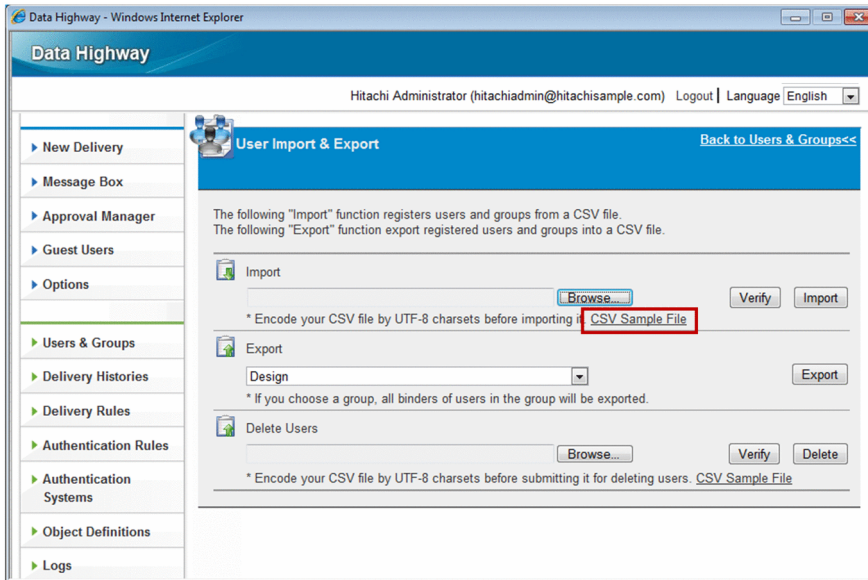
Important note

In batch creation of users and groups, either all or none of the records are stored. The entire processing is successful only if all the records are successfully processed. If one of the records fails to be processed, the entire processing is unsuccessful.

(a) Format of a CSV file for import

You can download and save the file `sample CSV file for import` by clicking the **CSV Sample File** link in the User Import & Export window.

You can easily create users and groups in batches by editing and modifying the record part in the saved file to users and groups you want to create.



The following figure illustrates the file sample CSV file for import.

Figure 3–2: Sample CSV file for import (four sections)

- : [users] definition section
 : [groups] definition section
 : [binders] definition section
 : [managers] definition section

```

[users]
USER_ID,EMAIL,PASSWORD,NAME,NAME_EN,NAME_KANA,LANG,MEMO,EXPIRE_DATE,QUOTA,USE_USER_OPTION,USE_GUEST_USERS,INPUT_ANY_ADDRESS
user1@company,user1@mailaddress.com,password,1-1,User 1,1-1,ja,,,,,
user2@company,user2@mailaddress.com,password,1-2,User 2,1-2,ja,1-2020/12/31,1024,TRUE,TRUE,TRUE
user3@company,user3@mailaddress.com,password,1-3,User 3,1-3,ja,1-3000
ε,UNLIMITED,1024,TRUE,TRUE,FALSE

[groups]
NAME_EN,NAME_JA,PARENT_NAME_EN,FOR_GUEST,EXPIRE_DATE,QUOTA,USE_USER_OPTION,USER_REGISTRABLE,INPUT_ANY_ADDRESS
Group 1,グループ1,Company,,,,,
Group 2,グループ2,Company,FALSE,,,TRUE,FALSE,TRUE
Group 3,グループ3,Group 1,TRUE,2015/12/31,1024,TRUE,FALSE,FALSE

[binders]
USER_ID,GROUP_NAME_EN,FLAG_DELETE
user1@company,Group 1,FALSE
user2@company,Group 2,FALSE
user3@company,Group 3,FALSE

[managers]
USER_ID,GROUP_NAME_EN
user1@company,Group 1
user2@company,Group 2
  
```

The CSV file for import consists of four major sections: [users], [groups], [binders], and [managers] definition sections.

The table below describes each major section. One or more empty lines are required between each major section.

Table 3–26: Major sections in the CSV file for import

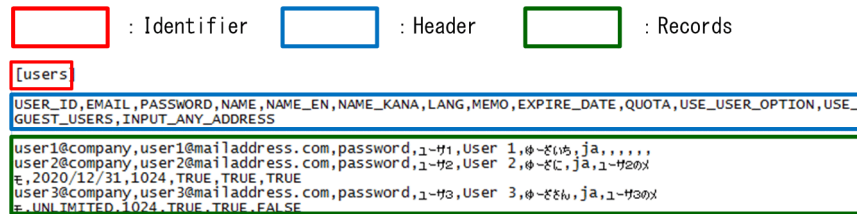
Major section	Description
[users] definition section	Defines user information to be created. Those users must be associated with any group in the [binders] definition section.
[groups] definition section	Defines group information to be created.
[binders] definition section	Associates users with groups. Users who have already been created or who are defined in the [users] definition section can be associated with or disassociated from groups.

Major section	Description
[managers] definition section	Defines group-manager users.

[users] definition section

This definition section specifies user information for creating a user or users. The [users] definition section consists of three elements, as shown in the following sample [users] definition section.

Figure 3–3: Sample CSV file for import ([users] definition section)



Identifier

This string is fixed, and specifies that the [users] definition section starts from the next line. Even if no user is created (there is no record), it is mandatory.

Header

This string is fixed, and indicates entry names of records. Even if no user is created (there is no record), it is mandatory.

Records

A record defines entries for one user to be created in a single row, separated by commas (,). The maximum number of records is 300. If optional entries are omitted, commas cannot be omitted.

The users defined in this section must be associated with any group in the [binders] definition section. The users associated with user groups in the [binders] definition section can be created as general users.

If the users are associated with guest groups, they can be created as guest users. The number of times a created guest user can send a file is set to zero. If you want to change this number of times, change it separately.

The following table describes and lists each entry in this definition section.

Table 3–27: CSV entries in the [users] definition section

No.	Entry	Meaning	Description	Omit
1	USER_ID	User ID	<p>Specify the user ID.</p> <ul style="list-style-type: none"> Format: <i>any-string</i> + @ + <i>domain-name</i> If a directory server is used to authenticate users who attempt to log in to JP1/DH - Server, the user ID must be specified in the following format: <i>user-ID-defined-in-the-directory-server</i> + @ + <i>domain-name</i>. The domain name is the same as that of the representative user. The user ID must be unique within a domain. You can enter no more than 100 (for Windows) or 256 (for Linux) alphanumeric characters and symbols, including the ID assigned to the domain. You cannot specify the same user ID as that for an existing user. If the domain (the string after the at mark (@)) does not exist or is different from the domain of the representative user, an error occurs. Some symbols (/ \ ? * : " < > # @ ^ [] \$) and space characters are not available. A user ID consisting of only a period or periods (.) is not available. 	Not allowed

No.	Entry	Meaning	Description	Omit
1	USER_ID	User ID	<ul style="list-style-type: none"> Reserved words in Windows are not available. For details about reserved words in Windows, see 3.4.2(2) Creating a user. Example: <code>user1@company</code>	Not allowed
2	EMAIL	Email address	Specify the email address. You cannot specify the same email address as that for an existing user. <ul style="list-style-type: none"> You can enter no more than 256 alphanumeric characters and symbols. Some symbols (<code>/\?* : "<>^</code>) and space characters are not available. Example: <code>user1@mailaddress.com</code>	Not allowed
3	PASSWORD	Password	Specify the password. JP1/DH - Server manages the password specified here. If a directory server is used to authenticate users, specify the JP1/DH - Server password, instead of using the password managed by the directory server. You cannot change the password managed by the directory server here. You need to define the password string ^{#1} in clear text or in the digest of the password string ^{#2} in hexadecimal format. Example in clear text: <code>password</code> In digest format, a digest string of 40 characters must be followed by the prefix <code>text:HEX:</code> . The digest string is case-insensitive. You can use the digest found in the password field when user data is exported. Example in digest format <pre>text:HEX: 5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8</pre> A string that starts with the string <code>text:HEX:</code> cannot be used as a clear text password.	Not allowed
4	NAME	Name (Japanese/Chinese)	Specify the name in Japanese or Chinese. If this entry is specified, the <code>NAME_EN</code> entry is mandatory. If omitted, an empty value is stored. <ul style="list-style-type: none"> You can enter no more than 256 characters. Some symbols (<code>/\?* : "<>#^[] \$</code>) are not available. A name consisting of only spaces or periods (<code>.</code>) is not available. Example: ユーザ ¹	Allowed
5	NAME_EN	Name (English)	Specify the name in English. If omitted, an empty value is stored. <ul style="list-style-type: none"> You can enter no more than 100 (for Windows) or 256 (for Linux) alphanumeric characters and symbols. Some symbols (<code>/\?* : "<>#^[] \$</code>) are not available. A name consisting of only spaces or periods (<code>.</code>) is not available. Example: <code>User 1</code>	Allowed
6	NAME_KANA	Name (Japanese kana)	Specify the name in Japanese kana characters. If omitted, an empty value is stored. <ul style="list-style-type: none"> You can enter no more than 256 characters. Some symbols (<code>/\?* : "<>#^[] \$</code>) are not available. A name consisting of only spaces or periods (<code>.</code>) is not available. Example: ゆーざいち	Allowed
7	LANG	User language	Specify one of the user languages below. This is case-insensitive.	Allowed

No.	Entry	Meaning	Description	Omit
7	LANG	User language	<ul style="list-style-type: none"> • ja: Japanese • en: English • zh: Chinese <p>If omitted, it is set to Japanese. Example: ja</p>	Allowed
8	MEMO	Note	<p>Specify a note. You can enter no more than 4,096 characters. If omitted, an empty value is stored. Example: User 1 note</p>	Allowed
9	EXPIRE_DATE	Expire date	<p>Specify the expiration date in <i>YYYY/MM/DD</i> or <i>YYYY-MM-DD</i> format. The possible date ranges from the current date to 2031/12/31 (Dec. 31, 2031).</p> <p>If omitted, the entry is either of the following case, depending on the type of the first group in the [binders] definition section:</p> <ul style="list-style-type: none"> • For a member of the user group: The entry inherits the property value from the group. • For a member of the guest group: The entry is the date when this user is imported. <p>If the string UNLIMITED is specified, the account never expires. However, if the account is associated with the guest group in the [binders] definition section, the entry is the date when this user is imported.</p> <p>The system ignores any space, line feed, and tab characters in the entry string. These characters cannot be between <i>YYYY</i>, <i>MM</i>, and <i>DD</i> arguments. Example: 2020/12/31</p>	Allowed
10	QUOTA ^{#3}	Amount of storage space	<p>Specify the amount of storage space in MB. The possible value ranges from 0 to 8,796,093,022,207. Example: 1024</p>	Allowed
11	USE_USER_OPTION ^{#3}	Is Options allowed	<p>Specify whether the user is allowed to use the Options function in either of the values below. This is case-insensitive.</p> <ul style="list-style-type: none"> • TRUE: Allowed • FALSE: Not allowed <p>Example: TRUE</p>	Allowed
12	USE_GUEST_USERS ^{#3}	Is Guest Users allowed	<p>Specify whether the user is allowed to use the Guest Users function in either of the values below. This is case-insensitive.</p> <ul style="list-style-type: none"> • TRUE: Allowed • FALSE: Not allowed <p>Example: TRUE</p>	Allowed
13	INPUT_ANY_ADDRESS ^{#3}	Is any recipient address allowed	<p>Specify whether the user is allowed to enter any recipient address in either of the values below. This is case-insensitive.</p> <ul style="list-style-type: none"> • TRUE: Allowed • FALSE: Not allowed <p>Example: TRUE</p>	Allowed

#1

You can use alphanumeric characters and symbols in a given length and type as defined by authentication rules. The symbols of !"#%&'()*+,-./:;<=>?@[\\]^_`{|}~ are available.

#2

A digest is a form of the password in which JP1/DH - Server stores passwords in its database, and from which the actual password string cannot be guessed. The export function outputs the password information in the form of digest into the password entry in the CSV file for export.

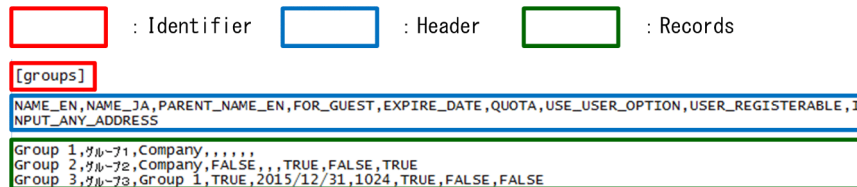
#3

If omitted, the entry inherits the property value from the first group associated in the [binders] definition section. For the INPUT_ANY_ADDRESS entry, the entry itself can be omitted.

[groups] definition section

This definition section specifies group information for creating a group or groups. The [groups] definition section consists of three elements, as shown in the following sample [groups] definition section.

Figure 3–4: Sample CSV file for import ([groups] definition section)



Identifier

This string is fixed, and specifies that the [groups] definition section starts from the next line. Even if no group is created (there is no record), it is mandatory.

Header

This string is fixed, and indicates entry names of records. Even if no group is created (there is no record), it is mandatory.

Records

A record defines entries for one group to be created in a single row, separated by commas (,). If optional entries are omitted, commas cannot be omitted.

The following table describes and lists each entry in this definition section.

Table 3–28: CSV entries in the [groups] definition section

No.	Entry	Meaning	Description	Omit
1	NAME_EN	Group name (English)	Specify the name of the group in English. You cannot specify the same English group name as that for an existing group. <ul style="list-style-type: none"> You can enter no more than 200 alphanumeric characters and symbols. Some symbols (/ \ ? * : " < > @ ^) are not available. A name consisting of only spaces or periods (.) is not available. Example: Group 1	Not allowed
2	NAME_JA	Group name (Japanese/Chinese)	Specify the name of the group in Japanese or Chinese. You cannot specify the same Japanese or Chinese group name as that for an existing group. <ul style="list-style-type: none"> You can enter no more than 200 characters. Some symbols (/ \ ? * : " < > @ ^) are not available. A name consisting of only spaces or periods (.) is not available. Example: グループ1	Not allowed
3	PARENT_NAME_EN	Parent group name (English)	Specify the name of the parent group in English. You cannot specify the name of a parent group that does not exist. The possible characters are the same as those for the NAME_EN entry. Example: Company	Not allowed

No.	Entry	Meaning	Description	Omit
4	FOR_GUEST	Group type	Specify whether the group is for guest users in either of the values below. This is case-insensitive. <ul style="list-style-type: none"> • TRUE: For the guest group • FALSE: For the user group If omitted, it is set to FALSE (which is for the user group). Example: TRUE	Allowed
5	EXPIRE_DATE	Expire date	Specify the expiration date in YYYY/MM/DD or YYYY-MM-DD format. The possible date ranges from the current date to 2031/12/31 (Dec. 31, 2031). If the string UNLIMITED is specified, the account never expires. If omitted, the account also never expires. The system ignores any space, line feed, and tab characters in the entry string. These characters cannot be between YYYY, MM, and DD arguments. Example: 2015/12/31	Allowed
6	QUOTA	Amount of storage space	Specify the amount of storage space in MB. If omitted, it is set to 1 GB. The possible value ranges from 0 to 8,796,093,022,207. Example: 1024	Allowed
7	USE_USER_OPTION	Is Options allowed	Specify whether the group is allowed to use the Options function in either of the values below. This is case-insensitive. <ul style="list-style-type: none"> • TRUE: Allowed • FALSE: Not allowed If omitted, it is set to TRUE (which means <i>allowed</i>). Example: TRUE	Allowed
8	USER_REGISTRABLE	Is Guest Users allowed	Specify whether the group is allowed to use the Guest Users function in either of the values below. This is case-insensitive. <ul style="list-style-type: none"> • TRUE: Allowed • FALSE: Not allowed If omitted, it is set to FALSE (which means <i>not allowed</i>). If the FOR_GUEST entry is set to TRUE, specify this entry as FALSE. Example: TRUE	Allowed
9	INPUT_ANY_ADDRESS	Is any recipient address allowed	Specify whether the group is allowed to enter any recipient address in either of the values below. This is case-insensitive. <ul style="list-style-type: none"> • TRUE: Allowed • FALSE: Not allowed This entry itself can be omitted. If omitted, it is set to FALSE (which means <i>not allowed</i>). Example: TRUE	Allowed

[binders] definition section

This definition section associates users with groups. A user can be associated with or disassociated from a group. The [binders] definition section consists of three elements, as shown in the following sample [binders] definition section.

Figure 3–5: Sample CSV file for import ([binders] definition section)

[binders] : Identifier USER_ID, GROUP_NAME_EN, FLAG_DELETE : Header user1@company, Group 1, FALSE
user2@company, Group 2, FALSE
user3@company, Group 3, FALSE : Records

[binders]

USER_ID, GROUP_NAME_EN, FLAG_DELETE

user1@company, Group 1, FALSE
user2@company, Group 2, FALSE
user3@company, Group 3, FALSE

Identifier

This string is fixed, and specifies that the [binders] definition section starts from the next line. Even if no user is associated with a group (there is no record), it is mandatory.

Header

This string is fixed, and indicates entry names of records. Even if no user is associated with a group (there is no record), it is mandatory.

Records

A record defines entries for one user-group association in a single row, separated by commas (,).

Records are processed from top to bottom. Then, if a user is not a member of any group, even temporarily, an error occurs.

If you want to move User A from Group A to Group B, define the record to associate User A with Group B first, and then define the record to disassociate User A from Group A. If optional entries are omitted, commas cannot be omitted.

The following table describes and lists each entry in this definition section.

Table 3–29: CSV entries in the [binders] definition section

No.	Entry	Meaning	Description	Omit
1	USER_ID	User ID	Specify the user ID of the user whose group is changed. <ul style="list-style-type: none"> You can enter no more than 100 (for Windows) or 256 (for Linux) alphanumeric characters and symbols. Some symbols (/ \ ? * : " < > # @ ^ [] \$) and space characters are not available. A user ID consisting of only a period or periods (.) is not available. Reserved words in Windows are not available. For details about reserved words in Windows, see 3.4.2(2) <i>Creating a user</i>. Example: user1@company	Not allowed
2	GROUP_NAME_EN	Group name (English)	Specify the English name of the group that the user is associated with or disassociated from. <p>A user who belongs to the guest group cannot be a member of the user group. A user who belongs to the user group cannot also be a member of the guest group.</p> <ul style="list-style-type: none"> You can enter no more than 200 alphanumeric characters and symbols. Some symbols (/ \ ? * : " < > @ ^) are not available. A name consisting of only spaces or periods (.) is not available. Example: Group 1	Not allowed
3	FLAG_DELETE	Deletion flag	Specify whether the user is associated with or disassociated from the group. <ul style="list-style-type: none"> TRUE: The user is disassociated from the group. FALSE: The user is associated with the group. 	Allowed

No.	Entry	Meaning	Description	Omit
3	FLAG_DELETE	Deletion flag	If omitted, it is set to FALSE.	Allowed

[managers] definition section

This definition section defines group managers. The [managers] definition section consists of three elements, as shown in the following sample [managers] definition section.

Figure 3–6: Sample CSV file for import ([managers] definition section)

[managers] : Identifier USER_ID, GROUP_NAME_EN : Header user1@company, Group 1
user2@company, Group 2 : Records

```
[managers]
USER_ID, GROUP_NAME_EN
user1@company, Group 1
user2@company, Group 2
```

Identifier

This string is fixed, and specifies that the [managers] definition section starts from the next line. Even if no group manager is defined (there is no record), it is mandatory.

Header

This string is fixed, and indicates entry names of records. Even if no group manager is defined (there is no record), it is mandatory.

Records

A record defines entries for one group manager to be defined in a single row, separated by commas (,).

The following table describes and lists each entry in this definition section.

Table 3–30: CSV entries in the [managers] definition section

No.	Entry	Meaning	Description	Omit
1	USER_ID	User ID	Specify the user ID of the user to be defined as a group manager. One user cannot be the group manager of two or more groups. <ul style="list-style-type: none"> You can enter no more than 100 (for Windows) or 256 (for Linux) alphanumeric characters and symbols, including the ID assigned to the domain. Some symbols (/ \ ? * : " < > # @ ^ [] \$) and space characters are not available. A user ID consisting of only a period or periods (.) is not available. Reserved words in Windows are not available. For details about reserved words in Windows, see 3.4.2(2) Creating a user. Example: user1@company	Not allowed
2	GROUP_NAME_EN	Group name (English)	Specify the English name of the managed group. <ul style="list-style-type: none"> You can enter no more than 200 alphanumeric characters and symbols. Some symbols (/ \ ? * : " < > @ ^) are not available. A name consisting of only spaces or periods (.) is not available. Example: Group 1	Not allowed

(b) What is verified when the Verify button is clicked

The table below describes and lists what the system verifies when the **Verify** button is clicked. During import, an error might occur because of what is not verified by the system. For details about the list of error messages, see [C. List of CSV Error Messages](#).

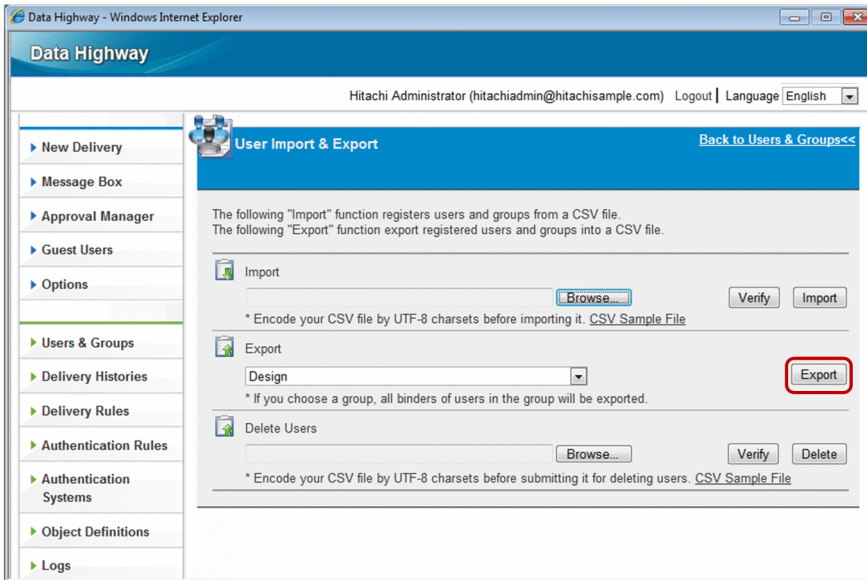
Table 3–31: Items to be verified

No.	Definition section	Item	Description
1	General	Count	The system verifies that the number of records is 300 or less.
2		Entry count	The system verifies that the number of entries for each record is the valid value.
3		Mandatory	The system verifies that the mandatory entries are not omitted.
4		Length of characters	The system verifies that the length of the string entered for each entry is within the valid value.
5		Type of characters	The system verifies that the string for each entry does not contain disallowed characters.
6		Format	The system verifies that each entry matches the format described in <i>(a) Format of a CSV file for import</i> . Example: For the <code>Expire Date</code> entry, the system verifies that it is in the range from the current date to December 31, 2031.
7		Duplication	The system verifies that any existing user does not have the same user ID or email address as those of the entered user.
8	[users] definition section	Binders	The system verifies that the specified user is also defined in the [binders] definition section.
9	[groups] definition section	Guest group	If a guest group is to be created, the system verifies that the Guest Users function is not allowed for use.
10	[binders] definition section	Existence	The system verifies that the specified user or group exists.
11	[managers] definition section	Existence	The system verifies that the specified user or group exists.

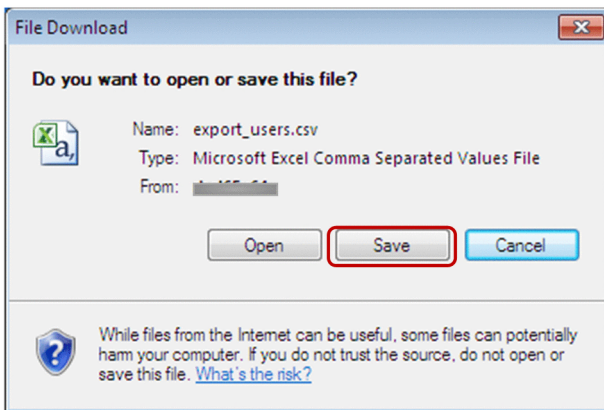
(3) Viewing multiple users and groups at a time

To view multiples users and groups at a time:

1. In the sidebar area, click **Users & Groups**.
The Users & Groups window appears in the content area.
2. In the upper right corner of the content area, click **To CSV User Import & Export**.
The User Import & Export window appears in the content area.
3. In the **Export** drop-down list box, select the group you want to view, and then click the **Export** button.



4. After downloading the CSV file for export `export_users.csv` starts, click the **Save** button to save the file. The CSV file for export contains user and group information.



(a) Format of a CSV file for export

The CSV file for export has the same format as the CSV file for import, as discussed in (2) *Creating multiple users and groups at a time*.

The following table describes record rules and record output orders for each major section.

Table 3–32: Major sections and record rules

Major section	Record rule
[users] definition section	Users in the specified group and its child groups are sorted and output to the file in dictionary order by user ID.
[groups] definition section	The specified group and its child groups are sorted and output to the file from top to bottom in the hierarchy. Multiple groups in the same level are sorted and output in dictionary order by group name (English).
[binders] definition section	Binder definition records for users in the specified group and its child groups are sorted and output to the file in dictionary order by user ID. A user in two or more groups is output several times in Groups belongs to order. In this case, any group that is not a child group of the specified group is also output.

Major section	Record rule
[managers] definition section	Group managers are sorted and output to the file in dictionary order by user ID.

(4) Deleting multiple users at a time

To delete multiples users at a time:

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

The Users & Groups window appears in the content area.

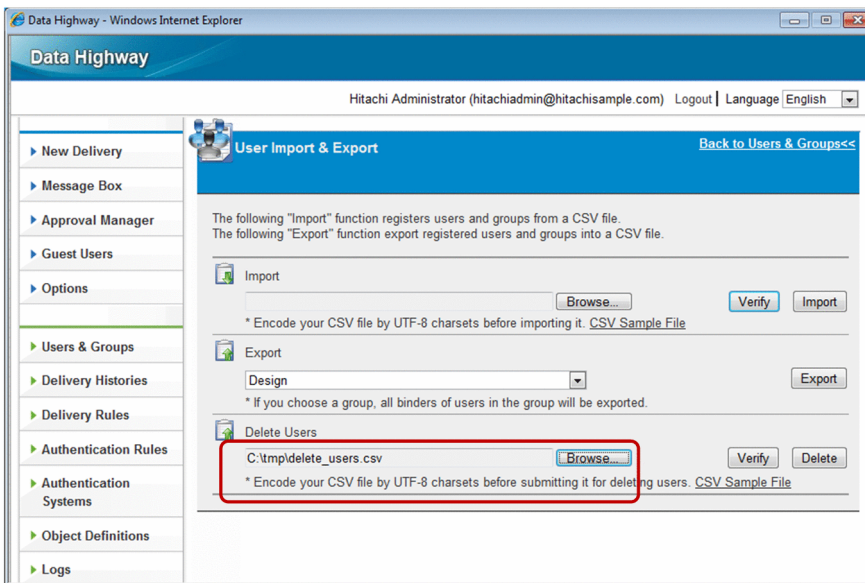
2. In the upper right corner of the content area, click **To CSV User Import & Export**.

For details about the Users & Groups window, see (2) *Creating multiple users and groups at a time*.

The User Import & Export window appears in the content area.

3. Specify the CSV file for deleting users. You can directly enter the full path to the CSV file for deleting users in the **Delete Users** field, or click the **Browse...** button to select the file.

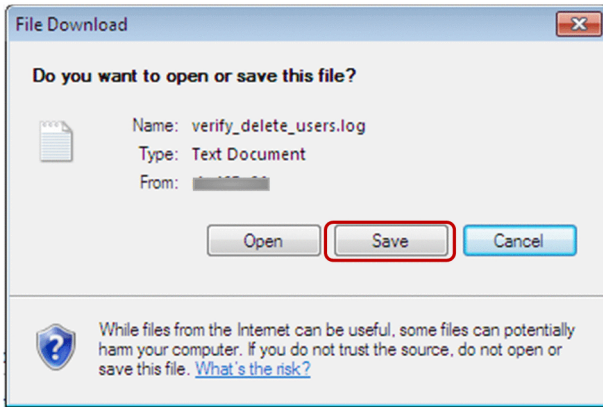
See (a) *Format of a CSV file for deleting users* and create the CSV file for deleting users beforehand.



4. Click the **Verify** button to check whether your CSV file for deleting users is in the valid format.

For details about what is checked by clicking the **Verify** button, see (b) *What is verified when the Verify button is clicked*.

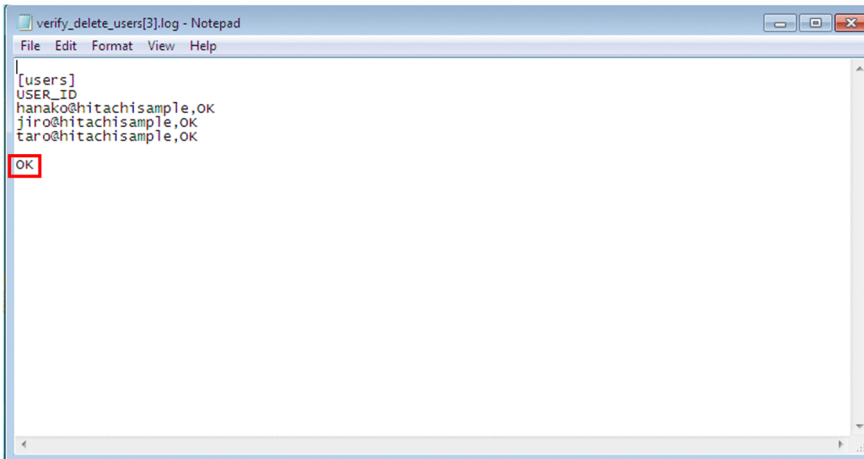
5. After downloading the file `verify_delete_users.log` starts, click the **Save** button to save the file.



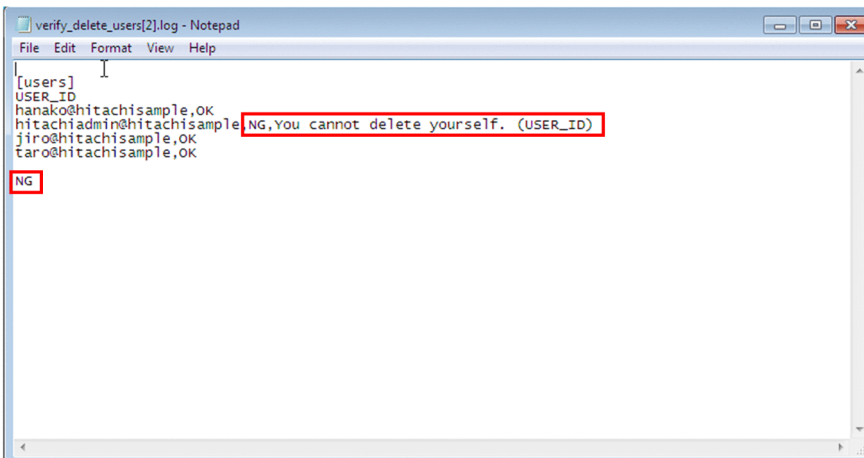
Important note

If nothing happens except for the window being refreshed, the file might not exist in the specified file path. In this case, specify the correct file path and click the **Verify** button again.

6. Open the saved file `verify_delete_users.log` and check the last line of the file.
If you see the word `OK` in the last line, your CSV file for deleting users is in the valid format.

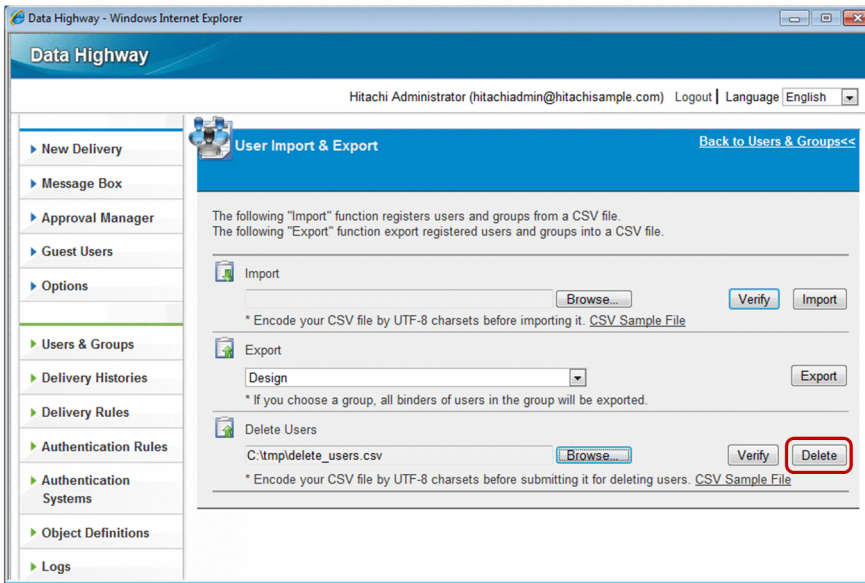


If you see the word `NG` in the last line, your CSV file for deleting users is not in the valid format. A verification result and an error description (for an error) are appended to each record (discussed later). In this case, fix the cause of the error and then click the **Verify** button again.



7. Click the **Delete** button.

After clicking the **Delete** button, do not do anything on the window until the `verify_delete_users.log` download starts. If you work with the window, the server keeps processing the deletion, but you might not be able to obtain the file `verify_delete_users.log` and might receive an unknown result.



8. Just like verifying the file, after a dialog box opens for downloading the file `verify_delete_users.log`, click the **Save** button.

Important note

If nothing happens except for the window being refreshed, the file might not exist in the file path specified in the **Delete Users** field. In this case, specify the correct file path and click the **Delete** button again.

9. Open the saved file `verify_delete_users.log` and check the last line of the file. If you see the word **OK** there, your batch deletion of users is successful.

If you see the word **NG** in the last line, your CSV file for deleting users is not in the valid format. A verification result and an error description (for an error) are appended to each record (discussed later). In this case, fix the cause of the error and then click the **Delete** button again.

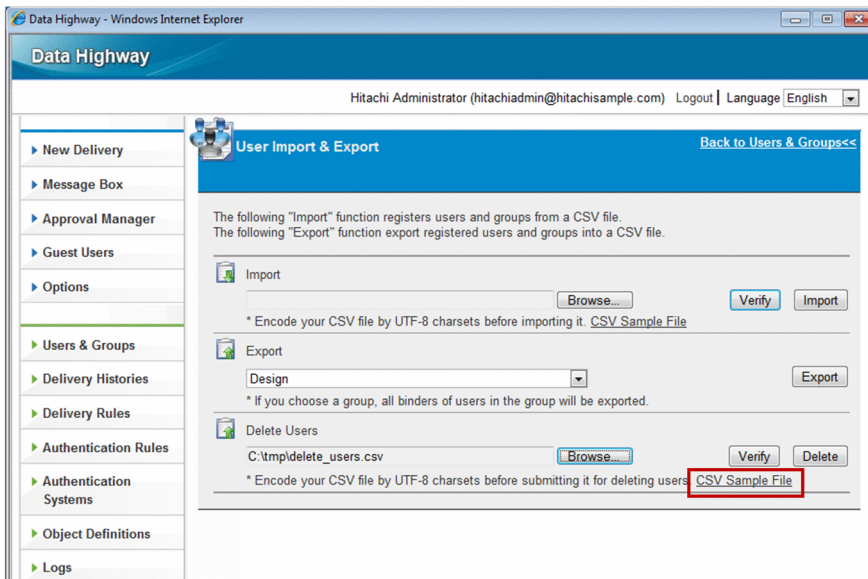
Important note

In batch deletion of users, either all or none of the records are processed. The entire processing is successful only if all the records are successfully processed. If one of the records fails to be processed, the entire processing is unsuccessful.

(a) Format of a CSV file for deleting users

You can download and save the file `sample CSV file for deleting users` by clicking the **CSV Sample File** link in the User Import & Export window.

You can easily delete users in batches by editing and modifying the record part in the saved file to users you want to delete.



The following figure illustrates the file sample CSV file for deleting users. The CSV file for deleting users only consists of the major section [users] definition section.

Figure 3–7: Sample CSV file for deleting users

: [users] definition section

```
[users]
USER_ID
hanako@hitachisample
jiro@hitachisample
taro@hitachisample
```

[users] definition section

This definition section specifies user information for deleting a user or users. The [users] definition section consists of three elements, as shown in the following sample [users] definition section.

Figure 3–8: Sample CSV file for deleting users ([users] definition section)

: Identifier : Header : Records

```
[users]
USER_ID
hanako@hitachisample
jiro@hitachisample
taro@hitachisample
```

Identifier

This string is fixed, and specifies that the [users] definition section starts from the next line. Even if no user is deleted (there is no record), it is mandatory.

Header

This string is fixed, and indicates entry names of records. Even if no user is deleted (there is no record), it is mandatory.

Records

A record defines an entry for one user to be deleted in a single row. The maximum number of records are 300. The following table describes and lists each entry in this definition section.

Table 3–33: Record entry (sample [users] definition section)

No.	Entry	Meaning	Description	Omit
1	USER_ID#	User ID	Specify the user ID of the user to be deleted. Format: <i>any-string</i> + @ + <i>domain-name</i> The domain name is the same as that of the representative user. <ul style="list-style-type: none">You cannot specify the user ID of a user if the user does not exist.You cannot delete an approver user if deleting the user causes an approval route to have no approver.You cannot delete the user representing yourself. Example: user1@company	Not allowed

#

The possible characters are the same as those when creating a user. For details, see [3.4.2\(2\) Creating a user](#).

(b) What is verified when the Verify button is clicked

The table below describes and lists what the system verifies when the **Verify** button is clicked. During import, an error might occur because of what is not verified by the system. For details about the list of error messages, see [C. List of CSV Error Messages](#).

Table 3–34: Items to be verified (sample [users] definition section)

No.	Definition section	Item	Description
1	[users] definition section	Count	The system verifies that the number of records are 300 or less.
2		Entry count	The system verifies that the number of entries for each record is the valid value.
3		Mandatory	The system verifies that the mandatory entries are not omitted.
4		Length of characters	The system verifies that the length of the string entered for each entry is within the valid value.
5		Type of characters	The system verifies that the string for each entry does not contain disallowed characters.
6		Existence	The system verifies that the specified user exists.
7		Approval route	The system verifies that the user in an approval route is not only the user specified in that approval route.
8		Operating user	The system verifies that you are not trying to delete the user representing yourself.

3.5.3 Delivery Rules

This subsection describes how to configure a delivery rule. For details about the delivery rule, see [A. Delivery Rule](#).

(1) Creating a delivery rule

To create a delivery rule:

1. In the sidebar area, click **Delivery Rules** and then **Delivery Rules**.

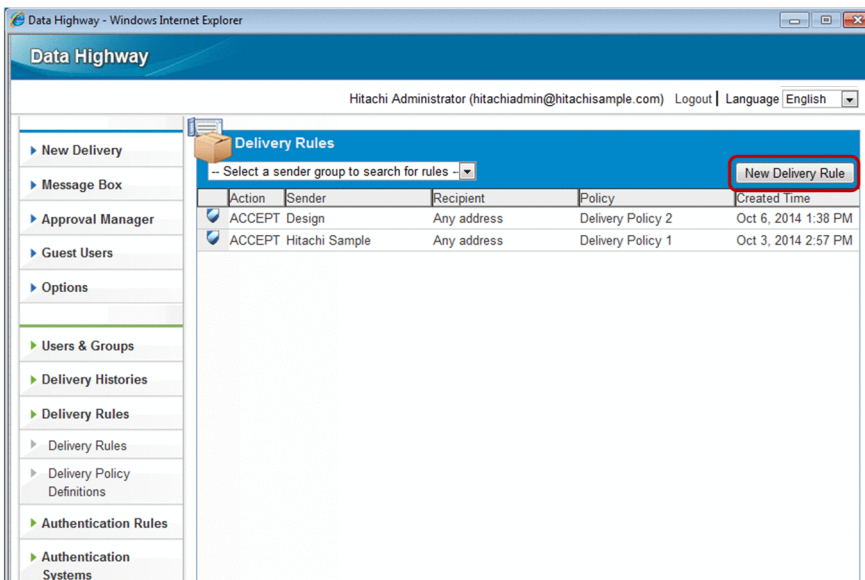
The Delivery Rules window appears in the content area.

Tip

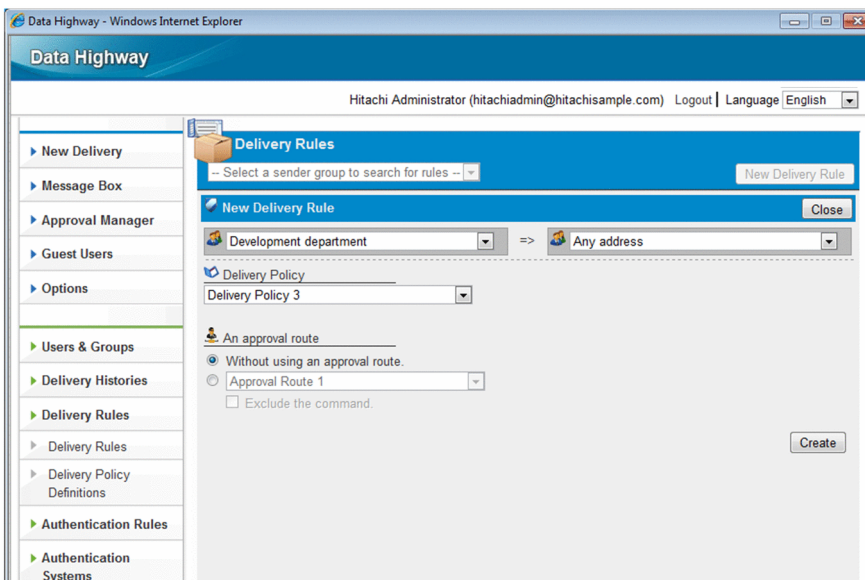
Selecting a sender group in the sender group selection drop-down list box allows you to filter delivery rules to be displayed. The filtered results contain delivery rules in which the parent group of the specified sender group is set to a sender.

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

The New Delivery Rule window appears.



3. Create a delivery rule.



The following table describes the items you specify.

Table 3–35: Settings for the delivery rule

Item	Description
Sender drop-down list box	Specify which groups the delivery rule apply to when a file and message are sent. When the Any address option is specified for the recipient, a user who is allowed to enter any recipient address can send an email message to any destination address, including an unregistered user address. You can specify an unregistered destination group for the recipient, but not for the sender.
Recipient drop-down list box	
Delivery Policy drop-down list box	Select a delivery policy to be applied. The selection of the delivery policy is mandatory. Any delivery policy that is used by another delivery rule is unavailable.
An approval route radio buttons	Specify an approval route. <ul style="list-style-type: none"> • Without using an approval route. Select this radio button if the approval route is not used. • Approval route drop-down list box The approval route selected in this drop-down list box is applied. • Exclude the command check box[#] This check box is only available if an approval route is selected. Selecting this check box skips the approval processing in JP1/Data Highway - AJE and a file is sent, even if the delivery rule has an approval route specified. This check box is selected by default. This function is available in file transfer by JP1/Data Highway - AJE 10-10 or later.

#

This check box might not appear depending on your system setting.

Tip

If the **Exclude the command** check box is selected, JP1/Data Highway - AJE actually behaves as follows:

- The system does not send an approval request email message to an approver.
- An approver does not have to accept or reject an application for approval.
- A recipient can immediately receive a file, instead of waiting for the approver to accept or reject the application for approval.
- A SKIP_DELIVERY_APPROVAL event is output to the audit log file.

4. Click the **Create** button.


The delivery rule is now created.

(2) Editing a delivery rule

To edit a delivery rule:

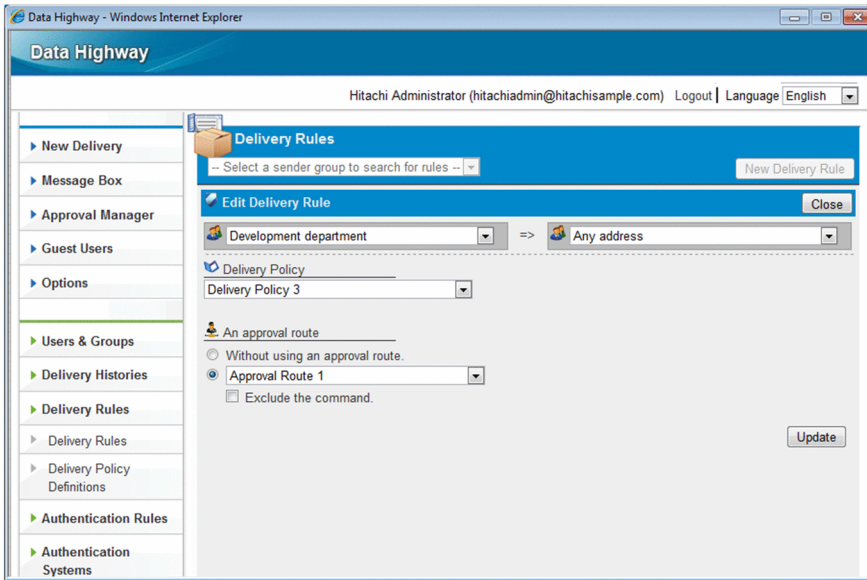
1. In the sidebar area, click **Delivery Rules** and then **Delivery Rules**.

The Delivery Rules window appears in the content area.

2. Click the menu icon () of the delivery rule you want to edit, and then select **Edit**.

The Edit Delivery Rule window appears.

3. Change the settings. For details about each item, see *(1) Creating a delivery rule*.



4. Click the **Update** button.

The delivery rule settings are updated.

(3) Activating, inactivating, or deleting a delivery rule

To activate, inactivate, or delete a delivery rule:

1. In the sidebar area, click **Delivery Rules** and then **Delivery Rules**.

The Delivery Rules window appears in the content area.


2. Click the menu icon () of your target delivery rule, and then select the menu item.

Table 3–36: Activating, inactivating, or deleting a delivery rule


Item	Description
Activate	Activates an inactivated delivery rule.
Inactivate	Inactivates a delivery rule. The inactivated delivery rule becomes unavailable. To make the inactivated rule available again, activate it.
Delete	Deletes a delivery rule. The deleted delivery rule cannot be restored.

3. A confirmation dialog box appears depending on your choice. Click the **OK** button to perform the action.

(4) Creating a delivery policy

To create a delivery policy:

Reference note

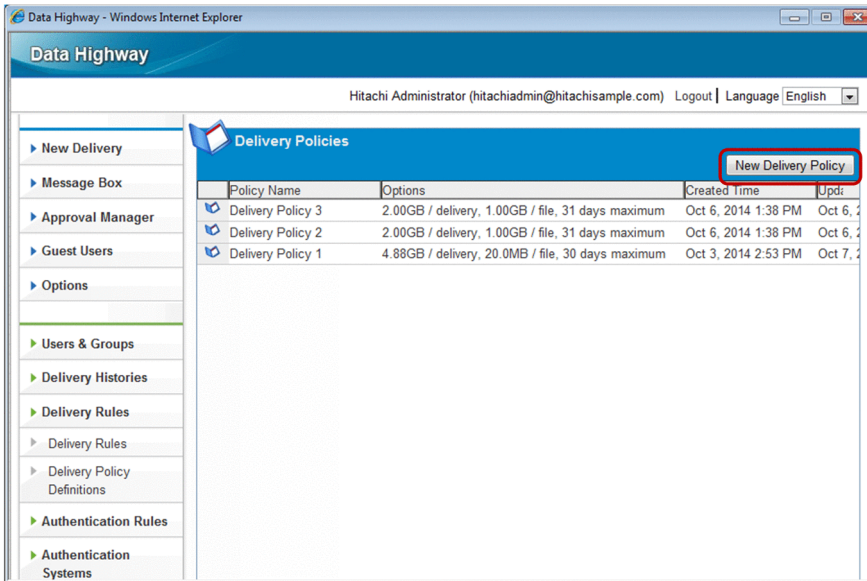
If you want to create a delivery policy with the same settings as one of the existing delivery policies, click the menu icon () of the delivery policy you want to edit and then select **Duplicate**. The New Delivery Policy window opens with all the settings copied except for the policy name. We recommend that you use this duplication, for example, when you create a delivery policy with the same settings and different policy name.

1. In the sidebar area, click **Delivery Rules** and then **Delivery Policy Definitions**.

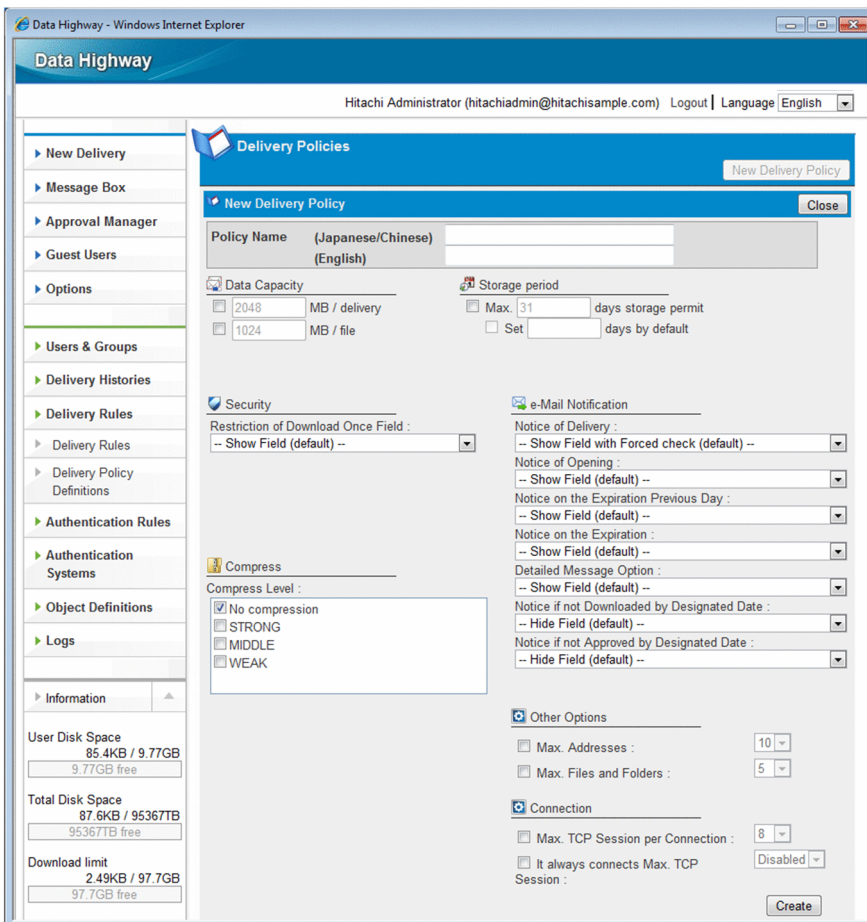
The Delivery Policies window appears in the content area.

2. Click the **New Delivery Policy** button.

The New Delivery Policy window appears.



3. Create a delivery policy.



The following table describes the items you specify.

Table 3–37: Settings for the delivery policy

Category	Item	Description
Policy Name ^{#1}	Policy Name (Japanese/Chinese) text box	Enter the name of the policy. The value you enter here is displayed in windows that use Japanese and Chinese.
	Policy Name (English) text box	Enter the name of the policy. You can enter alphanumeric characters and symbols. The value you enter here is displayed in windows that use English.
Data Capacity	Data capacity check boxes and text boxes	Specify the upper limit of the amount of data that can be delivered. You can select any of the check boxes you want to activate. The possible maximum value depends on the setting specified by the system administrator. <ul style="list-style-type: none"> • MB/delivery Indicates the upper limit of the amount of data that can be delivered per delivery. If the check box is not selected, the system uses its default value (2,048 MB/delivery). • MB/file Indicates the maximum size per file that can be delivered. If the check box is not selected, the system uses its default value (2,048 MB/file). The value in the MB/file text box must be no more than the value in the MB/delivery text box.
Storage period	Storage period check boxes and text boxes	<ul style="list-style-type: none"> • Max. XX days storage permit Specify the maximum value for the storage period that a user can set when sending a file. If the check box is not selected, the system uses the value specified by the system administrator. • Set XX days by default Specify the default value for the storage period that is applied when a user does not set a specific value. If the check box is not selected, the system uses the value specified in Max. XX days storage permit. The possible maximum value depends on the setting specified by the system administrator.
Security	Restriction of Download Once Field: drop-down list box	This function restricts the number of times a recipient can download a file to once. Select how the function works in this drop-down list box.
e-Mail Notification	Notice of Delivery: drop-down list box	The function sends a notification email to a sender and recipients when a file is uploaded or a message is sent. Select how the function works in this drop-down list box.
	Notice of Opening: drop-down list box	The function notifies a sender of a file being opened. Select how the function works in this drop-down list box.
	Notice on the Expiration Previous Day: drop-down list box	The function notifies a sender of a file not being opened before the day before the expiration date of file storage. Select how the function works in this drop-down list box.
	Notice on the Expiration: drop-down list box	The function notifies a sender of a file being expired. Select how the function works in this drop-down list box.
	Detailed Message Option: drop-down list box	The function specifies whether a file delivery email message contains detailed information about the file and other information. Select how the function works in this drop-down list box.

Category	Item	Description
e-Mail Notification	Notice if not Downloaded by Designated Date: drop-down list box	The function sends an email message to notify the recipient of a file if the recipient has not downloaded the file by the date specified by the sender. Select how the function works in this drop-down list box. The notification email is not sent if JP1/Data Highway - AJE 10-00 is used to send the file.
	Notice if not Approved by Designated Date: drop-down list box	The function sends an email message to notify an approver who has not accepted or rejected a delivery by the date specified by the sender. Select how the function works in this drop-down list box. If the delivery rule with this delivery policy applied does not have an approval route, the system ignores the value of the drop-down list box. The notification email is not sent if JP1/Data Highway - AJE 10-00 is used to send the file.
Compress	Compress Level	Select one or more compression levels for a sender's option. If no check box is selected, the system uses its default value (only No compression selectable). <ul style="list-style-type: none"> • No compression: The file or files are not compressed. • STRONG: The file or files are compressed with a method that provides the best compression ratio. • MIDDLE: The file or files are compressed with a method that provides a moderate compression ratio. • WEAK: The file or files are compressed with a method that provides the lowest compression ratio.
	Compress Method ^{#2}	Select a compression method. <ul style="list-style-type: none"> • Standard: If a folder is sent, or if one of STRONG, MIDDLE, and WEAK is selected for Compress Level, a ZIP-compressed file is sent. In this case, you cannot send files and folders that exceed 3.96 GB (4,252,017,623 bytes). • Extended: If a folder is sent, or if one of STRONG, MIDDLE, and WEAK is selected for Compress Level, the extended compression method is used. The file is compressed and sent in ZIP format if JP1/Data Highway - AJE 10-00 is used to send the file. Also, a system with JP1/Data Highway - AJE 10-00 cannot receive the file compressed in Extended compression method.
Other Options	Max. Addresses check box	If this check box is selected, the maximum number of destination addresses per delivery can be specified. If this check box is not selected, the system uses the value specified by the system administrator.
	Max. Files and Folders check box	If this check box is selected, the maximum number of files per delivery can be specified. If this check box is not selected, the system uses its default value (it is set to 5).
Connection ^{#3}	Max. TCP sessions per Connection check box	If this check box is selected, the maximum number of connections for sending and receiving files can be specified. The default value is the value in the standard delivery policy.
	Always connect with Max. TCP sessions check box	If this check box is selected, whether the system always uses the number of connections specified in the Max. TCP sessions per Connection field can be specified. <ul style="list-style-type: none"> • Enabled: The system always uses the maximum number of connections.

Category	Item	Description
Connection ^{#3}	Always connect with Max. TCP sessions check box	<ul style="list-style-type: none"> • Disabled: The system automatically determines the number of connections, depending on the network distance. The default value is the value in the standard delivery policy.

#1

- Some symbols (/ \ ? * : | " < > @ ^) are not available in the text box.
- A name consisting of only spaces or periods (.) is not available.
- You can enter no more than 256 characters.

#2

When a system with JP1/Data Highway - AJE 10-00 receives a delivery that contains files compressed with the extended compression method, the system skips the reception of the delivery and only receives deliveries other than the extended compression method. If your system uses JP1/Data Highway - AJE 10-00, you must change the delivery policy, based on the version.

#3

The check box might not appear depending on the setting specified by the system administrator.

4. Click the **Create** button.

The delivery policy is now created.

(5) Editing a delivery policy

To edit a delivery policy:

1. In the sidebar area, click **Delivery Rules** and then **Delivery Policy Definitions**.

The Delivery Policies window appears in the content area.

2. Click the menu icon () of the delivery policy you want to edit, and then select **Edit**.

The Edit Delivery Policy window appears.

3. Change the settings. For details about each item, see *(4) Creating a delivery policy*.

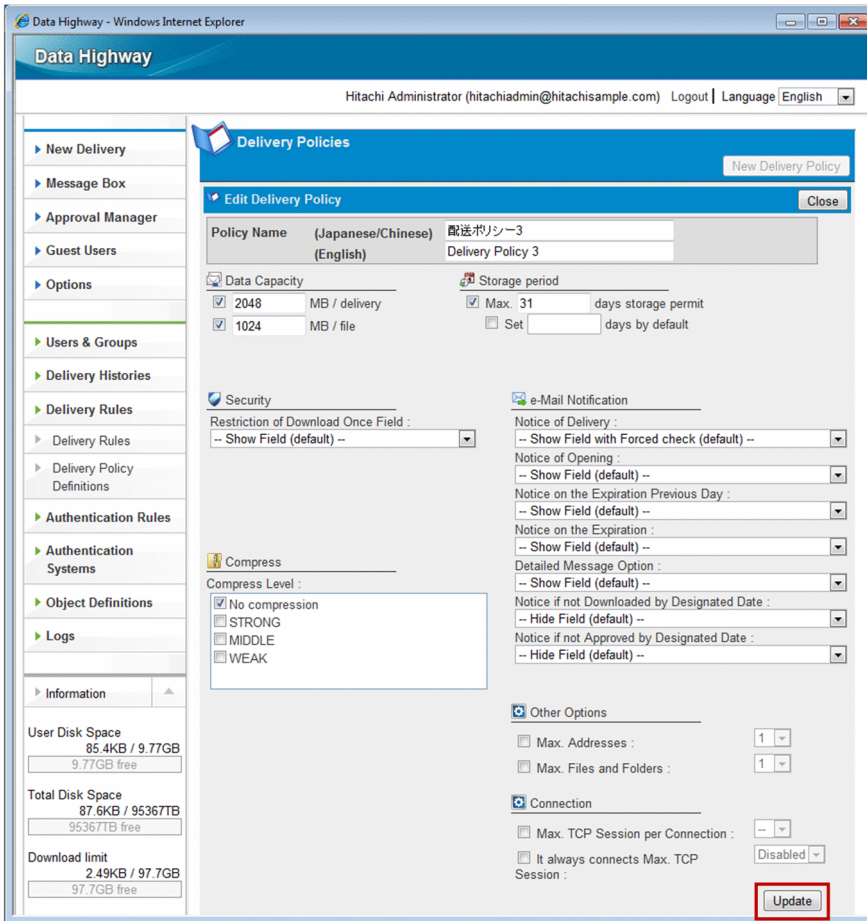


Important note

The upper limit of the amount of data cannot be below the total data size already delivered.


4. Click the **Update** button.

The delivery policy settings are updated.



(6) Deleting a delivery policy

To delete a delivery policy:

1. In the sidebar area, click **Delivery Rules** and then **Delivery Policy Definitions**.
The Delivery Policies window appears in the content area.
2. Click the menu icon () of the delivery policy you want to delete, and then select **Delete**.
A confirmation dialog box appears.
3. Click the **OK** button to delete the delivery policy.

Important note

Deleting a delivery policy also removes delivery rules that have the delivery policy you are trying to delete.

3.5.4 Authentication Rules

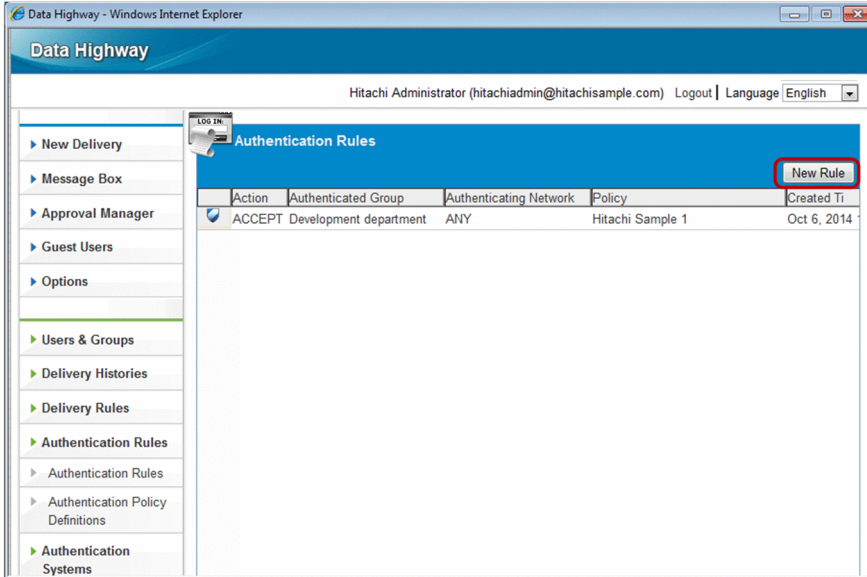
This subsection describes how to configure an authentication rule.

For details about the authentication rule, see *B. Authentication Rule*.

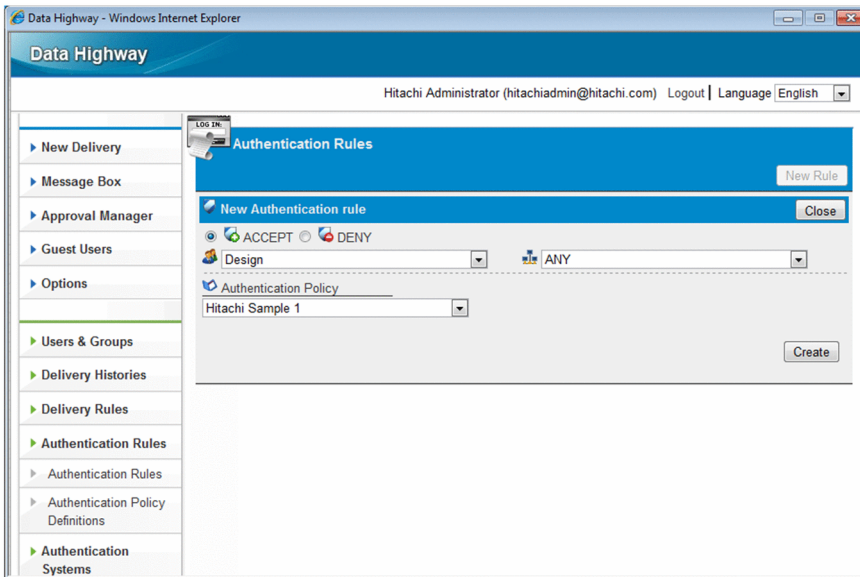
(1) Creating an authentication rule

To create an authentication rule:

1. In the sidebar area, click **Authentication Rules** and then **Authentication Rules**.
The Authentication Rules window appears in the content area.
2. Click the **New Rule** button.
The New Authentication rule window appears.



3. Create an authentication rule.



The following table describes the items you specify.

Table 3–38: Settings for the authentication rule

Item	Description
ACCEPT and DENY radio buttons	<ul style="list-style-type: none"> • ACCEPT Select this radio button to accept the specified rule. • DENY

Item	Description
ACCEPT and DENY radio buttons	Select this radio button to reject the specified rule.
Group drop-down list box	Select a group that the rule applies to.
Network set drop-down list box	Select a network set that the rule applies to.
Authentication Policy drop-down list box	Select an authentication policy to be applied.

4. Click the **Create** button.

The authentication rule is created, and a dialog box appears indicating the rule is registered.

5. Click the **OK** button.


The Authentication Rules window appears.

(2) Editing an authentication rule

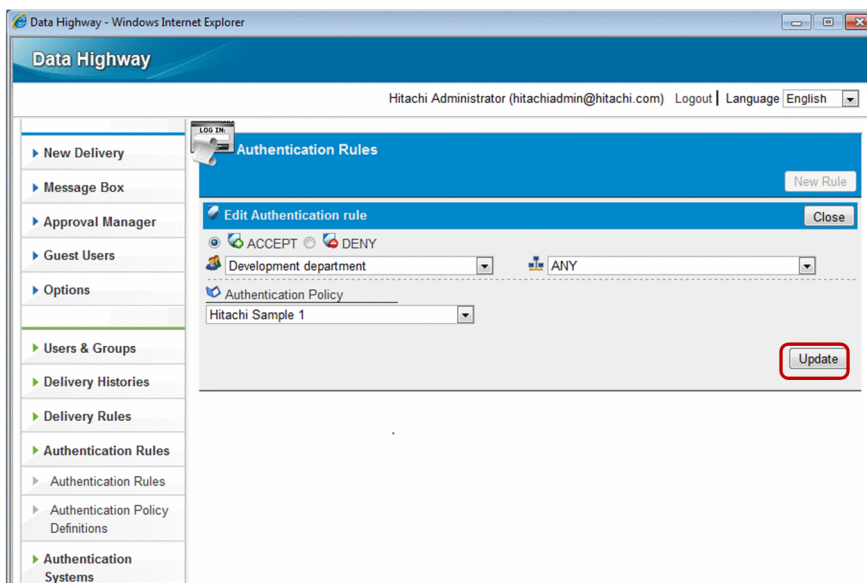
To edit an authentication rule:

1. In the sidebar area, click **Authentication Rules** and then **Authentication Rules**.

The Authentication Rules window appears in the content area.

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

The Edit Authentication rule window appears.



3. Change the settings. For details about each item, see *(1) Creating an authentication rule*.

4. Click the **Update** button.

The authentication rule settings are updated, and a dialog box appears indicating the updated rule is registered.

5. Click the **OK** button.

The Authentication Rules window appears.

(3) Activating, inactivating, or deleting an authentication rule

To activate, inactivate, or delete an authentication rule:


1. In the sidebar area, click **Authentication Rules** and then **Authentication Rules**.
The Authentication Rules window appears in the content area.
2. Click the menu icon () of your target authentication rule, and then select the menu item.

Table 3–39: Activating, inactivating, or deleting an authentication rule

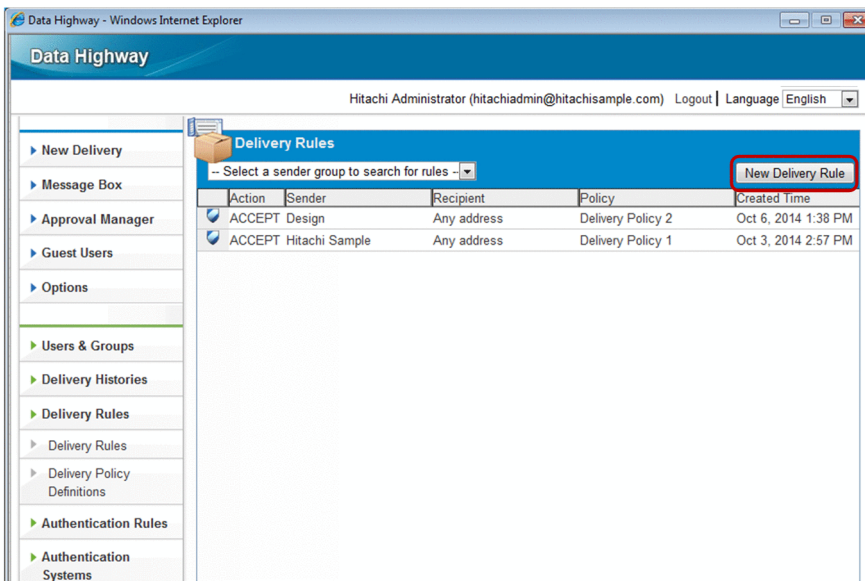
Item	Description
Activate	Activates an authentication rule.
Inactivate	Inactivates an authentication rule. The inactivated authentication rule becomes temporarily unavailable. To make the inactivated rule available, activate it again.
Delete	Deletes an authentication rule. The deleted authentication rule cannot be restored.

3. A confirmation dialog box appears depending on your choice. Click the **OK** button to perform the action.

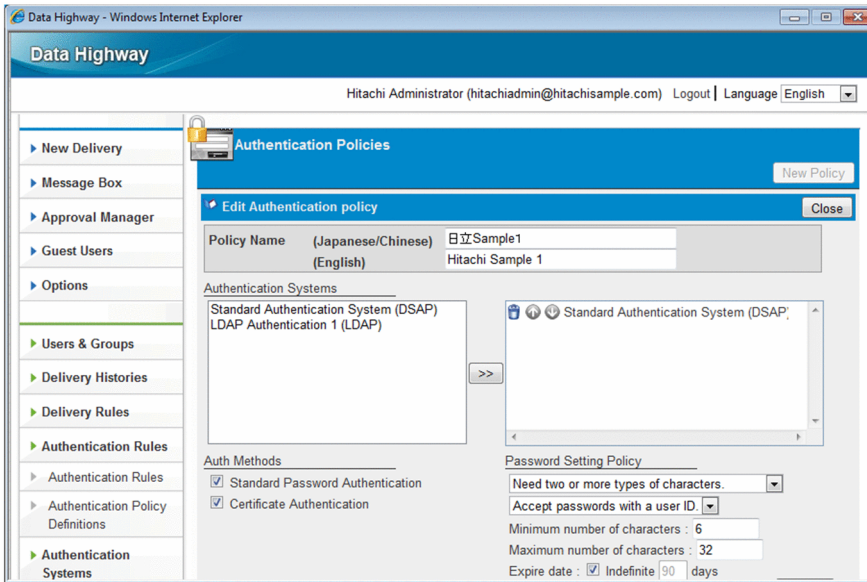
(4) Creating an authentication policy

To create an authentication policy:

1. In the sidebar area, click **Authentication Rules** and then **Authentication Policy Definitions**.
The Authentication Policies window appears in the content area.
2. Click the **New Policy** button.
The New Authentication policy window appears.




3. Create an authentication policy.



The following table describes the items you specify.

Table 3–40: Settings for the authentication policy

Item	Description
Policy Name (Japanese/Chinese) text box ^{#1}	Enter the name of the policy. The value you enter here is displayed in windows that use Japanese and Chinese.
Policy Name (English) text box ^{#1}	Enter the name of the policy. The value you enter here is displayed in windows that use English. You can enter alphanumeric characters and symbols.
Authentication Systems	Select an authentication system that this authentication policy uses by using the >> button. You cannot select more than one authentication system. If one authentication system is selected, clicking the >> button does not add a new system to the list. To cancel the selected authentication system, click the  icon.
Auth Methods	Select an authentication method. You can select both authentication methods. These check boxes cannot be selected if an LDAP authentication system is selected for the authentication system. <ul style="list-style-type: none"> • Standard Password Authentication check box: Select to use the password authentication. • Certificate Authentication check box: Select to use electronic certificates to authenticate users.
Password Setting Policy	Specify the rules of available characters for passwords. This section cannot be specified if an LDAP authentication system is selected for the authentication system. <ul style="list-style-type: none"> • Need two or more types of characters.: A password must contain two or more of the following four types: digit, lowercase alphabetic character, uppercase alphabetic character, and symbol • Do not need two or more types of characters. Specify whether a password can include a user ID. <ul style="list-style-type: none"> • Accept passwords with a user ID. • Reject passwords with a user ID.
	Expire date^{#2} The Indefinite check box is selected by default. If you want to set an expiration date, clear the Indefinite check box and enter the number of days in the range from 1 to 365. The value is set to 90 by default.

#1

- Some symbols (/ \ ? * : | " < > @ ^) are not available in the text box.

- A name consisting of only spaces or periods (.) is not available.
- You can enter no more than 100 (for Windows) or 256 (for Linux) characters.

#2

If you clear the **Indefinite** check box and enter the number of days, users who use this authentication policy must change their password the next time they log in.

4. Click the **Create** button.

The authentication policy is created, and a dialog box appears indicating the policy is registered.

5. Click the **OK** button.


The Authentication Policies window appears.

(5) Editing an authentication policy

To edit an authentication policy:

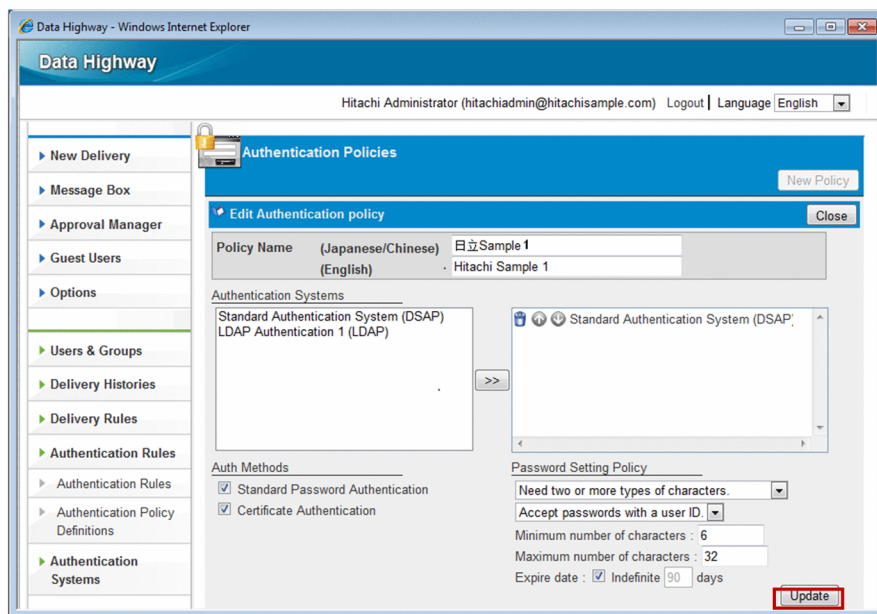
1. In the sidebar area, click **Authentication Rules** and then **Authentication Policy Definitions**.

The Authentication Policies window appears in the content area.

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

The Edit Authentication policy window appears.

3. Change the settings. For details about each item, see (4) *Creating an authentication policy*.



4. Click the **Update** button.

The authentication policy settings are updated, and a dialog box appears indicating the information is updated.

5. Click the **OK** button.


The Authentication Policies window appears.

Important note

The edited authentication policy might not take effect unless the user logs out of JP1/DH - Server.

(6) Deleting an authentication policy

To delete an authentication policy:

1. In the sidebar area, click **Authentication Rules** and then **Authentication Policy Definitions**.
The Authentication Policies window appears in the content area.
2. Click the menu icon () of the authentication policy you want to delete, and then select **Delete**.
A dialog box appears asking you to confirm that you want to delete the policy.
3. Click the **OK** button.
The authentication policy is deleted, and the Authentication Policies window appears.

Important note

Deleting an authentication policy also removes authentication rules that have the authentication policy you are trying to delete.

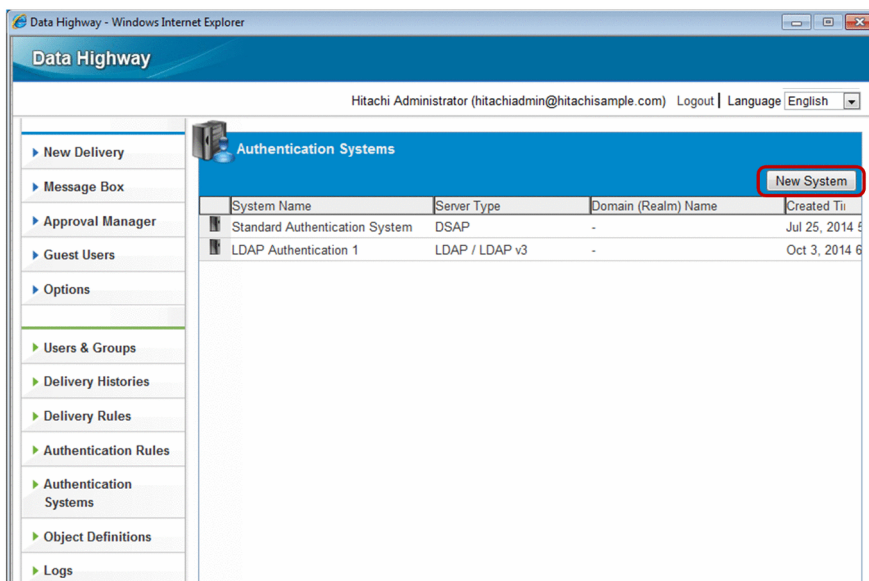
3.5.5 Authentication Systems

This subsection describes how to configure an authentication system.

(1) Creating an authentication system

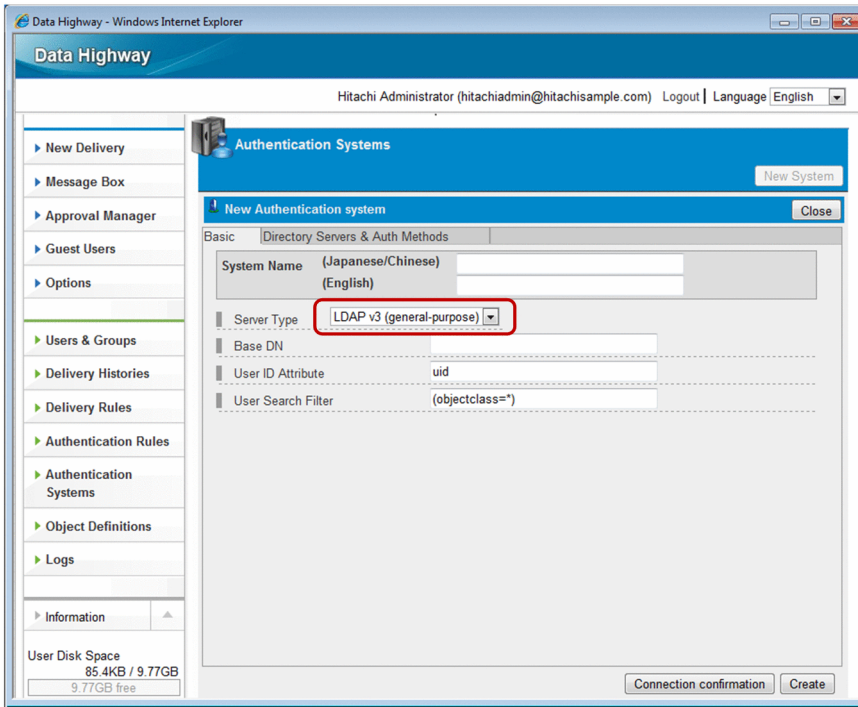
To create an authentication system:

1. In the sidebar area, click **Authentication Systems**.
The Authentication Systems window appears in the content area.
2. Click the **New System** button.
The New Authentication system window appears.

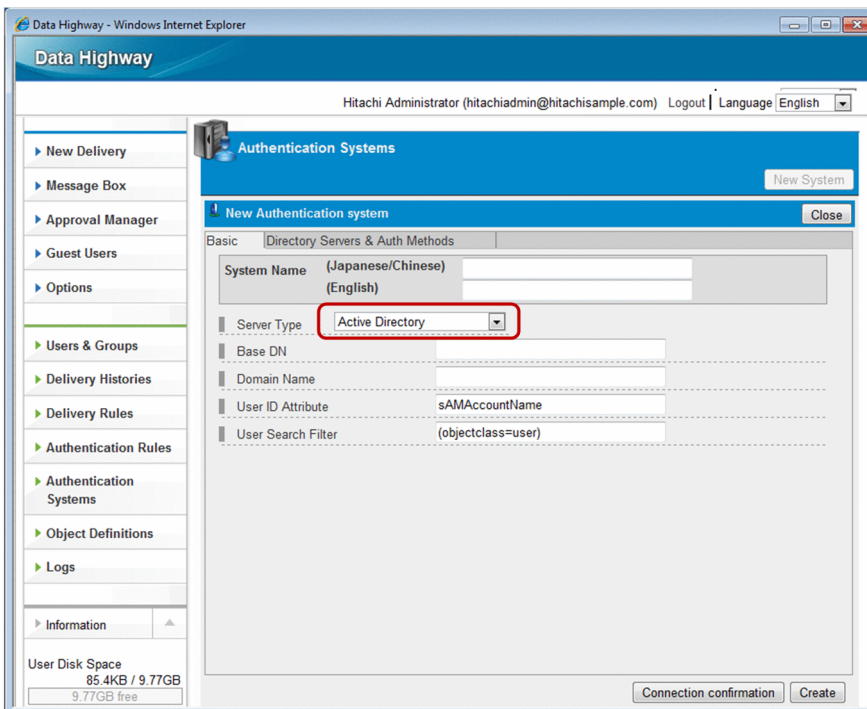


3. Configure the settings in the **Basic** tab.

If the **Server Type** drop-down list box is set to **LDAP v3**:



If the **Server Type** drop-down list box is set to **Active Directory**:



The following table describes the items you specify.

Table 3–41: Setting items in the Basic tab

Item	Description
System Name (Japanese/Chinese)	<p>Enter any name by which you can identify the authentication system.</p> <p>The value you enter here is displayed in windows that use Japanese and Chinese.</p> <ul style="list-style-type: none"> You can enter no more than 256 characters. Some symbols (/ \ ? * : " < > @ ^) are not available.

Item	Description
System Name (Japanese/Chinese)	<ul style="list-style-type: none"> A name consisting of only spaces or periods (.) is not available.
System Name (English)	<p>Enter any name by which you can identify the authentication system. The value you enter here is displayed in windows that use English.</p> <ul style="list-style-type: none"> You can enter no more than 256 alphanumeric characters and symbols. Some symbols (/ \ ? * : " < > @ ^) are not available. A name consisting of only spaces or periods (.) is not available.
Server Type	<p>Select the type of the directory server you use.</p> <ul style="list-style-type: none"> LDAP v3 (general-purpose): LDAPv3-compatible directory server other than Active Directory Active Directory: Active Directory server <p>The default value is LDAP v3 (general-purpose).</p> <p>When the server type is changed, the settings are initialized except for the values in System Name (Japanese/Chinese), System Name (English), and Server Type.</p> <p>Before the type is changed, a dialog box appears asking you to confirm that you want to change the setting. Clicking the OK button makes the server-type change take effect.</p>
Base DN[#]	<p>Specify the DN that serves as the starting point for a user search in the DIT of the directory server. In general, it must be the root DN, but if you want to narrow down which directory trees are searched for, you can specify a starting point DN for your search.</p> <p>If Server Type is set to Active Directory, a DN that represents a domain on the directory server cannot be specified. In this case, specify a DN containing OU or CN.</p>
Domain Name	<p>Specify the domain name for Active Directory, separated by dots, if Server Type is set to Active Directory.</p>
User ID Attribute	<p>Specify the attribute that stores the user ID in the user entry of the DIT.</p> <p>If Server Type is set to LDAP v3 (general-purpose), the default value is <code>uid</code>. You can change this value, depending on your system design.</p> <p>If Server Type is set to Active Directory, the User ID Attribute text box must have the value of <code>sAMAccountName</code>.</p>
User Search Filter	<p>Specify user search criteria in the DIT of the directory server.</p> <p>If Server Type is set to LDAP v3 (general-purpose), the User Search Filter text box must have the value of <code>(objectclass=*)</code>.</p> <p>If Server Type is set to Active Directory, the User Search Filter text box must have the value of <code>(objectclass=user)</code>.</p>

#

- If the following LDAP special characters are used, they must be escaped:

Comma (,), plus sign (+), equal sign (=), double quotation mark ("), backslash (\), less-than sign (<), greater-than sign (>), semicolon (;), hash mark (#) (only if it precedes the DN string), and forward slash (/)

- In Active Directory, \\ must be preceded by a symbol.

For example, a # character must be escaped like: \\#. However, a \ character must be escaped like \\ \, and /, like \/.

- In OpenLdap, \ must be preceded by a symbol.

For example, a # character must be escaped like \#, and \, like \\.

Values in the **User ID Attribute** and **User Search Filter** text boxes form a search filter expression, which can be used to identify a user. By default, the following filter expression is used to search the directory server for a user:

- If **Server Type** is set to **LDAP v3**: `(&(uid=%s)(objectclass=*))`
- If **Server Type** is set to **Active Directory**: `(&(sAMAccountName=%s)(objectclass=user))`

Important note

The variable %s means the left part of the @ in the user ID that is specified for the system login. If the filter expression above identifies more than one user entries, the users are not allowed to log in when they have the same login credentials (such as a password).

The **User ID Attribute** text box must have an attribute that can uniquely identify a user entry.

4. Configure the settings in the **Directory Servers & Auth Methods** tab.

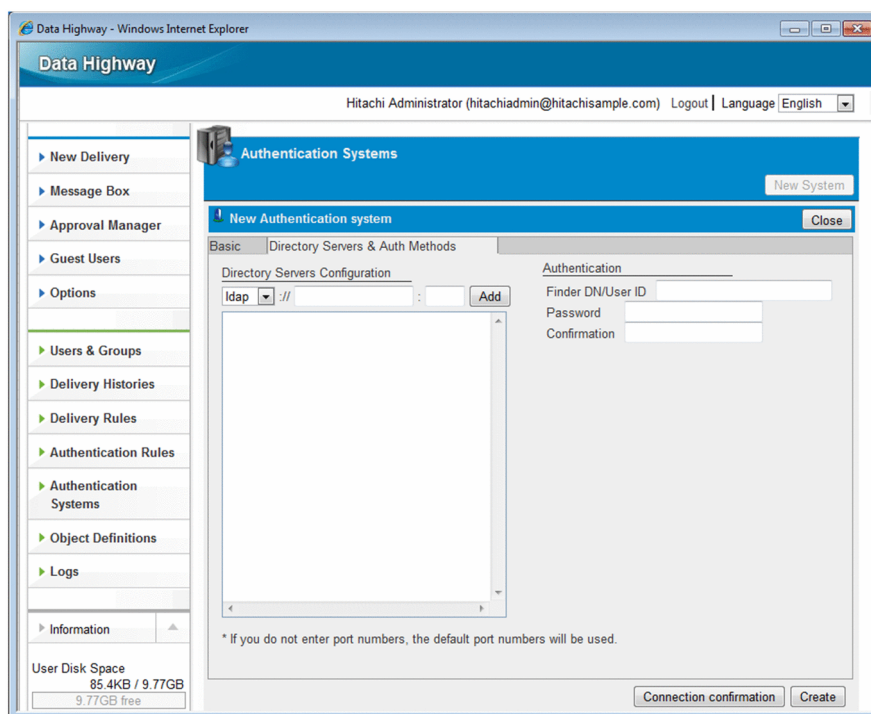


Table 3–42: Setting items in the Directory Servers & Auth Methods tab


Category	Item	Description
Directory Servers Configuration	Protocol	Select either of the following: <ul style="list-style-type: none"> • ldap: Select to use the non-encrypted LDAP protocol to communicate with the directory server. We recommend that you select this option only in a LAN environment because traffic is not encrypted. • ldaps: Select to use SSL to encrypt traffic to communicate with the directory server. The directory server must support the LDAPS protocol. The default value is ldap .
	Host name	Specify the host name of the directory server.
	Port number	Specify the port number that the system uses to communicate with the directory server. If omitted, it is set to the default port number. The default port number for each option is as follows: <ul style="list-style-type: none"> • ldap: 389 • ldaps: 636
	Add button	Clicking this button generates one directory server URL based on the information you entered, and adds the URL to the directory server list. However, if the list already has an entry, the URL is not added. The list can have only one directory server in it.
Authentication	Finder DN/User ID	Specify the DN or user ID of the user that is used to search the DIT of the directory server.

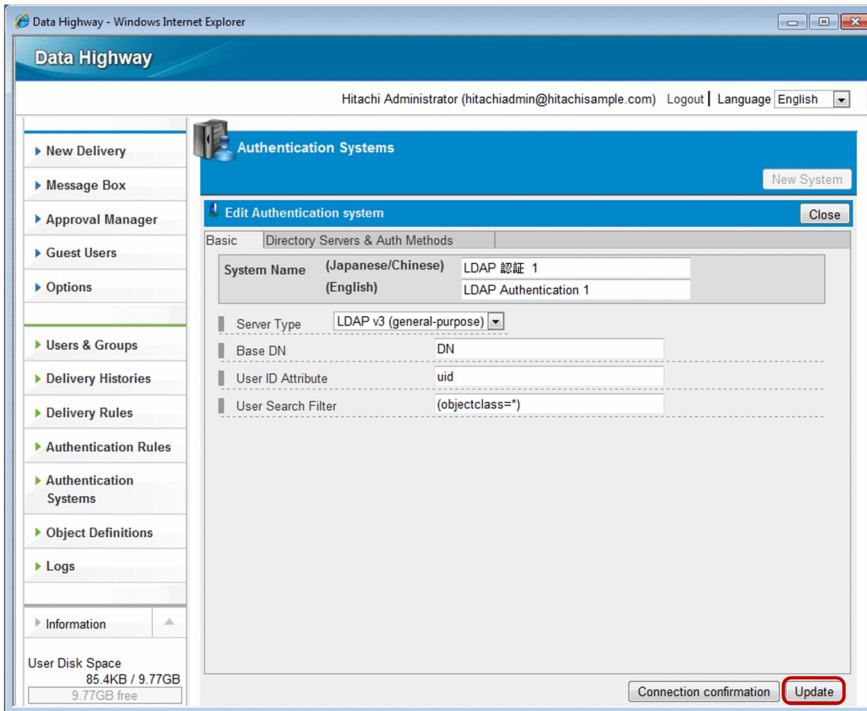
Category	Item	Description
Authentication	Finder DN/User ID	This user must have permission to search the DIT. If the Server Type drop-down list box in the Basic tab is set to LDAP v3 (general-purpose) , the DN of the user that is used for searching must be specified. If it is set to Active Directory , the user ID (sAMAccountName) must be specified. In Active Directory, the string <code>Administrator</code> is usually specified. If the user who searches the DIT of the directory server does not have the correct permission, the directory server authentication does not work properly, possibly causing unexpected behavior.
	Password	Specify the password of the user you entered in the Finder DN/User ID text box.
	Confirmation	Enter the password again to confirm it.

5. Click the **Connection confirmation** button to make sure that the system can connect to the configured directory server.
6. Click the **Create** button. The authentication system is created and appears in the Authentication Systems window.

(2) Editing an authentication system

To edit an authentication system:

1. In the sidebar area, click **Authentication Systems**.
The Authentication Systems window appears in the content area.
2. Click the menu icon () of the authentication system you want to edit, and then select **Edit**.
The Edit Authentication system window appears.
3. Change the settings. For details about each item, see [3.5.5\(1\) Creating an authentication system](#).
4. Click the **Connection confirmation** button to make sure that the system can connect to the directory server, with the changed settings.
5. Click the **Update** button.
The authentication system settings are updated, and a dialog box appears indicating the updated authentication system is registered.



6. Click the **OK** button.


The Authentication Systems window appears.

(3) Deleting an authentication system

To delete an authentication system:

1. In the sidebar area, click **Authentication Systems**.

The Authentication Systems window appears in the content area.

2. Click the menu icon () of the authentication system you want to delete, and then select **Delete**.

A dialog box appears asking you to confirm that you want to delete the authentication system.

3. Click the **OK** button.

The authentication system is deleted, and the Authentication Systems window appears.

Important note

An authentication system used in an authentication policy cannot be deleted.

3.5.6 Object Definitions

This subsection describes how to configure a network set and approval route.

(1) Creating a network set

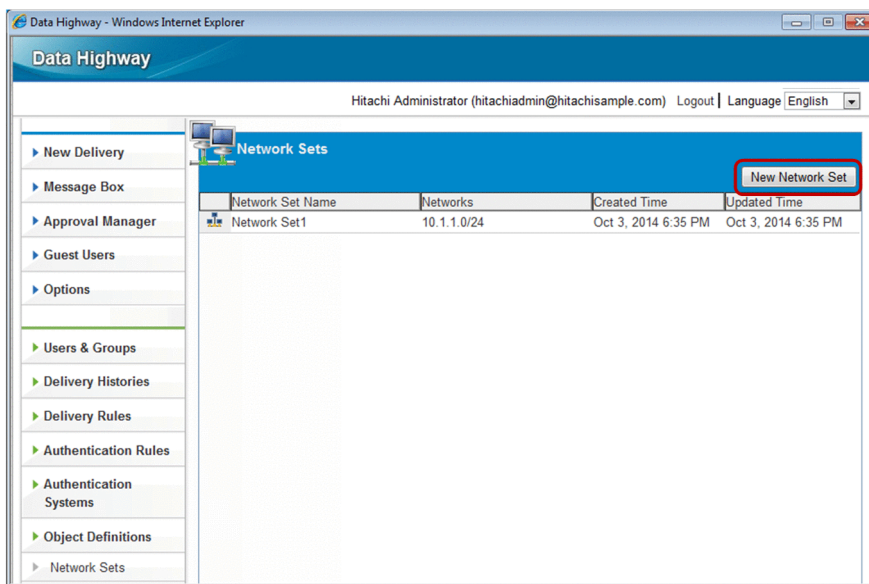
To create a network set:

1. In the sidebar area, click **Object Definitions** and then **Network Sets**.

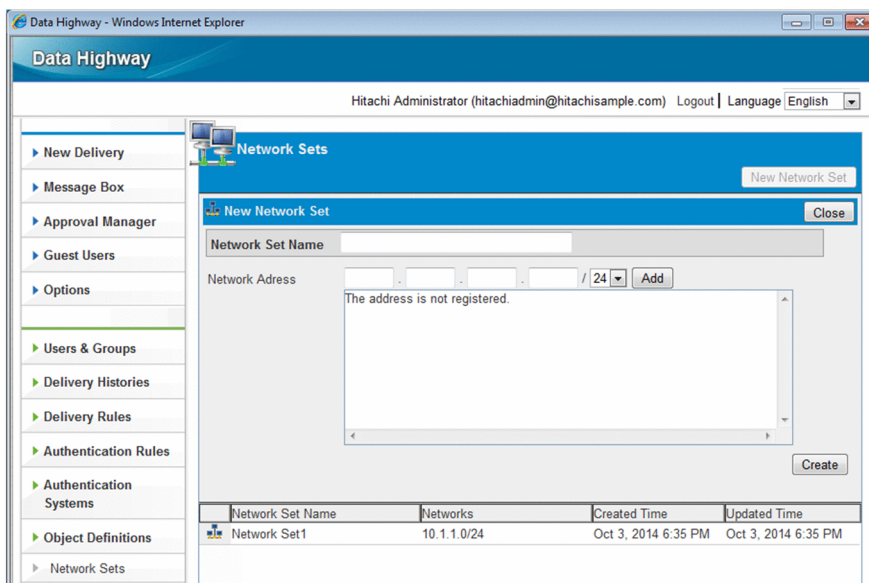
The Network Sets window appears in the content area.

2. Click the **New Network Set** button.

The New Network Set window appears.



3. Create a network set.



The following table describes the items you specify.

Table 3–43: Settings for the network set

Item	Description
Network Set Name text box	Enter the name of the network set. Some symbols (/ \ ? * : " < > @ ^) are not available in the text box. A name consisting of only spaces or periods (.) is not available. You can enter no more than 256 characters.
Network Address text box	Enter the network address. Clicking the Add button sets the address you entered. A single network set can have multiple network addresses.

Item	Description
Network Address text box	Each text box must have the number ranging from 0 to 255. A single network set can have no more than 100 network addresses.

4. Click the **Create** button.


The network set is now created.

(2) Editing a network set

To edit a network set:

1. In the sidebar area, click **Object Definitions** and then **Network Sets**.

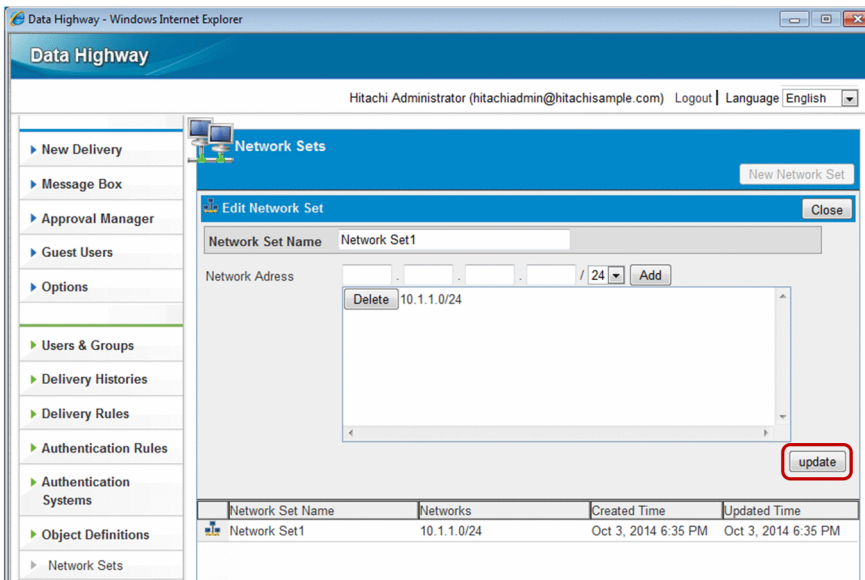
The Network Sets window appears in the content area.

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

The Edit Network Set window appears.

3. Change the settings. For details about each item, see *(1) Creating a network set*.

4. Click the **update** button.




5. The settings of the network set are now updated.

(3) Deleting a network set

To delete a network set:

1. In the sidebar area, click **Object Definitions** and then **Network Sets**.

The Network Sets window appears in the content area.

2. Click the menu icon () of the network set you want to delete, and then select **Delete**.

A confirmation dialog box appears.

3. Click the **OK** button to delete the network set.

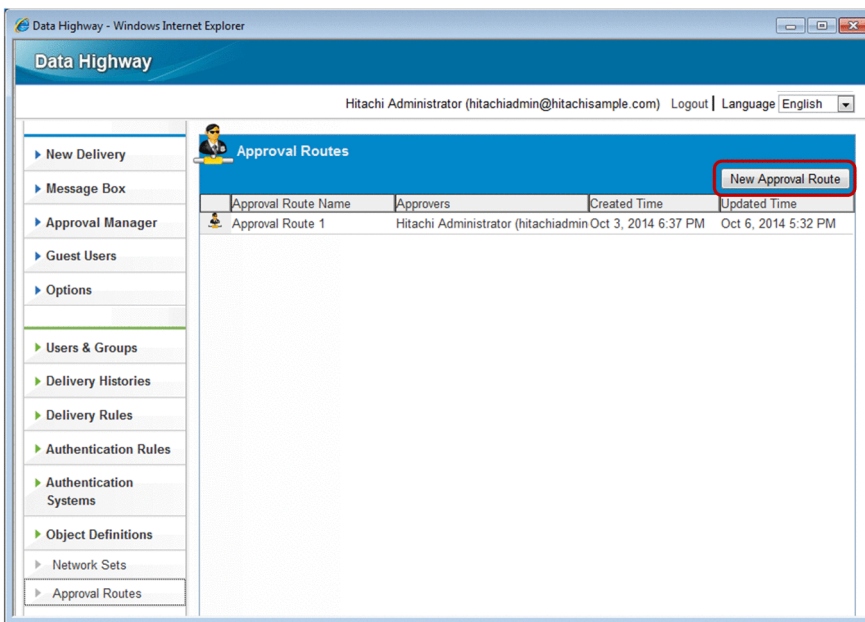
Important note

Deleting a network set also removes authentication rules that have the network set you are trying to delete.

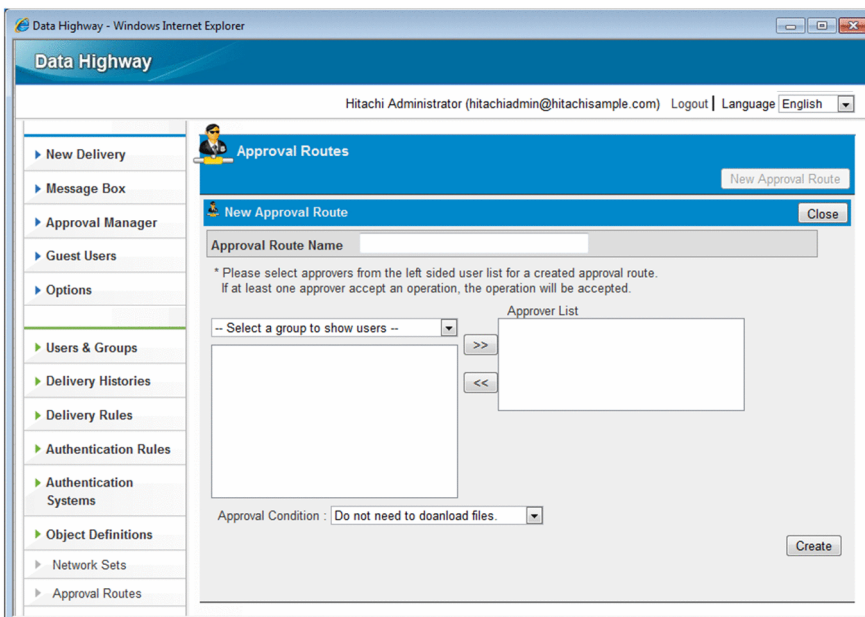
(4) Creating an approval route

To create an approval route:

1. In the sidebar area, click **Object Definitions** and then **Approval Routes**.
The Approval Routes window appears in the content area.
2. Click the **New Approval Route** button.
The New Approval Route window appears.



3. Create an approval route.



The following table describes the items you specify.

Table 3–44: Settings for the approval route

Item	Description
Approval Route Name text box	Enter the name of the approval route. Some symbols (/ \ ? * : " < > @ ^) are not available in the text box. A name consisting of only spaces or periods (.) is not available. You can enter no more than 256 characters.
Approver List list box	Use it to add approver user to the list. Clicking the >> button adds a selected user to the list. Clicking the << button removes a selected user from the list. If one of the users in this approver list performs the approval operation, an application for approval can be accepted or rejected. A guest user cannot be an approver, and guest groups and guest users are not displayed in the selection list.
Approval Condition drop-down list box	Select the condition for the approval. <ul style="list-style-type: none">• Do not need to download files. Select this option to allow an approver to perform the approval operation without downloading any file.• Need to download at least one file. Select this option to force an approver to download at least one file out of uploaded files in order to perform the approval operation.• Need to download all files. Select this option to force an approver to download all the uploaded files in order to perform the approval operation.

4. Click the **Create** button.


The approval route is now created.

(5) Editing an approval route

To edit an approval route:

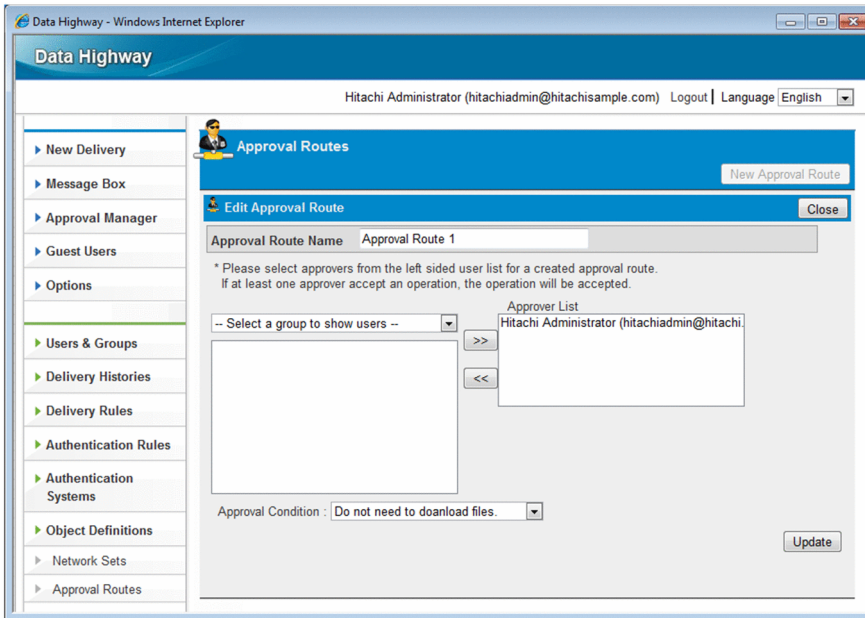
1. In the sidebar area, click **Object Definitions** and then **Approval Routes**.

The Approval Routes window appears in the content area.

2. Click the menu icon () of the approval route you want to edit, and then select **Edit**.

The Edit Approval Route window appears.

3. Change the settings. For details about each item, see *(4) Creating an approval route*.



4. Click the **Update** button.

The settings of the approval route are now updated.


(6) Deleting an approval route

To delete an approval route:

1. In the sidebar area, click **Object Definitions** and then **Approval Routes**.

The Approval Routes window appears in the content area.

For details about the Approval Routes window, see (4) *Creating an approval route*.

2. Click the menu icon () of the approval route you want to delete, and then select **Delete**.

A confirmation dialog box appears.

3. Click the **OK** button to delete the approval route.

3.5.7 Logs

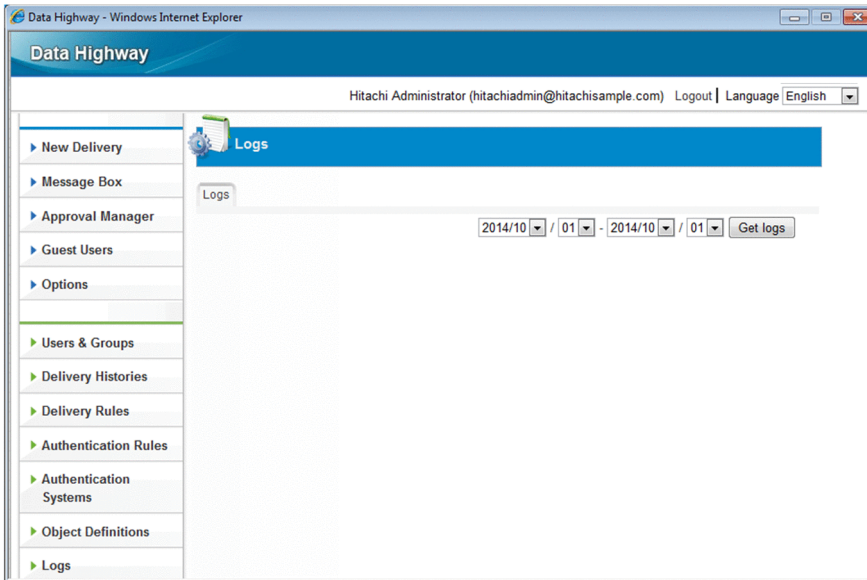
This subsection describes how to operate the Logs window.

(1) Obtaining the audit log file

To obtain the audit log file:

1. In the sidebar area, click **Logs**.

2. The Logs window appears in the content area.



The following table describes the items you specify.

Table 3–45: Settings for the log

Item	Description
Start date drop-down list box	Select the start date of the audit log entries you want to obtain.
End date drop-down list box	Select the end date of the audit log entries you want to obtain. If the specified end date is before the start date, an empty file is downloaded.

3. Click the **Get logs** button.

The audit log entries are now downloaded.

The audit log file to be downloaded is encoded in UTF-8. If you see corrupted characters in your viewer, specify the UTF-8 encoding to view the audit log file.

4

Troubleshooting

This chapter describes how to solve problems that you might encounter while using JP1/DH - Server.

For details about how to troubleshoot problems that a general user might encounter, visit our website to download and see the *Job Management Partner 1/Data Highway - Server User's Guide*.

4.1 FAQs

4.1.1 FAQs related to operations performed by the group manager

The following table describes the FAQs related to operations performed by the group manager.

Table 4–1: FAQs related to the group manager's operations

No.	Question	Answer
1	How do I manually unlock a user account that is locked?	You can do this by activating the user who you want to unlock the account for in the Users & Groups window.
2	When I attempted to create a user in the New User window or edit a user in the Edit User window, I received a message saying <code>The email address (xxx@xxx.xx) is already registered.</code> and I was not able to create or edit the user. How can I deal with this situation?	JP1/DH - Server does not allow you to register an email address that is already registered. Ask your representative user and other guest users whether the email address of the user you want to create or edit is in use.
3	When I attempted to create a user in the New User window, I received a message saying <code>You exceeded limits of your number of users. Please delete users before you create this user.</code> and I was not able to create the user. How can I deal with this situation?	The maximum number of users that can be registered is the number of users that the system administrator allocates to the domain. If you want to add users, contact your system administrator.
4	Users and groups are displayed in the tree view of the Users & Groups window. But when I click a user or group whose name is long in the view, I cannot see any menu item such as Edit . How can I deal with this situation?	The menu items are displayed further to right side of the window. If you press the right-arrow key on your keyboard after clicking the group or user, you can see and click the menu item.

4.1.2 FAQs related to operations performed by the representative user

The following table describes the FAQs related to operations performed by the representative user.

Table 4–2: FAQs related to the representative user's operations

No.	Question	Answer
1	How many setting objects, such as delivery rules, can I create?	The maximum numbers of objects you can create are as follows: <ul style="list-style-type: none">• Users: The number of users allocated by your system administrator• Groups: 1000• Groups that a user can belong to: 10• Depths of nested group levels: 10• Delivery rules: 100• Delivery policies: 100• Authentication rules: 100• Authentication policies: 100• Network sets: 100• Approval routes: 100
2	Characters are corrupted in the audit log. How can I fix them?	The audit log file is encoded in UTF-8. Open the file by using an application that supports the UTF-8 encoding.

No.	Question	Answer
3	Characters are corrupted in the CSV file for export and in the sample CSV file. How can I fix them?	The CSV file for export and sample CSV file are encoded in UTF-8. Open the file by using an application that supports the UTF-8 encoding.
4	Are there any notes in creating a network set?	A network address defined in a network set must be a global address that is valid on the Internet. If clients from which you want to restrict access use a proxy server to connect to the Internet, provide the network address that includes the global address of the proxy server.

4.2 Temporary restrictions

This section describes temporary restrictions of JP1/DH - Server. Keep them in mind when using JP1/DH - Server.

4.2.1 Restrictions related to operations performed by the group manager

The following table describes the restrictions related to operations performed by the group manager.

Table 4–3: Restrictions related to the group manager's operations

No.	Restriction
1	<p><i>Inactivating a user while the user is working with JP1/DH - Server</i></p> <p>If you inactivate a user who has already logged in to and is working with JP1/DH - Server, the user can still use some of the JP1/DH - Server functions until the user logs out.</p>
2	<p><i>Deleting a user while the user is working with JP1/DH - Server</i></p> <p>If you delete a user who has already logged in to and is working with JP1/DH - Server, an unexpected error might occur when the user tries to perform an operation in the JP1/DH - Server window.</p>
3	<p><i>A drop-down list box with unselectable option in the Users & Groups window</i></p> <p>If the following steps are performed, a drop-down list box in the field labeled as (English) in the Users & Groups window is displayed, from which a user cannot select any option:</p> <ol style="list-style-type: none">1. In the Users & Groups window, a user selects a group and then clicks Edit.2. In the Edit Group window, a user selects the Address Book Manager tab to display the Shown groups window, and then clicks the Close button.3. In the Users & Groups window again, a user selects a group and then clicks Edit. <p>To solve the problem above, select the Address Book Manager tab and then select the previous tab.</p>
4	<p><i>Inactivating a group</i></p> <p>Even if a group is inactivated, users who also belong to any group other than the inactivated group are not inactivated. Those users who are not inactivated can still use the settings for the inactivated group, such as a delivery rule. To avoid this situation, you must disassociate the users from the inactivated group.</p>

4.2.2 Restrictions related to operations performed by the representative user

The following table describes the restrictions related to operations performed by the representative user.

Table 4–4: Restrictions related to the representative user's operations

No.	Restriction
1	<p><i>Specifying the start and end dates to download audit-log records</i></p> <p>When you download audit-log records, you must specify the start and end dates of the log records by considering the following restrictions:</p> <ul style="list-style-type: none">• If a non-existent date is specified, the system cannot determine the date period correctly. Example September 31, 2010 (which does not exist): If 2010/09/31 is specified, you will receive the log file that contains log records up to October 1, 2010.• If the specified end date is before the start date, you will receive an empty file.
2	<p><i>Settings for the authentication policy</i></p>

No.	Restriction
2	When you modify an authentication policy, it might take some time for the change to take effect. For the change to be in effect, log out of the system after you modify the authentication policy.
3	<p data-bbox="240 255 1469 315"><i>If the maximum number of destinations that can be specified in the New Delivery window is decreased due to the automatically changed delivery policy</i></p> <p data-bbox="240 320 1469 376">If you have multiple delivery policies created and they have different maximum numbers of recipient addresses, the following problem might occur:</p> <p data-bbox="240 380 1469 499">After a user enters recipient addresses in the New Delivery window, the delivery policy can be changed. In this case, the maximum number of recipient addresses in the changed delivery policy might have less recipient addresses already entered in the recipient address fields. If this happens, any users that exceed the maximum number in the new delivery policy are removed from the recipient address fields.</p>
4	<p data-bbox="240 524 820 551"><i>Storage period for delivery policy and time-zone difference</i></p> <p data-bbox="240 555 1469 725">If you use JP1/DH - Server outside of your country, the storage period for a new delivery is set based on the local time. However, the actual storage period is set according to the time zone specified for the server on which JP1/DH - Server is installed. Therefore, if you use JP1/DH - Server from one area (for example, the U.S.) whose time zone is behind the time zone of another area (for example, Japan) where JP1/DH - Server is located, you might encounter a problem. The problem is that the storage period might expire immediately after the file transmission when you specify one day for the storage expiration date of a file and send the file. If you use JP1/DH - Server from such an area, extend the storage expiration date of a file.</p>



Appendixes

A. Delivery Rule

In the list of delivery rules, the settings for delivery rules are displayed from top to bottom.

If the condition of a delivery matches any of the delivery rules, the system uses the delivery policy defined in the matched rule to perform the delivery. The condition here means the sender and recipient groups. When the group contains a child group, its child groups are also taken into consideration.

This system adopts the first-match rule. In the first-match rule, if the specified sender and recipient addresses match addresses defined in the delivery rules in the list, the delivery rule at the top of the list applies.

If you want to send a delivery to multiple recipients, a recipient group containing all possible recipients must be selected in the delivery rule.

Examples of the application of delivery rules

To a single recipient:

Sender: Sender 1 who is a member of group A

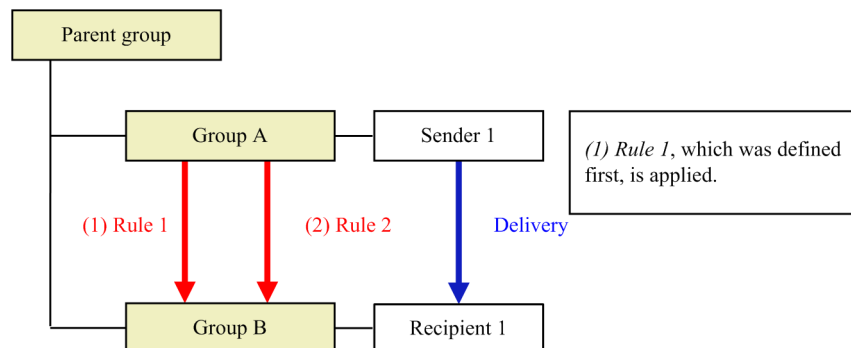
Recipient: Recipient 1 who is a member of group B

If the delivery rules in the table below are configured, delivery rule 1 is selected by applying the first-match rule. Delivery rule 2 is not selected.

Table A–1: Configuration example of delivery rules

No.	Sender	Recipient	Delivery policy
1	Group A	Group B	Delivery policy 1
2	Group A	Group B	Delivery policy 2

Figure A–1: Delivery example (to a single recipient)



To two recipients:

Sender: Sender 1 who is a member of group A

Recipient: Recipient 1 who is a member of group B and recipient 2 who is a member of group C

Group hierarchy: Group D is a parent group of groups B and C.

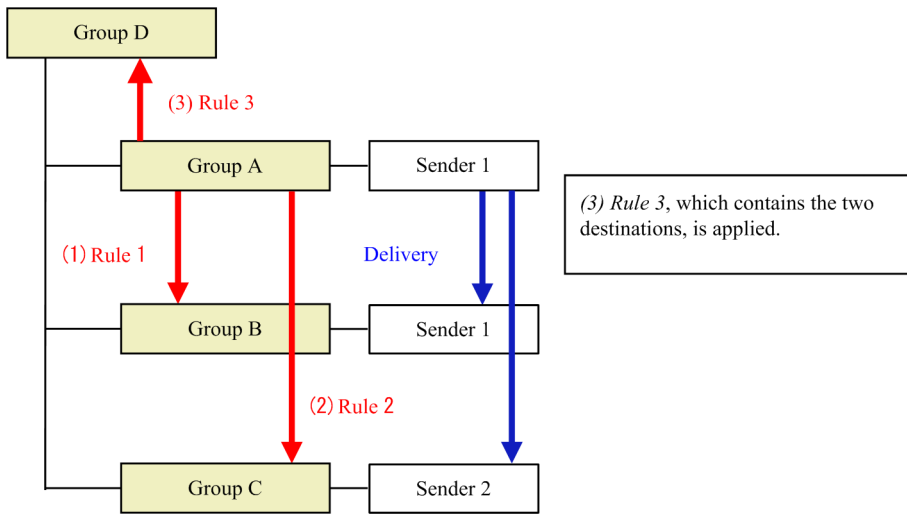
If the delivery rules in the following table are configured, delivery rule No. 3 that contains sender group A and recipient groups B and C matches.

Table A–2: Possible delivery rule settings

No.	Sender	Recipient	Delivery policy
1	Group A	Group B	Delivery policy 1
2	Group A	Group C	Delivery policy 2

No.	Sender	Recipient	Delivery policy
3	Group A	Group D	Delivery policy 3

Figure A–2: Possible delivery example (to two recipients)

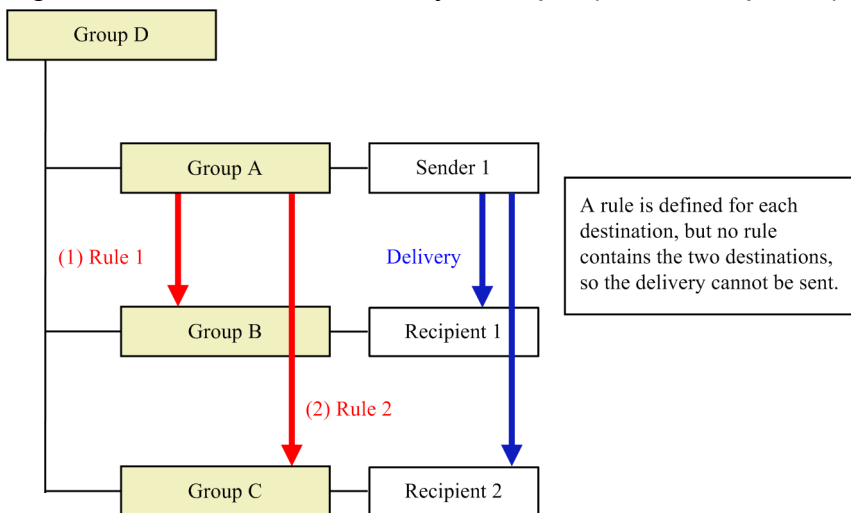


If the configured delivery rules include only the rules shown in the table below, sending the delivery is impossible. The reason is that the rule containing both groups B and C as a recipient is not included in the configured delivery rules. However, a file delivery is possible from group A to group B, and also from group A to group C.

Table A–3: Ineffective delivery rule settings

No.	Sender	Recipient	Delivery policy
1	Group A	Group B	Delivery policy 1
2	Group A	Group C	Delivery policy 2

Figure A–3: Ineffective delivery example (to two recipients)



When a user belongs to multiple groups

The first-match rule is also applied when a user belongs to multiple groups. The order of the groups in the user setting does not matter.

The following table shows an example of a group hierarchy in which a *Parent* group has *A*, *B*, and *C* groups as its children.

Table A–4: Example of the application of delivery rules when a user belongs to multiple groups

No.	Group sender belongs to (from top to bottom)	Group recipient(s) belongs to (from top to bottom)	Delivery rule (from top to bottom)	Rule to be applied
1	A	C	B -> C	A -> C
2	A B	C	A -> C A -> B A -> A	B -> C
3	B A	C	Parent -> Parent	B -> C
4	A	A B		A -> B
5	A	B A		A -> B
6	B A	B A		A -> B
7	A B	B A		A -> B
8	A B	A		A -> A
9	A	A B (first recipient) C (second recipient)		Parent -> Parent

B. Authentication Rule

In the list of authentication rules, the settings for authentication rules are displayed from top to bottom. The users with the setting conditions that match the authentication rules with **ACCEPT** in the **Action** column are accepted for authentication.

If the user is accepted for authentication, the corresponding policy is applied for authentication of the user. If the authentication group and authentication network (which is the address of a network that users connect to) of the user match those of the rules, the authentication policy specified in the rule is applied.

This system adopts the first-match rule. If the user with the settings matches two or more authentication rules, the system selects the first rule that was found in the matched authentication rules.

In the first-match rule, if the same authentication group and authentication network are specified for different authentication rules, the authentication rule at the top of the list is applied. This is applied only to a rule that shows **ACCEPT** in the **Action** column.

When the rules are scanned from top to bottom, and a rule that matches the user setting is set to **DENY**, the policy defined in the matched rule is rejected.

However, if the same policy defined in the rule whose action is set to **DENY** is also defined in the rule whose action is set to **ACCEPT**, the policy is not rejected as long as a rule with **ACCEPT** is in the higher position in the list.

In general, the rule for accepting the authentication (the rules with **ACCEPT** selected) is created first so that the rule can be located at a higher position in the list of authentication rules. Then, the rule to reject all the default settings (the rule with **DENY** selected) is created so that it can be located at the end of the list. This makes the application of authentication rules easy-to-understand and more reasonable. You can add another **DENY** rule between the rules with **ACCEPT** status and **DENY** in the list only if you want to add an exceptional rule.

If no authentication rule is matched with the user's settings, the standard authentication rule is applied, which is the default value throughout the JP1/DH - Server system.

When a user belongs to multiple groups

The first-match rule is also applied when a user belongs to multiple groups. The order of the groups in the user setting does not matter.

The following table shows an example of a group hierarchy in which a *Parent* group has *A*, *B*, and *C* groups as its children.

Table B–1: Example of the application of authentication rules when a user belongs to multiple groups

No.	Group user belongs to (from top to bottom)	Authentication rule definition (from top to bottom)	Rule to be applied
1	A	1. B ACCEPT	2. A ACCEPT
2	A B	2. A ACCEPT	1. B ACCEPT
3	B A		1. B ACCEPT
4	A	1. B ACCEPT	2. A DENY
5	A	2. A DENY	1. B ACCEPT

No.	Group user belongs to (from top to bottom)	Authentication rule definition (from top to bottom)	Rule to be applied
5	B	1. B ACCEPT 2. A DENY	1. B ACCEPT
6	A	1. B DENY 2. A ACCEPT	2. A ACCEPT
7	A B		1. B DENY

C. List of CSV Error Messages

The following table describes and lists CSV error messages.

Table C–1: List of error messages that are output to the CSV file

No.	Error message	Description
1.	Unit verification failures exist.	An invalid line was found somewhere in the entire CSV file. See the error message for details and correct the invalid line.
2.	Joint verification failures exist.	This message is output when the user attempts to create inconsistent data such as a user without group definition. Create a correct CSV file.
3.	Previous registration failed.	An error occurred on a line prior to this message. Correct the error on that line.
4.	Previous deleting failed.	An error occurred on a line prior to this message. Correct the error on that line.
5.	Users, groups, binders or managers cannot be parsed (usersParsed=XXX,groupsParsed=XXX,bindersParsed=XXX,managersParsed=XXX).	Any of the following identifiers was not defined for import: [users], [groups], [binders], and [managers] Either true or false is output to XXX. <ul style="list-style-type: none"> • true: The identifier is defined. • false: The identifier is not defined. In the CSV file, every definition section must have its identifier and header, even with no record in the definition section. Add the identifier and/or header to the definition section.
6.	A XXX column is too long.Please confirm the number of columns.	The record has a greater number of columns than the valid value. Make sure that the record has the valid number of columns. One of the followings is output to XXX: [users], [groups], [binders], or [managers]
7.	A XXX column is too short.Please confirm the number of columns.	A record has a smaller number of columns than the valid value. Make sure that the record has the valid number of columns. One of the followings is output to XXX: [users], [groups], [binders], or [managers]
8.	Unknown XXX's field detected	This message is output when one of the header columns is incorrect. The header cannot be modified. Specify the correct header. One of the followings is output to XXX: user, group, binder, or manager
9.	Unexpected problems occurred.	An unexpected exception occurred. Your server might be overloaded. Try again after a while. If the same error keeps occurring even after some retries, contact our sales representative or support contact.
10.	The number of XXX lines exceeds 300.Please input XXX within 300 lines.	The number of records in the file exceeds 300 records. Make sure that each definition section has 300 records or less. One of the followings is output to XXX: users, groups, binders, or managers
11.	A user ID is null or empty. (USER_ID)	The user ID is not provided. Provide the user ID.
12.	A user email is null or empty. (EMAIL)	The email address is not provided. Provide the email address.
13.	A user password is null or empty. (PASSWORD)	The password is not provided.

No.	Error message	Description
13.	A user password is null or empty. (PASSWORD)	Provide the password.
14.	An english user name is null or empty. (NAME_EN)	The name (English) is not provided. Provide the name (English).
15.	A group english name is null or empty. (XXX)	The group name (English) is not provided. Provide the name for the column indicated by <i>XXX</i> . One of the followings is output to <i>XXX</i> : NAME_EN or GROUP_NAME_EN
16.	Japanese name/Chinese name of the group is null or empty. (NAME_JA)	The group name (Japanese/Chinese) is not provided. Provide the group name (Japanese/Chinese).
17.	A parent group english name is null or empty. (PARENT_NAME_EN)	The parent group name (English) is not provided. Provide the parent group name (English).
18.	Please enter a user ID (includes static ID following @) within 100 characters maximum. (USER_ID)	The user ID has 100 characters or more in length. Make sure that the value for user ID does not exceed 100 characters.
19.	Please enter a user's email address within 256 characters maximum. (EMAIL)	The email address has 256 characters or more in length. Make sure that the value for email address does not exceed 256 characters.
20.	Please enter a user's name within 256 characters maximum. (XXX)	The user name has 256 characters or more in length. The value for the column indicated by <i>XXX</i> cannot exceed 256 characters. One of the followings is output to <i>XXX</i> : NAME, NAME_EN, or NAME_KANA
21.	The length of a user password(text:HEX) is wrong. (PASSWORD).	The length of the digest password is invalid. Make sure that the digest is 40 characters in length.
22.	Please enter a memo within 4096 characters maximum. (MEMO)	The note is 4,096 characters or more in length. Make sure that the value for the note does not exceed 4,096 characters.
23.	Please enter a group name within 200 characters maximum. (XXX)	The group name is 200 characters or more in length. The value for the column indicated by <i>XXX</i> cannot exceed 200 characters. One of the followings is output to <i>XXX</i> : NAME_EN, NAME_JA, PARENT_NAME_EN, or GROUP_NAME_EN
24.	Please enter a user ID. You cannot use a user ID which includes some symbols (/ \ ? * : " " < > # @ ^) including white spaces or is a white space or a period only. (USER_ID)	The user ID contains an illegal character or characters. Do not use these characters.
25.	A password includes restricted strings. (PASSWORD)	The password contains an illegal character or characters. Do not use these characters.
26.	A mismatch in domain part of user ID. (XXX,YYY)	The domain specified for the user ID is incorrect. Provide the correct domain. The specified incorrect domain is output to <i>XXX</i> and the correct domain is output to <i>YYY</i> .
27.	The domain is not included in user ID. Please input user ID including the domain. (USER_ID)	The user ID does not have the domain. The valid format is <code>user@domain</code> , in which the symbol @ must be followed by the domain name.
28.	Please enter an e-mail address. You cannot use an email string which includes some symbols (/ \ ? * : " " < >) or white spaces. (EMAIL)	The email address has an invalid format or contains an illegal character. Provide a valid email address.
29.	You cannot use a name which includes some symbols (/ \) ? * : " " < > @ ^) or is a white space or a period only. (XXX)	Any of the name, name (kana), and group name (Japanese/Chinese) columns contains an illegal character or characters, or consists of only spaces or periods (.).

No.	Error message	Description
29.	You cannot use a name which includes some symbols (/ \) ? * : " " < > @ ^) or is a white space or a period only. (XXX)	Do not use these characters in the column indicated by XXX. Provide a string that also contains characters other than spaces or periods. One of the followings is output to XXX: NAME, NAME_KANA, or NAME_JA
30.	Please enter an english name. You cannot use an english name which includes some symbols (/ \) ? * : " " < > @ ^) or is a white space or a period only. (XXX)	The name (English) or group name (English) column contains an illegal character or characters, or consists of only spaces or periods (.). Do not use these characters in the column indicated by XXX. Provide a string that also contains characters other than spaces or periods. One of the followings is output to XXX: NAME_EN, PARENT_NAME_EN, or GROUP_NAME_EN
31.	Unknown user locale (XXX). It should be 'ja', 'en' or 'zh'. (LANG).	A string unavailable for the user language is provided. Provide one of the following for the user language: ja, en, or zh.
32.	A user expire date is after 2031/12/31. (EXPIRE_DATE)	The expiration date of the user account is after December 31, 2031. Provide a date on or before December 31, 2031 for the expiration date of the account.
33.	A group expire date is after 2031/12/31. (EXPIRE_DATE)	The expiration date of the group account is after December 31, 2031. Provide a date on or before December 31, 2031 for the expiration date of the account.
34.	A user expire date is before the current date & time. (EXPIRE_DATE)	The expiration date of the user account is before current date. Provide a date on or after the current date for the expiration date of the account.
35.	A group expire date is before the current date & time. (EXPIRE_DATE)	The expiration date of the group account is before current date. Provide a date on or after the current date for the expiration date of the account.
36.	A date format may be invalid because of 'The input date does not exist.'. (EXPIRE_DATE).	The provided expiration date does not exist. Specify a date that exists on the calendar for the expiration date of the account.
37.	A date format may be invalid because of 'The input is not a date format (yyyy/mm/dd or yyyy-mm-dd)'. (EXPIRE_DATE)	The expiration date has an invalid format. Provide the date in yyyy/mm/dd or yyyy-mm-dd format.
38.	A quota size is not a number. (QUOTA)	The provided amount of storage space is not a number. Provide a numeric value, ranging from 0 to 8796093022207.
39.	A quota size is not a natural number. (QUOTA)	The provided amount of storage space is not a natural number. Provide a numeric value, ranging from 0 to 8796093022207.
40.	A quota size is greater than 8796093022207. (QUOTA)	The provided amount of storage space exceeds 8796093022207 MB. Provide a numeric value, ranging from 0 to 8796093022207.
41.	The format of use_user_option is wrong. Please input 'TRUE' or 'FALSE'. (USE_USER_OPTION)	The USE_USER_OPTION column has an invalid format. Provide one of the following values: TRUE or FALSE.
42.	The format of use_guest_user is wrong. Please input 'TRUE' or 'FALSE'. (USE_GUEST_USERS)	The USE_GUEST_USERS column has an invalid format. Provide one of the following values: TRUE or FALSE.
43.	The format of for_guest is wrong. Please input 'TRUE' or 'FALSE'. (FOR_GUEST)	The FOR_GUEST column has an invalid format. Provide one of the following values: TRUE or FALSE.
44.	The format of user_registerable is wrong. Please input 'TRUE' or 'FALSE'. (USER_REGISTERABLE)	The USER_REGISTERABLE column has an invalid format. Provide one of the following values: TRUE or FALSE.

No.	Error message	Description
45.	The format of input_any_address is wrong. Please input 'TRUE' or 'FALSE'.(INPUT_ANY_ADDRESS)	The INPUT_ANY_ADDRESS column has an invalid format. Provide one of the following values: TRUE or FALSE.
46.	The format of flag_delete is wrong. Please input 'TRUE' or 'FALSE'. (FLAG_DELETE)	The FLAG_DELETE column has an invalid format. Provide one of the following values: TRUE or FALSE.
47.	The guest group (XXX) does not allow user registerable. (USER_REGISTERABLE)	For a guest group, the value TRUE cannot be specified for the USER_REGISTERABLE column. Make sure that FALSE is specified. The specified group name (English) is output to XXX.
48.	You can not create the root group manager. (GROUP_NAME_EN)	The top-most group in the hierarchy cannot be specified to GROUP_NAME_EN when creating a group manager. Specify the second or lower level group when creating a group manager.
49.	You exceeded limits of your number of users. Please delete users before you create this user. (USER_ID)	The maximum number of users has been reached, and more users cannot be created. Delete extra users before creating additional users.
50.	This user(XXX)'s belonging is undefined. Please define this user's belonging in [binders]. (USER_ID)	The user cannot be deleted because the system cannot determine the group of the user. Associate the user with a group by using the binder definition section. The provided user ID is output to XXX.
51.	The user (XXX) already exist. (USER_ID)	The user cannot be created because a user with the same user ID already exists. Specify a different user ID. The specified user ID is output to XXX.
52.	The e-mail (XXX) already exist. (EMAIL)	The user cannot be created because a user with the same email address already exists. Specify a different email address. The provided email address is output to XXX.
53.	The group (XXX) already exist. (YYY)	The group cannot be created because a group with the same English group name or with the same Japanese/Chinese group name already exists. Specify another group name (English) or group name (Japanese/Chinese). The provided English group name or Japanese/Chinese group name is output to XXX. For YYY, either of the following is output: NAME_EN or NAME_JA
54.	There is no parent group. (PARENT_NAME_EN)	The specified parent group name (English) does not exist. Specify an existing group name (English).
55.	The user (XXX) does not exist. (USER_ID)	The specified user does not exist. Specify the user ID of an existing user. The specified user ID is output to XXX.
56.	The group (XXX) does not exist. (GROUP_NAME_EN)	The specified group name (English) does not exist. Specify an existing Group name (English). The specified group name (English) is output to XXX.
57.	This user(XXX) already belongs to this group (YYY). (USER_ID)	The specified user is already in the group. The specified user ID is output to XXX.
58.	This user(XXX) cannot be removed from the group(YYY) because the user doesn't belong to it. (USER_ID)	The specified user cannot be disassociated from the group because the user is not a member of the group. The specified user ID is output to XXX and the specified group name is output to YYY.
59.	It is not possible to belong to both a general group and a guest group. (USER_ID)	A user cannot be a member of a user group and a guest group at the same time.
60.	A guest user can belong to only 1 group. (USER_ID)	The guest user cannot be a member of the specified group because the user can be only in a single group.

No.	Error message	Description
61.	This user(XXX) is already a group manager of this group(YYY). (USER_ID)	The specified user is the group manager of the group.
62.	You can not create the root group manager. (GROUP_NAME_EN)	The group manager cannot be specified for the top-level group in the hierarchy.
63.	This user(XXX) cannot become the group manager of this group because this user doesn't belong to this group(YYY). (USER_ID)	The specified user cannot be the group manager because the user is not a member of the group. The user must be a member of the group before being assigned to the group manager.
64.	This user(XXX) cannot become the group manager of this group because this user is already a group manager of another group(YYY). (USER_ID)	The specified user cannot be the manager of the group because the user is already the manager of another group. The user must be unassigned from the group manager before the user can be a group manager of another group.
65.	You cannot delete yourself. (USER_ID)	The user that represents yourself cannot be deleted.
66.	You cannot delete this user (admin@hoge) because some approval routes have only this user as approvers. (USER_ID)	The specified user cannot be deleted because the user is the only approver set in the approval route. Specify a different user as the approver before deleting the user.
67.	The user was not deleted since the user does not exist. (USER_ID)	The specified user cannot be deleted because the user does not exist.
68.	The group hierarchical depth is over the limit 10.	The group is nested to a depth of over 10 levels. Make sure that the parent group is specified so that the entire depth of groups is 10 levels or less.
69.	User cannot belong to more than 10 groups.	The user cannot be a member of 11 groups or more. Make sure that the user belongs to no more than 10 groups.

D. List of Email Messages

JP1/DH - Server sends email messages such as delivery and approval notifications. The table below lists and describes the types of JP1/DH - Server email messages.

Depending of the setting specified by your system administrator, the subjects of the email messages might be different.

Table D–1: List of email messages

No.	Type	Subject of the email message	Description
1	File delivery notification	When the subject is not specified in the New Delivery window: [JP1/DH - Server] File delivery notification	Recipients receive this message when a sender sends a file.
		When the subject is specified in the New Delivery window: [JP1/DH - Server] <i>a-given-subject</i>	
		When the subject is not specified in the New Delivery window: [Reminder] [JP1/DH - Server] File delivery notification	Recipients receive this message if they did not download the file by the specified date.
		When the subject is specified in the New Delivery window: [Reminder] [JP1/DH - Server] <i>a-given name</i>	
2	File delivery confirmation	[JP1/DH - Server] File delivery confirmation	A sender receives this message when the sender sends a file.
3	File delivery notification (opened)	[JP1/DH - Server] File delivery notification (opened)	A sender receives this message when the recipient opens the file. You need to select the Notify me if recipients open my delivery check box in the New Delivery window to have the system send this email to you.
4	File delivery notification (expires soon)	[JP1/DH - Server] File delivery notification (expires soon)	A sender receives this message when the file delivery expires in one more day. You need to select the Notify me if recipients haven't opened my delivery until the day before the expiration. check box in the New Delivery window to have the system send this email to you.
5	File delivery notification (expired)	[JP1/DH - Server] File delivery notification (expired)	A sender receives this message when the file delivery expired. You need to select Notify me if recipients haven't opened my delivery until the expiration. check box in the New Delivery window to have the system send this email to you.
6	Message delivery notification	When the subject is not specified in the New Delivery window: [JP1/DH - Server] Message delivery notification	Recipients receive this message when a sender sends a message.

No.	Type	Subject of the email message	Description
6	Message delivery notification	When the subject is specified in the New Delivery window: [JP1/DH - Server] <i>a-given-subject</i>	Recipients receive this message when a sender sends a message.
7	Message delivery confirmation	[JP1/DH - Server] Message delivery confirmation	A sender receives this email message when the sender sends a message.
8	Approval request notification	[JP1/DH - Server] Approval request notification	Approvers receive this email message if the file delivery requires an approval from them.
		[Reminder] [JP1/DH - Server] Approval request notification	Approvers receive this email message if they do not accept or reject an application for approval by the specified date.
9	Approved-delivery notification	[JP1/DH - Server] Approved-delivery notification	A sender receives this email message when the approver accepts the application for approval.
10	Rejected-delivery notification	[JP1/DH - Server] Rejected-delivery notification	A sender receives this email message when the approver rejects the application for approval.

E. Reference Material for This Manual

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

E.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):

- *Job Management Partner 1 Version 10 Job Management Partner 1/Data Highway - Server User's Guide* (3021-3-361(E))

E.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
Job Management Partner 1/Data Highway - Automatic Job Executor	JP1/Data Highway - AJE	
Job Management Partner 1/Data Highway - Server	JP1/DH - Server	
Red Hat Enterprise Linux 5	Linux	
Red Hat Enterprise Linux 6		

E.3 Conventions: Acronyms

This manual also uses the following acronyms:

Acronym	Full name or meaning
Ajax	Asynchronous JavaScript + XML
CGI	Common Gateway Interface
CN	Common Name
CSS	Cascading Style Sheets
CSV	Comma Separated Values
DIT	Directory Information Tree
DN	Distinguished Name
DOM	Document Object Model
FAQ	Frequently Asked Question
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol over Secure Socket Layer

Acronym	Full name or meaning
ID	Identification Data
JRE	Java(TM) Runtime Environment
LDAP	Lightweight Directory Access Protocol
OS	Operating System
OU	Organization Unit
PC	Personal Computer
PC/AT	Personal Computer/Advanced Technology
SSL	Secure Socket Layer
URL	Uniform Resource Locator
XML	Extensible Markup Language

E.4 Default installation folder

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

Default installation folder

`system-drive:\Program Files\Hitachi\jpldh\server`

E.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.

E.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.

F. Glossary

A

approval route

A rule that consists of approvers of a delivery and conditions of approval. An approval route is included in a delivery rule.

Two or more approvers can be assigned to an approval route. In this case, an approval operation is completed when one of the approvers accepts or rejects the application for approval.

An approval route is managed by a representative user.

approver

A general user who approves applications for deliveries.

audit log

A text file in CSV format in which delivery history in the JP1/DH - Server system is recorded. A representative user can download the file.

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 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 representative user.

authentication system

An authentication system defines and manages the authentication infrastructure information that is used when a user logs in to JP1/DH - Server. An authentication system consists of the standard authentication system and LDAP authentication system.

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

An action of sending files or messages in JP1/DH - Server.

delivery policy

A policy on file transmission including the maximum size and storage period of a file.

A delivery policy is managed by a representative user.

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 representative user is assigned to a domain.

download limit

Total amount of data that can be downloaded in one month. A representative user specifies the download limit.

F

fast communication mode

A setting for high-speed file transmission. A user can select this mode when sending files. However, depending on the environment, files might not be sent in fast communication mode due to the settings of the proxy server and firewall.

G

general user

Sends and receives files by using JP1/DH - Server.

If a general user is granted authority by a representative user or a group manager, the general user is also able to create guest users and manage them.

A general user is managed by a representative user or group manager.

group

A management unit of users.

A group is managed by a representative user or group manager.

group manager

A user who is allowed to manage a group by a representative user or another group manager.

A group manager is able to manage the groups and users in the management target group and view the sending and receiving histories of the group.

guest user

A general user created by another general user with authority to create guest users. A guest user can send and receive files by using JP1/DH - Server. However, a guest user cannot create other users.

A guest user is managed by a representative user or the general user who created the guest user.

L

LDAP authentication system

An authentication system that uses a directory server to authenticate users who try to log in to JP1/DH - Server. The LDAP authentication system is not defined by default.

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 representative user.

P

primary group

The group displayed at the top of the **Groups Belong to** section in the windows for creating or editing a user.

A user inherits the values of some properties (**Expire Date**, **Quota**, **Using User Options**, and **Using Guest Users**) from this group.

The primary group can be changed on the **Groups belongs to** tab in the Edit User window.

Group managers of the primary group and its parent groups can edit, activate, inactivate, or delete a user.

R

recipient

A general user who receives files and messages.

representative user

A user who manages a whole domain. A representative user is managed by the system administrator.

S

sender

A general user who sends files and messages.

standard authentication system

An authentication system that uses a user ID and password or an electronic certificate that are managed by this product for authenticating users who try to log in to JP1/DH - Server. When the product is installed, this authentication system is defined. The standard authentication system cannot be modified or deleted.

T

Total Disk Space

A storage space allocated to a domain. A user cannot send files that exceed the amount of free disk space. A representative user specifies the Total Disk Space.

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 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.

user language

The language used in emails that are sent to a sender, such as a delivery notification. It can be specified in the Users & Groups, Guest Users, and Options windows. The user language specified for the sender is selected by default in the language option field of the New Delivery window.

Index

A

- approval manager 69
- auditing histories 24
- audit log error messages 36
- audit log function 14
- audit log output details 29
- audit logs 29
 - error messages 36
 - example of output audit log 38
 - output details 29
 - output format 29
- authentication linked to directory server 25
- authentication methods 25
 - linked to directory server 25
 - setting 26
 - using user management information in JP1/DH - Server 25
- authentication rule 155
- authentication rules 128
- authentication systems 134
- authentication using user management information in JP1/DH - Server 25

B

- basic operations 46
 - changing display language 50
 - list 46
 - logging in by using directory server 49
 - logging in to JP1/DH - Server by using electronic certificate authentication 48
 - logging in to JP1/DH - Server by using standard password authentication 46
 - logging out of JP1/DH - Server 50

C

- changing display language 50
- configuring authentication system 20
- configuring system 21
- creating guest user 23

D

- delivery histories 96
- delivery rule 152
- delivery rules 120

E

- example of output audit log 38
- explanations of JP1/DH - Server operations 40

F

- faqs 147
 - related to operations performed by group manager 147
 - related to operations performed by representative user 147
- faqs related to operations performed by group manager 147
- faqs related to operations performed by representative user 147
- features in terms of functionality 11
- features in terms of installation and operation 11
- features of JP1/DH - Server 11
- file send and receive function 12
- function
 - audit log 14
 - file send and receive 12
 - user and group management 13
- functional overview of JP1/DH - Server 12

G

- general operation procedure for JP1/DH - Server 20
- general-user operations 52
 - approval manager 69
 - guest user settings 72
 - list 52
 - new delivery 52
 - options 76
 - receiving file by accessing URL in delivery notification email 61
 - receiving file in in-box 63
 - viewing or deleting user's own delivery history 65
- group-manager operations 79
 - delivery histories 96
 - list 79
 - users & groups 79
- guest user settings 72

H

- hardware

prerequisite hardware 16
recommended hardware 16

J

JP1/DH - Server
audit logs 29
authentication methods 25
basic operations 46
features 11
features in terms of functionality 11
features in terms of installation and operation 11
functional overview 12
general operation procedure 20
general-user operations 52
group-manager operations 79
operating 19
operations 40
overview 9
prerequisites for installation 16
representative-user operations 100
user type and authority 39
what is JP1/DH - Server? 10

L

list of icons 42
list of messages
CSV error 157
email 162
list of operations
basic operations 46
general-user operations 52
group-manager operations 79
representative-user operations 100
logging in by using directory server 49
logging in to JP1/DH - Server by using electronic certificate authentication 48
logging in to JP1/DH - Server by using standard password authentication 46
logging out of JP1/DH - Server 50

M

managing users and groups 21
messages
CSV error 157
email 162

N

new delivery 52

O

object definitions 139
operating JP1/DH - Server 19
auditing histories 24
configuring authentication system 20
configuring system 21
creating guest user 23
managing users and groups 21
sending and receiving files 23
setting delivery rule 22
output format of audit log 29

P

prerequisite hardware 16
prerequisite products for specific function or with conditions 18
prerequisites for installation 16
prerequisite software 16

R

receiving file by accessing URL in delivery notification email 61
receiving file in in-box 63
recommended hardware 16
representative-user operations 100
authentication rules 128
authentication systems 134
delivery rules 120
list 100
logs 144
object definitions 139
users & groups (batch management) 101
restrictions related to operations performed by group manager 149
restrictions related to operations performed by representative user 149

S

sending and receiving files 23
setting delivery rule 22
software
prerequisite software 16

T

- temporary restrictions 149
 - related to operations performed by group manager 149
 - related to operations performed by representative user 149
- troubleshooting 146
 - faqs 147
 - temporary restrictions 149

U

- user and group management function 13
- users & groups 79
- users & groups (batch management) 101
- user type and authority 39

V

- viewing or deleting user's own delivery history 65

W

- what is JP1/DH - Server? 10
- window
 - common specifications 41
- window common specifications 41
 - icons 42
 - notes 44
 - window structure 41
- window structure 41