HITACHI
Inspire the Next

Job Management Partner 1 Version 10

Job Management Partner 1/Data Highway - Server Configuration and Administration Guide

Description, User's Guide, Reference, Operator's Guide

3021-3-358(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

This product includes RSA BSAFE Cryptographic software of 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) 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		

■ 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.

■ Issued

Dec. 2014: 3021-3-358(E)

■ Copyright

Preface

This manual describes how to install and set up 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:

- System administrators who introduce, configure, and operate a system that uses JP1/DH - Server

■ 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.

■ File path notation

In this manual, file paths are written on the assumption that a Windows OS is used. If a Linux OS is used and there is no coding for Linux, change a backslash (\) in a file path for Windows to a forward slash (/).

Contents

1 Overview of JP1/DH - Server

This chapter provides an overview of JP1/DH - Server and describes its prerequisites.

1.1 JP1/DH - Server

JP1/DH - Server is a server system that enables high-speed passing of large files among domestic and overseas bases.

If you use JP1/DH - Server in an Internet environment, you can transfer files at high speed to remote locations due to multiplex communication technology. You can also transfer a multiple gigabyte file that is too large to be sent by email over an existing Internet connection without dividing the file into two or more parts.

1.1.1 Features of JP1/DH - Server

Features of JP1/DH - Server are as follows.

(1) Fast, secure, safe transfer of large data via a long-distance low-quality network

JP1/DH - Server adopts multiplex transfer technology# to improve the performance and certainty of file transfers. For this reason, JP1/DH - Server can securely and safely deliver large data at high speed to remote locations including overseas that are a narrow-band area or an area in which network communication is likely to be interrupted.

#: Technology for using multiple HTTPS sessions concurrently.

(2) System operation log that allows you to check who used the system when

You can view events to check who sent or received which file when. In addition, you can download other operation log files to audit the usage status of the system.

(3) Easy introduction for users

You do not need to arrange any dedicated line because your 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.

(4) Multilingual support

Because, in addition to Japanese, web windows in English and simplified Chinese are supported as the JP1/DH - Server user interface, local users in overseas bases can use web windows smoothly.

(5) Automatic data transfer by using JP1/AJS3

By using Job Management Partner 1/Automatic Job Management System 3 (JP1/AJS3), and Job Management Partner 1/Data Highway - Automatic Job Executor (JP1/Data Highway - AJE), you can automate high-speed large file transfer communication by JP1/DH - Server. You can create a job by defining a JP1 jobnet so that large files stored on business servers can be automatically sent to and received from remote locations on a regular basis.

1.2 JP1/DH - Server software configuration

JP1/DH - Server consists mainly of the following three pieces of software: JP1/DH Web application server, JP1/DH Web server, and JP1/DH applet program.

Table 1–1: JP1/DH - Server software configuration

Software configuration	Description
JP1/DH Web application server	This is the main software of JP1/DH - Server. The JP1/DH Web application server runs on a server machine on which JP1/DH - Server is configured and provides the functionality of JP1/DH - Server. This software is the requisite software for JP1/DH - Server.
JP1/DH Web server	This built-in reverse proxy server analyzes SSL communication from a client over HTTPS protocol and transfers it to the JP1/DH Web application server over HTTP protocol. Depending on the network configuration when JP1/DH - Server is configured, JP1/DH Web server can be replaced by another reverse proxy server.
JP1/DH applet program	This applet program is automatically downloaded onto a client machine that communicates with JP1/DH - Server. This software is the requisite software for JP1/DH - Server.

1.3 Prerequisites

This section describes the prerequisites for using JP1/DH - Server.

1.3.1 Prerequisite products and prerequisite products for a specific function or with conditions

Table 1–2: Prerequisite products and prerequisite products for a specific function or with conditions

Server	Prerequisite products and prerequisite products for a specific function or with conditions	
JP1/DH - Server	Prerequisite products	One of the following OSs is required: • Windows Server(R) 2008 R2 Standard (Service Pack 1) • Windows Server(R) 2008 R2 Enterprise (Service Pack 1) • Windows Server(R) 2008 R2 Datacenter (Service Pack 1) • Windows Server(R) 2012 Standard • Windows Server(R) 2012 Datacenter • Windows Server(R) 2012 R2 Standard (with or without Update) • Windows Server(R) 2012 R2 Datacenter (with or without Update) • Red Hat Enterprise Linux 5 • Red Hat Enterprise Linux 6
	Prerequisite products for a specific function or with conditions	If you want to use the delivery notification function, you need a mail server that supports SMTP protocol. The following mail servers have been verified: • Postfix 2.9.5 • Mailstream Switch/MTA 3.3 • Groupmax Version 7 • Microsoft Exchange Server 2010 Note that JP1/DH - Server does not support any email text and message encryption methods (such as S/MIME and PGP).
		If you want to perform user authentication by using a directory server when a user logs in to this product, you need one of the following products: • Windows Server 2012 R2 Active Directory server • Windows Server 2012 Active Directory server • Windows Server 2008 R2 Active Directory server • OpenLDAP V2.4

2 System Configuration

This chapter provides information for determining the configuration of a high-speed file transfer system that uses JP1/DH - Server.

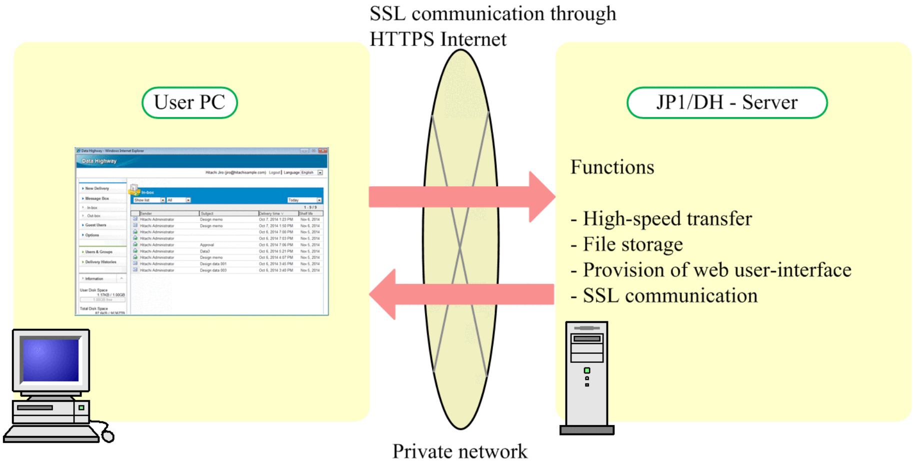
2.1 Network configurations

This section describes different kinds of network configurations for building JP1/DH - Server. JP1/DH - Server is a secure product and only supports SSL (HTTPS) communication. JP1/DH - Server includes a built-in reverse proxy server (JP1/DH Web server), which is responsible for encryption and multiplexing of SSL traffic. However, you can replace the server with another reverse proxy server. A key point to examine when determining your network configuration is how you will install this reverse proxy server.

2.1.1 Example configuration where a JP1/DH - Server machine acts as an access point

This subsection describes a configuration where a single server machine has both the JP1/DH application server and web server installed and configured, and can be directly accessed from a web browser on a client machine.

Figure 2–1: Example configuration where the JP1/DH - Server machine acts as an access point



(1) Features

This configuration can be built and operated by using just a single JP1/DH - Server machine. It is easy to build and operate, but can be adopted only if JP1/DH - Server is used in your private network. If you want to operate JP1/DH - Server on a network connected to the Internet, from a security point of view, consider the other configurations described in *2.1.2 Example configuration for working with a reverse proxy with SSL traffic analyzer* or *2.1.3 Example configuration for working with a reverse proxy with SSL traffic forwarding*.

(2) Software requirements for each machine

Each machine requires the following software:

- Client machine
  A client machine requires a web browser and a JP1/DH applet program.
- JP1/DH - Server machine
  The machine for installation of JP1/DH - Server. The following pieces of software are required:
  - JP1/DH Web application server
  - JP1/DH Web server

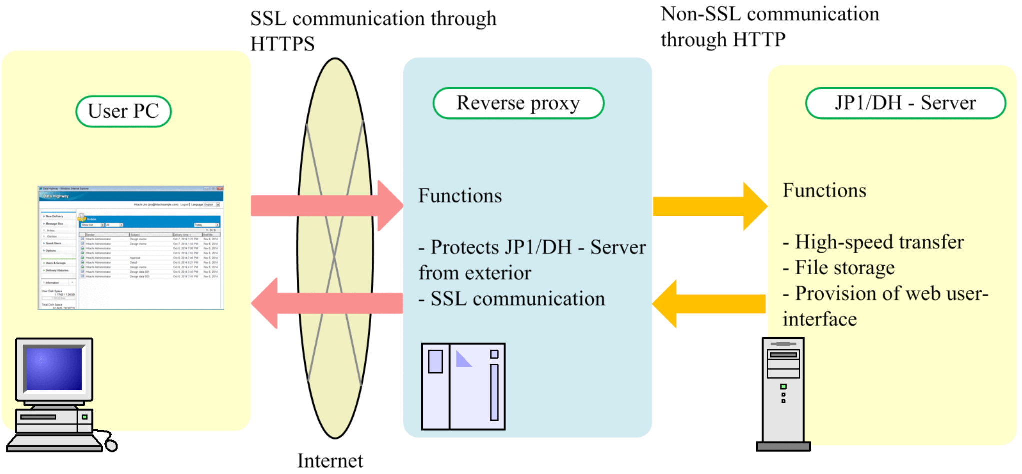
2.1.2 Example configuration for working with a reverse proxy with SSL traffic analyzer

This subsection describes a configuration where a DMZ is secured between a web browser on a client machine and the JP1/DH - Server machine, and a reverse proxy server# with an SSL traffic analyzer resides on the DMZ. If you want to operate your JP1/DH - Server on a network connected to the Internet, use this example configuration as a reference to examine and determine your network configuration.

#

The JP1/DH Web server (built-in reverse proxy server) does not run separately on a machine other than the JP1/DH - Server machine. Therefore, a different reverse proxy server from the JP1/DH Web server is used in this example configuration.

Figure 2–2: Example configuration for working with a reverse proxy with SSL traffic analyzer


SSL communication through HTTPS
Non-SSL communication through HTTP
User PC
Reverse proxy
Functions
- Protects JP1/DH - Server from exterior
- SSL communication
JP1/DH - Server
Functions
- High-speed transfer
- File storage
- Provision of web user-interface
Internet

(1) Features

- This configuration can limit access to JP1/DH - Server only from the reverse proxy server placed on the DMZ and prevent JP1/DH - Server from being accessed directly by client machines.
- A web browser on the client machine communicates with the reverse proxy server over HTTPS, while the reverse proxy server communicates with JP1/DH - Server over HTTP.
- You can separate high-load encryption and multiplexing processes of SSL traffic from the JP1/DH - Server machine, resulting in taking full advantage of performance of the JP1/DH - Server machine for transfer in higher speed.

(2) Software requirements for each machine

Each machine requires the following software:

- Client machine

  A client machine requires a web browser and a JP1/DH applet program.
- Reverse proxy server machine

  A reverse proxy server in this configuration requires functions that analyze HTTPS traffic from web browsers on client machines and forwards the traffic to JP1/DH - Server as HTTP traffic.
- JP1/DH - Server machine

  The machine for installation of JP1/DH - Server. The following pieces of software are required:
  - JP1/DH Web application server

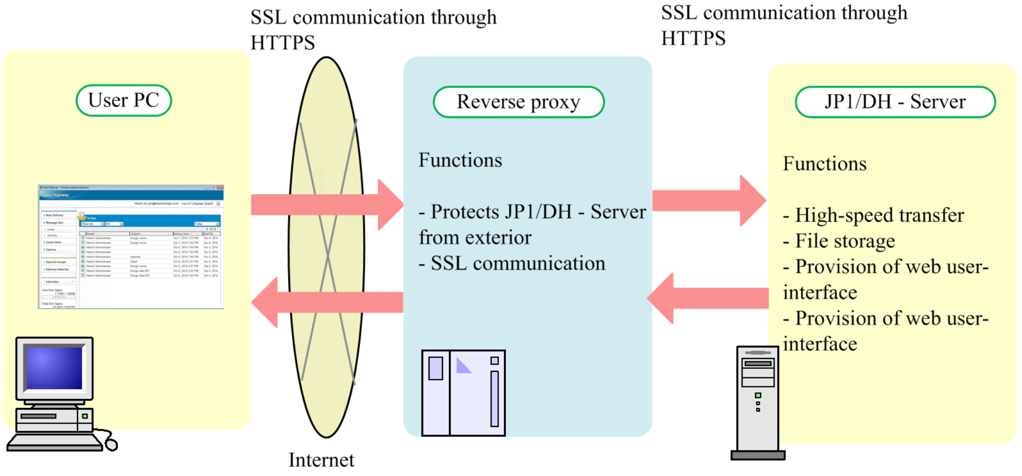
2.1.3 Example configuration for working with a reverse proxy with SSL traffic forwarding

This subsection describes a configuration example where a DMZ is secured between a web browser on a client machine and the JP1/DH - Server machine, and a reverse proxy server# that can forward SSL traffic resides on the DMZ. If you want to operate your JP1/DH - Server on a network connected to the Internet, use this example configuration as a reference to examine and determine your network configuration.

#

The JP1/DH Web server (built-in reverse proxy server) does not run separately on a machine other than the JP1/DH - Server machine. Therefore, a different reverse proxy server from the JP1/DH Web server is used in this example configuration.

Figure 2–3: Example configuration for working with a reverse proxy with SSL traffic forwarding


SSL communication through HTTPS
SSL communication through HTTPS
User PC
Reverse proxy
Functions
- Protects JP1/DH - Server from exterior
- SSL communication
JP1/DH - Server
Functions
- High-speed transfer
- File storage
- Provision of web user-interface
- Provision of web user-interface
Internet

(1) Features

- This configuration can limit access to JP1/DH - Server only from the reverse proxy server placed on the DMZ and prevent JP1/DH - Server from being accessed directly by client machines.
- A web browser on the client machine and the reverse proxy server, as well as the reverse proxy server and JP1/DH - Server, communicate with each other over HTTPS.

(2) Software requirements for each machine

Each machine requires the following software:

- Client machine
  A client machine requires a web browser and a JP1/DH applet program.
- Reverse proxy server machine
  A reverse proxy server in this configuration requires a function that forwards HTTPS traffic from web browsers on client machine to a JP1/DH - Server.
- JP1/DH - Server machine
  The machine for installation of JP1/DH - Server. The following pieces of software are required:
  - JP1/DH Web application server
  - JP1/DH Web server

2.1.4 Notes about the reverse proxy server

A proven reverse proxy server, other than the JP1/DH Web server, that has actually worked is as follows:

- Pound-2.6

2.1.5 Ensuring the network bandwidth

To use the high-speed transfer through multiplexing featured in JP1/DH - Server, the network to which the server is connected must have a sufficient bandwidth. You must use a network environment with a bandwidth of 1 Gbps or higher in order to effectively use this high-speed transfer.

Note that limiting the bandwidth of the network path that reaches the servers where JP1/DH - Server is installed reduces the performance of data transfer and reception.

2.1.6 Notes on network configurations

(1) TCP/UDP port numbers used by JP1/DH - Server

JP1/DH - Server uses the TCP/UDP port numbers listed below. Management software and other software programs that are installed on the JP1/DH - Server machine must be configured not to use these port numbers.

Table 2–1: List of TCP/UDP port numbers used by JP1/DH - Server

Port number	Description
80	Port on which the server listens for HTTP requests
443	Port on which the server listens for HTTPS requests
900	Port on which the server listens for naming-service requests
5432	Port to communicate with the database
8080	Communication port for management
8007	Port on which the server listens for requests from the redirector
14000	Communication port for smart agents
20302	Communication port for processing transaction recovery
20351	Port on which the server listens for events from the shared queue function
23152	Port on which the server listens for RMI registry requests
20295	Communication port for operations management agents

(2) Firewall or proxy setup

A client machine must be able to communicate with JP1/DH - Server by using HTTPS (TCP port 443). The port number is fixed to 443 and cannot be changed.

In addition, a content firewall, proxy, or any other program must not limit the number of concurrent HTTPS connections in order to use high-speed transfers through the multiplexing of JP1/DH - Server.

(3) "hosts" file on the reverse proxy server machine

A host name (computer name) or FQDN that is associated with the global IP address of the reverse proxy server is sometimes defined in the `hosts` file on the proxy server machine. In this case, the following JP1/DH - Server functions have limitations:

- Audit log
  The audit log records IP addresses of client machines accessed to the server. In the environment mentioned above, however, the global IP address of the reverse proxy server machine will be recorded as a client IP address.
- Access control with the network set function
  The network set function, which limits access based on IP addresses of client machines accessed to the server, does not work properly in the above environment.

(4) Number of characters of the authentication ID and password for the proxy server

If a web browser on a client machine accesses the JP1/DH - Server machine via a proxy server, you can specify a maximum of 57 characters for the authentication ID and password for the proxy server.

2.2 Software

This section provides information about software required for building your JP1/DH - Server.

2.2.1 JP1/DH - Server software

Determine the software components to be run on the JP1/DH - Server machine by seeing *2.1 Network configurations*.

Table 2–2: Software components to be run on the JP1/DH - Server machine

JP1/DH - Server software components	Running	Description
JP1/DH Web application server	Required	It must be installed and run on the JP1/DH - Server machine.
JP1/DH Web server	Optional	It does not need to be run if you use a reverse proxy server other than the JP1/DH Web server.#

Legend:

Required: It must be running.

Optional: It is run only if this software component is used.

#

The JP1/DH Web server is always installed on the JP1/DH - Server machine.

2.2.2 Reverse proxy server

If you want to use a reverse proxy server other than the JP1/DH Web server, determine the reverse proxy to be used. In particular, if you build a configuration shown in *2.1.2 Example configuration for working with a reverse proxy with SSL traffic analyzer*, you need a reverse proxy# with the SSL wrapper function.

#

A reverse proxy that has the ability to communicate with client machines over an SSL communication through HTTPS

2.3 Hardware equipment

This section provides information about hardware equipment on which JP1/DH - Server runs.

2.3.1 JP1/DH - Server machine

(1) Preparing dedicated server machine

Your JP1/DH - Server machine must be dedicated to running JP1/DH - Server, and any other system must not reside on this machine together.

JP1/DH - Server features the high-speed file transfer. For functions to perform their best, the system must be able to intensively use resources on the machine, such as CPU, memory, disk I/Os, and bandwidth of the network interface.

(2) Hardware specifications

Information about hardware specifications required for building a JP1/DH - Server machine is as follows.

(a) CPU

CPU performance significantly affects the performance of data transfer and reception. With poor CPU performance, you cannot obtain a satisfactory transfer rate, even with sufficient network bandwidth. The performance of CPUs is affected by some factors, including the clock frequency and number of cores. The CPU requirement for the JP1/DH - Server machine is as follows:

- Dual core 64-bit processor (2.4 GHz or higher)

(b) Memory

JP1/DH - Server consumes a significant amount of memory when transferring and receiving large files or concurrently accepting multiple connections to the system. If the machine has a smaller amount of memory, you cannot obtain a satisfactory transfer rate when a large file is transferred and received, or when multiple files are transferred concurrently. The memory requirement for the JP1/DH - Server machine is as follows:

- 3 GB or more

(c) Required amount of disk space

You can estimate the required amount of disk space by adding together the following disk space amounts:

- Disk space for installing the application: Approximately 2,048 MB#
- Disk space required for the database at run-time: Approximately 32,768 MB#
- Disk space for storing delivery data

  You can estimate this amount based on the average file size of deliveries, the number of deliveries per day, and the storage period of the data by using the calculation formula mentioned below.

  Disk space for storing delivery data:

  Average file size of deliveries (in MB) × number of deliveries per day × maximum storage period of the data (in days)

#: The amount contains a temporary space consumed by the running database, and the actual usage might be somewhat different.

(d) Network interface

Performance of the network interface significantly affects the performance of data transfer and reception. The network-interface requirement for the JP1/DH - Server machine is as follows:

- 1 Gbps or greater

(3) Cluster operations

For the configuration to operate your JP1/DH - Server in a clustered environment, see *C. Configurations for Clustered System Operations*.

(4) Storage redundancy

Storage devices of the JP1/DH - Server machine must be redundant to improve their availability. For example, you can set up your system drives or data-storage drives in a RAID configuration.

In this case, make sure that the redundant configuration will not deteriorate disk I/O performance. Poor disk I/O performance prevents JP1/DH - Server from providing a sufficient transfer rate.

2.3.2 Client machines

(1) Hardware specifications

Information about the hardware specifications required for a client machine is as follows:

(a) CPU

CPU performance significantly affects the performance of data transfer and reception. With poor CPU performance, you cannot obtain a satisfactory transfer rate, even with sufficient network bandwidth. The CPU requirement for the client machine is as follows:

- Dual-core processor (2.0 GHz or higher)

(b) Memory

If the machine has a smaller amount of memory, you cannot obtain a satisfactory transfer rate when a large file is transferred and received. The memory requirement for the client machine is as follows:

- 1 GB or more

(c) Calculation formula for estimating the amount of disk space

When a client accesses JP1/DH - Server, a JP1/DH applet program will be downloaded to that client. The applet program outputs applet logs during data transfer and reception with the system. Make sure that your system has adequate disk space for these logs. You can estimate the capacity necessary for the applet logs by using the calculation formula below.

Capacity necessary for the applet logs:

Average file size of the deliveries (in MB) × 0.06 × number of deliveries per day × 14

(d) Network interface

Performance of the network interface significantly affects the performance of data transfer and reception. The network-interface requirement for the client machine is as follows:

- 100 Mbps or greater

3 Operational Details

This chapter provides information about how to operate JP1/DH - Server.

3.1 Operational parameters

Configure the parameters necessary for installation and environment settings before installing JP1/DH - Server. The parameters consist of required and optional parameters. Make sure that you configure the required parameters before installation. You can configure the optional parameters if necessary. If the optional parameters are not set or modified, JP1/DH - Server runs with its default settings.

3.2 Required parameters

This section provides information about the required parameters.

3.2.1 Installation folder

JP1/DH - Server is installed in the folder below by default. Determine whether you need to change the default folder.

Table 3–1: Default settings for the installation folder

OS	Path to the folder
Windows Server 2008 R2	`C:\Program Files\Hitachi\jp1dh\server\`
Windows Server 2012	
Windows Server 2012 R2	
Linux	`/opt/jp1dh/server`

For a Windows OS, the installation folder can be changed during JP1/DH - Server installation.

3.2.2 Storage folder for delivery data

By default, JP1/DH - Server stores data to be transferred and received in the location listed below. Determine whether you need to change the default folder. We recommend that you estimate the required disk space based on the average file size of delivery data and how frequent the data is sent, prepare a dedicated drive with sufficient free space, and then specify a folder on the drive as a storage location. With regard to the storage folder for the delivery data, note the following:

- Specify a folder on the local file system. You cannot use any network folder or a folder on a network drive.
- The length of the path must be from 4 to 70 characters.

Table 3–2: Default settings for the storage folder for the delivery data

OS	Path to the folder
Windows Server 2008 R2	`C:\Program Files\Hitachi\jp1dh\server\data\`
Windows Server 2012	
Windows Server 2012 R2	
Linux	`/opt/jp1dh/server/data`

The storage folder for the delivery data can be changed in environment setup after JP1/DH - Server installation.

3.2.3 Mail server used by the system

JP1/DH - Server uses email notifications to notify users of data transfers and reception.

If you want to use this function, you need to determine which mail server (SMTP server) receives the email notifications. You can use your choice of mail server as long as it supports the SMTP protocol. If you want to use one of the proven mail servers that have actually worked, see *1.3.1 Prerequisite products and prerequisite products for a specific function or with conditions*.

You can use SMTPS or STARTTLS to encrypt SMTP traffic. To do this, you must first obtain the root certificate of a certificate authority that signed the certificate for SSL traffic that is stored in the mail server that JP1/DH - Server works with. You must then store the root certificate in the JP1/DH - Server server. For information about how to obtain the root certificate, consult with your certificate authority. For details about how to store the root certificate in the JP1/DH - Server server, see *5.3.4 Registering a root certificate*.

The mail server that JP1/DH - Server works with is specified in environment setup after JP1/DH - Server installation.

3.2.4 Sender email address

Determine a sender email address for email notifications that JP1/DH - Server sends to users. This email address is set on the From header of those email notifications.

The sender email address is specified in environment setup after JP1/DH - Server installation.

3.2.5 Directory server used by the system

JP1/DH - Server can use a directory server for user authentication when users log in. If you want to use this function, you need to determine which directory server works with the JP1/DH - Server system.

For details about a list of proven directory servers that have actually worked, see *1.3.1 Prerequisite products and prerequisite products for a specific function or with conditions*. JP1/DH - Server uses the LDAP protocol to communicate with the directory server. You can use LDAPS to encrypt traffic. To do this, you must first obtain the root certificate of a certificate authority that signed the certificate for SSL traffic that is stored in the directory server that JP1/DH - Server works with. You must then store the root certificate in the JP1/DH - Server server.

For information about how to obtain the root certificate, consult with your certificate authority. For details about how to store the root certificate in the JP1/DH - Server server, see *5.3.4 Registering a root certificate*.

3.3 Optional parameters

This section provides information about the optional parameters.

3.3.1 The Java heap memory size

Determine the Java heap memory size for your system. Insufficient Java heap memory size could cause a lower transfer rate or an improper operation of the system during transfer over concurrent connections or during delivery of a large file. You can specify both initial and maximum sizes (in MB) for the Java heap memory. You must set the maximum size to a minimum of 1,024 MB, which is the default setting. You can estimate the preferred value for the maximum size by using the following calculation formula:

Maximum size ≥ default setting of 1,024 MB + (maximum number of concurrent connections × buffer size for transfer and reception)

For details about the maximum number of concurrent connections, see *3.3.4 Concurrent connections*. For details about the buffer size for transfer and reception, see *3.3.8 Buffer size during transfer and reception*.

We recommend that you specify the same size for both initial and maximum values. The following table describes the default settings.

Table 3–3: Default settings for the Java heap memory size

Setting item	Default value
Initial size	1,024 MB
Maximum size	1,024 MB

The Java heap memory size is specified in environment setup after JP1/DH - Server installation.

3.3.2 Network bandwidth limit

JP1/DH - Server provides high-speed data communications by multiplexing connections to take full advantage of the bandwidth of the network on the path. This could occupy the network bandwidth during data communications, thus adversely affecting other communication services. To avoid this situation in your environment, you might have to limit the network bandwidth available to JP1/DH - Server. You can set the limit (in Mbps) separately for both uploading to and downloading from JP1/DH - Server. The following table describes the default settings.

Table 3–4: Default settings for the network bandwidth limit

Setting item	Default value
Upload	Not limited
Download	Not limited

The network bandwidth limit is specified in environment setup after JP1/DH - Server installation.

3.3.3 Keep-alive timeoutperiod

Determine a keep-alive timeout period for data communications. During data communications, JP1/DH - Server clients and servers send and receive bidirectional keep-alive packets to confirm their active connection with each other. If a client or server does not receive any keep-alive packet after the timeout period has elapsed, it assumes that the connection is no longer active and suspends the data communications. It might take some time to send and receive keep-alive packets to and from locations outside of your country or with poor communication line quality. In this case, a short timeout period can often cause interruption of data communications. You can specify the separate timeout periods (in seconds) for both clients and server. The following table describes the default settings.

Table 3–5: Default settings for the keep-alive timeout period

Setting item	Default value
Client	180 seconds
Server	180 seconds

The keep-alive timeout period is specified in environment setup after JP1/DH - Server installation.

3.3.4 Concurrent connections

JP1/DH - Server can accept concurrent connections from multiple clients for transfer. Determine the number of concurrent connections. Specifically, this includes determining the number of initial connections and the maximum number of connections. When starting up, JP1/DH - Server first reserves server resources that allow for as many connections as the number of initial connections. When the number of concurrent connections increases over time and exceeds the initial number of connections, the system dynamically assigns more server resources until the maximum number of concurrent connections is reached.

We recommend that if you know the specific average number of concurrent connections, set the initial number of connections to a value a little greater than the average.

You can set the maximum number of connections to a value based on your own environment, such as the network bandwidth. However, the upper limit for the maximum number of concurrent connections is 64. If the number of concurrent connection requests from clients exceeds the maximum number of connections, those requests are put into the connection queue (which is discussed later) and wait for a connection to become available.

Table 3–6: Default settings for the number of concurrent connections

Setting item	Default value
Number of initial connections	16
Maximum number of connections	16

The number of concurrent connections is specified in environment setup after JP1/DH - Server installation.

3.3.5 Connection queue size

JP1/DH - Server might receive connection requests, from clients, that exceed the defined maximum number of connections (see *3.3.4 Concurrent connections*). If this happens, JP1/DH - Server first stores those requests in its connection queue, making them wait for an available connection. If the system receives additional connection requests from a client when the connection queue is full, the system immediately lets the client know that the server is currently busy.

We recommend that you set the connection queue size to the same value as the maximum number of concurrent connections or greater.

Table 3–7: Default settings for the connection queue

Setting item	Default value
Connection queue size	16

The connection queue size is specified in environment setup after JP1/DH - Server installation.

3.3.6 Storage period of the audit log

JP1/DH - Server records its usage in the audit log. The audit log contains the series of transfers and reception history of files, as well as the operating history such as user or group administrative tasks performed on JP1/DH - Server. Determine how many days the audit log is to be kept in the system. The audit log will have a separate file every day. Audit log files will be removed after their storage period.

Table 3–8: Default settings for the storage period of the audit log

Setting item	Default value
Audit log storage period	365

The audit log storage period is specified in environment setup after JP1/DH - Server installation.

3.3.7 Block size during transfer and reception

Data is transferred in a unit of a particular size, which is called a *block*. Determine a block size for a client to send data to, and to download data from JP1/DH - Server.

By default, the system automatically determines the block sizes depending on the network condition at the beginning of transfer and reception. We recommend the default settings. If, however, you want to always send and receive data in specific block sizes, you can use fixed block sizes. Note that the block size is associated with the buffer size, so you also need to determine the buffer size during transfer and reception.

Table 3–9: Default settings for the block sizes during transfer and reception

Setting item	Default value
Block size for transfer	Automatically determined by the system (maximum: 256 KB)
Block size for downloading	Automatically determined by the system (maximum: 256 KB)

3.3.8 Buffer size during transfer and reception

Determine the size of the buffer per client connection that JP1/DH - Server uses in transfer and reception. You can estimate the buffer size for optimal performance by using the following calculation formula:

Buffer size per client connection ≥ maximum number of TCP connections × block size

For details about the maximum number of TCP connections, see the *Job Management Partner 1/Data Highway - Server System Administrator Guide* and the *Job Management Partner 1/Data Highway - Server Administrator Guide*. For details about the block size, see *3.3.7 Block size during transfer and reception*.

These settings can limit allocation of communication buffer memory to the specified values even if the size of data to be transferred or received is larger than one of the values set here. However, too small of a value can slow the transfer rate.

Table 3–10: Default settings for the buffer size for transfer and reception

Setting item	Default value
Transfer buffer size in JP1/DH - Server	8 MB
Reception buffer size in JP1/DH - Server	8 MB

3.3.9 Packet queue size of clients

Determine the packet queue size for clients. You can estimate the packet queue size for optimal performance by using the following calculation formula:

Packet queue size ≥ maximum number of connections × block size × 2

For details about the maximum number of connections, see *3.3.4 Concurrent connections*. For details about the block size, see *3.3.7 Block size during transfer and reception*.

Table 3–11: Default setting for the packet queue size of clients

Setting item	Default value
Packet queue size of clients	16 MB

3.3.10 Maximum size of files available for transfer

Determine the maximum size of a single delivery attempt and the maximum file size per file. You can see the specified values in the window for creating or editing delivery policy on the web interface.

If you want any files or folders over 4 GB to be compressed when transferred, see *3.3.16 Displaying the Compress Method options*.

Table 3–12: Default settings for the maximum size of files available for transfer

Setting item	Default value
Maximum size per delivery	50 GB
Maximum size per file	50 GB

3.3.11 Password obfuscation (SALT string)

Consider using a SALT string so that user passwords cannot be cracked easily. Specifying the SALT string makes it difficult to analyze an encrypted password, preventing the original password from being guessed easily.

Table 3–13: Default settings for the password

Setting item	Default value
Password	Clear text

3.3.12 Maximum storage period of files

Determine how many days files to be transferred are to be kept in the system.

Table 3–14: Default setting for the maximum storage period of files

Setting item	Default value
Storage period	31 days

3.3.13 Maximum number of destinations

Determine the maximum number of destinations that a user can specify for a delivery on the web interface. The maximum number represents the sum of approvers and recipients. For details about this value when JP1/Data Highway - AJE is used, see *3.3.22 Maximum number of destinations when using JP1/Data Highway - AJE*.

Table 3–15: Default setting for the maximum number of destinations

Setting item	Default value
Maximum number of destinations	100

3.3.14 Enabling or disabling the initial environment setup function

Determine whether to create a default address book and delivery policy when you create a domain. If you use this function, the address book, delivery policy, and delivery rule will be automatically created when you create a domain. This allows you to reduce the time to actually start a file delivery after the domain creation.

Table 3–16: Default setting for the initial environment setup function

Setting item	Default value
Initial environment setup function	FALSE

3.3.15 Default setting for the processing status type of deliveries to be displayed in the in-box

Determine delivery data with which processing status is displayed in the in-box by default. A user's in-box displays deliveries with the specified default status type. You can choose one of the following processing statuses: **Not opened**, **Opened**, and **All**. Setting the default delivery status for display on the window allows users to identify processing statuses in the in-box at a glance.

Table 3–17: Default setting for the processing status type for deliveries to be displayed in the in-box

Setting item	Default value
Status	**All**

3.3.16 Displaying the Compress Method options

Determine whether to display the Compress Method options in the window for creating or editing delivery policy.

If the Compress Method options are not displayed in the window, the system uses the extended compression method for file transfer. The extended compression method allows you to compress files and folders over 4 GB in size.

If the Compress Method options are displayed, both **Standard**, and **Extended** are displayed as options for Compress Method. If you need to transfer data in the standard compression method, display the Compress Method options.

For JP1/Data Highway - AJE, the JP1/Data Highway - AJE 10-10 and later versions can receive delivery data in the extended compression method. JP1/Data Highway - AJE 10-00 ignores delivery data in the extended compression method. In addition, a single reception attempt might contain mixed data deliveries in extended and other compression methods, which causes an error with the delivery only in the extended compression method. To avoid this, you must use an appropriate delivery policy according to the version of JP1/Data Highway - AJE for reception.

Table 3–18: Default settings for whether the Compress Method options are displayed

Setting item	Default value
Whether the Compress Method options are displayed upon new installation	FALSE

3.3.17 External storage options for the data sent by using the extended compression method

If you want to scan delivery data for viruses on the server, determine where and how the data is stored on the server.

When sending files or folders, JP1/DH - Server stores copies of the sent files or folders on the server. If a folder is sent with a delivery policy by using the extended compression method, or if a file or folder is sent in one of **STRONG**, **MIDDLE**, or **WEAK** of the **Compress Level** setting, the system uses its own compression scheme to store the file or folder on the server. As a result, a virus scan on the delivery data cannot detect any virus. In such a case, consider storing (to an external location) some of the sent files without compression. The settings for externally stored files consist of the number of files stored externally and the upper limit of the total file size (in KB).

Externally-stored files consume disk space where the delivery data is stored. We recommend that you do not store the delivery data externally unless you intend to scan the data for viruses.

Table 3–19: Default settings for the external storage options for extended compression method

Setting item	Default value
Maximum number of files to be externally stored from among files or files in a folder in a single delivery	0 (not stored externally)
Maximum total file size of files to be externally stored from among files or files in a folder in a single delivery	0 (not stored externally)

3.3.18 Displaying the options related to number of TCP connections

Determine whether to display the items for **Max. TCP sessions per Connection** and **Always connect with Max. TCP sessions** in the window for creating or editing delivery policy. If these items are displayed, you can configure settings related to TCP connections not only in the window for the default delivery policy but also in other delivery policy windows.

Table 3–20: Default settings for the options related to number of TCP connections

Setting item	Default value
Displaying **Max. TCP sessions per Connection**	FALSE
Displaying **Always connect with Max. TCP sessions**	FALSE

3.3.19 Timeout period when using a directory server

You can use a directory server to authenticate users who try to log in to JP1/DH - Server. Before doing this, you need to determine the timeout period for connecting to the directory server and for searching the directory server for a user.

Table 3–21: Default settings for the timeout period when using the directory server

Setting item	Default value
Timeout period for connecting to the directory server	30,000 milliseconds (30 seconds)
Timeout period for searching for a user	30,000 milliseconds (30 seconds)

3.3.20 Approval exclusion function when using JP1/Data Highway - AJE

Consider using this function when using JP1/Data Highway - AJE. If you activate this function, an approval route can be skipped for transfer when a delivery rule specifies the approval route if JP1/Data Highway - AJE is used to transfer a file or folder.

Table 3–22: Default setting for the approval exclusion function

Setting item	Default value
Approval exclusion function	FALSE

3.3.21 Using the file validation disabling function when using JP1/Data Highway - AJE

Consider using this function when using JP1/Data Highway - AJE. This function disables the file validation when JP1/Data Highway - AJE is used to transfer a file, thus reducing the time spent on transferring. Receiving delivery data through this function on JP1/Data Highway - AJE version 10-00 causes an error, and the system ignores that delivery. If the file validation disabling function is not enabled, the system can receive that delivery data without any error.

Table 3–23: Default setting for the file validation disabling function

Setting item	Default value
File validation disabling function	FALSE

3.3.22 Maximum number of destinations when using JP1/Data Highway - AJE

Consider specifying this item when JP1/Data Highway - AJE is used. You need to determine the maximum number of possible destinations when using JP1/Data Highway - AJE to transfer a file or folder. With a valid value specified, the number of destinations set here takes precedence over the maximum number of destinations defined in a delivery policy. The maximum number represents the sum of approvers and recipients.

Table 3–24: Default setting for the maximum number of destinations when using JP1/Data Highway - AJE

Setting item	Default value
Maximum number of destinations	0 (uses the maximum number of destinations defined in the delivery policy)

3.4 Operations with system capacity in mind

This section covers capacity planning of the JP1/DH - Server system, such as the number of groups, users, and delivery rules. Before the system goes live, you need to plan operations with the capacity in mind.

For details about how to configure individual capacity settings mentioned below, see the *Job Management Partner 1/Data Highway - Server System Administrator Guide* and the *Job Management Partner 1/Data Highway - Server Administrator Guide*.

3.4.1 User capacity

As the number of users increases, more users access the system at the same time.

Therefore, you need to limit the maximum number of users of the system. For example, the number of concurrently-logged-in users to a single server system must be 100 users or less. The number of concurrent connections for high-speed transfer must be within the range mentioned in *3.3.4 Concurrent connections*. The size of the connection queue for high-speed transfer must be within the range mentioned in *3.3.5 Connection queue size*.

If the number of users will exceed the upper limit of a single server system, you need to choose to add a further JP1/DH - Server server so that users can share the servers. Note that one JP1/DH - Server server cannot send and receive files with another server.

3.4.2 Group capacity

As the number of groups increases, it takes a longer time to display the list of groups in the Users & Groups window, which system administrators or representative users can use.

The number of groups must be 1,000 groups or less within an entire single server system.

The groups can be nested to a maximum of 10 levels. You need to consider the upper limit of the level to determine the hierarchical structure of your groups.

3.4.3 Address book capacity

A user uses an address book for sending a file on JP1/DH - Server. As the number of users to be displayed in the address book increases, it takes proportionally more time to display all the addresses in the address book. Therefore, you need to determine the structure and display settings of groups so that the minimum number of required users appear in a user's address book.

We recommend the setting such that 100 or less users are displayed in an address book.

3.4.4 Other objects capacity

The table below lists and describes what impacts arise when system administrators or representative users create more objects, and the capacities of each object. You need to plan operations such that the minimum required number of objects is created.

Table 3–25: Capacities of other objects

Object	Impacts	Capacity#
Delivery rule and delivery policy	• Increased time to fill destination data in the destination fields when a user chooses an address in the address book for sending a new file. • Increased time for a list of delivery rules or delivery policies to be displayed to system administrators or representative users.	100 each for rules and policies in an entire single server system
Authentication rule and authentication policy	• Increased time for the initial window to be displayed after a user logs in to JP1/DH - Server. • Increased time for a list of authentication rules or authentication policies to be displayed to system administrators or representative users.	100 each for rules and policies in an entire single server system
Network set	• Increased time for the initial window to be displayed after a user logs in to JP1/DH - Server. • Increased time for a list of network sets for system to be displayed to administrators or representative users.	100 in an entire single server system
Approval route	• Increased time for a list of approval routes to be displayed to system administrators or representative users.	100 in an entire single server system

#: If you have multiple domains created, the capacity represents the total of objects in each domain.

3.5 Operational tasks

This section describes operational tasks performed on the JP1/DH - Server machine.

For details about system administrative tasks, such as creating authentication policies or setting representative users, see the *Job Management Partner 1/Data Highway - Server System Administrator Guide*. For details about representative user's or group manager's operational tasks, such as adding groups or users, see the *Job Management Partner 1/Data Highway - Server Administrator Guide*.

3.5.1 Secure operations

If you want to operate your JP1/DH - Server accessible to and from the Internet, you need to protect the system against server attacks or unauthorized access from a third-party. This subsection covers information related to secure operations of the system.

Also, even if you operate JP1/DH - Server in your private network, you can make use of the information depending on the security level you want.

(1) OS operations that follow security guides from your OS vendor

Examples of measures required to build and maintain a secure JP1/DH - Server machine environment include the following:

- Having appropriate control over users, roles, and privileges for the OS
- Eliminating unnecessary services and applications and limiting the role that the JP1/DH - Server machine plays
- Monitoring logs and audit records

Security guides for Windows are available from the Microsoft web site. Follow these guides to take necessary measures.

(2) Access permissions

To control who and which systems have access to JP1/DH - Server, example measures include the following:

- Filter access to the JP1/DH - Server server by using, for example, a reverse proxy.
- Check logs of the reverse proxy periodically for any unauthorized access or attacks.
- Consider taking measures such as blocking access from terrorist-supporting states or countries under a trade embargo.

(3) Virus scanning

When a user attempts to send a file, JP1/DH - Server copies it to a folder on the JP1/DH - Server machine, keeping it temporarily. This might result in storing a virus-infected file in the JP1/DH - Server machine if a user sends an infected file. JP1/DH - Server does not execute these files on the machine or open them with a corresponding application. However, spreading the virus-infected file to recipients must be avoided. For this purpose, you need to consider operations to install an anti-virus software on the JP1/DH - Server machine, and to monitor whether any virus-infected files are detected.

For details about the storage location for files sent and received by users, see *3.2.2 Storage folder for delivery data*.

If an anti-virus program removes a file to be transferred or received from the disk on the JP1/DH - Server machine, the system deactivates the **Download** button on the web user-interface, disabling downloads of the file.

3.5.2 Resource monitoring

You need to use a tool, such as a resource monitoring tool, to monitor the usage of resources listed in the table below in order to check the running JP1/DH - Server for resource shortage.

You can view system and resource usage summaries in the System Monitor window, which system administrators can open on the web interface. For more information, see the *Job Management Partner 1/Data Highway - Server System Administrator Guide*.

Table 3–26: Monitored resource

Monitored resource	Description
CPU usage	High CPU usage can lead to a declining system response time over time. In this case, the system might be running out of CPU resources compared to CPU usage. If this happens, you need to consider operations, such as installing additional CPUs, or adding a JP1/DH - Server server so that users can share the servers.
Memory usage	High memory usage can lead to an out-of-memory error or a declining system response time over time. In this case, the system might be running out of memory resources compared to memory usage. If this happens, you need to consider operations, such as installing extra memory to set a larger value for the Java heap size of the JP1/DH - Server server, or adding a JP1/DH - Server server so that users can share the servers.
Disk I/O	High disk I/O can lead to a declining system response time over time. In this case, the system might be running out of disk I/O performance compared to disk usage. If this happens, you need to take measures such as replacing your hard disks with ones that offer higher disk I/O performance.
Disk usage	Insufficient free disk space due to high disk usage can cause an error, preventing the system from working properly. The errors include storage errors of files to be sent or received, data storage errors in the database, and write errors of files necessary to run the system such as server logs. If disk usage becomes higher, you need to have free disk space by backing up unnecessary log files and other files, or consider adding extra disk space by installing another disk drive.
Network usage	High network usage can lead to declining throughput values of file transfers recorded in the JP1/DH - Server audit log. In this case, the system can be running out of network bandwidth compared to system usage. If this happens, you need to consider increasing the capacity in your network infrastructure so that the system can use more network bandwidth.

3.5.3 Alive monitoring

With your system operation, you need to consider whether to adopt the alive monitoring mechanism which monitors for a continuous operation of the JP1/DH - Server server. Note the following points when performing alive monitoring:

- To perform the alive monitoring of JP1/DH - Server over the network, send HTTP GET requests to the login window (`https://servername/index.jspx`) of JP1/DH - Server at regular intervals, and check for responses. If the system does not respond to successive requests, or if server error responses (HTTP status code 5*xx*) are continuously returned, contact your operational administrator.
- Sending an HTTP GET request to the login window of JP1/DH - Server causes access from the web server to the database. Thus, this approach allows you to detect whether the JP1/DH - Server database has a failure or is down.

- Perform the alive monitoring over the network on a different machine from the JP1/DH - Server machine. Also, use the same network path as the one that users actually use for access to JP1/DH - Server. In this way, you must monitor whether the service is down because of a failure in the network infrastructure or a device before JP1/DH - Server is reached.

3.5.4 Monitoring the mail server

JP1/DH - Server uses a mail server to send email messages such as file delivery notifications. You might have to consider monitoring the mail server for proper delivery of the email messages. Keep the following in mind when considering this for operation:

- An email delivery error can occur on the mail server, but JP1/DH - Server does not detect the error. Examples of causes of the errors include an incorrect or removed email address for a user in the JP1/DH - Server system, a stopped destination mail server, rejected delivery of email messages on the destination mail server.

  Because of this, you must use the logs or monitoring function offered by your mail server to check for proper delivery of email messages.
- JP1/DH - Server does not provide a function that resends email messages such as delivery notifications. If an email message needs to be resent because of an email delivery error, use the function on the mail server to resend the message.

  If your mail server cannot resend the message, identify and resolve the cause of the error, and then transfer the file again on JP1/DH - Server. Email messages sent from JP1/DH - Server are intended to notify users and prompt them to download a delivered file or approve the delivery. The users can use these functions by logging in to JP1/DH - Server, instead of clicking a URL on the body of the email message.

3.5.5 Import/export control on files sent or received

Users must comply with laws and regulations related to importing and exporting if they send or receive electronic files or information contained in those files to or from users outside of your country or non-resident users. For import and export control, consult with your import and export control department, and determine how you handle it.

3.6 Maintenance

This section describes maintenance tasks performed on the JP1/DH - Server machine.

3.6.1 Notes about the What's new function

The What's new function displays messages from the system administrator to JP1/DH - Server users in the login window. It can be used for notifying the users of events, such as shutting down the JP1/DH - Server machine for system maintenance. The following steps show how to use the What's new function:

1. Log in as a built-in Administrator user (for Windows) or root user (for Linux).

2. Determine which file you need to edit.

   Each display language has its own language file to be edited. You must choose the file you need and edit it.

   For Japanese:

   ```
   installation-folder#\uCPSB\CC\web\containers\jp1dh\webapps\digikatsuwide
   \digikatsuwide\WEB-INF\jsp\themes\digivery\index_information_ja.jsp
   ```

   For English:

   ```
   installation-folder#\uCPSB\CC\web\containers\jp1dh\webapps\digikatsuwide
   \digikatsuwide\WEB-INF\jsp\themes\digivery\index_information_en.jsp
   ```

   For Chinese:

   ```
   installation-folder#\uCPSB\CC\web\containers\jp1dh\webapps\digikatsuwide
   \digikatsuwide\WEB-INF\jsp\themes\digivery\index_information_zh.jsp
   ```

   #: In Linux, change *installation-folder* to `/opt/jp1dh/server`.

3. Edit the message.

   Enter the message# you want to display in the login window.

   ```
   <div style="font-size: 12px;">your-message</div>
   ```

   #: The field you edit is part of the HTML code. Do not use any special characters of the HTML language.

   Example:

   ```
   <div style="font-size: 12px;">[Maintenance notice] This service will
   be unavailable because of system maintenance during the following
   period: From 21:00 to 22:00 on MM DD, YYYY</div>
   ```

4. Apply the changes.

   Start the command prompt and run the command below for the edited message to take effect in the login window.

   In Windows

   ```
   installation-folder\bin\reload_app.bat
   ```

   In Linux

   ```
   /opt/jp1dh/server/bin/reload_app.sh
   ```

Important note

If the login window does not appear properly after this edit operation is performed, restore the edited message in the file to its original message. If the message cannot be reverted to the original one, copy the following files to the file path mentioned above and overwrite these files:

- *installation-folder*#`\misc\digikatsuwide\digikatsuwide\WEB-INF\jsp\themes\digivery\index_information_ja.jsp`
- *installation-folder*#`\misc\digikatsuwide\digikatsuwide\WEB-INF\jsp\themes\digivery\index_information_en.jsp`
- *installation-folder*#`\misc\digikatsuwide\digikatsuwide\WEB-INF\jsp\themes\digivery\index_information_zh.jsp`

#: In Linux, change *installation-folder* to `/opt/jp1dh/server`.

3.6.2 Registering the number of purchased user licenses

You can register the number of user licenses you purchased in JP1/DH - Server. The number of user licenses you registered appears in the sidebar area of the JP1/DH - Server window, together with the number of registered users in the entire system.# This function allows you to easily confirm that the number of registered users across the entire system does not exceed the number of purchased user licenses.

For details about how to register the number of purchased user licenses, see *8.3.4 regist_users_number.bat (registering the number of purchased user licenses)*.

#: Only a system administrator can see it.

3.6.3 Time clock synchronization of the server

JP1/DH - Server records file-transfer-and-reception times in the audit log. You need to consider time clock synchronization with an NTP server so that the system can record correct times in the log. If the date changes due to time synchronization with the NTP server, log integrity cannot be maintained. To avoid this, do not synchronize the server time around midnight.

3.6.4 Maintaining log files

After starting operation, the JP1/DH - Server server (and related systems) output data to various logs.

Log files for the data output from JP1/DH - Server roll over when they reach a certain size, and older generations of the log files are removed automatically.

You need to maintain logs of related systems such as the OS on which JP1/DH - Server is installed, mail server, and reverse proxy, by backing up or removing the log files periodically according to the logging specifications for each system.

The following table lists and describes folders in which JP1/DH - Server outputs its log files.

Table 3–27: Log output folders

Log output folder	Description
installation-folder# `\log`	The JP1/DH Web application server outputs its data to the log file in this folder.
installation-folder# `\uCPSB\httpsd\logs`	The JP1/DH Web server outputs its data to the log file in this folder.
installation-folder# `\PostgreSQL\9.2\data\pg_log`	The database used by JP1/DH - Server outputs its data to the log file in this folder.

#: In Linux, change *installation-folder* to `/opt/jp1dh/server`.

The following table lists and describes the maximum capacity per file and number of output files for each log file.

Table 3–28: Maximum capacities and number of output files for log files

Log output folder	Log file name	Description	Maximum capacity per file	Number of files
installation-folder#1 `\log`	`jp1dh-audit.log.`*YYYY_MM_DD*#4	JP1/DH - Server audit log	Variable#2	365#3
	`user_err[`*n*`].log`	JP1/DH - Server error log	1,024 KB	2
	`user_out[`*n*`].log`	JP1/DH - Server log	1,024 KB	2
	`web_servlet[`*n*`].log`	Web servlet log	1,024 KB	4
	`javalog[`*nn*`].log`	Log for maintenance information and garbage collection of Java VM	256 KB	4
	`ehjavalog[`*nn*`].log`	Event log for the Explicit heap function	4,096 KB	4
	`cjmessage[`*n*`].log`	Operation log	1,024 KB	2
	`cjexception[`*n*`].log`	Exception information in the event of a failure	1,024 KB	2
installation-folder#1 `\log\WS`	`c4webcl-default-[`*n*`].log`	Trace file	2,048 KB	2
installation-folder#1 `\log\WS\maintenance`	`c4webcl-default-[`*n*`].log`	Trace file	2,048 KB	2
installation-folder#1 `\log\watch`	`cjhttpsessionwatch[`*n*`].log`	Monitoring log for HTTP sessions	1,024 KB	2
	`cjmemorywatch[`*n*`].log`	Monitoring log for memory usage	1,024 KB	2
	`cjrequestqueuewatch[`*n*`].log`	Monitoring log for the HTTP request execution queue	1,024 KB	2
	`cjthreaddumpwatch[`*n*`].log`	Monitoring log for thread dump files	1,024 KB	2
	`cjthreadwatch[`*n*`].log`	Monitoring log for threads	1,024 KB	2
installation-folder#1 `\log\http`	`cjhttp_access.inprocess_http[`*n*`].log`	Processing results of the in-process HTTP server	4,096 KB	16

Log output folder	Log file name	Description	Maximum capacity per file	Number of files
installation-folder[#1]\log\http\maintenance\comm	cjhttp_comm.[*YYYYMMDDHHmmssSSS*].inprocess_http.mm[#4]	Communication tracing information	16,998.4 KB	16
installation-folder[#1]\log\http\maintenance\thr	cjhttp_thr.*YYYYDDMMHHmmssSSS*.inprocess_http.mm[#4]	Thread tracing information	3,276.8 KB	16
installation-folder[#1]\log\CC\maintenance	cj_shutdown[*n*].log	Finished-process information	1,096 KB	2
	cjconsole[*n*].log	Console message	1,024 KB	2
	cjejbcontainer[*n*].log	Maintenance information on the EJB container	1,024 KB	2
	cjmaintenance[*n*].log	Maintenance information	16 KB	4
	cjstdout.log	Standard output information from running processes	1,048 KB	1
	cjstdout_save.log	Backup of the standard output information from running processes	1,048 KB	1
	cjwebcontainer[*n*].log	Maintenance information on the web container	1,024 KB	2
installation-folder[#1]\log\CC\rmi	cjrmi[*n*].log	RMI communication log of the J2EE server	1,024 KB	4
installation-folder[#1]\PostgreSQL\9.2\data\pg_log	postgresql-[*DD*].log	Database log	Variable[#2]	31
installation-folder[#1]\uCPSB\httpsd\logs	access.[*nnnnnnnnnn*]	JP1/DH Web server access log	Variable[#2]	8
	error.[*nnn*].	JP1/DH Web server error log	8,192 KB	5
	hwsrequest.[*nnnnnnnnnn*]	JP1/DH Web server request log	Variable[#2]	8

#1

In Linux, change *installation-folder* to /opt/jp1dh/server.

#2

The system creates one file per day. The size of the file depends on usage.

#3

The storage period of the audit log is an adjustable operational parameter.

#4

YYYY: Year
MM: Month

DD: Day

HH: Hour

mm: Minute

ss: Second

SSS: millisecond

3.6.5 Backup and restore

This section describes how to back up and restore part of JP1/DH - Server data.

To back up and restore the entire system on the server where JP1/DH - Server is installed, use a backup tool, such as a commercially available tool.

(1) Performing a backup operation

Perform the procedures described below to back up the JP1/DH - Server database, storage folders for delivery data, log files, and configuration files.

You can perform a backup operation with the JP1/DH Web application server running. If, however, you want to take snapshot of the system before the backup, let users know that the service will be down, shut down the JP1/DH Web application server, and then back data up while JP1/DH - Server is unavailable to the users.

- Use the `dbbackup.bat` command to back up the database. For details about how to use the command, see *8.3.1 dbbackup.bat (backing up the database)*.
- Back up all files and folders in the storage folder for delivery data defined in *3.2.2 Storage folder for delivery data* in some way, such as a file copy command.
- Back up log files output from JP1/DH - Server in some way such as a file copy command. For details about where the log files are output, see *3.6.4 Maintaining log files*.
- Back up the files edited and created in *5.3 Setting up the JP1/DH Web application server environment* in some way, such as a file copy command.

(2) Performing a restore operation

Perform the procedures described below to restore the JP1/DH - Server database, storage folders for delivery data, log files, and configuration files.

Before the restore operation is performed, let users know that the service will be down, shut down the JP1/DH Web application server, and then restore data while JP1/DH - Server is unavailable to the users.

- Restore the files edited and created in *5.3 Setting up the JP1/DH Web application server environment* from their backups in some way, such as a file copy command, if necessary.
- Restore backups of the log files output from JP1/DH - Server in some way, such as a file copy command, if necessary. For details about where the log files are output, see *3.6.4 Maintaining log files*.
- Restore all the backed-up files and folders to the storage folder for delivery data defined in *3.2.2 Storage folder for delivery data* in some way, such as a file copy command.
- Use the `dbrestore.bat` command to restore the database. For details about how to use the command, see *8.3.2 dbrestore.bat (restoring the database)*. To use the `dbrestore.bat` command, the database service (`JP1_DH_DATABASE_SVR`) must be running.

3.6.6 Emergency login

If a system administrator cannot log in to the system because an incorrect authentication rule for system administrators is applied, perform the procedures described below to allow for an emergency login to the system#. After the successful emergency login, disable the authentication rule for system administrators in question. For details about the authentication rule for system administrators, see the *Job Management Partner 1/Data Highway - Server System Administrator Guide*.

#

With the emergency login active, users other than system administrators cannot log in to the system. After disabling the authentication rule for system administrators in question, remember to disable the emergency login.

1. Log in as a built-in Administrator user.

2. Stop the JP1/DH Web application server.

   You must stop the `JP1_DH_WEB CONTAINER` service for Windows, or the `JP1_DH_WEBCON` service for Linux. For details about how to stop the service, see *6. Starting and Stopping*.

3. Edit the `digikatsuwide.xml` file.

   (a) File path

   ```
   installation-folder#\uCPSB\CC\web\containers\jp1dh\webapps\digikatsuwide
   \digikatsuwide\WEB-INF\digikatsuwide.xml
   ```

   #: In Linux, change *installation-folder* to `/opt/jp1dh/server`.

   (b) Part you must edit in the file

   Change the value in the following element from `false` to `true`.

   [Before change]

   ```
   <biz-connect>
       <emergency-login>false</emergency-login>
   </biz-connect>
   ```

   [After change]

   ```
   <biz-connect>
       <emergency-login>true</emergency-login>
   </biz-connect>
   ```

4. Start the JP1/DH Web application server.

   You must start the `JP1_DH_WEB CONTAINER` service for Windows, or the `JP1_DH_WEBCON` service for Linux. For details about how to start the service, see *6. Starting and Stopping*.

5. Disable the authentication rule for system administrators.

   Log in to JP1/DH - Server, and then disable the authentication rule for system administrators in question. After this is done, change the value of the emergency-login element back from `true` to `false` and restart the JP1/DH Web application server.

3.7 Email customization

If you want to use email notifications for deliveries or approvals, you can customize the subject and body of email messages sent by JP1/DH - Server.

3.7.1 List of customizable email notifications

The following table describes email notifications you can customize and names of their email template files.

Table 3–29: Customizable email templates

No.	Type of email notification	Email template file name#	Related subsection
1	File delivery notification	`delivery_notification_ja.xml`	*3.7.5*
2	File delivery notification (reminder)	`notification_not_downloaded_ja.xml`	*3.7.6*
3	File delivery confirmation	`delivery_ confirmation_ja.xml`	*3.7.7*
4	File delivery notification (opened)	`delivery_opened_notification_ja.xml`	*3.7.8*
5	File delivery notification (expires soon)	`notification_before_expired_ja.xml`	*3.7.9*
6	File delivery notification (expired)	`notification_after_expired_ja.xml`	*3.7.10*
7	Approval request notification	`delivery_approval_notification_ja.xml`	*3.7.11*
8	Approval request notification (reminder)	`notification_not_approved_ja.xml`	*3.7.12*
9	Approved-delivery notification	`delivery_accepted_confirmation_ja.xml`	*3.7.13*
10	Rejected-delivery notification	`delivery_rejected_confirmation_ja.xml`	*3.7.14*

#

These are the names of the Japanese files. For the names of English or Chinese files, see the sections for each template file in the later sections.

3.7.2 How to customize email notifications

To customize your email notifications:

1. Stop the JP1/DH - Server services by seeing *6.1.2(1) Stopping services* for Windows, or *6.2.2(1) Stopping services* for Linux.

2. Select the email template file to be customized in *installation-folder*# `\misc\digikatsuwide\digikatsuwide\WEB-INF\classes\jp\clealink\digivery\notifier\template\` where the email template files for editing are stored.

3. Edit the message subject or message body in the template file, and then save the file.

4. Change the configuration of your application by seeing *5.3.2 Changing the application configuration*.

5. Start the JP1/DH - Server services by seeing *6.1.1(1) Starting services* for Windows, or *6.2.1(1) Starting services* for Linux.

#: In Linux, change *installation-folder* to `/opt/jp1dh/server`.

3.7.3 Restoring an email template file

If editing an email template file causes JP1/DH - Server to malfunction, you must return the file back to its original state.

To restore the email template file:

1. Stop the JP1/DH - Server services by seeing *6.1.2(1) Stopping services* for Windows, or *6.2.2(1) Stopping services* for Linux.

2. Copy the email template file from the *installation-folder*#`\template\mail_template\` folder where the original files are stored, to the *installation-folder*#`\misc\digikatsuwide\digikatsuwide\WEB-INF\classes\jp\clealink\digivery\notifier\template\` folder, overwriting the template file for editing with the original one.

3. Change the configuration of your application by seeing *5.3.2 Changing the application configuration*.

4. Start the JP1/DH - Server services by seeing *6.1.1(1) Starting services* for Windows, or *6.2.1(1) Starting services* for Linux.

#: In Linux, change *installation-folder* to `/opt/jp1dh/server`.

3.7.4 Structure and notes on editing of an email template file

This section describes a structure and notes on editing of the email template file.

(1) Structure of the email template file

The email template is a file in XML format. You can only edit the message subject and message body parts in the file.

The structure of the file is as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
  <notification-template type=type-of-email-template lang=language>
    <headers>
    </headers>
      <contents>
        <subject>
        message-subject
        </subject>
        <body>
        message-body
        </body>
      </contents>
  </notification-template>
```

(2) Notes on editing

An email template file must be created in XML format.

To represent an element with no content, use the form of <*tag-name*/>, which combines a start tag and end tag together. You cannot use the form of <*tag-name*><*tag-name*/>.

Also, if the content of an element contains any format control character or characters in XML, such as a left angle bracket (<), you must follow the notation as defined in the XML specifications to use such characters. This allows you to represent those characters by using the entity reference or CDATA section.

The following table describes notations of several format control characters of XML if the characters are used as an entity reference in an email template file.

Table 3–30: Entity-referenced notations of format control characters of XML used in an email template file

No.	Format control character	Notation in the email template file
1	Left angle bracket (<)	`&lt;`
2	Right angle bracket (>)	`&gt;`
3	Ampersand (&)	`&amp;`
4	Double quotation mark (")	`&quot;`
5	Apostrophe mark (')	`&apos;`

The message subject and body can contain a *placeholder element* that consists of particular characters.

If a placeholder element is specified, the system replaces it with a particular value when forming the message subject or message body. Possible placeholder elements vary depending on the type of email notifications. For details about the placeholder element, see the description for each template file.

3.7.5 File delivery notification

This subsection provides information about editing the email template for a file delivery notification.

(1) Target file for edit

The template files for editing the file delivery notification are as follows:

- For Japanese: `delivery_notification_ja.xml`
- For English: `delivery_notification_en.xml`
- For Chinese: `delivery_notification_zh.xml`

(2) Editing the message subject

For the file delivery notification, you can edit the message subjects for when a sender enters the subject of a new transfer, and when not.

The structure of elements for editing the message subject of the file delivery notification is as follows:

```
...
  <subject>
    <subject-with-user-input>
      <file-delivery-subject>message-subject-for-file-transfer</file-
```

```
delivery-subject>
      <message-delivery-subject>message-subject-for-sending-messages-only</
message-delivery-subject>
    </subject-with-user-input>
    <subject-without-user-input>
      <file-delivery-subject>message-subject-for-file-transfer</file-
delivery-subject>
      <message-delivery-subject>message-subject-for-sending-messages-only</
message-delivery-subject>
    </subject-without-user-input>
  </subject>
...
```

The following table describes relevant message subject elements in the file delivery notification.

Table 3–31: Message subject elements for the file delivery notification

Element	Number of elements	Edit	Omit	Description
`subject`	1	No	No	Element that indicates the message subject in the file delivery notification.
`subject-with-user-input`	1	No	No	Element that indicates the message subject if the sender enters the subject for a new transfer.
`file-delivery-subject`	1	Yes	No	Element that indicates the message subject when a file is sent.
`message-delivery-subject`	1	Yes	No	Element that indicates the message subject when only a message is sent.
`subject-without-user-input`	1	No	No	Element that indicates the message subject if the sender does not enter the subject for a new transfer.
`file-delivery-subject`	1	Yes	No	Element that indicates the message subject when a file is sent.
`message-delivery-subject`	1	Yes	No	Element that indicates the message subject when only a message is sent.

Legend:

Yes: You can edit or omit the element.

No: You cannot edit or omit the element.

The following table describes placeholder elements available in editing the message subject.

Table 3–32: Placeholder elements available in editing the message subject

No.	Placeholder element	Description	Possible parent element
1	`<system-name-subject />`	Replaced with the following system-name string: `[Data Highway]`	• `file-delivery-subject` • `message-delivery-subject`
2	`<user-input-subject/>`	Replaced with the subject that the sender entered in the New Delivery window.	• `subject-with-user-input/file-delivery-subject` • `subject-with-user-input/message-delivery-subject`

(3) Editing the message body

The structure of elements for editing the message body of the file delivery notification is as follows:

```
...
  <body>
    message-body-in-the-file-delivery-notification
  </body>
...
```

The following table describes relevant message body elements in the file delivery notification.

Table 3–33: Message body elements for the file delivery notification

Element	Number of elements	Edit	Omit	Description
`body`	1	Yes	No	Indicates text in the message body. In the body of the text, the elements listed in the rows below can be included.
`file-delivery-title`	1	Yes	Yes	Indicates the predefined subject format text that is included in the message body. The predefined subject format text introduced by this element is used when sending a file. If a message is sent without any file, the predefined subject format text introduced by this element is not included in the message body.
`message-delivery-title`	1	Yes	Yes	Indicates the predefined subject format text that is included in the message body. The predefined subject format text introduced by this element is used for sending a message without any file. If a message is sent with a file, the predefined subject format text introduced by this element is not included in the message body.
`file-delivery-auto-message`	1	Yes	Yes	Indicates predefined message format text that is included in the message body. The predefined message format text introduced by this element is used for sending a file. If a message is sent without any file, the predefined message format text introduced by this element is not included in the message body.
`message-delivery-auto-message`	1	Yes	Yes	Indicates predefined message format text that is included in the message body. The predefined message format text introduced by this element is used for sending a message without any file. If a message is sent with a file, the predefined message format text introduced by this element is not included in the message body.
`user-id-part`	1	Yes	Yes	Used to enclose a string containing the placeholder element `<user-id-suffix/>`. For details about the placeholder element, see *Table 3-34*.

Element	Number of elements	Edit	Omit	Description
`sender-message-part`	1	Yes	Yes	Used to enclose a string included in the message body when a sender enters message text in the New Delivery window. The string enclosed in the elements is not included in the message body if the sender does not enter message text in the New Delivery window.
`recipient-check`	1	Yes	Yes	Used to specify information included in the message body if a sender does not select the **Hide the detailed information of this delivery from the notification.** check box on the **Extended Options** tab in the New Delivery window.
`from-part`	1	Yes	Yes	Used to enclose a string containing the placeholder element `<from />`. For details about the placeholder element, see *Table 3-34*.
`file-part`	1	Yes	Yes	Used to enclose a string that is included in the message body only when a file is sent. The string enclosed in the elements is not included in the message body if only a message is sent.

Legend:

Yes: You can edit or omit the element.

No: You cannot edit or omit the element.

The following table describes placeholder elements available in editing the message body in the file delivery notification.

Table 3–34: Placeholder elements available in editing the message body in the file delivery notification

No.	Placeholder element	Description	Possible parent element
1	`<system-name-body-top />`	Replaced with the following system-name string: `Data Highway`	`body`
2	`<to-name />`	Replaced with the name of the recipient. • In Japanese and Chinese: Name of the recipient • In English: Name of the recipient (in English)	• `body` • `recipient-check`
3	`<from-name />`	Replaced with the name of the sender. • In Japanese and Chinese: Name of the sender • In English: Name of the sender (in English)	• `body` • `recipient-check`
4	`<user-id-suffix />`	Replaced with the name of the domain that the recipient belongs to.	`user-id-part`
5	`<sender-message />`	Replaced with the message text that a sender entered in the New Delivery window.	`sender-message-part`
6	`<url />`	Replaced with the download URL for the recipient.	`body`
7	`<check-number />`	Replaced with the following string:	`recipient-check`

No.	Placeholder element	Description	Possible parent element
7	`<check-number />`	*delivery-date-and-time−delivery-ID* (*recipient-number*)	`recipient-check`
8	`<from />`	Replaced with the email address of the sender.	`from-part`
9	`<shelf-life-time />`	Replaced with the storage expiration date.	`recipient-check`
10	`<delivery-files />`	Replaced with a list of delivery files.	`file-part`
	`left-margin` attribute	Specifies the left margin for a list of delivery files included in the message body by using the number of space characters.	--
11	`<delivery-time />`	Replaced with the date and time of the delivery.	`recipient-check`
12	`<system-name-body-bottom />`	Replaced with the following system-name string: `Data Highway`	`body`

3.7.6 File delivery notification (reminder)

This subsection provides information about editing the email template for a file delivery notification (reminder).

(1) Target file for edit

The template files for the file delivery notification (reminder) are as follows:

- For Japanese: `notification_not_downloaded_ja.xml`
- For English: `notification_not_downloaded_en.xml`
- For Chinese: `notification_not_downloaded_zh.xml`

(2) Editing the message subject

For the file delivery notification (reminder), you can edit the message subjects for when a sender enters the subject of a new transfer, and when not.

The structure of elements for editing the message subject of the file delivery notification (reminder) is as follows:

```
...
  <subject>
    <subject-with-user-input>
      <file-delivery-subject>message-subject-for-file-transfer</file-
delivery-subject>
      <message-delivery-subject>message-subject-for-sending-messages-only</
message-delivery-subject>
    </subject-with-user-input>
    <subject-without-user-input>
      <file-delivery-subject>message-subject-for-file-transfer</file-
delivery-subject>
      <message-delivery-subject>message-subject-for-sending-messages-only</
message-delivery-subject>
    </subject-without-user-input>
  </subject>
...
```

The following table describes relevant message subject elements in the file delivery notification (reminder).

Table 3–35: Message subject elements for the file delivery notification (reminder)

Element	Number of elements	Edit	Omit	Description
`subject`	1	No	No	Element that indicates the message subject in the file delivery notification (reminder).
`subject-with-user-input`	1	No	No	Element that indicates the message subject if the sender enters the subject for a new transfer.
`file-delivery-subject`	1	Yes	No	Element that indicates the message subject when a file is sent.
`message-delivery-subject`	1	Yes	No	Element that indicates the message subject when only a message is sent.
`subject-without-user-input`	1	No	No	Element that indicates the message subject if the sender does not enter the subject for a new transfer.
`file-delivery-subject`	1	Yes	No	Element that indicates the message subject when a file is sent.
`message-delivery-subject`	1	Yes	No	Element that indicates the message subject when only a message is sent.

Legend:

Yes: You can edit or omit the element.

No: You cannot edit or omit the element.

The following table describes placeholder elements available in editing the message subject.

Table 3–36: Placeholder elements available in editing the message subject

No.	Placeholder element	Description	Possible parent element
1	`<system-name-subject />`	Replaced with the following system-name string: `[Data Highway]`	• `file-delivery-subject` • `message-delivery-subject`
2	`<user-input-subject/>`	Replaced with the subject that the sender entered in the New Delivery window.	• `subject-with-user-input/file-delivery-subject` • `subject-with-user-input/message-delivery-subject`

(3) Editing the message body

The structure of elements for editing the message body of the file delivery notification (reminder) is as follows:

```
...
  <body>
    message-body-in-the-file-delivery-notification-(reminder)
  </body>
...
```

The following table describes editable message body elements in the file delivery notification (reminder).

Table 3–37: Message body elements for the file delivery notification (reminder)

Element	Number of elements	Edit	Omit	Description
body	1	Yes	No	Indicates text in the message body. In the body of the text, the elements listed in the rows below can be included.
file-delivery-title	1	Yes	Yes	Indicates the predefined subject format text that is included in the message body. The predefined subject format text introduced by this element is used when sending a file. If a message is sent without any file, the predefined subject format text introduced by this element is not included in the message body.
message-delivery-title	1	Yes	Yes	Indicates the predefined subject format text that is included in the message body. The predefined subject format text introduced by this element is used for sending a message without any file. If a message is sent with a file, the predefined subject format text introduced by this element is not included in the message body.
file-delivery-auto-message	1	Yes	Yes	Indicates predefined message format text that is included in the message body. The predefined message format text introduced by this element is used for sending a file. If a message is sent without any file, the predefined message format text introduced by this element is not included in the message body.
message-delivery-auto-message	1	Yes	Yes	Indicates predefined message format text that is included in the message body. The predefined message format text introduced by this element is used for sending a message without any file. If a message is sent with a file, the predefined message format text introduced by this element is not included in the message body.
user-id-part	1	Yes	Yes	Used to enclose a string containing the placeholder element <user-id-suffix/>. For details about the placeholder element, see *Table 3-38*.
sender-message-part	1	Yes	Yes	Used to enclose a string included in the message body when a sender enters message text in the New Delivery window. The string enclosed in the elements is not included in the message body if the sender does not enter message text in the New Delivery window.
recipient-check	1	Yes	Yes	Used to specify information included in the message body if a sender does not select the **Hide the detailed information of this delivery from the notification.** check box on the **Extended Options** tab in the New Delivery window.

Element			Number of elements	Edit	Omit	Description
		from-part	1	Yes	Yes	Used to enclose a string containing the placeholder element <from />. For details about the placeholder element, see *Table 3-38*.
		file-part	1	Yes	Yes	Used to enclose a string that is included in the message body only when a file is sent. The string enclosed in the elements is not included in the message body if only a message is sent.

Legend:

Yes: You can edit or omit the element.

No: You cannot edit or omit the element.

The following table describes placeholder elements available in editing the message body in the file delivery notification (reminder).

Table 3–38: Placeholder elements available in editing the message body in the file delivery notification (reminder)

No.	Placeholder element		Description	Possible parent element
1	<system-name-body-top />		Replaced with the following system-name string: Data Highway	body
2	<to-name />		Replaced with the name of the recipient. • In Japanese and Chinese: Name of the recipient • In English: Name of the recipient (in English)	• body • recipient-check
3	<from-name />		Replaced with the name of the sender. • In Japanese and Chinese: Name of the sender • In English: Name of the sender (in English)	• body • recipient-check
4	<user-id-suffix />		Replaced with the name of the domain that the recipient belongs to.	user-id-part
5	<sender-message />		Replaced with the message text that a sender entered in the New Delivery window.	sender-message-part
6	<url />		Replaced with the download URL for the recipient.	body
7	<check-number />		Replaced with the following string: *delivery-date-and-time*−*delivery-ID*（*recipient-number*）	recipient-check
8	<from />		Replaced with the email address of the sender.	from-part
9	<shelf-life-time />		Replaced with the storage expiration date.	recipient-check
10	<delivery-files />		Replaced with a list of delivery files.	file-part
		left-margin attribute	Specifies the left margin for a list of delivery files included in the message body by using the number of space characters.	--

No.	Placeholder element	Description	Possible parent element
11	`<delivery-time />`	Replaced with the date and time of the delivery.	`recipient-check`
12	`<system-name-body-bottom />`	Replaced with the following system-name string: `Data Highway`	`body`

3.7.7 File delivery confirmation

This subsection provides information about editing the email template for a file delivery confirmation.

(1) Target file for edit

The template files for the file delivery confirmation are as follows:

- For Japanese: `delivery_confirmation_ja.xml`
- For English: `delivery_confirmation_en.xml`
- For Chinese: `delivery_confirmation_zh.xml`

(2) Editing the message subject

The structure of elements for editing the message subject of the file delivery confirmation is as follows:

```
...
  <subject>
    <file-delivery-subject>message-subject-for-file-transfer</file-delivery-
subject>
    <message-delivery-subject>message-subject-for-sending-messages-only</
message-delivery-subject>
  </subject>
...
```

The following table describes relevant message subject elements in the file delivery confirmation.

Table 3–39: Message subject elements for the file delivery confirmation

Element		Number of elements	Edit	Omit	Description
`subject`		1	No	No	Element that indicates the message subject in the file delivery confirmation.
	`file-delivery-subject`	1	Yes	No	Element that indicates the message subject when a file is sent.
	`message-delivery-subject`	1	Yes	No	Element that indicates the message subject when only a message is sent.

Legend:

Yes: You can edit or omit the element.

No: You cannot edit or omit the element.

The following table describes a placeholder element available in editing the message subject in the file delivery confirmation.

Table 3–40: Placeholder element available in editing the message subject in the file delivery confirmation

No.	Placeholder element	Description	Possible parent element
1	`<system-name-subject />`	Replaced with the following system-name string: `[Data Highway]`	`subject`

(3) Editing the message body

The structure of elements for editing the message body of the file delivery confirmation is as follows:

```
...
  <body>
    message-body-in-the-file-delivery-confirmation
  </body>
...
```

The following table describes relevant message body elements in the file delivery confirmation.

Table 3–41: Message body elements for the file delivery confirmation

Element	Number of elements	Edit	Omit	Description
`body`	1	Yes	No	Indicates text in the message body. In the body of the text, the elements listed in the rows below can be included.
`file-delivery-title`	1	Yes	Yes	Indicates the predefined subject format text that is included in the message body. The predefined subject format text introduced by this element is used when sending a file. If a message is sent without any file, the predefined subject format text introduced by this element is not included in the message body.
`message-delivery-title`	1	Yes	Yes	Indicates the predefined subject format text that is included in the message body. The predefined subject format text introduced by this element is used for sending a message without any file. If a message is sent with a file, the predefined subject format text introduced by this element is not included in the message body.
`file-delivery-auto-message`	1	Yes	Yes	Indicates predefined message format text that is included in the message body. The predefined message format text introduced by this element is used for sending a file. If a message is sent without any file, the predefined message format text introduced by this element is not included in the message body.

Element	Number of elements	Edit	Omit	Description
`message-delivery-auto-message`	1	Yes	Yes	Indicates predefined message format text that is included in the message body. The predefined message format text introduced by this element is used for sending a message without any file. If a message is sent with a file, the predefined message format text introduced by this element is not included in the message body.
`recipients`	1	Yes	Yes	Element that is used for including a list of recipients in the message body. If more than one recipient is specified, the system iterates through the element the same number of times as the number of recipients. Example: Value: `<receipts>Dear Mr./Ms. </receipts>` In the actual message body: Dear Mr./Ms. *recipient-name* (1) Dear Mr./Ms. *recipient-name* (2)
`information`	1	Yes	Yes	Used to specify information included in the message body if a sender does not select the **Hide the detailed information of this delivery from the notification.** check box on the **Extended Options** tab in the New Delivery window.
`from-part`	1	Yes	Yes	Used to enclose a string containing the placeholder element `<from />`. For details about the placeholder element, see *Table 3-42*.
`file-part`	1	Yes	Yes	Used to enclose a string that is included in the message body only when a file is sent. The string enclosed in the elements is not included in the message body if only a message is sent.

Legend:

Yes: You can edit or omit the element.

No: You cannot edit or omit the element.

The following table describes placeholder elements available in editing the message body in the file delivery confirmation.

Table 3–42: Placeholder elements available in editing the message body in the file delivery confirmation

No.	Placeholder element	Description	Possible parent element
1	`<system-name-body-top />`	Replaced with the following system-name string: `Data Highway`	`Body`
2	`<to-name />`	Replaced with a list of recipient names. • In Japanese and Chinese: Name of the recipient	`recipients`

No.	Placeholder element	Description	Possible parent element
2	`<to-name />`	• In English: Name of the recipient (in English)	`recipients`
	`left-margin` attribute	Specifies the left margin for a list of recipient names included in the message body by using the number of space characters.	--
3	`<from-name />`	Replaced with the name of the sender. • In Japanese and Chinese: Name of the sender • In English: Name of the sender (in English)	`body`
4	`<check-number />`	Replaced with the following string: *delivery-date-and-time−delivery-ID* (*recipient-number*)	`body`
5	`<from />`	Replaced with the email address of the sender.	`from-part`
6	`<shelf-life-time />`	Replaced with the storage expiration date.	`body`
7	`<delivery-files />`	Replaced with a list of delivery files.	`file-part`
	`left-margin` attribute	Specifies the left margin for a list of delivery files included in the message body by using the number of space characters.	--
8	`<delivery-time />`	Replaced with the date and time of the delivery.	`body`
9	`<system-name-body-bottom />`	Replaced with the following system-name string: `Data Highway`	`body`

3.7.8 File delivery notification (opened)

This subsection provides information about editing the email template for a file delivery notification (opened).

(1) Target file for edit

The template files for editing the file delivery notification (opened) are as follows:

- For Japanese: `delivery_opened_notification_ja.xml`
- For English: `delivery_opened_notification_en.xml`
- For Chinese: `delivery_opened_notification_zh.xml`

(2) Editing the message subject

The structure of elements for editing the message subject of the file delivery notification (opened) is as follows:

```
...
  <subject>
    message-subject-in-the-file-delivery-notification-(opened)
  </subject>
...
```

The following table describes a relevant message subject element in the file delivery notification (opened).

Table 3–43: Message subject element for the file delivery notification (opened)

Element	Number of elements	Edit	Omit	Description
`subject`	1	Yes	No	Element that indicates the message subject in the file delivery notification (opened).

Legend:

Yes: You can edit or omit the element.

No: You cannot edit or omit the element.

The following table describes a placeholder element available in editing the message subject in the file delivery notification (opened).

Table 3–44: Placeholder element available in editing the message subject in the file delivery notification (opened)

No.	Placeholder element	Description	Possible parent element
1	`<system-name-subject />`	Replaced with the following system-name string: `[Data Highway]`	`subject`

(3) Editing the message body

The structure of elements for editing the message body of the file delivery notification (opened) is as follows:

```
...
  <body>
    message-body-in-the-file-delivery-notification-(opened)
  </body>
...
```

The following table describes relevant message body elements in the file delivery notification (opened).

Table 3–45: Message body elements for the file delivery notification (opened)

Element	Number of elements	Edit	Omit	Description
`body`	1	Yes	No	Indicates text in the message body. In the body of the text, the elements listed in the rows below can be included.
`from-part`	1	Yes	Yes	Used to enclose a string containing the placeholder element `<from />`. For details about the placeholder element, see *Table 3-46*.

Legend:

Yes: You can edit or omit the element.

No: You cannot edit or omit the element.

The following table describes placeholder elements available in editing the message body in the file delivery notification (opened).

Table 3–46: Placeholder elements available in editing the message body in the file delivery notification (opened)

No.	Placeholder element	Description	Possible parent element
1	`<system-name-body-top />`	Replaced with the following system-name string: `Data Highway`	`body`
2	`<to-name />`	Replaced with the name of the recipient. • In Japanese and Chinese: Name of the recipient • In English: Name of the recipient (in English)	`body`
3	`<from-name />`	Replaced with the name of the sender. • In Japanese and Chinese: Name of the sender • In English: Name of the sender (in English)	`body`
4	`<check-number />`	Replaced with the following string: *delivery-date-and-time*−*delivery-ID*（*recipient-number*）	`body`
5	`<shelf-life-time />`	Replaced with the storage expiration date.	`body`
6	`<delivery-files />`	Replaced with a list of delivery files.	`body`
	`left-margin` attribute	Specifies the left margin for a list of delivery files included in the message body by using the number of space characters.	--
7	`<delivery-time />`	Replaced with the date and time of the delivery.	`body`
8	`<system-name-body-bottom />`	Replaced with the following system-name string: `Data Highway`	`body`

3.7.9 File delivery notification (expires soon)

This subsection provides information about editing the email template for a file delivery notification (expires soon).

(1) Target file for edit

The template files for editing the file delivery notification (expires soon) are as follows:

- For Japanese: `notification_before_expired_ja.xml`
- For English: `notification_before_expired_en.xml`
- For Chinese: `notification_before_expired_zh.xml`

(2) Editing the message subject

The structure of elements for editing the message subject of the file delivery notification (expires soon) is as follows:

```
...
  <subject>
    message-subject-in-the-file-delivery-notification-(expires-soon)
  </subject>
...
```

The following table describes a relevant message subject element in the file delivery notification (expires soon).

Table 3–47: Message subject element for the file delivery notification (expires soon)

Element	Number of elements	Edit	Omit	Description
`subject`	1	Yes	No	Element that indicates the message subject in the file delivery notification (expires soon).

Legend:

Yes: You can edit or omit the element.

No: You cannot edit or omit the element.

The following table describes a placeholder element available in editing the message subject in the file delivery notification (expires soon).

Table 3–48: Placeholder element available in editing the message subject in the file delivery notification (expires soon)

No.	Placeholder element	Description	Possible parent element
1	`<system-name-subject />`	Replaced with the following system-name string: `[Data Highway]`	`subject`

(3) Editing the message body

The structure of elements for editing the message body of the file delivery notification (expires soon) is as follows:

```
...
  <body>
    message-body-in-the-file-delivery-notification-(expires-soon)
  </body>
...
```

The following table describes relevant message body elements in the file delivery notification (expires soon).

Table 3–49: Message body elements for the file delivery notification (expires soon)

Element		Number of elements	Edit	Omit	Description
`body`		1	Yes	No	Indicates text in the message body. In the body of the text, the elements listed in the rows below can be included.
	`for-recipient-checks`	1	Yes	Yes	Used to specify information included in the message body if a sender does not select the **Hide the detailed**

Element		Numb er of eleme nts	Edit	Omit	Description

	`for-recipient-checks`	1	Yes	Yes	**information of this delivery from the notification.** check box on the **Extended Options** tab in the New Delivery window.
					If more than one recipient is specified, the system iterates through the element the same number of times as the number of recipients.
					Example:
					Value:
					`<for-recipient-checks>`
					`----------`
					`Dear Mr./Ms. <to-name/>`
					`----------`
					`</ for-recipient-checks >`
					In the actual message body:
					---------- 	
					Dear Mr./Ms. *recipient-1*
					---------- 	
					---------- 	
					Dear Mr./Ms. *recipient-2*
					---------- 	
					---------- 	
					Dear Mr./Ms. *recipient-3*
					---------- 	

	`from-part`	1	Yes	Yes	Used to enclose a string containing the placeholder element `<from />`. For details about the placeholder element, see *Table 3-50*.

Legend:

Yes: You can edit or omit the element.

No: You cannot edit or omit the element.

The following table describes placeholder elements available in editing the message body in the file delivery notification (expires soon).

Table 3–50: Placeholder elements available in editing the message body in the file delivery notification (expires soon)

No.	Placeholder element	Description	Possible parent element
1	`<system-name-body-top />`	Replaced with the following system-name string: `Data Highway`	`body`
2	`<to-name />`	Replaced with the name of the recipient. • In Japanese and Chinese: Name of the recipient • In English: Name of the recipient (in English)	`for-recipient-checks`
3	`<from-name />`	Replaced with a list of sender names. • In Japanese and Chinese: Name of the sender	• `body` • `for-recipient-checks`

No.	Placeholder element	Description	Possible parent element
3	`<from-name />`	- In English: Name of the sender (in English)	- `body` - `for-recipient-checks`
4	`<check-number />`	Replaced with the following string: *delivery-date-and-time*−*delivery-ID*（*recipient-number*）	`for-recipient-checks`
5	`<from />`	Replaced with the email address of the sender.	`from-part`
6	`<shelf-life-time />`	Replaced with the storage expiration date.	`for-recipient-checks`
7	`<delivery-files />`	Replaced with a list of delivery files.	`for-recipient-checks`
8	`<delivery-time />`	Replaced with the date and time of the delivery.	`for-recipient-checks`
9	`<system-name-body-bottom />`	Replaced with the following system-name string: `Data Highway`	`body`

3.7.10 File delivery notification (expired)

This subsection provides information about editing the email template for a file delivery notification (expired).

(1) Target file for edit

The template files for editing the file delivery notification (expired) are as follows:

- For Japanese: `notification_after_expired_ja.xml`
- For English: `notification_after_expired_en.xml`
- For Chinese: `notification_after_expired_zh.xml`

(2) Editing the message subject

The structure of elements for editing the message subject of the file delivery notification (expired) is as follows:

```
...
  <subject>
    message-subject-in-the-file-delivery-notification-(expired)
  </subject>
...
```

The following table describes a relevant message subject element in the file delivery notification (expired).

Table 3–51: Message subject element for the file delivery notification (expired)

Element	Number of elements	Edit	Omit	Description
`subject`	1	Yes	No	Element that indicates the message subject in the file delivery notification (expired).

Legend:

Yes: You can edit or omit the element.

No: You cannot edit or omit the element.

The following table describes a placeholder element available in editing the message subject in the file delivery notification (expired).

Table 3–52: Placeholder element available in editing the message subject in the file delivery notification (expired)

No.	Placeholder element	Description	Possible parent element
1	`<system-name-subject />`	Replaced with the following system-name string: `[Data Highway]`	`subject`

(3) Editing the message body

The structure of elements for editing the message body of the file delivery notification (expired) is as follows:

```
...
  <body>
    message-body-in-the-file-delivery-notification-(expired)
  </body>
...
```

The following table describes relevant message body elements in the file delivery notification (expired).

Table 3–53: Message body elements for the file delivery notification (expired)

Element	Number of elements	Edit	Omit	Description
`body`	1	Yes	No	Indicates text in the message body. In the body of the text, the elements listed in the rows below can be included.

`for-recipient-checks`	1	Yes	Yes	Used to specify information included in the message body if a sender does not select the **Hide the detailed information of this delivery from the notification.** check box on the **Extended Options** tab in the New Delivery window.
				If more than one recipient is specified, the system iterates through the element the same number of times as the number of recipients.
				Example:
				Value:
				`<for-recipient-checks>`
				`----------`
				`Dear Mr./Ms. <to-name/>`
				`----------`
				`</ for-recipient-checks >`
				In the actual message body:
				---------- 	
				Dear Mr./Ms. *recipient-1*

Element		Number of elements	Edit	Omit	Description
	`for-recipient-checks`	1	Yes	Yes	---------- ---------- Dear Mr./Ms. *recipient-2* ---------- ---------- Dear Mr./Ms. *recipient-3* ----------
	`from-part`	1	Yes	Yes	Used to enclose a string containing the placeholder element `<from />`. For details about the placeholder element, see *Table 3-54*.

Legend:

Yes: You can edit or omit the element.

No: You cannot edit or omit the element.

The following table describes placeholder elements available in editing the message body in the file delivery notification (expired).

Table 3–54: Placeholder elements available in editing the message body in the file delivery notification (expired)

No.	Placeholder element		Description	Possible parent element
1	`<system-name-body-top />`		Replaced with the following system-name string: `Data Highway`	`body`
2	`<to-name />`		Replaced with the name of the recipient. • In Japanese and Chinese: Name of the recipient • In English: Name of the recipient (in English)	`for-recipient-checks`
		`left-margin` attribute	Specifies the left margin for a list of recipient names included in the message body by using the number of space characters.	--
3	`<from-name />`		Replaced with the name of the sender. • In Japanese and Chinese: Name of the sender • In English: Name of the sender (in English)	• `body` • `for-recipient-checks`
4	`<check-number />`		Replaced with the following string: *delivery-date-and-time*−*delivery-ID*（*recipient-number*）	`for-recipient-checks`
5	`<from />`		Replaced with the email address of the sender.	`from-part`
6	`<shelf-life-time />`		Replaced with the storage expiration date.	`for-recipient-checks`
7	`<delivery-files />`		Replaced with a list of delivery files.	`for-recipient-checks`
8	`<delivery-time />`		Replaced with the date and time of the delivery.	`for-recipient-checks`
9	`<system-name-body-bottom />`		Replaced with the following system-name string:	`body`

No.	Placeholder element	Description	Possible parent element
9	`<system-name-body-bottom />`	`Data Highway`	`body`

3.7.11 Approval request notification

This subsection provides information about editing the email template for an approval request notification.

(1) Target file for edit

The template files for editing the approval request notification are as follows:

- For Japanese: `delivery_approval_notification_ja.xml`
- For English: `delivery_approval_notification_en.xml`
- For Chinese: `delivery_approval_notification_zh.xml`

(2) Editing the message subject

The structure of elements for editing the message subject of the approval request notification is as follows:

```
...
  <subject>
    message-subject-in-the-approval-request-notification
  </subject>
...
```

The following table describes a relevant message subject element in the approval request notification.

Table 3–55: Message subject element for the approval request notification

Element	Number of elements	Edit	Omit	Description
`subject`	1	Yes	No	Element that indicates the message subject in the approval request notification.

Legend:

Yes: You can edit or omit the element.

No: You cannot edit or omit the element.

The following table describes a placeholder element available in editing the message subject in the approval request notification.

Table 3–56: Placeholder element available in editing the message subject in the approval request notification

No.	Placeholder element	Description	Possible parent element
1	`<system-name-body-subject />`	Replaced with the following system-name string: `[Data Highway]`	`subject`

(3) Editing the message body

The structure of elements for editing the message body of the approval request notification is as follows:

```
...
  <body>
    message-body-in-the-approval-request-notification
  </body>
...
```

The following table describes relevant message body elements in the approval request notification.

Table 3–57: Message body elements for the approval request notification

Element	Number of elements	Edit	Omit	Description
`body`	1	Yes	No	Indicates text in the message body. In the body of the text, the elements listed in the rows below can be included.
`recipient-check`	1	Yes	Yes	Used to specify information included in the message body if a sender does not select the **Hide the detailed information of this delivery from the notification.** check box on the **Extended Options** tab in the New Delivery window.
`recipients`	1	Yes	Yes	Used to include information on the recipient in the message body. If more than one recipient is specified, the system iterates through the element the same number of times as the number of recipients. Example: Value: `<receipts>`Dear Mr./Ms. `</receipts>` In the actual message body: Dear Mr./Ms. *recipient-name* (1) Dear Mr./Ms. *recipient-name* (2)
`information`	1	Yes	Yes	Used to specify information included in the message body if a sender does not select the **Hide the detailed information of this delivery from the notification.** check box on the **Extended Options** tab in the New Delivery window.
`from-part`	1	Yes	Yes	Used to enclose a string containing the placeholder element `<from />`. For details about the placeholder element, see *Table 3-58*.
`file-part`	1	Yes	Yes	Used to enclose a string that is included in the message body only when a file is sent. The string enclosed in the elements is not included in the message body if only a message is sent.

Legend:

Yes: You can edit or omit the element.

No: You cannot edit or omit the element.

The following table describes placeholder elements available in editing the message body in the approval request notification.

Table 3–58: Placeholder elements available in editing the message body in the approval request notification

No.	Placeholder element	Description	Possible parent element
1	`<system-name-body-top />`	Replaced with the following system-name string: `Data Highway`	`body`
2	`<to-name />`	Replaced with the name of the approver. • In Japanese and Chinese: Name of the approver • In English: Name of the approver (in English)	`body`
		Replaced with a list of recipient names. • In Japanese and Chinese: Name of the recipient • In English: Name of the recipient (in English)	`body` / `recipient-check` / `recipients`
	`left-margin` attribute	Specifies the left margin for a list of recipient names included in the message body by using the number of space characters.	`body` / `recipient-check` / `recipients` / `to-name`
3	`<from-name />`	Replaced with the name of the sender. • In Japanese and Chinese: Name of the sender • In English: Name of the sender (in English)	• `body` • `information`
4	`<user-id-suffix />`	Replaced with the name of the domain that the recipient belongs to.	`body`
5	`<url />`	Replaced with the download URL for the recipient.	`body`
6	`<check-number />`	Replaced with the following string: *delivery-date-and-time*−*delivery-ID* (*recipient-number*)	`recipient-check`
7	`<from />`	Replaced with the email address of the sender.	`from-part`
8	`<shelf-life-time />`	Replaced with the storage expiration date.	`information`
9	`<delivery-files />`	Replaced with a list of delivery files.	`information`
	`left-margin` attribute	Specifies the left margin for a list of delivery files included in the message body by using the number of space characters.	--
10	`<delivery-time />`	Replaced with the date and time of the delivery.	`recipient-check`
11	`<system-name-body-bottom />`	Replaced with the following system-name string: `Data Highway`	`body`

3.7.12 Approval request notification (reminder)

This subsection provides information about editing the email template for an approval request notification (reminder).

(1) Target file for edit

The template files for editing the approval request notification (reminder) are as follows:

- For Japanese: `notification_not_approved_ja.xml`
- For English: `notification_not_approved_en.xml`
- For Chinese: `notification_not_approved_zh.xml`

(2) Editing the message subject

The structure of elements for editing the message subject of the approval request notification (reminder) is as follows:

```
...
  <subject>
    message-subject-in-the-approval-request-notification-(reminder)
  </subject>
...
```

The following table describes a relevant message subject element in the approval request notification (reminder).

Table 3–59: Message subject element for the approval request notification (reminder)

Element	Number of elements	Edit	Omit	Description
`subject`	1	Yes	No	Element that indicates the message subject in the approval request notification (reminder).

Legend:
Yes: You can edit or omit the element.
No: You cannot edit or omit the element.

The following table describes a placeholder element relevant in editing the message subject in the approval request notification (reminder).

Table 3–60: Placeholder element available in editing the message subject in the approval request notification (reminder)

No.	Placeholder element	Description	Possible parent element
1	`<system-name-body-subject />`	Replaced with the following system-name string: `[Data Highway]`	`subject`

(3) Editing the message body

The structure of elements for editing the message body of the approval request notification (reminder) is as follows:

```
...
  <body>
```

```
    message-body-in-the-approval-request-notification-(reminder)
  </body>
...
```

The following table describes editable message body elements in the approval request notification (reminder).

Table 3–61: Message body elements for the approval request notification (reminder)

Element	Number of elements	Edit	Omit	Description
`body`	1	Yes	No	Indicates text in the message body. In the body of the text, the elements listed in the rows below can be included.
`recipient-check`	1	Yes	Yes	Used to specify information included in the message body if a sender does not select the **Hide the detailed information of this delivery from the notification.** check box on the **Extended Options** tab in the New Delivery window.
`recipients`	1	Yes	Yes	Used to include a list of recipients in the message body. If more than one recipient is specified, the system iterates through the element the same number of times as the number of recipients. Example: Value: `<receipts>`Dear Mr./Ms. `</receipts>` In the actual message body: Dear Mr./Ms. *recipient-name* (1) Dear Mr./Ms. *recipient-name* (2)
`information`	1	Yes	Yes	Used to specify information included in the message body if a sender does not select the **Hide the detailed information of this delivery from the notification.** check box on the **Extended Options** tab in the New Delivery window.
`from-part`	1	Yes	Yes	Used to enclose a string containing the placeholder element `<from />`. For details about the placeholder element, see *Table 3-62*.
`file-part`	1	Yes	Yes	Used to enclose a string that is included in the message body only when a file is sent. The string enclosed in the elements is not included in the message body if only a message is sent.

Legend:

Yes: You can edit or omit the element.

No: You cannot edit or omit the element.

The following table describes placeholder elements available in editing the message body in the approval request notification (reminder).

Table 3–62: Placeholder elements available in editing the message body in the approval request notification (reminder)

No.	Placeholder element		Description	Possible parent element
1	`<system-name-body-top />`		Replaced with the following system-name string: `Data Highway`	`body`
2	`<to-name />`		Replaced with the name of the approver. - In Japanese and Chinese: Name of the approver - In English: Name of the approver (in English)	`body`
			Replaced with a list of recipient names. - In Japanese and Chinese: Name of the recipient - In English: Name of the recipient (in English)	`body` / `recipient-check` / `recipients`
		`left-margin` attribute	Specifies the left margin for a list of recipient names included in the message body by using the number of space characters.	`body` / `recipient-check` / `recipients` / `to-name`
3	`<from-name />`		Replaced with the name of the sender. - In Japanese and Chinese: Name of the sender - In English: Name of the sender (in English)	- `body` - `information`
4	`<user-id-suffix />`		Replaced with the name of the domain that the recipient belongs to.	`body`
5	`<url />`		Replaced with the download URL for the recipient.	`body`
6	`<check-number />`		Replaced with the following string: *delivery-date-and-time*−*delivery-ID*（*recipient-number*）	`recipient-check`
7	`<from />`		Replaced with the email address of the sender.	`from-part`
8	`<shelf-life-time />`		Replaced with the storage expiration date.	`information`
9	`<delivery-files />`		Replaced with a list of delivery files.	`information`
		`left-margin` attribute	Specifies the left margin for a list of delivery files included in the message body by using the number of space characters.	--
10	`<delivery-time />`		Replaced with the date and time of the delivery.	`recipient-check`
11	`<system-name-body-bottom />`		Replaced with the following system-name string: `Data Highway`	`body`

3.7.13 Approved-delivery notification

This section provides information about editing the email template for an approved-delivery notification.

(1) Target file for edit

The template files for editing the approved-delivery notification are as follows:

- For Japanese: `delivery_accepted_confirmation_ja.xml`
- For English: `delivery_accepted_confirmation_en.xml`
- For Chinese: `delivery_accepted_confirmation_zh.xml`

(2) Editing the message subject

The structure of elements for editing the message subject of the approved-delivery notification is as follows:

```
...
  <subject>
    message-subject-in-the-approved-delivery-notification
  </subject>
...
```

The following table describes a relevant message subject element in the approved-delivery notification.

Table 3–63: Message subject element for the approved-delivery notification

Element	Number of elements	Edit	Omit	Description
`subject`	1	Yes	No	Element that indicates the message subject in the approved-delivery notification.

Legend:

Yes: You can edit or omit the element.

No: You cannot edit or omit the element.

The following table describes a placeholder element available in editing the message subject in the approved-delivery notification.

Table 3–64: Placeholder element available in editing the message subject in the approved-delivery notification

No.	Placeholder element	Description	Possible parent element
1	`<system-name-body-subject />`	Replaced with the following system-name string: `[Data Highway]`	`subject`

(3) Editing the message body

The structure of elements for editing the message body of the approved-delivery notification is as follows:

```
...
  <body>
    message-body-in-the-approved-delivery-notification
  </body>
...
```

The following table describes editable message body elements in the approved-delivery notification.

Table 3–65: Message body elements for the approved-delivery notification

Element	Number of elements	Edit	Omit	Description
`body`	1	Yes	No	Indicates text in the message body. In the body of the text, the elements listed in the rows below can be included.
`approval-message`	1	Yes	Yes	Indicates the predefined subject format text that is included in the message body. The predefined subject format text introduced by this element is used when sending a file. If a message is sent without any file, the predefined subject format text introduced by this element is not included in the message body.
`recipients`	1	Yes	Yes	Element that is used for including a list of recipients in the message body. If more than one recipient is specified, the system iterates through the element the same number of times as the number of recipients. Example: Value: `<receipts>`Dear Mr./Ms. `</receipts>` In the actual message body: Dear Mr./Ms. *recipient-name* (1) Dear Mr./Ms. *recipient-name* (2)
`information`	1	Yes	Yes	Used to specify information included in the message body if a sender does not select the **Hide the detailed information of this delivery from the notification.** check box on the **Extended Options** tab in the New Delivery window.
`from-part`	1	Yes	Yes	Used to enclose a string containing the placeholder element `<from />`. For details about the placeholder element, see *Table 3-66*.
`file-part`	1	Yes	Yes	Used to enclose a string that is included in the message body only when a file is sent. The string enclosed in the elements is not included in the message body if only a message is sent.

Legend:

Yes: You can edit or omit the element.

No: You cannot edit or omit the element.

The following table describes placeholder elements available in editing the message body in the approved-delivery notification.

Table 3–66: Placeholder elements available in editing the message body in the approved-delivery notification

No.	Placeholder element	Description	Possible parent element
1	`<system-name-body-top />`	Replaced with the following system-name string:	`Body`

No.	Placeholder element	Description	Possible parent element
1	`<system-name-body-top />`	`Data Highway`	`Body`
2	`<to-name />`	Replaced with a list of recipient names. • In Japanese and Chinese: Name of the recipient • In English: Name of the recipient (in English)	`recipients`
	`left-margin` attribute	Specifies the left margin for a list of recipient names included in the message body by using the number of space characters.	--
3	`<from-name />`	Replaced with the name of the sender. • In Japanese and Chinese: Name of the sender • In English: Name of the sender (in English)	`body`
4	`<approver-name />`	Replaced with the name of the approver.	`body`
5	`<approval-message-content />`	Replaced with the message text that an approver entered in the Application for Approval window when accepting an approval request.	`approval-message`
6	`<check-number />`	Replaced with the following string: *delivery-date-and-time*−*delivery-ID*（*recipient-number*）	`body`
7	`<from />`	Replaced with the email address of the sender.	`from-part`
8	`<shelf-life-time />`	Replaced with the storage expiration date.	`body`
9	`<delivery-files />`	Replaced with a list of delivery files.	`body`
	`left-margin` attribute	Specifies the left margin for a list of delivery files included in the message body by using the number of space characters.	--
10	`<delivery-time />`	Replaced with the date and time of the delivery.	`body`
11	`<system-name-body-bottom />`	Replaced with the following system-name string: `Data Highway`	`body`

3.7.14 Rejected-delivery notification

This section provides information about editing the email template for a rejected-delivery notification.

(1) Target file for edit

The template files for editing the rejected-delivery notification are as follows:

- For Japanese: `delivery_rejected_confirmation_ja.xml`
- For English: `delivery_rejected_confirmation_en.xml`
- For Chinese: `delivery_rejected_confirmation_zh.xml`

(2) Editing the message subject

The structure of elements for editing the message subject of the rejected-delivery notification is as follows:

```
...
  <subject>
    message-subject-in-the-rejected-delivery-notification
  </subject>
...
```

The following table describes an editable message subject element in the rejected-delivery notification.

Table 3–67: Message subject element for the rejected-delivery notification

Element	Number of elements	Edit	Omit	Description
subject	1	Yes	No	Element that indicates the message subject in the rejected-delivery notification.

Legend:

Yes: You can edit or omit the element.

No: You cannot edit or omit the element.

The following table describes a placeholder element available in editing the message subject in the rejected-delivery notification.

Table 3–68: Placeholder element available in editing the message subject in the rejected-delivery notification

No.	Placeholder element	Description	Possible parent element
1	<system-name-subject />	Replaced with the following system-name string: [Data Highway]	subject

(3) Editing the message body

The structure of elements for editing the message body of the rejected-delivery notification is as follows:

```
...
  <body>
    message-body-in-the-rejected-delivery-notification
  </body>
...
```

The following table describes editable message body elements in the rejected-delivery notification.

Table 3–69: Message body elements for the rejected-delivery notification

Element	Number of elements	Edit	Omit	Description
body	1	Yes	No	Indicates text in the message body.

Element	Number of elements	Edit	Omit	Description
`body`	1	Yes	No	In the body of the text, the elements listed in the rows below can be included.
`approval-message`	1	Yes	Yes	The string that is introduced by this element is included in the message body if an approver enters message text in the Application for Approval window when rejecting an approval request.
`recipients`	1	Yes	Yes	Element that is used for including a list of recipients in the message body. If more than one recipient is specified, the system iterates through the element the same number of times as the number of recipients. Example: Value: `<receipts>`Dear Mr./Ms. `</receipts>` In the actual message body: Dear Mr./Ms. *recipient-name* (1) Dear Mr./Ms. *recipient-name* (2)
`information`	1	Yes	Yes	Used to specify information included in the message body if a sender does not select the **Hide the detailed information of this delivery from the notification.** check box on the **Extended Options** tab in the New Delivery window.
`from-part`	1	Yes	Yes	Used to enclose a string containing the placeholder element `<from />`. For details about the placeholder element, see *Table 3-70*.
`file-part`	1	Yes	Yes	Used to enclose a string that is included in the message body only when a file is sent. The string enclosed in the elements is not included in the message body if only a message is sent.

Legend:

Yes: You can edit or omit the element.

No: You cannot edit or omit the element.

The following table describes placeholder elements available in editing the message body in the rejected-delivery notification.

Table 3–70: Placeholder elements available in editing the message body in the rejected-delivery notification

No.	Placeholder element	Description	Possible parent element
1	`<system-name-body-top />`	Replaced with the following system-name string: `Data Highway`	`body`
2	`<to-name />`	Replaced with a list of recipient names. • In Japanese and Chinese: Name of the recipient • In English: Name of the recipient (in English)	`recipients`

No.	Placeholder element	Description	Possible parent element
2	`left-margin` attribute	Specifies the left margin for a list of recipient names included in the message body by using the number of space characters.	--
3	`<from-name />`	Replaced with the name of the sender. • In Japanese and Chinese: Name of the sender • In English: Name of the sender (in English)	`body`
4	`<approver-name />`	Replaced with the name of the approver.	`body`
5	`<approval-message-content />`	Replaced with the message text that an approver entered in the Application for Approval window when rejecting an approval request.	`approval-message`
6	`<check-number />`	Replaced with the following string: *delivery-date-and-time*−*delivery-ID* (*recipient-number*)	`body`
7	`<from />`	Replaced with the email address of the sender.	`from-part`
8	`<shelf-life-time />`	Replaced with the storage expiration date.	`body`
9	`<delivery-files />`	Replaced with a list of delivery files.	`body`
	`left-margin` attribute	Specifies the left margin for a list of delivery files included in the message body by using the number of space characters.	--
10	`<system-name-body-bottom />`	Replaced with the following system-name string: `Data Highway`	`body`

4 Before Installation

This chapter describes the points you need to check before installing JP1/DH - Server.

4.1 Notes on installation

This section describes the notes on installation.

4.1.1 Common notes

- In Windows Server 2012 or Windows Server 2012 R2, to use the *command prompt with elevated privileges* installed together with JP1/DH - Server, you need to install Microsoft .NET Framework 3.5. For details about how to install Microsoft .NET Framework 3.5, see *D. Installing .NET Framework 3.5*.
- If a file or folder named `Program` exists directly under the system drive, a program does not run properly. If a file or folder named `Program` exists there, delete it before installing JP1/DH - Server.
- In Red Hat Enterprise Linux 6, make sure that the host name and IP address of the local host are registered in the `/etc/hosts` file. If they are not registered, the local host name cannot be resolved and the installation fails. Edit the `/etc/hosts` file to register the host name and IP address of the local host.

4.1.2 Notes on new installation

- You cannot install JP1/DH - Server in an environment in which PostgreSQL is already installed. Uninstall PostgreSQL first, and then install JP1/DH - Server.
- You cannot install JP1/DH - Server in an environment in which the `postgres` user exists. Delete the `postgres` user, and then install JP1/DH - Server.

  In Linux, also delete the home directory of the `postgres` user. Before deleting the home directory, check the contents in it and save the necessary files, if any.
- To install JP1/DH - Server again after uninstalling it, either delete the installation folder or empty the folder before re-installation.

4.1.3 Notes on overwrite installation and upgrade installation

In a Windows OS, when you perform an overwrite or upgrade installation of JP1/DH - Server, JP1/DH - Server resets the password for the database service user to `p@ssw0rd`.

For this reason, if you have changed the password for the `postgres` user registered in the OS (database service user) or you have changed the password for the database by using the `dbchangepassword.bat` command, specify the passwords again after the installation as needed.

4.2 Functions provided by the installer

This section describes the functions provided by the installer for JP1/DH - Server.

4.2.1 New installation

You can newly install JP1/DH - Server.

Note that you need to edit the configuration file and change the application configuration after completing the installation.

4.2.2 Overwrite installation and upgrade installation

In any of the following cases, you can install JP1/DH - Server by overwrite installation or upgrade installation:

- When you install the same version of JP1/DH - Server by overwriting existing JP1/DH - Server
- When you upgrade the existing JP1/DH - Server to the newer version

4.2.3 Uninstallation

You can uninstall JP1/DH - Server.

When you re-install JP1/DH - Server after uninstalling it, perform the following operations to prevent unexpected problems:

- Delete all the folders and files under the installation folder.
- Before re-installing JP1/DH - Sever, restart the machine.

5 Installation and Setup

This chapter describes how to install and set up JP1/DH - Server.

5.1 Installation for Windows

This section describes how to install JP1/DH - Server on a Windows OS.

In Windows Server 2012 or Windows Server 2012 R2, to use the *command prompt with elevated privileges* installed together with JP1/DH - Server, you need to install Microsoft .NET Framework 3.5. For details about how to install Microsoft .NET Framework 3.5, see *D. Installing .NET Framework 3.5*.

5.1.1 New installation (in Windows)

To newly install JP1/DH - Server:

1. Log in to the machine on which you want to newly install JP1/DH - Server as a built-in Administrator user.

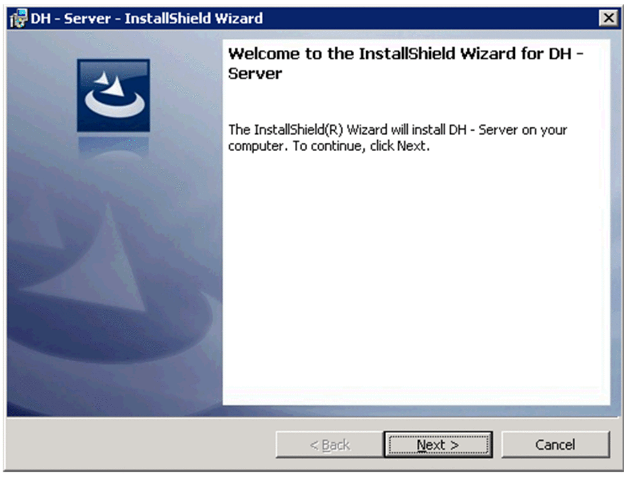
2. Exit all the Windows programs. (Recommended)

3. Start Hitachi Integrated Installer.

   Insert the Hitachi Integrated Installer medium (CD-ROM) including JP1/DH - Server in the drive, and then start Hitachi Integrated Installer.

4. Start the JP1/DH - Server installer.

   In Hitachi Integrated Installer, select **JP1/Data Highway - Server**, and then click the **Install** button. The Welcome to JP1/DH - Server Setup window appears.



DH - Server - InstallShield Wizard

Welcome to the InstallShield Wizard for DH - Server

The InstallShield(R) Wizard will install DH - Server on your computer. To continue, click Next.

5. Click the **Next** button. The User Information window appears.

6. Enter user information.

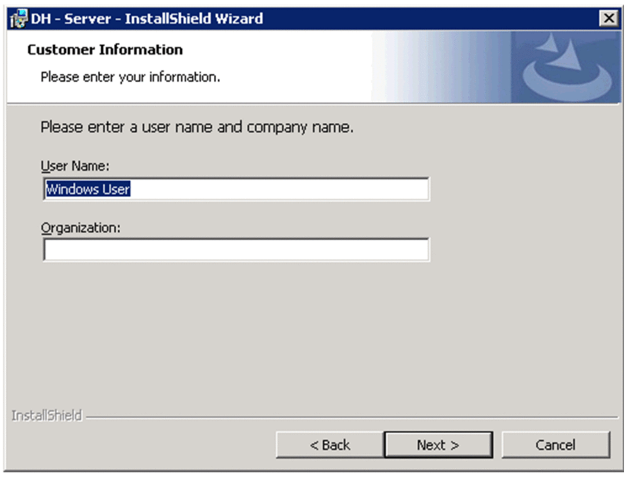
   Enter values for **User name** and **Company name**.

   - **User name**

     Specify a user name using no more than 50 characters. Any character can be specified. The user name registered in the system is displayed by default.

   - **Company name**

     Specify a company name using no more than 80 characters. Any character can be specified. The company name registered in the system is displayed by default.



DH - Server - InstallShield Wizard

Customer Information

Please enter your information.

Please enter a user name and company name.

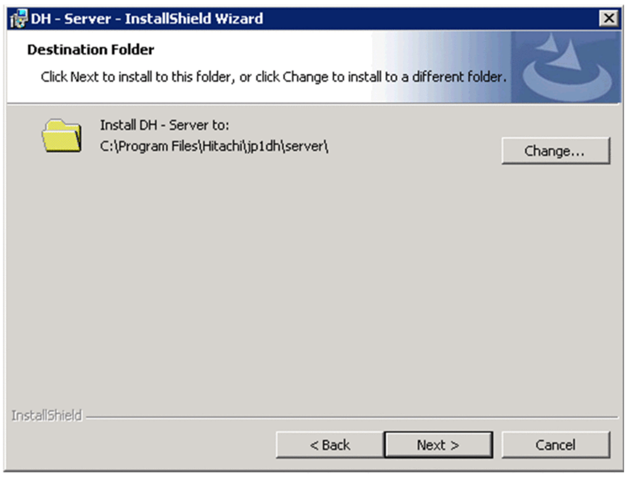
User Name: Windows User

Organization:

7. Click the **Next** button. The Installation Folder window appears.

8. Specify the installation folder.

   To change the installation location, in the dialog box displayed by clicking the **Change...** button, select the installation folder[#].



DH - Server - InstallShield Wizard

Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install DH - Server to:
C:\Program Files\Hitachi\jp1dh\server\

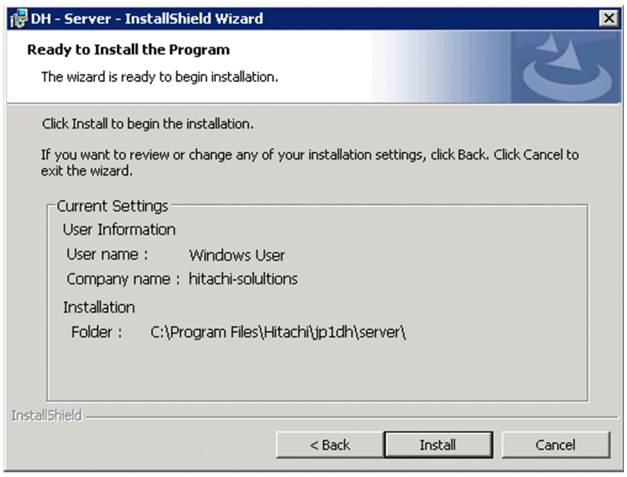
#

A maximum of 44 characters can be specified for the length of the path of the installation folder. You cannot specify a folder whose name contains a single-byte hash mark (#) or double-byte characters. Do not install JP1/DH - Server under the root of the system drive or under the system folder.

9. Click the **Next** button. The Ready to Install window appears.

10. Before starting installation, check the entered data.

    In the Ready to Install window, make sure that the entered information is correct.



Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Current Settings

User Information

User name : Windows User

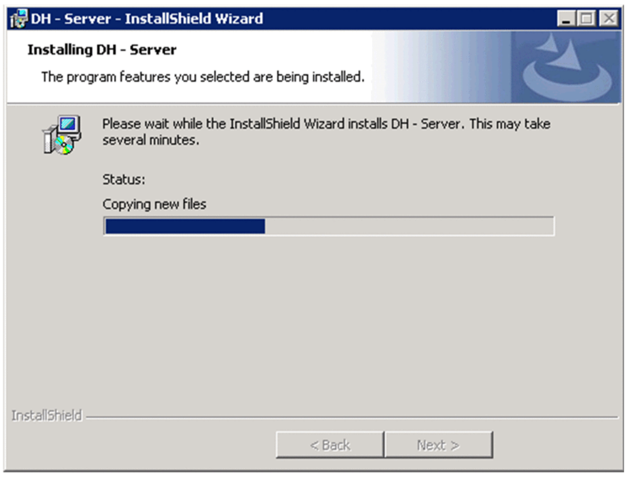
Company name : hitachi-solultions

Installation

Folder : C:\Program Files\Hitachi\jp1dh\server\

11. Start a new installation of JP1/DH - Server.

    In the Ready to Install window, click the **Install** button. The installation of JP1/DH - Server starts.



Installing DH - Server

The program features you selected are being installed.

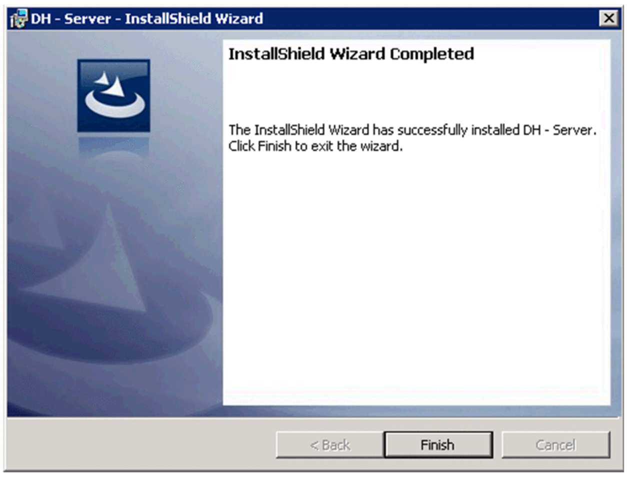
Please wait while the InstallShield Wizard installs DH - Server. This may take several minutes.

Status:

Copying new files

12. Finish the new installation of JP1/DH - Server.

    When the installation is completed, the InstallShield Wizard Complete window appears. Click the **Finish** button to finish the new installation of JP1/DH - Server.



InstallShield Wizard Completed

The InstallShield Wizard has successfully installed DH - Server. Click Finish to exit the wizard.

13. Exit Hitachi Integrated Installer.

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

Important note

- After the new installation of JP1/DH - Server is completed, set up the JP1/DH - Server environment. For details about how to set up the environment, see *5.3 Setting up the JP1/DH Web application server environment*.
- If the installation ends due to an error, the status of the location to which JP1/DH - Server is installed is invalid. In this case, eliminate the cause of that error, start the installer again, make sure that the installer ends normally, and then complete the installation.

5.1.2 Overwrite installation (in Windows)

To perform an overwrite installation of JP1/DH - Server:

1. Log in to the machine in which you want to perform an overwrite installation of JP1/DH - Server as a built-in Administrator user.

2. Exit all the Windows programs.

   If another application is using a file that is part of JP1/DH - Server, the File in Use dialog box might appear. In this case, click the **Cancel** button to stop the overwrite installation, exit all the Windows programs, and then perform the overwrite installation again.

3. Stop JP1/DH - Server.

   From Windows **Administrative Tools**, open the Services window, and then select **Stop the service** for the services in the following order:

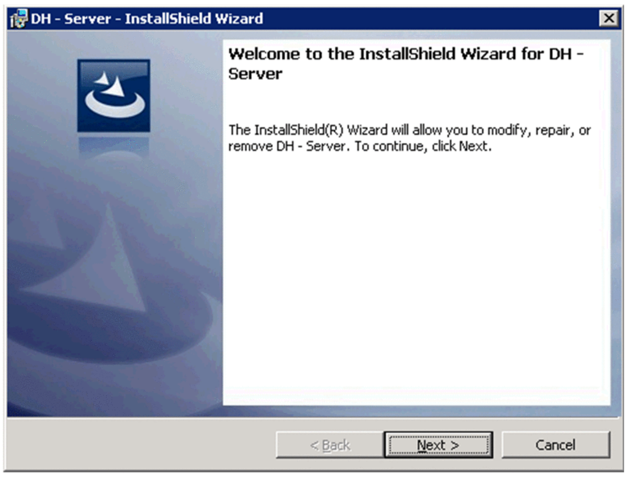
   - `JP1_DH_WEB SVR` (if the JP1/DH Web server is used)
   - `JP1_DH_WEB CONTAINER`
   - `JP1_DH_DATABASE_SVR`

4. Start Hitachi Integrated Installer.

   Insert the Hitachi Integrated Installer medium (CD-ROM) including JP1/DH - Server in the drive, and then start Hitachi Integrated Installer.

5. Start the JP1/DH - Server installer.

   In Hitachi Integrated Installer, select **JP1/Data Highway - Server**, and then click the **Install** button. The Welcome to JP1/DH - Server Setup window appears.

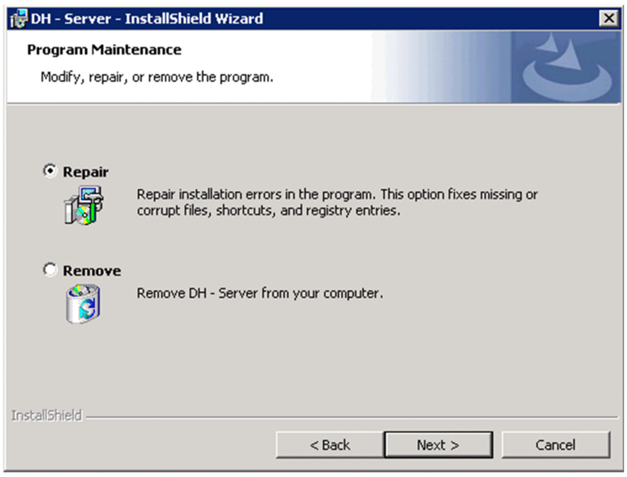


Welcome to the InstallShield Wizard for DH - Server

The InstallShield(R) Wizard will allow you to modify, repair, or remove DH - Server. To continue, click Next.

6. Click the **Next** button. The Program Maintenance window appears.

7. Select **Repair**.
   In the Program Maintenance window, select **Repair**.



Program Maintenance

Modify, repair, or remove the program.

● Repair

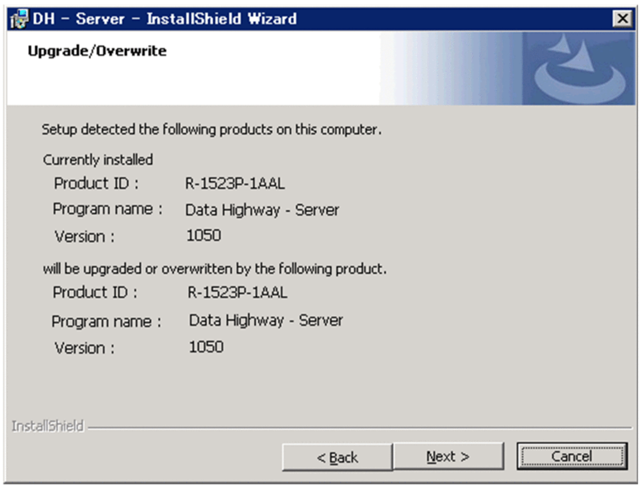
Repair installation errors in the program. This option fixes missing or corrupt files, shortcuts, and registry entries.

○ Remove

Remove DH - Server from your computer.

8. Click the **Next** button. The Upgrade/Overwrite window appears.

9. Check the details of the installed version before starting an overwrite installation.
   The Upgrade/Overwrite window appears. Check the details of the installed version.



Upgrade/Overwrite

Setup detected the following products on this computer.

Currently installed

Product ID : R-1523P-1AAL

Program name : Data Highway - Server

Version : 1050

will be upgraded or overwritten by the following product.

Product ID : R-1523P-1AAL

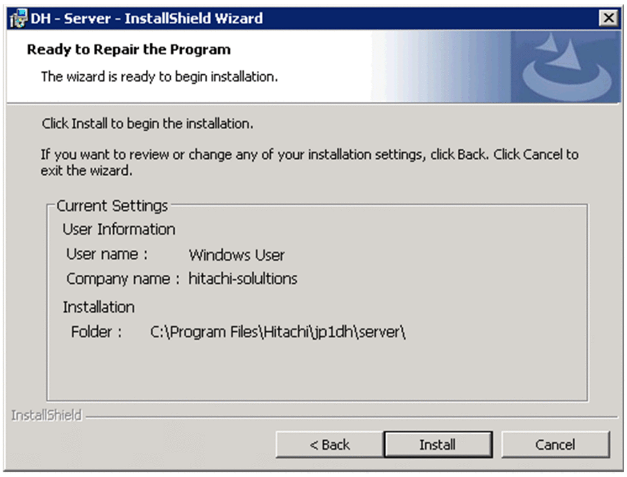
Program name : Data Highway - Server

Version : 1050

10. Click the **Next** button. The Ready to Repair Program window appears.

11. Check the entered data before starting an overwrite installation.

    In the Ready to Repair Program window, make sure that the entered information is correct.



DH - Server - InstallShield Wizard

Ready to Repair the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Current Settings

User Information

User name : Windows User

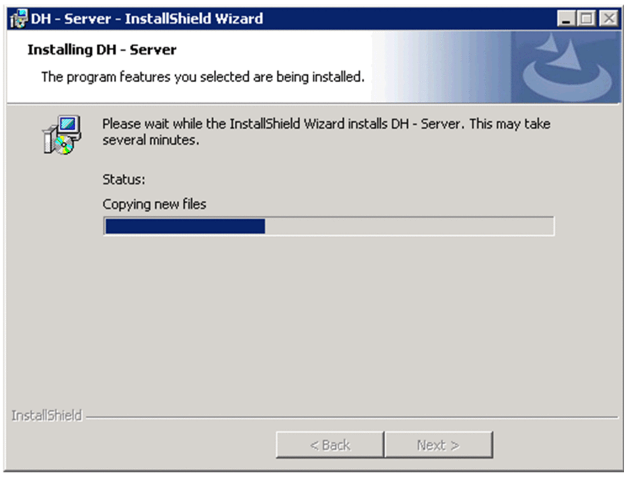
Company name : hitachi-solultions

Installation

Folder : C:\Program Files\Hitachi\jp1dh\server\

12. Start an overwrite installation of JP1/DH - Server.

    In the Ready to Repair Program window, click the **Install** button. The overwrite installation of JP1/DH - Server starts.



DH - Server - InstallShield Wizard

Installing DH - Server

The program features you selected are being installed.

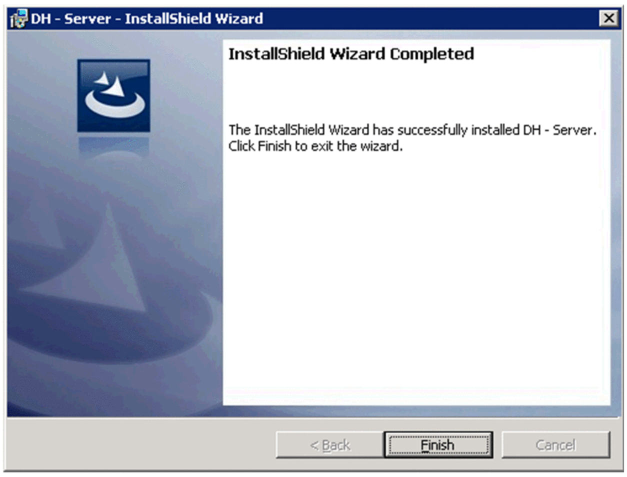
Please wait while the InstallShield Wizard installs DH - Server. This may take several minutes.

Status:

Copying new files

13. Finish the overwrite installation of JP1/DH - Server.

    When the overwrite installation is completed, the InstallShield Wizard Complete window appears. Click the **Finish** button to finish the overwrite installation of JP1/DH - Server.



InstallShield Wizard Completed

The InstallShield Wizard has successfully installed DH - Server. Click Finish to exit the wizard.

14. Exit Hitachi Integrated Installer.

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

> **Important note**
>
> - After the overwrite installation of JP1/DH - Server is completed, start the database service (`JP1_DH_DATABASE_SVR`), and then set up the JP1/DH - Server environment. For details about how to set up the environment, see *5.3 Setting up the JP1/DH Web application server environment*.
> - If the installation ends due to an error, the status of the location to which JP1/DH - Server is installed is invalid. In this case, eliminate the cause of that error, start the installer again, make sure that the installer ends normally, and then complete the installation.
> - The database-related passwords are reset to `p@ssw0rd`. Specify them again as needed. For details, see *4.1.3 Notes on overwrite installation and upgrade installation*.

5.1.3 Upgrade installation (in Windows)

To perform an upgrade installation of JP1/DH - Server:

1. Log in to the machine in which you want to perform an upgrade installation of JP1/DH - Server as a built-in Administrator user.

2. Exit all the Windows programs.

   If another application is using a file that is part of JP1/DH - Server, the File in Use dialog box might appear. In this case, click the **Cancel** button to stop the upgrade installation, exit all the Windows programs, and then perform the upgrade installation again.

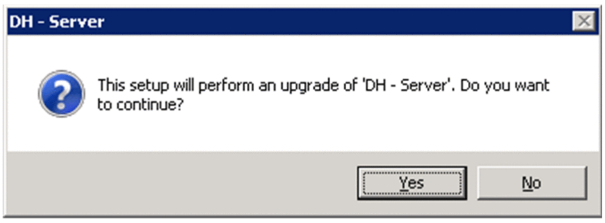
3. Stop JP1/DH - Server.

   From Windows **Administrative Tools**, open the Services window, select `JP1_DH_WEB CONTAINER`, and then click **Stop the service**.

4. Start Hitachi Integrated Installer.

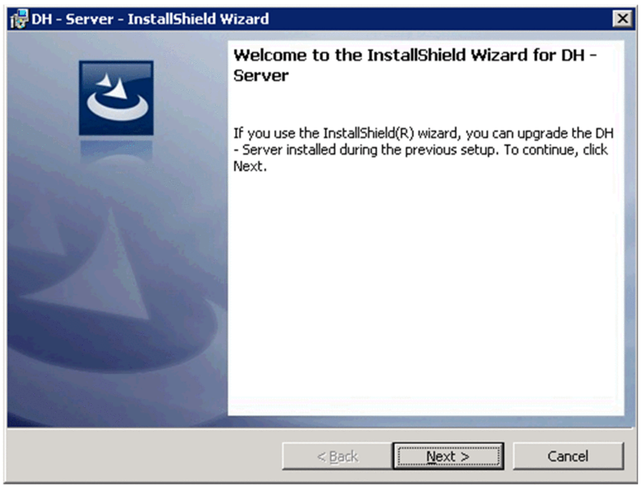
   Insert the Hitachi Integrated Installer medium (CD-ROM) including JP1/DH - Server in the drive, and then start Hitachi Integrated Installer.

5. The confirmation dialog box for upgrading appears. Click the **Yes** button. The Start Upgrade Installation window appears.



This setup will perform an upgrade of 'DH - Server'. Do you want to continue?

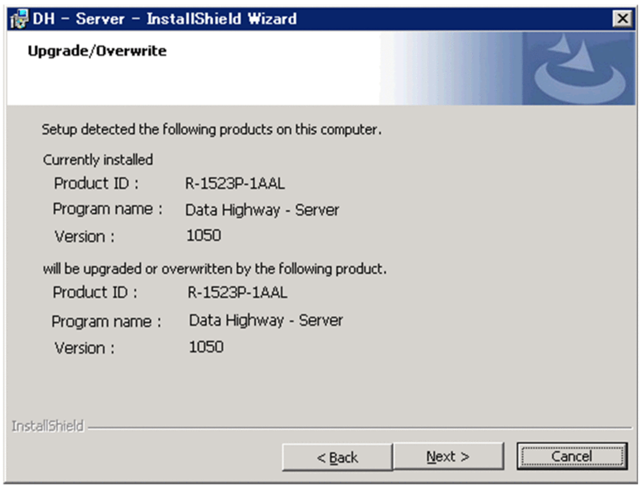
6. Click the **Next** button. The Upgrade/Overwrite window appears.



Welcome to the InstallShield Wizard for DH - Server

If you use the InstallShield(R) wizard, you can upgrade the DH - Server installed during the previous setup. To continue, click Next.

7. Check the details of the installed version before starting an upgrade installation.



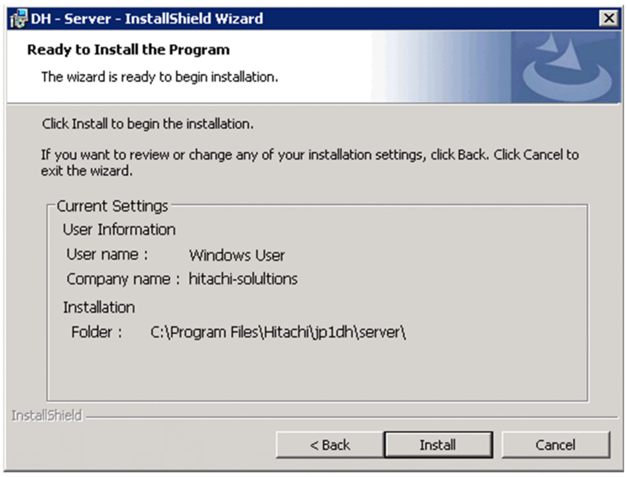
Upgrade/Overwrite

Setup detected the following products on this computer.

Currently installed
Product ID : R-1523P-1AAL
Program name : Data Highway - Server
Version : 1050

will be upgraded or overwritten by the following product.
Product ID : R-1523P-1AAL
Program name : Data Highway - Server
Version : 1050

8. Click the **Next** button. The Ready to Install window appears.
In the Ready to Install window, make sure that the entered information is correct.



Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Current Settings

User Information

User name : Windows User

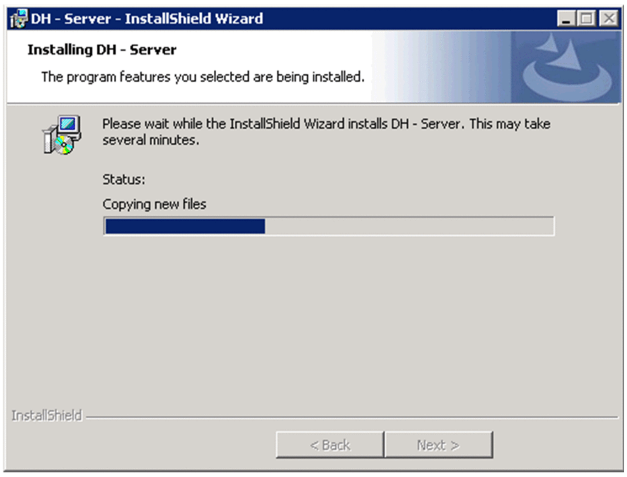
Company name : hitachi-solultions

Installation

Folder : C:\Program Files\Hitachi\jp1dh\server\

9. Start an upgrade installation of JP1/DH - Server.

In the Ready to Install window, click the **Install** button. The upgrade installation of JP1/DH - Server starts.



Installing DH - Server

The program features you selected are being installed.

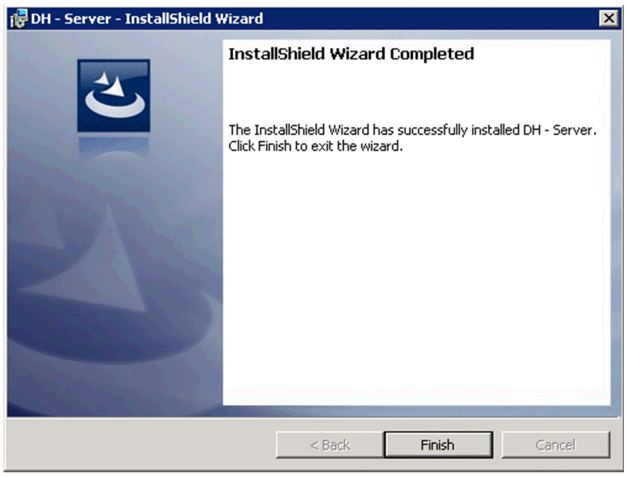
Please wait while the InstallShield Wizard installs DH - Server. This may take several minutes.

Status:

Copying new files

10. Finish the upgrade installation of JP1/DH - Server.

When the upgrade installation is completed, the InstallShield Wizard Complete window appears. Click the **Finish** button to finish the upgrade installation of JP1/DH - Server.



InstallShield Wizard Completed

The InstallShield Wizard has successfully installed DH - Server. Click Finish to exit the wizard.

11. Exit Hitachi Integrated Installer.

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

Important note

- After the upgrade installation of JP1/DH - Server is completed, start the database service (`JP1_DH_DATABASE_SVR`), and then set up the JP1/DH - Server environment. For details about how to set up the environment, see *5.3 Setting up the JP1/DH Web application server environment*.
- If the upgrade installation ends due to an error, the status of the location to which JP1/DH - Server is installed is invalid. In this case, eliminate the cause of that error, start the installer again, make sure that the installer ends normally, and then complete the upgrade installation.
- The database-related passwords are reset to `p@ssw0rd`. Specify them again as needed. For details, see *4.1.3 Notes on overwrite installation and upgrade installation*.

5.1.4 Uninstallation (in Windows)

This subsection describes how to uninstall JP1/DH - Server. There are two ways to uninstall JP1/DH - Server: uninstallation using Windows **Programs and Features** and uninstallation using Hitachi Integrated Installer.

If the uninstallation ends due to an error, the status of the location from which JP1/DH - Server is uninstalled is invalid. In this case, eliminate the cause of that error, perform the uninstallation again, and then make sure that the uninstallation ends normally.

(1) Uninstalling JP1/DH - Server by using Windows Programs and Features

1. Log in to the machine from which you want to uninstall JP1/DH - Server as a built-in Administrator user#.

   #

   If you have Administrator permissions, you cannot uninstall JP1/DH - Server by using Windows **Programs and Features**. To uninstall JP1/DH - Server with Administrator permissions, use Hitachi Integrated Installer.

2. Exit all the Windows programs.

   If another application is using a file that is part of JP1/DH - Server, the File in Use dialog box might appear. In this case, click the **Cancel** button to stop the uninstallation, exit all the Windows programs, and then perform the uninstallation again.

3. Stop JP1/DH - Server.

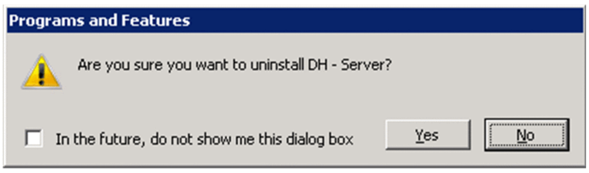
   From Windows **Administrative Tools**, open the Services window, and then select **Stop the service** for the services in the following order:

   - `JP1_DH_WEB SVR` (if the JP1/DH Web server is used)
   - `JP1_DH_WEB CONTAINER`
   - `JP1_DH_DATABASE_SVR`

4. From the Windows **Control Panel**, open the Programs and Features window.

5. Start uninstalling JP1/DH - Server.

   In the Programs and Features window, select **JP1/DH - Server**, and then click the **Uninstall** button. The confirmation dialog box for uninstalling JP1/DH - Server appears. To continue the uninstallation, click the **Yes** button.


Programs and Features

Are you sure you want to uninstall DH - Server?

□ In the future, do not show me this dialog box

6. Delete the user.

   From Windows **Administrative Tools**, open the Computer Management window. From **Local Users and Groups**, manually delete the user `postgres` that was added when JP1/DH - Server was installed.

7. Delete the data folder.

   Manually delete the data folder created when JP1/DH - Server was installed (*JP1/DH-Server-installation-folder* `\PostgreSQL\9.2\data`).

(2) Uninstalling JP1/DH - Server by using Hitachi Integrated Installer (in Windows)

1. Log in to the machine from which you want to uninstall JP1/DH - Server with Administrator permissions.

2. Exit all the Windows programs.

   If another application is using a file that is part of JP1/DH - Server, the File in Use dialog box might appear. In this case, click the **Cancel** button to stop the uninstallation, exit all the Windows programs, and then perform the uninstallation again.

3. Stop JP1/DH - Server.

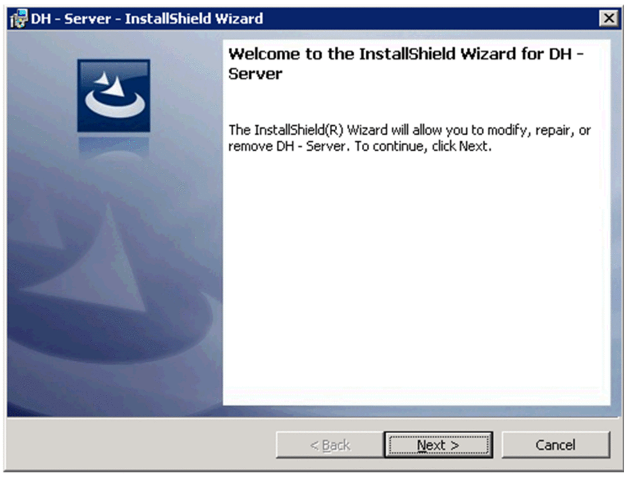
   From Windows **Administrative Tools**, open the Services window, select `JP1_DH_WEB CONTAINER`, and then click **Stop the service**.

4. Start Hitachi Integrated Installer.

   Insert the Hitachi Integrated Installer medium (CD-ROM) including JP1/DH - Server in the drive, and then start Hitachi Integrated Installer.

5. Start the JP1/DH - Server installer.

   In Hitachi Integrated Installer, select **JP1/Data Highway - Server**, and then click the **Install** button. The Welcome to JP1/DH - Server Setup window appears.


DH - Server - InstallShield Wizard

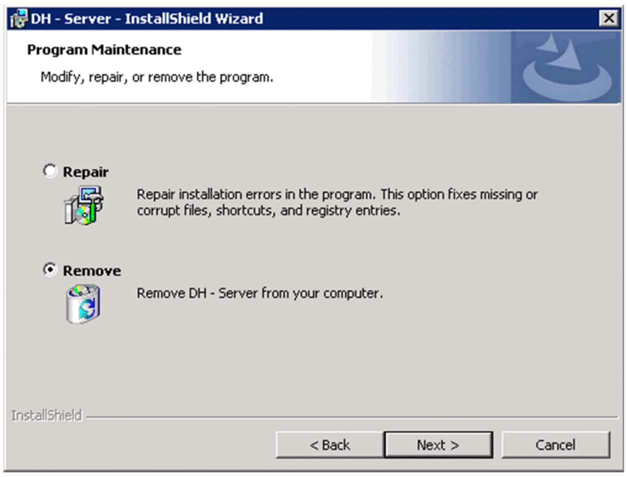
Welcome to the InstallShield Wizard for DH - Server

The InstallShield(R) Wizard will allow you to modify, repair, or remove DH - Server. To continue, click Next.

6. Click the **Next** button. The Program Maintenance window appears.

7. Select **Remove**.

   In the Program Maintenance window, select **Remove**.



DH - Server - InstallShield Wizard

Program Maintenance

Modify, repair, or remove the program.

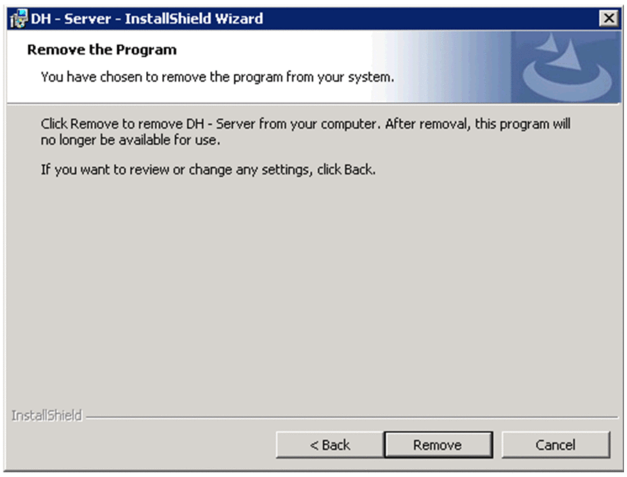
○ **Repair**

Repair installation errors in the program. This option fixes missing or corrupt files, shortcuts, and registry entries.

● **Remove**

Remove DH - Server from your computer.

8. Click the **Next** button. The Delete Program window appears.



DH - Server - InstallShield Wizard

Remove the Program

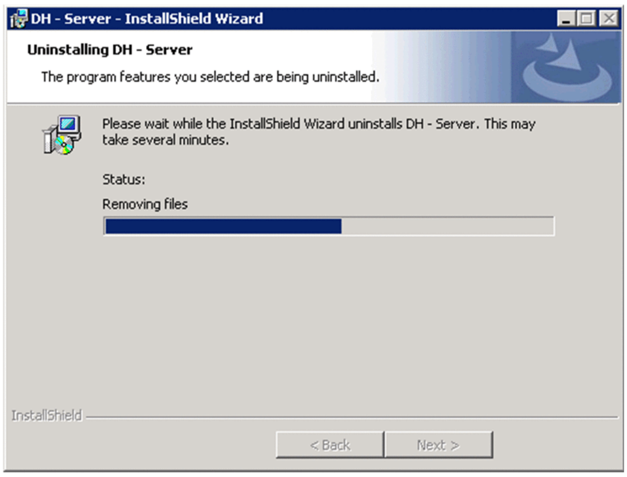
You have chosen to remove the program from your system.

Click Remove to remove DH - Server from your computer. After removal, this program will no longer be available for use.

If you want to review or change any settings, click Back.

9. Start uninstalling JP1/DH - Server.

   In the Delete Program window, click the **Remove** button. The Now Uninstalling window appears.



DH - Server - InstallShield Wizard

Uninstalling DH - Server

The program features you selected are being uninstalled.

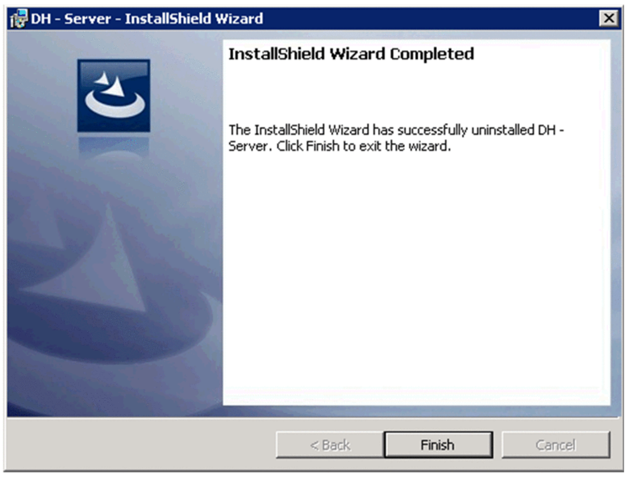
Please wait while the InstallShield Wizard uninstalls DH - Server. This may take several minutes.

Status:

Removing files

10. Finish the uninstallation of JP1/DH - Server.

    The InstallShield Wizard Complete window appears. Click the **Finish** button to finish the uninstallation of JP1/DH - Server.



InstallShield Wizard Completed

The InstallShield Wizard has successfully uninstalled DH - Server. Click Finish to exit the wizard.

11. Exit Hitachi Integrated Installer.

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

12. Delete the user.

    From Windows **Administrative Tools**, open the Computer Management window. From **Local Users and Groups**, manually delete the user `postgres` that was added when JP1/DH - Server was installed.

13. Delete the data folder.

    Manually delete the data folder created when JP1/DH - Server was installed (*JP1/DH-Server-installation-folder* `\PostgreSQL\9.2\data`).

5.2 Installation in Linux

This section describes how to install JP1/DH - Server on a Linux OS.

5.2.1 New installation, overwrite installation, and upgrade installation (in Linux)

This subsection describes how to newly install JP1/DH - Server.

In Linux, there is no distinction among new installation, overwrite installation, and upgrade installation. For details about overwrite installation and upgrade installation, see the procedure described in this subsection.

First, install Hitachi PP Installer. If Hitachi PP Installer is already installed, execute the following command to start Hitachi PP Installer:

```
/etc/hitachi_x64setup -i /cdrom
```

Note: The portion in italics is different depending on your environment.

1. Log in to the host on which you want to install JP1/DH - Server as a super user. Alternatively, use the `su` command to change the user to a super user.
2. For both overwrite installation and upgrade installation, stop JP1/DH - Server in the following order:
   - `JP1_DH_WEBSVR` (if the JP1/DH Web server is used)
   - `JP1_DH_WEBCON`
   - `JP1_DH_DATABASE_SVR`
3. Insert the CD-ROM containing JP1/DH - Server in the drive.
4. Mount the CD-ROM device.
   In this example, the command mounts the CD-ROM onto `/cdrom`:
   ```
   /bin/mount -r -o mode=0544device-special-file-name /mnt/cdrom
   ```
5. Execute the following command to install and start Hitachi PP Installer:
   ```
   mnt/cdrom/X64LIN/setup /mnt/cdrom
   ```
   After Hitachi PP Installer is running, install JP1/DH - Server.
6. After Hitachi PP Installer is running, the initial window appears.
   An example of the initial window is as follows:
   ```
   Hitachi PP Installer 05-16

   L) List Installed Software
   I) Install Software
   D) Delete Software
   Q) Quit
   ```

```
Select Procedure ===>
...
```

7. In the initial window, enter `I`.

   A list of software programs you can install is displayed.

8. Move the cursor to `JP1/DH - Server`, and then select it by using the spacebar. Enter `I`.

   JP1/DH - Server is installed.

9. When the installation is completed, enter `Q`. The initial window appears again.

Important note

- After the new, overwrite, or upgrade installation of JP1/DH - Server is completed, start the database service (`JP1_DH_DATABASE_SVR`), and then set up the JP1/DH - Server environment. For details about how to set up the environment, see *5.3 Setting up the JP1/DH Web application server environment*.
- If the installation ends due to an error, the status of the location to which JP1/DH - Server is installed is invalid. In this case, eliminate the cause of that error, start the installer again, make sure that the installer ends normally, and then complete the installation.
- For the overwrite or upgrade installation, the database-related passwords are reset to `p@ssw0rd`. Specify them again as needed. For details, see *4.1.3 Notes on overwrite installation and upgrade installation*.

5.2.2 Uninstallation (in Linux)

To uninstall JP1/DH - Server:

1. Log in to the host on which you want to install JP1/DH - Server as a super user. Alternatively, use the `su` command to change the user to a super user.

2. On the local host, stop the JP1/DH - Server program and services.

   Display information about services to make sure that no JP1/DH - Server service is running. If any JP1/DH - Server program and services are running on the local host, stop all of them.

3. Execute the following command to start Hitachi PP Installer:

   ```
   /etc/hitachi_x64setup
   ```

4. The Hitachi PP Installer initial window appears. For details about the initial window, see *5.2.1 New installation, overwrite installation, and upgrade installation (in Linux)*.

5. In the initial window, enter `D`.

   A list of software programs you can uninstall is displayed.

6. Move the cursor to `JP1/DH - Server`, and then select it by using the spacebar. Enter `D`.

   JP1/DH - Server is uninstalled.

7. When the uninstallation is completed, enter `Q`. The initial window appears again.

8. Delete the user.

Manually delete the user `postgres` that was added when JP1/DH - Server was installed and the home directory. Before deleting the home directory, check the contents in it and save any necessary files.

9. Delete the data folder.

   Manually delete the data folder created when JP1/DH - Server was installed (`/opt/jp1dh/server/PostgreSQL/9.2/data`).

5.3 Setting up the JP1/DH Web application server environment

This section describes how to set up the JP1/DH Web application server environment.

Before performing the following procedures, log in to the JP1/DH - Server machine as a built-in Administrator user.

5.3.1 Changing the configuration file

After a new installation, set up the environment according to the procedure described below. For an overwrite installation, set up the environment according to the procedure described below only when changing the configuration file. If there is no need to change the configuration file, go to *5.3.2 Changing the application configuration*. The following describes the details of the configuration file.

(1) Editing the digikatsuwide.xml

(a) File path

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

#: In Linux, change *installation-folder* to `/opt/jp1dh/server`.

(b) Content of the configuration file

Edit only the items described in this subsection. If you edit the other items, the system might fail to start properly.

- Specifying the server IP address

  Specify the server IP address.

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

> **Important note**
>
> To make the server accessible from the Internet, specify a global IP address.

Example:

```
<end-point>
    <ip>192.168.0.2</ip>
</end-point>
<end-point protocol="https">
    <ip>192.168.0.2</ip>
</end-point>
```

- Specifying the mail server

Specify the mail server information. For details about the mail server information, see *3.2.3 Mail server used by the system* and *3.2.4 Sender email address*.

```
<mail-notification>
    <mail-server>
        <host>mail-server-host-name</host>
        <port>mail-server-port-number</port>
        <user>SMTP-authentication-user-ID</user>
        <password>SMTP-authentication-password</password>
        <secure-protocol>SMTP-type#</secure-protocol>
    </mail-serer>
    <notification-from>
        <system-address>sender-email-address</system-address>
    </notification-from>
    ...
</mail-notification>
```

#

For the `<secure-protocol>` tag, specify the type of protocol used for transmission path encryption. If nothing is specified, encryption is not applied. For encryption, specify either of the following:

- `SMTPS`: Encrypts the transmission path using SSL or TLS.
- `STARTTLS`: Encrypts the transmission path using STARTTLS.

Important note

To use SMTP authentication, specify a user ID and password for SMTP authentication for the `<user>` and `<password>` tags. If you do not use SMTP authentication, leave the `<user>` and `<password>` tags empty. The *sender-email-address* is used as the email address of the sender of notification emails sent from JP1/DH - Server to the users.

Example:

```
<mail-notification>
    <mail-server>
        <host>smtp.foo1.foo2.co.jp</host>
        <port>587</port>
        <user>user01</user>
        <password>password01</password>
        <secure-protocol>SMTPS</secure-protocol>
    </mail-serer>
    <notification-from>
        <system-address>jp1dh-system@foo1.foo2.co.jp</system-address>
    </notification-from>
    ...
</mail-notification>
```

- Specifying the server FQDN and domain name

  Specify the FQDN (Fully Qualified Domain Name) and domain name of the server.

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

#

Do not use an underscore (_) for the host name (computer name). Using an underscore for the host name causes a malfunction.

Examples of the settings are as follows:

Example 1: When the server FQDN is `xxx.yyy.zzz.co.jp`

Server domain name: `zzz.co.jp`

Server subdomain name: `xxx.yyy`

Example 2: When the server FQDN is `xxx.yyy.zzz.com`

Server domain name: `zzz.com`

Server subdomain name: `xxx.yyy`

Example:

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

- Changing the storage folder for delivery data

  Change the storage folder for delivery data# (absolute path) as needed. For details about the storage folder for delivery data, see *3.2.2 Storage folder for delivery data*.

```
<biz-connect id="bizconnect">
    ...
    <persistence>
        <storage>
            <directory>absolute-path-of-the-storage-folder-for-delivery-
data</directory>
        </storage>
    </persistence>
    ...
</biz-connect>
```

#

For the storage folder for delivery data, note the following points:

- Specify a folder on the local file system. If you specify a network folder, the file I/O might become a bottleneck, decreasing the transmission speed.
- Specify a path in 4 to 70 characters.

- Before changing the current storage folder for delivery data, create a new storage folder for delivery data in advance.

Example:

```
<biz-connect id="bizconnect">
    ...
    <persistence>
        <storage>
            <directory>D:\data</directory>
        </storage>
    </persistence>
    ...
</biz-connect>
```

- Changing the network bandwidth limit
  Change the network bandwidth limit as needed. For details about the network bandwidth limit, see *3.3.2 Network bandwidth limit*.

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

#

For values you can specify, note the following points:

- A specified value is recognized as a value in Mbps.
- Specify a value in the range from 0 to 1,000. You cannot omit the value.
- `0` means *no bandwidth limit*.

Example:

When you specify 80 Mbps for the bandwidth limit for uploading and 100 Mbps for the bandwidth limit for downloading

```
<biz-connect id="bizconnect">
    <service>
        ...
        <throughput-limit>
            <upload>80</upload>
            <download>100</download>
        </throughput-limit>
        ...
    </service>
</biz-connect>
```

- Changing the keep-alive timeout period

Change the keep-alive timeout period as needed. For details about the keep-alive timeout period, see *3.3.3 Keep-alive timeout period*.

```
<biz-connect id="bizconnect">
    <service>
        ...
        <keep-alive>
            <client>client-keep-alive-timeout-period#</client>
            <server>server-keep-alive-timeout-period#</server>
        </keep-alive>
        ...
    </service>
</biz-connect>
```

#

For values you can specify, note the following points:

- A specified value is recognized as a value in seconds.
- Specify a value as 0 or in the range from 30 to 7,200. You cannot omit the value.
- `0` means disabled timeout (no timeout).

Example:

When you specify 180 seconds for the client keep-alive timeout period and 180 seconds for the server keep-alive timeout period

```
<biz-connect id="bizconnect">
    <service>
        ...
        <keep-alive>
            <client>180</client>
            <server>180</server>
        </keep-alive>
        ...
    </service>
</biz-connect>
```

- Changing the number of concurrent connections

  Change the number of concurrent client-server connections as needed. For details about the number of concurrent connections, see *3.3.4 Concurrent connections*.

```
<biz-connect id="bizconnect">
    <service>
        ...
        <service-task>
            <initial>number-of-initial-connections#</client>
            <maximum>maximum-number-of-connections#</server>
        </service-task>
        ...
    </service>
</biz-connect>
```

#

For values you can specify, note the following points:

- Specify a value in the range from 1 to 64. You cannot omit the value.

  - Specify values so that the `initial` value is equal to or less than the `maximum` value.

Example:

When you specify 4 for the number of initial connections and 64 for the maximum number of connections

```
<biz-connect id="bizconnect">
    <service>
        ...
        <service-task>
            <initial>4</initial>
            <maximum>64</maximum>
        </service-task>
        ...
    </service>
</biz-connect>
```

- Changing the connection queue size

  Change the connection queue size as needed. For details about the connection queue, see *3.3.5 Connection queue size*.

```
<biz-connect id="bizconnect">
    <service>
        <backlog>connection-queue-size#</backlog>
        ...
    </service>
    ...
</biz-connect>
```

#

Specify a value in the range from 2 to 64. You cannot omit the value.

Example:

When you specify 16 for the connection queue size

```
<biz-connect id="bizconnect">
    <service>
        <backlog>16</backlog>
        ...
    </service>
    ...
</biz-connect>
```

- Specifying the block size during transfer and reception

  Specify the block size for sending a file from a client to JP1/DH - Server, or for downloading a file from JP1/DH - Server as needed. For details about the block sizes during transfer and reception by default, see *3.3.7 Block size during transfer and reception*.

```
<biz-connect id="bizconnect">
    <service>
      ...
      <communication-engine>
        <block-size>
          <send>block-size-for-transfer#</send>
          <receive>block-size-for-downloading#</receive>
        </block-size>
      </communication-engine>
      ...
    </service>
    ...
</biz-connect>
```

#

For the block size, specify a value as 0 or in the range from 32 to 512. A value is set in KB.

If you omit the value or specify `0`, the system automatically determines the size depending on the network condition when starting to send or receive a file. If you specify a value in the range from 32 to 512, regardless of the network condition, communication is performed based on the specified block size.

Example:

When you specify the fixed block size during transfer and reception (512 KB)

```
<biz-connect id="bizconnect">
    <service>
      ...
      <communication-engine>
        <block-size>
          <send>512</send>
          <receive>512</receive>
        </block-size>
      </communication-engine>
      ...
    </service>
    ...
</biz-connect>
```

- Specifying the buffer size during transfer and reception

  Specify the buffer size used for sending a file from JP1/DH - Server to a client and receiving a file from a client. For details about the buffer size during transfer and reception by default, see *3.3.8 Buffer size during transfer and reception*.

```
<biz-connect id="bizconnect">
    <service>
      ...
      <communication-engine>
        <server-buffer-size>
          <send>transfer-buffer-size#</send>
          <receive>reception-buffer-size#</receive>
        </server-buffer-size>
      </communication-engine>
      ...
    </service>
    ...
</biz-connect>
```

#

For the buffer size during transfer and reception for JP1/DH - Server, you can specify a value in the range below. A value is set in KB. If you omit the value, operation is performed in the default value, 8,192 KB (8 MB).

Minimum value: 64

Maximum value: 65,536

Example:

When you specify 65,536 (64 MB) for the buffer size during transfer and reception

```
<biz-connect id="bizconnect">
    <service>
      ...
      <communication-engine>
        <server-buffer-size>
          <send>65536</send>
          <receive>65536</receive>
        </server-buffer-size>
      </communication-engine>
      ...
    </service>
    ...
</biz-connect>
```

- Specifying the packet queue size of clients

  Specify the packet queue size of clients as needed. For details about the packet queue size of clients by default, see *3.3.9 Packet queue size of clients*.

```
<biz-connect id="bizconnect">
    <service>
      <communication-engine>
        <packet-queue-capacity>packet-queue-size-of-clients#
        </packet-queue-capacity>
      </communication-engine>
      ...
    </service>
    ...
</biz-connect>
```

#

For the packet queue size of clients, you can specify a value in the range below. A value is set in KB.

If you omit the value or specify a value outside the range, the system assumes that the default value is specified.

Minimum value: 16,384

Maximum value: 131,072

Example:

When you specify 131,072 (128 MB) for the packet queue size of clients

```
<biz-connect id="bizconnect">
    <service>
      ...
      <communication-engine>
        <packet-queue-capacity>131072</packet-queue-capacity>
      </communication-engine>
      ...
    </service>
    ...
</biz-connect>
```

- Specifying the maximum size of files available for transfer

  Specify the maximum size of a single delivery attempt and the maximum file size per file as needed. For details about the maximum size of files available for transfer by default, see *3.3.10 Maximum size of files available for transfer*.

The specified values are displayed in the delivery policy window. When the administrator creates or edits a delivery policy, the values specified here are applied. For this reason, even if you change the maximum size of files available for transfer, the maximum values before the change are effective for a file transfer that uses the delivery policy created by using the maximum values before the change.

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

#

For the maximum size per delivery and the maximum size per file, you can specify a value in the range below. A value is set in GB. Note that if you omit the values, the JP1/DH Web application server fails to start.

Minimum value: 1

Maximum value: 1,024

If you specify a value less than 1, the system assumes that 1 is specified. If you specify a value more than 1,024, the system assumes that 1,024 is specified.

Example:

When you specify 1,024 GB for the maximum size of files available for transfer

```
<biz-connect id="bizconnect">
    <service>
      ...
      <data-capacity>
        <per-file>1024</per-file>
        <per-delivery>1024</per-delivery>
      </data-capacity>
      ...
    </service>
    ...
</biz-connect>
```

- Specifying the SALT string for password obfuscation

  Specify as needed the SALT string for obfuscating a user password (a user password used for connecting to JP1/DH - Server). For details about how to specify the SALT string, see *3.3.11 Password obfuscation (SALT string)*.

```
<biz-connect id="bizconnect">
  ...
  <security>
    <password-salt>SALT-string#</password-salt>
  </security>
  ...
</biz-connect>
```

#

Specify the SALT string to be added to a JP1/DH - Server user password. If you specify an empty character or omit a value, a SALT is not added. The characters that you can use for a SALT string are the same as those used for a password. You can use no more than 20 characters for a SALT string.

Example:

When you specify `HITACHI1234` for the SALT string:

```
<biz-connect id="bizconnect">
  ...
  <security>
    <password-salt>HITACHI1234</password-salt>
  </security>
  ...
</biz-connect>
```

Important note

- Do not change the SALT string immediately after starting operation. If you change the SALT string after starting operation, you must register the registered user passwords again. Before starting operation, sufficiently consider the SALT string and then specify it.
- When you specify the SALT string, you must reset the password for the system administrator. See *5.5.2 Changing the password for the system administrator*, and then reset the password for the system administrator.

- Specifying the maximum storage period of files

  Specify the maximum file storage period as needed. For details about the maximum storage period of files, see *3.3.12 Maximum storage period of files*.

```
<biz-connect id="bizconnect">
  ...
  <persistence>
    <storage>
      <max-storage-period>number-of-days-for-the-maximum-file-storage-
period</max-storage-period>
    </storage>
  </persistence>
  ...
</biz-connect>
```

#

For the number of days for the maximum file storage period, specify a value in the range from 1 to 3,650 (10 years).

Example:

When you specify 100 days for the maximum file storage period

```
<biz-connect id="bizconnect">
  ...
  <persistence>
    <storage>
      <max-storage-period>100</max-storage-period>
    </storage>
  </persistence>
  ...
</biz-connect>
```

- Specifying the maximum number of destinations

  In the web window, specify the maximum number of destinations that can be specified by the user for sending as needed. For details about the maximum number of destinations for sending, see *3.3.13 Maximum number of destinations*.

```
<digivery id="dh">
    ...
    <mail-notification>
      <send-screen-maximum-destinations>maximum-number-of-destinations-
for-sending#</send-screen-maximum-destinations>
    </mail-notification>
    ...
</digivery>
```

#

For the maximum number of destinations for sending, specify a value in the range from 1 to 500.

Example:

When you specify 500 for the maximum number of destinations that can be specified for sending

```
<digivery id="dh">
    ...
    <mail-notification>
      <send-screen-maximum-destinations>500</send-screen-maximum-
destinations>
    </mail-notification>
    ...
</digivery>
```

- Specifying whether to enable the initial environment setup function

  If necessary, specify whether to automatically create a default address book, a default delivery policy, and default delivery rules when creating a domain. For details about the default setting of the initial environment setup function, see *3.3.14 Enabling or disabling the initial environment setup function*.

```
<digivery id="dh">
    ...
    <biz-connect id="bizconnect">
      ...
      <use-domain-initialization>whether-to-enable-the-initial-
environment-setup-function</use-domain-initialization>
    </biz-connect>
    ...
</digivery>
```

Example:

When you use the initial environment setup function

```
<digivery id="dh">
    ...
    <biz-connect id="bizconnect">
      ...
      <use-domain-initialization>TRUE</use-domain-initialization>
    </biz-connect>
    ...
</digivery>
```

- Specifying the default delivery status type for the in-box

  Specify the default delivery status type for the display of the user's in-box as needed. For details about the default delivery status type for the in-box, see *3.3.15 Default setting for the processing status type of deliveries to be displayed in the in-box*.

```
<digivery id="dh">
    ...
    <user-interface>
        ...
        <mail-box>
          <receiving-box-default-status>default-display-type-for-the-in-
box#</receiving-box-default-status>
        </mail-box>
        ...
    </user-interface>
    ...
</digivery>
```

#

You can specify one of the types below for the default display type. The default display type is not case-sensitive.

- NOTOPENED
- OPENED
- ALL

Example:

When you specify OPENED for the default display type for the in-box

```
<digivery id="dh">
    ...
    <user-interface>
        ...
        <mail-box>
          <receiving-box-default-status>OPENED</receiving-box-default-
status>
        </mail-box>
        ...
    </user-interface>
    ...
</digivery>
```

- Specifying whether to display the Compress Method options

  If necessary, specify whether to display the Compress Method options in the window for creating or editing delivery policy. For details about whether to display the Compress Method options by default, see *3.3.16 Displaying the Compress Method options*.

  Standard and **Extended** are displayed as options. By using a delivery policy based on the **Extended** compression method, you can compress and send a file or folder exceeding 4 GB. Note that even if the system parameter settings are changed during operation, the already-set delivery policy data is not changed. The system parameter values are applied when the representative user edits the above delivery policy.

```
<digivery id="dh">
  ...
  <user-interface >
    <delivery-policy >
      <display-compression-method >Compress-Method-options-display</
display-compression-method>
    </delivery-policy >
    ...
  </user-interface >
  ...
</digivery>
```

Example:

When you display the Compress Method options

```
<digivery id="dh">
  ...
  <user-interface >
    <delivery-policy >
      <display-compression-method >TRUE</display-compression-method>
    </delivery-policy >
    ...
  </user-interface >
  ...
</digivery>
```

- Specifying the method for storage on the server for the **Extended** compression method

  If necessary, specify whether to store the sending target data in an external folder on the server when sending a folder by using a delivery policy based on the **Extended** compression method or when sending a file or folder by selecting **STRONG**, **MIDDLE**, or **WEAK** for **Compress Level**. For details about the default method for storage on the server for the **Extended** compression method, see *3.3.17 External storage options for the data sent by using the extended compression method*.

```
<digivery id="dh">
  ...
  <biz-connect id="bizconnect">
    ...
    <persistence>
      ...
      <gcp-external-file-saving-condition>
        <count-threshold>maximum-number-of-files-to-be-externally-stored-
from-among-files-or-files-in-a-folder-in-a-single-delivery#1
        </count-threshold>
        <size-threshold>maximum-total-file-size-of-files-to-be-externally-
stored-from-among-files-or-files-in-a-folder-in-a-single-delivery#2
        </size-threshold><!--KB-->
      </gcp-external-file-saving-condition>
    </persistence>
    ...
  </biz-connect>
  ...
</digivery>
```

#1

For the maximum number of files to be externally stored from among files or files in a folder in a single delivery, you can specify one of the following values:

- `-1`: All files are externally stored without limit.
- `0`: No files are externally stored.
- `1` to `262144`: As many files as specified are externally stored.

#2

For the maximum total file size of files to be externally stored from among files or files in a folder in a single delivery, you can specify one of the values below. A value is set in KB.

- `-1`: All files are externally stored without limit.
- `0`: No files are externally stored.
- `1` to `1048576`: Files that are smaller than the specified file size are to be externally stored.

Example:

When you store files in an external folder

```
<digivery id="dh">
  ...
  <biz-connect id="bizconnect">
    ...
    <persistence>
      ...
      <gcp-external-file-saving-condition>
        <count-threshold>262144</count-threshold>
        <size-threshold>1048576</size-threshold><!--KB-->
      </gcp-external-file-saving-condition>
    </persistence>
    ...
  </biz-connect>
  ...
</digivery>
```

- Specifying whether to display the number of TCP connections

  If necessary, specify whether to display the following items in a delivery policy other than the standard delivery policy: **Max. TCP sessions per Connection** and **Always connect with Max. TCP sessions**. For details about the default display of the number of TCP connections, see *3.3.18 Displaying the options related to number of TCP connections*.

  If you specify to display the items, you can specify the number of TCP connections for each policy.

```
<digivery id="dh">
  ...
  <user-interface>
    <delivery-policy>
      ...
      <display-max-tcp-connections>displaying-Max.-TCP-sessions-per-
Connection</display-max-tcp-connections>
      <display-always-connect-max-tcp-connections> Always-connect-with-
Max.-TCP-sessions</display-always-connect-max-tcp-connections>
    </delivery-policy>
    ...
  </user-interface>
  ...
</digivery>
```

Example:

When you display the items for the number of the TCP connections

```
<digivery id="dh">
  ...
  <user-interface>
    <delivery-policy>
      ...
      <display-max-tcp-connections>TRUE</display-max-tcp-connections>
      <display-always-connect-max-tcp-connections>TRUE</display-always-
connect-max-tcp-connections>
    </delivery-policy>
    ...
  </user-interface>
  ...
</digivery>
```

- Specifying the timeout period when using a directory server

  If the directory server is used for user authentication for login to JP1/DH - Server, specify the LDAP connection timeout period and the timeout period for user searches by the directory server in milliseconds. For details about the default timeout period, see *3.3.19 Timeout period when using a directory server*.

  If you specify a value equal to or less than 0, the timeout period specified in the network protocol such as TCP is used.

```
<digivery id="dh">
  ...
  <biz-connect id="bizconnect">
    ...
    <authentication-system>
      <ldap-connection-timeout>timeout-period-for-connecting-to-the-
directory-server#</ldap-connection-timeout>
      <ldap-search-timeout>timeout-period-for-searching-a-user#</ldap-
search-timeout>
      </authentication-system>
      ...
  </biz-connect>
  ...
</digivery>
```

#

For values you can specify, note the following points:

- A specified value is recognized as a value in milliseconds.
- Specify a value in the range from 0 to 30,000.

Example:

When you specify 10 seconds for the timeout period:

```
<digivery id="dh">
  ...
  <biz-connect id="bizconnect">
    ...
    <authentication-system>
      <ldap-connection-timeout>10000</ldap-connection-timeout>
      <ldap-search-timeout>10000</ldap-search-timeout>
      </authentication-system>
      ...
  </biz-connect>
  ...
</digivery>
```

- Specifying whether to enable the approval exclusion function when using JP1/Data Highway - AJE

  When you use JP1/Data Highway - AJE, specify whether to exclude the approval processing in the specified approval route at the time of sending.

  For details about the default setting of the approval processing when using JP1/Data Highway - AJE, see *3.3.20 Approval exclusion function when using JP1/Data Highway - AJE*. If you enable the approval exclusion function, approval request emails are not sent to the approver. This makes the approval processing (accept or reject) unnecessary. In addition, a recipient can receive a file or folder without waiting for the approval processing by the approver.

```
<digivery id="dh">
  ...
  <biz-connect id="bizconnect">
      ...
      <use-command-approval-exclusion>approval-exclusion-function</use-
command-approval-exclusion>
      ...
  </biz-connect>
  ...
</digivery>
```

Example:

When you exclude the approval processing in JP1/Data Highway - AJE

```
<digivery id="dh">
  ...
  <biz-connect id="bizconnect">
      ...
      <use-command-approval-exclusion>TRUE</use-command-approval-
exclusion>
      ...
  </biz-connect>
  ...
</digivery>
```

- Specifying whether to enable the file validation disabling function when using JP1/Data Highway - AJE

  When you use JP1/Data Highway - AJE, specify whether to disable file validation at the time of sending and receiving. For details about the default setting of the file validation disabling function when using JP1/Data Highway - AJE, see *3.3.21 Using the file validation disabling function when using JP1/Data Highway - AJE*.

  If you enable this function, file validation is not carried out when a file sent from JP1/Data Highway - AJE is received in the web window. In addition, even if the specified value is changed while a file is being sent or received, the value specified at the time of sending or receiving is effective. However, if sending or receiving is suspended by the suspend command in *7.4.1 Suspension and cancellation of the active file transfer*, the specified value after the change is applied when the suspended sending or receiving is resumed because the specified values are checked again when resuming the transfer.

Important note

This function is enabled only when JP1/Data Highway - AJE 10-10 or later is used.

```
<digivery id="dh">
  ...
  <biz-connect id="bizconnect">
      ...
      <use-command-digest-validation-exclusion>file-validation-disabling-
function
      </use-command-digest-validation-exclusion>
      ...
  </biz-connect>
  ...
</digivery>
```

Example:

When you enable the file validation disabling function in JP1/Data Highway - AJE

```
<digivery id="dh">
  ...
  <biz-connect id="bizconnect">
      ...
      <use-command-digest-validation-exclusion>TRUE</use-command-digest-
validation-exclusion>
      ...
  </biz-connect>
  ...
</digivery>
```

- Specifying the maximum number of destinations when using JP1/Data Highway - AJE

  Specify the maximum number of destinations that can be specified when a file or folder is sent by using JP1/Data Highway - AJE. For details about the maximum number of destinations by default when a file or folder is sent by using JP1/Data Highway - AJE, see *3.3.22 Maximum number of destinations when using JP1/Data Highway - AJE*.

  If you enable this function, for the maximum number of destinations when a file is sent by using JP1/Data Highway - AJE, the value specified here is given priority over the value defined in the delivery policy. However, if you omit the value or specify a value equal to or less than 0, the maximum number of destinations defined in the delivery policy is applied.

```
<digivery id="dh">
  ...
  <user-interface>
    <delivery-policy>
      <force-command-maximum-destinations>maximum-number-of-destinations-
when-using-JP1/Data-Highway-AJE#</force-command-maximum-destinations>
    ...
    </delivery-policy>
  </user-interface>
  ...
</digivery>
```

#

For values you can specify, note the following points:

- 0: Follows the definition of a delivery policy.
- 1 to 500: Allows a user to specify as many destinations as specified.

Example:

When you specify 500 for the maximum number of destinations in JP1/Data Highway - AJE

```
<digivery id="dh">
  ...
  <user-interface>
    <delivery-policy>
      <force-command-maximum-destinations>500</force-command-maximum-
destinations>
      ...
    </delivery-policy>
  </user-interface>
  ...
</digivery>
```

(c) Procedure for recovering digikatsuwide.xml

If the system ceases to operate normally due to reasons such as inadvertently changing the value of an item other than the above, overwrite the file described in *5.3.1 Changing the configuration file* with the file shown below, and then edit the overwritten file again. Then, perform the procedures described in *5.3.2 Changing the application configuration* and the subsequent subsections again.

```
installation-folder\template\digikatsuwide.xml.template
```

(2) Editing ROOT_SERVICE.srv

Edit the configuration file (`ROOT_SERVICE.srv`) to specify the number of days to store audit logs as needed.

(a) File path

```
installation-folder#\misc\digikatsuwide\digikatsuwide\WEB-INF\services
\ROOT_SERVICE.srv
```

#: In Linux, change *installation-folder* to `/opt/jp1dh/server`.

(b) Content of the configuration file

Edit only the items described in this subsection. If you edit the other items, the system might fail to start properly.

- Changing the storage period of the audit log

  Specify the number of days to store the audit log as needed. For details about the storage period of the audit log, see *3.3.6 Storage period of the audit log*.

  ```
  log.persist-duration-days = storage-period-of-the-audit-log#
  ```

#

For values you can specify, note the following points:

- A specified value is recognized as a value in days.
- Specify a value as 0 or in the range from 1 to 3,650. You cannot omit the value.

- 0 means no time limit.

Example:

When you specify 365 days for the storage period of the audit log

```
log.persist-duration-days = 365
```

(c) Procedures for recovering ROOT_SERVICE.srv

If the system ceases to operate normally due to reasons such as inadvertently changing the value of an item other than the above, overwrite the file described in *(2) Editing ROOT_SERVICE.srv* with the file shown below, and then edit the overwritten file again. Then, perform the procedures described in *5.3.2 Changing the application configuration* and the subsequent subsections again.

```
installation-folder\template\ROOT_SERVICE.srv.template
```

(3) Editing usrconf.cfg

(a) File path

```
installation-folder#\misc\CC\server\usrconf\ejb\jp1dh\usrconf.cfg
```

#: In Linux, change *installation-folder* to `/opt/jp1dh/server`.

(b) Content of the configuration file

Edit only the items described in this subsection. If you edit the other items, the system might fail to start properly.

- Changing the Java heap memory size

  Specify the Java heap memory size as needed. For details about the Java heap memory size, see *3.3.1 The Java heap memory size*.

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

#

For values you can specify, note the following points:

- A value for the memory size is specified in MB.
- For the maximum size, specify a value equal to or more than 1,024 MB.
- Specify the values so that the minimum size is equal to or less than the maximum size. We recommend that you specify the same value for the minimum size and the maximum size.

Example:

When you specify 1,024 MB for the minimum size and maximum size of Java heap memory

```
#------ JP1/DH - Server ---------
add.jvm.arg=-Xms1024m
add.jvm.arg=-Xmx1024m
```

(c) Procedure for recovering usrconf.cfg

If the system ceases to operate normally due to reasons such as inadvertently changing the value of an item other than the above, overwrite the file described in *(a) File path* with the file shown below, and then edit the overwritten file again. Then, perform the procedures described in *5.3.2 Changing the application configuration* and the subsequent subsections again.

```
installation-folder\template\usrconf.cfg.template
```

(4) Editing usrconf.properties

Specify the maximum number of connections between the reverse proxy server and Web clients as needed.

If the machine where the JP1/DH Web application server is installed and the reverse proxy server are different machines, you need to allow the reverse proxy server to access the machine where the JP1/DH Web application server is installed. For overwrite installation, you need to perform this procedure only when the IP address of the reverse proxy server is changed.

If there are many TCP connections (for example, 64 connections), change the maximum number of Web client connections to 1,024. For details about how to specify the number of TCP connections, see the *Job Management Partner 1/Data Highway - Server System Administrator Guide*.

(a) File path

```
installation-folder#\misc\CC\server\usrconf\ejb\jp1dh\usrconf.properties
```

#: In Linux, change *installation-folder* to `/opt/jp1dh/server`.

(b) Content of the configuration file

Edit only the items described in this subsection. If you edit the other items, the system might fail to start properly.

- IP address of the reverse proxy server
- Maximum number of Web client connections
- Number of concurrent request handling processes

```
#------ JP1/DH - Server ---------
...
mwebserver.connector.inprocess_http.permitted.hosts=IP-address-of-the-
reverse-proxy-server#1
webserver.connector.inprocess_http.max_connections=maximum-number-of-web-
client-connections#2
webserver.connector.inprocess_http.max_execute_threads=number-of-
concurrent-request-handling-processes#2
```

#1

Specify an IPv4 address.

#2

A maximum of 1,024 can be specified for the maximum number of Web client connections and the number of concurrent request handling processes.

Note that the number of concurrent request handling processes must be equal to or less than the value specified for the maximum number of Web client connections.

Example:

When you specify `192.168.0.1` for the IP address of the reverse proxy server and 1,024 for the maximum number of Web client connections and the number of concurrent request handling processes

```
#------ JP1/DH - Server ---------
...
webserver.connector.inprocess_http.permitted.hosts=192.168.0.1
webserver.connector.inprocess_http.max_connections=1024
webserver.connector.inprocess_http.max_execute_threads=1024
```

(c) Procedure for recovering usrconf.properties

If the system ceases to operate normally due to reasons such as inadvertently changing the value of an item other than the above, overwrite the file described in *(a) File path* with the file shown below, and then edit the overwritten file again. Then, perform the procedures described in *5.3.2 Changing the application configuration* and the subsequent subsections again.

```
installation-folder#\template\usrconf.properties.template
```

#: In Linux, change *installation-folder* to `/opt/jp1dh/server`.

5.3.2 Changing the application configuration

After editing the configuration file, change the application configuration by applying the edited settings to the system. Perform the procedure below to change the application configuration.

Important note

For all installations other than a new installation, make sure that the database service is running. If it is not running, start it, and then perform the procedure below.

(1) Starting the JP1/DH Web application server

Execute either of the following batches:

- In Windows

```
installation-folder\setup_util\start_webcon.bat
```

- In Linux

```
/opt/jp1dh/server/setup_util/start_webcon.sh
```

When you execute the batch, the command prompt starts. Follow the given instructions. If the message below appears, the JP1/DH Web application server is running properly. Do not close the command prompt. Go to the next step.

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

(2) Preparing to change the application configuration

Execute either of the following batches:

- In Windows

```
installation-folder\setup_util\prepare_deploy.bat
```

- In Linux

```
/opt/jp1dh/server/setup_util/prepare_deploy.sh
```

When you execute the batch, the command prompt starts. Follow the given instructions. When you have finished preparing to change the application configuration, go to the next step.

(3) Restarting the JP1/DH Web application server

When you are ready to change the application configuration, restart the JP1/DH Web application server. To stop the JP1/DH Web application server temporarily, execute either of the following batches:

- In Windows

```
installation-folder\setup_util\stop_webcon.bat
```

- In Linux

```
/opt/jp1dh/server/setup_util/stop_webcon.sh
```

When you execute the batch, the command prompt starts. Follow the given instructions. If the JP1/DH Web application server normally stops, in the command prompt started in step (1), a message appears notifying you that the JP1/DH Web application server has stopped normally.

Then, execute the operation in step (1) again to start the JP1/DH Web application server.

(4) Changing the application configuration

Execute either of the following batches:

- In Windows

```
installation-folder\setup_util\deploy_app.bat
```

- In Linux

```
/opt/jp1dh/server/setup_util/deploy_app.sh
```

When you execute the batch, the command prompt starts. Follow the given instructions. When you have completed the changing of the application configuration successfully, go to the next step.

(5) Stopping the JP1/DH Web application server

Execute either of the following batches:

- In Windows

```
installation-folder\setup_util\stop_webcon.bat
```

- In Linux

```
/opt/jp1dh/server/setup_util/stop_webcon.sh
```

When you execute the batch, the command prompt starts. Follow the given instructions. If the JP1/DH Web application server normally stops, in the command prompt started in step (3), a message appears notifying you that the JP1/DH Web application server has normally stopped.

5.3.3 Specifying the settings for the electronic certificate authentication function

Execute either of the commands below to create a root certificate used for the electronic certificate authentication function. After a new installation, specify the settings for the electronic certificate authentication function according to the procedure described below. For an overwrite installation, you do not have to perform the procedure below.

- In Windows

```
installation-folder\setup_util\init_system_signer.bat
```

- In Linux

```
/opt/jp1dh/server/setup_util/init_system_signer.sh
```

Enter values for the required items interactively.

```
CN(Common Name) : FQDN-of-the-server-host
OU(Organization Unit Name) : organization-unit-name
O(Organization Name) : organization-name
L(Locality Name) : city-or-area-name
S(State or Province Name) : state-or-province-name
C(Country Name) : 2-character-country-code (JP for Japan)
```

Example:

```
CN(Common Name) : jp1dhserver.foo1.foo2.co.jp
OU(Organization Unit Name) : Software Development
O(Organization Name) : Hitachi, Ltd.
L(Locality Name) : Shinagawa-ku
S(State or Province Name) : Tokyo
C(Country Name) : JP
```

5.3.4 Registering a root certificate

To encrypt communication with the linked mail server through SSL (SMTPS/STARTTLS) in mail server linkage while using the delivery notification function, you need to register a root certificate of the Certificate Authority. The root certificate of the Certificate Authority that signed the certificate for SMTPS/STARTTLS communication that is registered in the linked mail server must be registered in the Java keystore contained in the JP1/DH Web application server. In the same way, to encrypt communication with the directory server through SSL (LDAPS) in authentication using the directory server when a user logs in to this product, you need to register a root certificate of the Certification Authority. The root certificate of the Certification Authority that signed the certificate for LDAPS communication that is registered in the linked directory server must be registered in the Java keystore contained in the JP1/DH Web application server.

Use either of the commands below to register the root certificate. For the certificate alias, you can specify any root certificate name.

- In Windows

```
installation-folder\uCPSB\jdk\jre\bin\keytool -import -alias certificate-
alias
  -file path-to-the-root-certificate-file
  -keystore installation-folder\uCPSB\jdk\jre\lib\security\cacerts
  -storepass changeit
```

- In Linux

```
/opt/jp1dh/server/uCPSB/jdk/jre/bin/keytool -import -alias certificate-
alias
  -file path-to-the-root-certificate-file
  -keystore /opt/jp1dh/server/uCPSB/jdk/jre/lib/security/cacerts
  -storepass changeit
```

5.3.5 Editing the hosts file

In Windows, define the server IP address[#] and host name (FQDN) in the `C:\WINDOWS\system32\drivers\etc\hosts` file.

In Linux, define the server IP address[#] and host name (FQDN) in the `/etc/hosts` file.

For an overwrite installation, you need to perform this procedure only when the server IP address is changed.

[#] For the IP address to be defined, note the following points:

- Instead of the loopback address (`127.0.0.1`), specify a server-specific IP address.
- Specify an IPv4 address.

5.3.6 Starting the JP1/DH Web application server from the service

In Windows, start `JP1_DH_WEB CONTAINER`. In Linux, start `JP1_DH_WEBCON`. For details about how to start the service, see *6. Starting and Stopping*.

If you want to start the JP1/DH Web application server automatically when the system restarts, specify **Automatic** for **Startup Type**.

5.3.7 Resetting the password for the system administrator

If you specify the SALT string, reset the password for the system administrator.

- In Windows

```
installation-folder\setup_util\init_admin_password.bat
```

- In Linux

```
/opt/jp1dh/server/setup_util/init_admin_password.sh
```

5.4 Using the JP1/DH Web server

This section describes how to create and set a server certificate for SSL communication when using the JP1/DH Web server.

If you want to create a self-signed server certificate when testing or evaluating the JP1/DH Web server, instead of *5.4.1 Creating a secret key file for SSL communication*, *5.4.2 Creating a password file*, and *5.4.3 Creating a certificate file for SSL communication*, see *8.3.5 selfsignedkeygen.bat (creating a secret key)*, *8.3.6 selfsignedcertreq.bat (creating a CSR (certificate signing request))*, and *8.3.7 selfsigned.bat (creating a self-signed server certificate)* to create a self-signed server certificate. Then perform the procedures in *5.4.4 Editing the settings for the JP1/DH Web server* and the subsequent subsections.

Before performing the procedures described in this section, log in to the JP1/DH - Server machine as a built-in Administrator user (in Windows) or the root user (in Linux).

5.4.1 Creating a secret key file for SSL communication

By using the `keygen` command, create a secret key file for SSL communication. The following subsections describe the `keygen` command format and operands.

(1) File path

```
installation-folder#\uCPSB\httpsd\sbin\keygen
```

#: In Linux, change *installation-folder* to `/opt/jp1dh/server`.

(2) Format

```
keygen -rand file-name [-des|-des3] -out key-file [-bits {1024|2048|4096}]
```

(3) Operands

- `-rand` *file-name*

  Specify any file used for generating a random number. For a file used for generating a random number, specify a sufficiently large and appropriate file. You can specify only one file name. You cannot specify multiple file names.

  An example of file specification is as follows:

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

  #: In Linux, change *installation-folder* to `/opt/jp1dh/server`.

- `[-des|-des3]`

  To encrypt a secret key, specify the encryption type. If this operand is specified, a password is requested when a secret key is created. A password must be no more than 64 characters long.

  A password is also requested when a certificate signing request (CSR) is created (described later) and when the reverse proxy server starts.

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

When `-des3` is specified, Triple DES is selected. This encryption type has nothing to do with the encryption type for SSL communication between the reverse proxy server and a Web browser.

Note that if you specify this operand, you need to create a password file. For details about how to create a password file, see *5.4.2 Creating a password file*.

- `-out` *key-file*

  Specify the file to which a secret key is output.

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

  Specify the bit length of a secret key to be created. If you omit this operand, the underlined value is used.

5.4.2 Creating a password file

If you have created a secret key file with password protection in *5.4.1 Creating a secret key file for SSL communication*, create a password file. If you have not created a secret key file with password protection, you do not have to perform this procedure.

(1) File path

```
installation-folder#\uCPSB\httpsd\sbin\sslpasswd
```

#: In Linux, change *installation-folder* to `/opt/jp1dh/server`.

(2) Format

```
Sslpasswd secret-key-file-name password-file-name
```

(3) Operands

- *secret-key-file-name*

  Specify the name of the secret key file created in *5.4.1 Creating a secret key file for SSL communication*.

- *password-file-name*

  Specify a file name used for password file output.

5.4.3 Creating a certificate file for SSL communication

By using the `certutil reqgen` command, create a CSR (certificate signing request).

(1) File path

```
installation-folder#\uCPSB\httpsd\sbin\certutil
```

#: In Linux, change *installation-folder* to `/opt/jp1dh/server`.

(2) Format

```
certutil reqgen [-sign {MD5|SHA1|SHA224|SHA256|SHA384|SHA512}] -key key-
file -out CSR-file
```

(3) Operands

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

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

  `MD5`: Use md5WithRSAEncryption.

  `SHA1`: Use sha1WithRSAEncryption.

  `SHA224`: Use sha224WithRSAEncryption.

  `SHA256`: Use sha256WithRSAEncryption.

  `SHA384`: Use sha384WithRSAEncryption.

  `SHA512`: Use sha512WithRSAEncryption.

- `-key` *key-file*

  Specify the name of the secret key file created in *5.4.1 Creating a secret key file for SSL communication*.

- `-out` *CSR-file*

  Specify the file to which the created CSR is output.

  Enter values for the required items interactively.

  ```
  C(Country Name) : 2-character-country-code (JP for Japan)
  S(State or Province Name) : state-or-province-name
  L(Locality Name) : city-or-area-name
  O(Organization Name) : organization-name
  OU(Organization Unit Name) : organization-unit-name
  CN(Common Name) : FQDN-of-the-server-host
  EA(Email Address) : email-address
  ```

Example:

```
C(Country Name) : JP
S(State or Province Name) : Tokyo
L(Locality Name) : Shinagawa-ku
O(Organization Name) : Hitachi, Ltd.
OU(Organization Unit Name) : Software Development
CN(Common Name) : jp1dhserver.foo1.foo2.co.jp
EA(Email Address) : jp1dh-system@foo1.foo2.co.jp
```

(4) Obtaining a certificate file

Send a CSR to the CA (Certificate Authority) to obtain a signed certificate file in PEM (Privacy Enhanced Mail) format.

5.4.4 Editing the settings for the JP1/DH Web server

The following subsections describe the details of the JP1/DH Web server settings.

(1) Editing httpsd.conf

(a) File path

```
installation-folder#\misc\httpsd\conf\httpsd.conf
```

#: In Linux, change *installation-folder* to `/opt/jp1dh/server`.

(b) Settings

Edit only the items described in this subsection. If you edit the other items, the system might fail to start properly.

Setting item		Setting value
`SSLCertificateFile`		Specify the path to the signed certificate file created in *5.4.3 Creating a certificate file for SSL communication*.
`SSLCertificateKeyFile`		Specify the path to the secret key file created in *5.4.1 Creating a secret key file for SSL communication*.
`SSLCertificateKeyPassword`		If you have created a secret key file with password protection in *5.4.1 Creating a secret file for SSL communication*, uncomment this setting item, and then specify the path to the password file created in *5.4.2 Creating a password file*.
`ProxyPass`		Specify as follows: `ProxyPass / http://`*FQDN-of-the-server-host*`/` Specify the server host name in lower-case characters. If you specify it in other characters, the JP1/DH Web server does not operate properly.
`ProxyPassReverse`		Specify as follows: `ProxyPassReverse / http://`*FQDN-of-the-server-host*`/` Specify the server host name in lower-case characters. If you specify it in other characters, the JP1/DH Web server does not operate properly.
In Windows	`ThreadsPerChild`	This is the maximum number of request handling processes for the reverse proxy server. To allow the system to always communicate at the maximum number of TCP connections, change the value to 1,024. The maximum value that you can specify is 1,024. For details about how to specify the number of TCP connections, see the *Job Management Partner 1/Data Highway - Server System Administrator Guide*.
In Linux	`MaxClients`	

Note: To comment out the setting item, insert a hash mark (`#`) at the beginning of the relevant line. To uncomment the setting item, delete the `#` at the beginning of the relevant line.

(c) Applying the settings

To apply the settings edited in *(1) Editing httpsd.conf* to the JP1/DH Web server, execute either of the following batches:

- In Windows

```
installation-folder\setup_util\deploy_websvr.bat
```

- In Linux

```
installation-folder/setup_util/deploy_websvr.sh
```

(d) Recovering httpsd.conf

If the system ceases to operate normally due to reasons such as inadvertently changing the value of an item other than the above, overwrite the file described in *(a) File path* with the file shown below, and then edit the overwritten file again. Then, perform the procedures described in *(b) Settings* and the subsequent subsections again.

```
installation-folder#\template\httpsd.conf.template
```

#: In Linux, change *installation-folder* to `/opt/jp1dh/server`.

5.4.5 Starting the JP1/DH Web server

Start `JP1_DH_WEB SVR`. For details about how to start the service, see *6. Starting and Stopping*.

If you want to start the JP1/DH Web server automatically when the system restarts, specify **Automatic** for **Startup Type**.

Important note

If you access JP1/DH - Server while `JP1_DH_WEB SVR` is running but the application server service `JP1_DH_WEB CONTAINER` is not running, `Bad Gateway` is displayed on screen. The start-up time of `JP1_DH_WEB CONTAINER` is longer than that of `JP1_DH_WEB SVR`. When you start these services, access JP1/DH - Server after a sufficient period of time has elapsed.

5.5 Operation check

Perform an operation check according to the following procedures.

5.5.1 Checking the operation of JP1/DH - Server

Check the operation of JP1/DH - Server. In Linux, perform only the procedure described in *(2) Checking access to JP1/DH - Server*.

(1) Checking the operation of JP1/DH Web application server

Confirm that the JP1/DH Web application server is installed and set up correctly.

Start the web browser on the JP1/DH - Server machine, and then access `http://localhost/`[#1]. If the JP1/DH Web application server is set up correctly, the JP1/DH - Server login window appears. If the login window does not appear, it is possible that the environment configuration of the JP1/DH Web application server is not correct. In this case, review the settings described in *5.3 Setting up the JP1/DH Web application server environment*.

After you have confirmed that the login window appears, confirm that you can log in as the following system administrator:

User ID: `admin`[#2]

Password: `password`[#2]

#1

Note that this operation check is performed through HTTP, not based on SSL communication.

#2

The above password is the initial setting.

When you access the JP1/DH Web application server for the first time after its installation, the display of the window takes time.

(2) Checking access to JP1/DH - Server

Confirm that you can access JP1/DH - Server correctly based on the network configuration determined in *2.1 Network configurations*.[# 1] Start the web browser on the client machine accessing JP1/DH - Server, and then access `https://`*FQDN-of-the-server-host*`/`[#2] to confirm that the JP1/DH - Server login window appears.

If the login window does not appear, it is possible that the settings of the reverse proxy server machine or other machines that exist between the client machine and the JP1/DH - Server machine in the network configuration are incorrect. Review the settings of such machines. When using the JP1/DH Web server, also review the settings specified in *5.4 Using the JP1/DH Web server*.

#1

Before this confirmation, you must perform the operation check described in *(1) Checking the operation of JP1/DH Web application server*.

#2

Note that this operation check is performed through HTTPS based on SSL communication.

5.5.2 Changing the password for the system administrator

You must change the password for the system administrator (user ID: `admin`) by following the procedure described in the *Job Management Partner 1/Data Highway - Server System Administrator Guide*.

6 Starting and Stopping

This chapter describes how to start and stop JP1/DH - Server.

6.1 Starting and stopping in Windows

This section describes how to start and stop JP1/DH - Server in Windows.

6.1.1 Procedure for starting (in Windows)

This subsection describes how to start JP1/DH - Server in Windows.

(1) Starting services

To start JP1/DH - Server services in Windows:

1. Log in as a built-in Administrator user.

2. Click **Control Panel**, and then **Services**.

3. Right-click the registered name of the desired JP1/DH - Server service, and then select **Start**. The following table describes the registered names of the JP1/DH - Server services.

Name	Description
`JP1_DH_DATABASE_SVR`	Database service
`JP1_DH_WEB CONTAINER`	JP1/DH Web application server service
`JP1_DH_WEB SVR`	JP1/DH Web server service#

#: Operate this service only when using the JP1/DH Web server.

To start all the services, operate them in the following order:

1. Database service (`JP1_DH_DATABASE_SVR`)

2. JP1/DH Web application server service (`JP1_DH_WEB CONTAINER`)

3. JP1/DH Web server service (`JP1_DH_WEB SVR`) (when using the JP1/DH Web server)

(2) Specifying the automatic startup settings of JP1/DH - Server services (in Windows)

The following table describes the automatic startup settings of JP1/DH - Server services when the system starts after a new installation.

Table 6–1: Automatic startup settings of JP1/DH - Server services (in Windows)

Name	Setting value
`JP1_DH_DATABASE_SVR`	Automatic
`JP1_DH_WEB CONTAINER`	Automatic
`JP1_DH_WEB SVR`	Manual

To change the automatic startup settings:

1. Log in as a built-in Administrator user.

2. Click **Control Panel**, and then **Services**.

3. Right-click the registered name of the desired JP1/DH - Server service, and then select **Properties**.

4. In **Startup Type**, select **Automatic** or **Manual**.
   If **Automatic** is selected, the service automatically starts when the system restarts.
   If **Manual** is selected, the service does not automatically start when the system restarts.

6.1.2 Procedure for stopping (in Windows)

(1) Stopping services

This subsection describes how to stop JP1/DH - Server in Windows.

1. Log in as a built-in Administrator user.

2. Click **Control Panel**, and then **Services**.

3. Right-click the registered name of the desired JP1/DH - Server service, and then select **Stop**.
   The following table describes the registered names of the JP1/DH - Server services.

Name	Description
`JP1_DH_DATABASE_SVR`	Database service
`JP1_DH_WEB CONTAINER`	JP1/DH Web application server service
`JP1_DH_WEB SVR`	JP1/DH Web server service#

#: Operate this service only when using the JP1/DH Web server.

To stop all the services, operate them in the following order:

1. JP1/DH Web server service (`JP1_DH_WEB SVR`) (when using the JP1/DH Web server)
2. JP1/DH Web application server service (`JP1_DH_WEB CONTAINER`)
3. Database service (`JP1_DH_DATABASE_SVR`)

6.2 Starting and stopping in Linux

This section describes how to start and stop JP1/DH - Server in Linux.

6.2.1 Procedure for starting (in Linux)

This subsection describes how to start JP1/DH - Server in Linux.

(1) Starting services

To start JP1/DH - Server services in Linux:

1. Log in as the root user.
2. Start the database service (JP1_DH_DATABASE_SVR).

```
/sbin/service JP1_DH_DATABASE_SVR start
```

3. Start the JP1/DH Web application server service (JP1_DH_WEBCON).

```
/sbin/service JP1_DH_WEBCON start
```

4. To use the JP1/DH Web server, start the JP1/DH Web server service (JP1_DH_WEBSVR).

```
/sbin/service JP1_DH_WEBSVR start
```

To start all the services, operate them in the following order:

1. Database service (JP1_DH_DATABASE_SVR)
2. JP1/DH Web application server service (JP1_DH_WEBCON)
3. JP1/DH Web server service (JP1_DH_WEBSVR) (when using the JP1/DH Web server)

(2) Specifying the automatic startup settings of JP1/DH - Server services (in Linux)

The following table describes the automatic startup settings of JP1/DH - Server services when the system starts after a new installation.

Table 6–2: Automatic startup settings of JP1/DH - Server services (in Linux)

Name	Setting value
JP1_DH_DATABASE_SVR	Enabled (on)
JP1_DH_WEBCON	Enabled (on)
JP1_DH_WEBSVR	Disabled (off)

To change the automatic startup settings:

1. Log in as the root user.

2. Change the setting of the database service (`JP1_DH_DATABASE_SVR`).

   To enable the automatic startup setting:

   ```
   /sbin/chkconfig JP1_DH_DATABASE_SVR on
   ```

   To disable the automatic startup setting:

   ```
   /sbin/chkconfig JP1_DH_DATABASE_SVR off
   ```

3. Change the setting of the JP1/DH Web application server service (`JP1_DH_WEBCON`).

   To enable the automatic startup setting:

   ```
   /sbin/chkconfig JP1_DH_WEBCON on
   ```

   To disable the automatic startup setting:

   ```
   /sbin/chkconfig JP1_DH_WEBCON off
   ```

4. Change the setting of the JP1/DH Web server service (`JP1_DH_WEBSVR`).

   To enable the automatic startup setting:

   ```
   /sbin/chkconfig JP1_DH_WEBSVR on
   ```

   To disable the automatic startup setting:

   ```
   /sbin/chkconfig JP1_DH_WEBSVR off
   ```

5. To check the changed automatic startup setting, execute the following command:

   ```
   /sbin/chkconfig --list service-name
   ```

6. If output results 0 to 6 are all `off`, the automatic startup setting is disabled. If output results 0, 1, and 6 are `off` and output results 2 to 5 are `on`, the automatic startup setting is enabled.

   - Execution example (when the automatic startup setting is disabled)

     ```
     /sbin/chkconfig --list JP1_DH_WEBSVR
     JP1_DH_WEBSVR   0:off   1:off   2:on   3:on   4:on   5:on   6:off
     ```

   - Execution example (when the automatic startup setting is enabled)

     ```
     /sbin/chkconfig --list JP1_DH_WEBSVR
     JP1_DH_WEBSVR   0:off   1:off   2:off   3:off   4:off   5:off   6:off
     ```

6.2.2 Procedure for stopping (in Linux)

This subsection describes how to stop JP1/DH - Server in Linux.

(1) Stopping services

To stop JP1/DH - Server services in Linux:

1. Log in as the root user.

2. When using the JP1/DH Web server, stop the JP1/DH Web server service (`JP1_DH_WEBSVR`).

   ```
   /sbin/service JP1_DH_WEBSVR stop
   ```

3. Stop the JP1/DH Web application server service (`JP1_DH_WEBCON`).

   ```
   /sbin/service JP1_DH_WEBCON stop
   ```

4. Stop the database service (`JP1_DH_DATABASE_SVR`).

   ```
   /sbin/service JP1_DH_DATABASE_SVR stop
   ```

To stop all the services, operate them in the following order:

1. JP1/DH Web server service (`JP1_DH_WEBSVR`) (when using the JP1/DH Web server)
2. JP1/DH Web application server service (`JP1_DH_WEBCON`)
3. Database service (`JP1_DH_DATABASE_SVR`)

7 Administrator Commands

This chapter describes the commands used by the JP1/DH - Server administrator.

7.1 Installing the JP1/DH - Server administrator commands (in Windows)

This section describes how to install the JP1/DH - Server administrator commands in Windows.

7.1.1 Checking the environment prerequisites

The JP1/DH - Server administrator commands run on a machine in which JP1/DH - Server is installed. Check if JP1/DH - Server is installed in the machine.

7.1.2 Installing the JP1/DH - Server administrator commands (in Windows)

The following shows how to install the JP1/DH - Server administrator commands:

(1) Setting the system environment variable

Set the environment variable. The procedure below describes how to set the environment variable on Windows Server 2008 R2.

If you are using Windows Server 2012 or Windows Server 2012 R2, the operation starting from the **Start** menu in Windows Server 2008 R2 can be started by right-clicking the Start window and opening **All Apps**.

1. From the Windows **Start** menu, right-click **Computer** and select **Properties**.

2. Select **Advanced system settings**.
   The System Properties window opens.

3. Select the **Advanced** tab, and then **Environment Variables...**

4. Either select **User variables for** *windows-user-name* and then **New...**or **System variables** and then **New...**

5. Enter `DW_CMD_JRE_HOME` for **Variable name** and the JRE installation folder's path for **Variable value** and then click **OK**.
   The following shows the path to the JRE installation folder when the program is installed in the default installation location:

   ```
   C:\Program Files\Hitachi\jp1dh\server\uCPSB\jdk\jre
   ```

6. Click **OK**.

(2) Installing the administrator commands

1. Decompress the administrator command archive file in the installation folder.
   The following shows the path to the JRE installation destination where the administrator commands are installed when the program is installed in the default installation location:

   ```
   C:\Program Files\Hitachi\jp1dh\server\AdminClient\DWAdminClient.zip
   ```

2. A `DWAdminClient` folder is created.

3. Move this `DWAdminClient` folder into any folder.

> **Important note**
>
> A user using the JP1/DH - Server administrator commands must have write permission to the following folders:
>
> - Installation folder for JP1/DH - Server administrator commands (`DWAdminClient` folder)
> - Temporary folder for the command executing user

(3) Setting the command property file (property.xml)

Open the command property file (`property.xml`), enter the following information, and then save:

- URL of the server to connect to
- User ID
- Password
- Authentication method
- Proxy server authentication information

For details about the command property file, see *7.3.6 Command property file (property.xml)*.

7.1.3 Uninstalling the JP1/DH - Server administrator commands (in Windows)

You must have the Windows administrator rights to uninstall the JP1/DH - Server administrator commands.

(1) Exiting the command programs

Before starting uninstallation, exit all the JP1/DH - Server command programs.

(2) Deleting the folder

Delete the folder into which the JP1/DH - Server administrator commands were copied (`DWAdminClient` folder). Note that the registry was not used for the installation of the command program.

(3) Deleting the environment variable

Delete the environment variable. The procedure below describes how to delete the environment variable on Windows Server 2008 R2.

If you are using Windows Server 2012 or Windows Server 2012 R2, the operation starting from the **Start** menu in Windows Server 2008 R2 can be started by right-clicking the Start window and opening **All Apps**.

1. From the Windows **Start** menu, right-click **Computer** and select **Properties**.
2. Select **Advanced system settings**.
   The System Properties window opens.

3. Select the **Advanced** tab, and then **Environment Variables...**

4. Select `DW_CMD_JRE_HOME` in **User variables for** *windows-user-name* or in **System variables**.

5. Click **Delete** for the corresponding section and then click **OK**.

6. Click **OK**.

7.1.4 Restrictions

For the JP1/DH - Server administrator commands, you cannot use surrogate pair characters. Do not use surrogate pair characters for the Windows user name, installation folder name, or argument such as the subject, message, and file path.

7.2 Installing the JP1/DH - Server administrator commands (in Linux)

This section describes how to install the JP1/DH - Server administrator commands in Linux.

7.2.1 Checking the environment prerequisites

The JP1/DH - Server administrator commands run on a machine in which JP1/DH - Server is installed. Check if JP1/DH - Server is installed in the machine.

7.2.2 Installing the JP1/DH - Server administrator commands (in Linux)

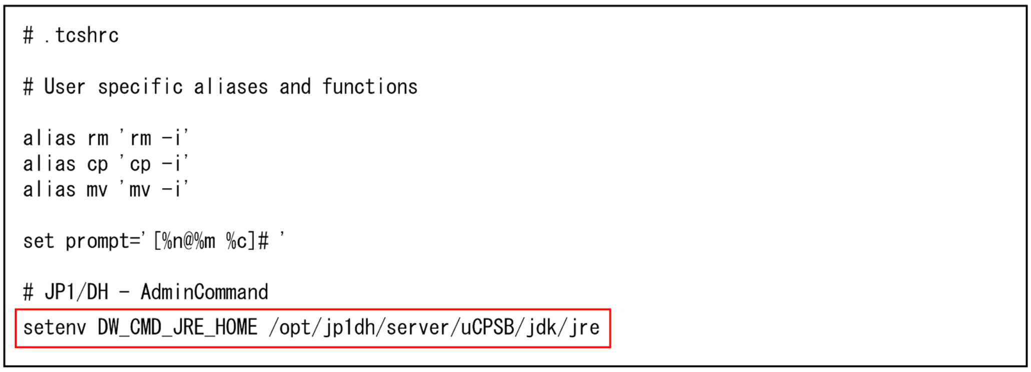
The following shows how to install the JP1/DH - Server administrator commands:

(1) Setting the system environment variable

1. Add the environment variable `DW_CMD_JRE_HOME` to the configuration file for the login shell you are using.
2. Set the path to the installation folder for JRE to the environment variable `DW_CMD_JRE_HOME`.

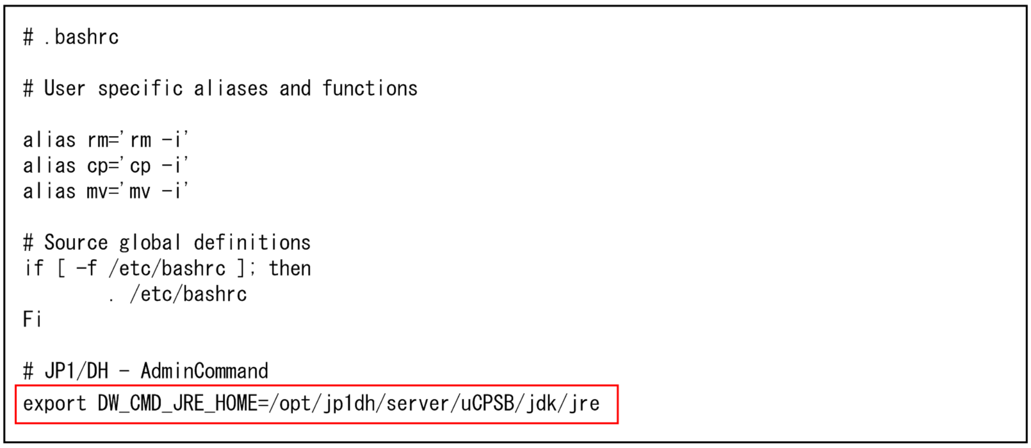
```
opt/jp1dh/server/uCPSB/jdk/jre
```

3. A setting example is shown below.
   When using tcsh as the login shell, add the setting to the .../`.tcshrc` file.



```
# .tcshrc

# User specific aliases and functions

alias rm 'rm -i'
alias cp 'cp -i'
alias mv 'mv -i'

set prompt='[%n@%m %c]# '

# JP1/DH - AdminCommand
setenv DW_CMD_JRE_HOME /opt/jp1dh/server/uCPSB/jdk/jre
```

When using bash as the login shell, add the setting to the .../`.bashrc` file.



```
# .bashrc

# User specific aliases and functions

alias rm='rm -i'
alias cp='cp -i'
alias mv='mv -i'

# Source global definitions
if [ -f /etc/bashrc ]; then
        . /etc/bashrc
Fi

# JP1/DH - AdminCommand
export DW_CMD_JRE_HOME=/opt/jp1dh/server/uCPSB/jdk/jre
```

(2) Installing the administrator commands

1. Create a directory for installing the JP1/DH - Server administrator commands. An example of a directory is as follows:

   ```
   mkdir .../DWAdminClient
   ```

2. Move to the created directory.

   ```
   cd .../DWAdminClient
   ```

3. Decompress the JP1/DH - Server administrator command archive file in the installation directory created in step 1.

   ```
   tar zxvf /opt/jp1dh/server/AdminClient/DWAdminClient.tar.gz
   ```

(3) Setting the command property file (property.xml)

Open the command property file (`property.xml`), enter the following information, and then save.

- URL of the server to connect to
- User ID
- Password
- Authentication method
- Proxy server authentication information

For details about the command property file, see *7.3.6 Command property file (property.xml)*.

7.2.3 Uninstalling the JP1/DH - Server administrator commands (in Linux)

(1) Exiting the command programs

Before starting uninstallation, exit all the JP1/DH - Server command programs.

(2) Deleting the folder

Delete the folder into which the JP1/DH - Server administrator commands were copied (`DWAdminClient` folder).

```
rm -rf .../DWAdminClient
```

(3) Deleting the environment variable

Delete the line added in *7.2.2(1) Setting the system environment variable*.

7.3 Common specifications

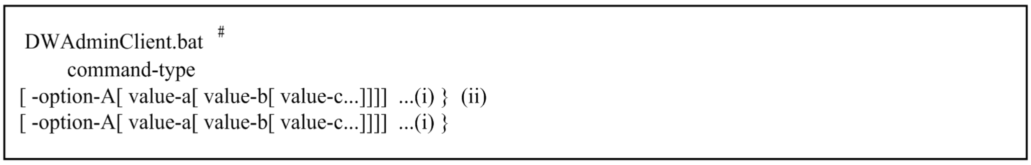
This section describes the common specifications for the JP1/DH - Server administrator commands. The following items are described:

- Command format and grammar rules
- Common options
- Exit code
- Log output
- File path
- Command property file (`property.xml`)
- Simultaneous execution on the same computer

7.3.1 Command format and grammar rules

This subsection describes the command format, grammar rules, and how to specify values.

The following figure shows the command format:



```
 DWAdminClient.bat  #
        command-type
[ -option-A[ value-a[ value-b[ value-c...]]]]  ...(i) }  (ii)
[ -option-A[ value-a[ value-b[ value-c...]]]]  ...(i) }
```

(i) is called an option and (ii) is called an argument.

#: For Linux, replace bat with sh.

Specify a command according to the following grammar rules:

- If you specify multiple options, you can specify them in any order.
- You cannot specify the same option more than once.
- If you specify a non-existing option, an error occurs.
- If you include a blank character in a value, surround a value with double quotation marks (`""`).
- If you specify a command line special character such as an ampersand (`&`) and a circumflex accent (`^`), write the caret (`^`) before it.
- You cannot use a double quotation mark (`"`) for a value.
- Specify a command so that its length does not exceed 8,191 characters.
- If you specify multiple values for a single option, separate each value with a space.
- If you specify multiple values for an option and when that option can have one value only, the value specified first is used. For an option that can have multiple values, all the values are used.

7.3.2 Common options

The common options for the commands are shown as follows:

Table 7–1: List of common options

No.	Option	Description
1	`-property`	Specifies the path to the command property file (`property.xml`), where information such as user IDs and passwords for transmission and reception is written. For details about the command property file, see *7.3.6 Command property file (property.xml)*.
2	`-concurrenttimeout`	Timeout time (in seconds) to wait for another command to end if it is already executed. You can specify a value in the range from 0 to 86,400 (24 hours). When you specify `0`, the specified command ends without waiting for another command to end. If you omit specifying a value, `0` is used.

7.3.3 Exit codes

The exit codes to be output by command execution are shown below.

In Windows, you can refer to the exit code value by using the environment variable `ERRORLEVEL` immediately after executing a JP1/DH - Server administrator command. For example, if you execute the `echo %ERRORLEVEL%` by using the command prompt immediately after you executed a command, you can output the exit code to the standard output. In Linux, execute `echo $?` by using the console to output the exit code to the standard output.

Table 7–2: List of exit codes

No.	Exit code	Description
1	`0`	Indicates that the command execution process ended normally.
2	`2`	Ended by suspension
3	`3`	Ended by delivery denial
4	`4`	Indicates that the command execution process ended with a warning. Indicates that an abnormal event occurred in some part of the process but the rest of the process continued.
5	`8`	Indicates that the command execution process was terminated because another JP1/DH - Server administrator command had already been activated.
6	`12`	Ended by cancellation
7	`16`	Indicates that the command execution process is terminated abnormally. The unfinished part of the process after the error occurrence is not executed. The error details are output to a log file.
8	`32`	Indicates that Java VM is terminated abnormally.
9	`64`	Indicates that the Java execution process failed because there was an error in the path specified for the environment variable.

7.3.4 Log output

This subsection describes application logs to be output by commands.

(1) Log level

The following table lists and describes the log levels for application logs.

Table 7–3: List of log levels for application log

No.	Log level	ID	Severity	Description	Monitoring
1	`Error`	`E`	Requires the representative user or the system administrator to correspond.	Indicates that the command processing cannot be continued due to a problem with the execution environment such as the network environment or due to a problem with a parameter entered in the command. This problem requires correspondence by the representative user. In some cases, correspondence by the system administrator might be required. Logs output for the cases of exit codes `16` and `8`.	Y
2	`Warn`	`W`	Temporary problem	Indicates that an abnormal event occurred during command processing. The command processing continues. Log output for the case of exit code `4`.	C
3	`Info`	`I`	Normal event	Log that notifies normal processing on going.	N

Legend:

Y: Log level for which monitoring is required

C: Level for which necessity of monitoring is considered depending on the character of the system

N: Log level for which monitoring is not required

(2) Log file

The following table describes the specifications for log files.

Table 7–4: Log file specifications

No.	Item	Format or value
1	File format	Text
2	Character code	UTF-8
3	Line feed	CR+LF

Log files are output to the path shown below. Storage period is 30 days.

```
installation-folder\log\dwc-yyyyMMddhhmmss-GUID.log
```

Legend:

- *installation-folder*: Folder to which the JP1/DH - Server commands are installed
- *yyyyMMddhhmmss*: Command execution date (*yyyy*: four-digit year, *MM*: two-digit month, *dd*: two-digit day, *hh*: two-digit hour (in 24-hour format), *mm*: minute, and *ss*: second)
- *GUID*: Random string in GUID format

Important note

Each time a command is executed, a new log is output to the predetermined output destination. If there is no log output destination, a log output destination folder is automatically created so that logs are output to it. Note that log files whose storage period has expired are automatically deleted when a command is started.

(3) Output format

The application log output format is as follows:

```
date delimiter-character time-of-day version-number log-level message-ID
message-text
```

An application log output example is as follows:

```
2011/04/19T20:38:21.500 10-50    INFO  DWCO1001_I Command start.
2011/04/19T20:38:28.250 10-50    INFO  DWCO1602_I User information
acquisition finished.
2011/04/19T20:38:28.250 10-50    INFO  DWCO1002_I Command finished.
```

The table below describes application log output details. For details about specific messages, see *10. Messages*.

Table 7–5: Log file output details

No.	Item	No. of digits	Output data
1	*date*	10	*yyyy*/*MM*/*dd* • *yyyy*: Four-digit year • *MM*: Two-digit month • *dd*: Two-digit day
2	*delimiter-character*	1	`T`
3	*time-of-day*	12	*HH*:*mm*:*ss*.*SSS* • *HH*: Two-digit hour (in 24-hour format) • *mm*: Minute • *ss*: Second • *SSS*: Millisecond Note that the output time of day is the time of day at the client side.
4	*version-number*	8	`10-50` Aligned left and filled with a blank character on the right.
5	*log-level*	5	Log level. Aligned left. For details, see *7.3.4(1) Log level*.
6	*message-ID*	10	ID for the message. *XXXXYYYY_Z* • *XXXX*: Product code • *YYYY*: Message number • *Z*: Log level ID (`I`: Info. `W`: Warn, `E`: Error)
7	*message-text*	Variable length	Message content. If a stack trace in Java is included, line feed may be included.

7.3.5 File path

Specify an absolute path for a file path used in JP1/DH - Server administrator commands.

You can use both UNC format and local path format for specifying a path. However, when sending a file on the network or when receiving a file into the network folder, the transmission speed between the client and the network folder might cause a bottleneck, slowing down the total transmission speed. In such cases, to take advantage of high-speed file transmission, characteristic of JP1/DH - Server, we recommend using a local file path for a path to be specified in a command.

7.3.6 Command property file (property.xml)

The command property file is an XML file where information such as the user IDs and passwords for the users is written. Specify this file as an argument when executing a command. A password string is written as-is. Make an appropriate security setting for it such as setting access privileges. The following table describes the specifications for the command property file.

Table 7–6: Command property file specifications

No.	Item	Format or value
1	File format	XML format
2	Character code	UTF-8
3	Line feed	CR+LF

Use the following format to write code in the command property file:

```
<?xml version="1.0" encoding="utf-8" ?>
<property>
    <serverUrl>value</serverUrl>
    <userId>value</userId>
    <password>value</password>
    <authenticationMethod>value</authenticationMethod>
    <certificatePath>value</certficatePath>
    <certificatePassword>value</certificatePassword>
    <useProxy>value</useProxy>
    <proxyHost>value</proxyHost>
    <proxyPort>value</proxyPort>
    <proxyId>value</proxyId>
    <proxyPassword>value</proxyPassword>
</property >
```

The following table describes the setting items.

Table 7–7: Command property file setting items

No.	Setting item	Element name	Description	Initial value
1	URL of the server to connect to	`serverUrl`	Specify the URL of the server to connect to. Example: `https://jp1dh.hitachi.co.jp/`	None
2	User ID	`userId`	Specify the login user ID for the server to connect to.	None

No.	Setting item	Element name	Description	Initial value
2	User ID	`userId`	For standard password authentication, you must always specify this item. Example: `user@company`	None
3	User password	`password`	Specify the login user password for the server to connect to, by using a character string[#]. For standard password authentication, you must always specify this item. Note that you cannot specify a string starting with `text:HEX` for the password. Example: `password`	None
4	Authentication method	`authenticationMethod`	Specify the authentication method. If you omit specifying a value, operation is performed based on standard password authentication. • `PASSWORD`: Standard password authentication • `CERTIFICATION`: Certificate authentication	`PASSWORD`
5	Path of the certificate file	`certificatePath`	Specify the path to the certificate file in absolute path format. You can omit specifying a value when using the standard password authentication as the authentication method. To use the electronic certificate authentication, you must always specify this item.	None
6	Certificate file password	`certificatePassword`	Specify the password for the certificate file. You can omit specifying a value when using the standard password authentication as the authentication method. To use the electronic certificate authentication, you must always specify this item.	None
7	Proxy use flag	`useProxy`	Specify whether to use a proxy server. • To use a proxy server: `true` • Not to use a proxy server: `false` This setting is not case-sensitive. If you specify a value other than specifiable values, an error occurs. Example: `true`	`false`
8	Proxy server host name	`proxyHost`	Specify the host name or IP address of the proxy server. Example 1: `Proxyserver` Example 2: `192.168.0.1`	None
9	Proxy server port number	`proxyPort`	Specify the port number of the proxy server. You can specify a value in the range from `0` to `65535`. Example: `3128`	None
10	Proxy authentication ID	`proxyId`	Specify the authentication ID of the proxy server. Example: `user`	None
11	Proxy authentication password	`proxyPassword`	Specify the authentication password for the proxy server. Example: `password`	None

#

You can use alphanumeric characters and symbols in a given length as defined by authentication rules.

You can use the following symbols: !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~.

Enter values according to the XML conventions. Specifically, be careful when using special symbols in XML. To use any of the following characters, either replace them with their corresponding entity reference (escape characters) or use a CDATA section.

Table 7–8: XML escape characters

No.	Character	Entity-referenced notations
1	<	&lt;
2	>	&gt;
3	&	&amp;
4	"	&quot;
5	'	&apos;

Note that a control character such as line feed might be displayed as an entity that follows the XML standards. For XML attributes, the order of appearance is irregular in accordance with the XML standards.

Data indicating date and time is expressed as *YYYY*-*MM*-*DD*T*hh*:*mm*:*ssTDZ* in W3C-DTF format in accordance with ISO8601:2004. The time zone (TDZ) is based on the offset time according to the OS time zone. For Japan, it is +09:00.

A setting example is shown below.

```
<?xml version="1.0" encoding="utf-8" ?>
<property>
    <serverUrl>https://jp1dh. hitachi.co.jp/</serverUrl>
    <userId>user@company</userId>
    <password>password</password>
    <authenticationMethod>PASSWORD</authenticationMethod>
            ...
            ...
    <useProxy>true</useProxy>
    <proxyHost>proxyserver</proxyHost>
    <proxyPort>8080</proxyPort>
    <proxyId>proxyid</proxyId>
    <proxyPassword>proxypassword</proxyPassword>
</property >
```

7.3.7 Simultaneous execution on the same computer

You cannot execute more than one JP1/DH - Server administrator command simultaneously on the same computer. If you execute more than one such command simultaneously on the same computer, the commands other than the current command stay in the standby state for the period specified in the timeout option.

However, even on the same computer, if you use a separate Windows account to execute an administrator command, you can simultaneously execute an equal number of commands as the number of such accounts.

In addition, when multiple commands were in the standby state, the order of execution might be different from the order of activation. For example, if command B and command C go into the standby state while command A is being executed, the command to be executed after command A ends is either command B or command C.

7.4 List of administrator commands

The following table lists and describes administrator commands.

Table 7–9: List of administrator commands

No.	Function	Command	Description	Related subsection
1	Suspension and cancellation of the active file transfer	`DWAdminClient.bat`# `SUSPEND|CANCEL`	Suspends or cancels the active file transfer.	*7.4.1*
2	Changing the delivery acceptance status for the file transfer function	`DWAdminClient.bat`# `STOPDELIVERY|STARTDELIVERY`	Changes the delivery acceptance status of the JP1/DH - Server file transfer function.	*7.4.2*
3	Acquisition of server status	`DWAdminClient.bat`# `GETSERVERSTATUS`	Acquires the number of connections by the clients currently executing file transfer.	*7.4.3*
4	Dynamic management of the server settings	`DWAdminClient.bat`# `GETCONFIG|SETCONFIG`	Refers to or changes the settings of the server without restarting JP1/DH - Server.	*7.4.4*
5	Audit log check	`DWAdminClient.bat`# `GETAUDITLOG`	Acquires audit logs.	*7.4.5*
6	Acquisition of delivery information	`DWAdminClient.bat`# `GETDELIVERYINFO`	Acquires a delivery information list containing information such as delivery IDs, files, sender/recipient user names, and dates and times.	*7.4.6*
7	Delivery deletion function	`DWAdminClient.bat`# `DELETEDELIVERY`	Deletes the specified delivery.	*7.4.7*
8	Acquisition of user information	`DWAdminClient.bat`# `EXPORTUSERINFO`	Acquires a list of user information containing such information as user IDs and mail addresses.	*7.4.8*
9	Importing user information	`DWAdminClient.bat`# `IMPORTUSERINFO`	Imports a list of user information containing such information as user IDs and mail addresses.	*7.4.9*

#: For Linux, replace `bat` with `sh`.

7.4.1 Suspension and cancellation of the active file transfer

This command suspends or cancels the file transfer being executed by JP1/Data Highway - AJE. Note that for file transfer using a command of JP1/Data Highway - AJE 10-00, you cannot use this command to suspend and cancel the processes.

(1) Format

```
DWAdminClient.bat SUSPEND|CANCEL
   -property property-file
   [-deliveryid delivery-ID]
```

(2) Arguments

Table 7–10: Arguments of the command for suspending and canceling the active file transfer

No.	Option	Description
1	`SUSPEND`	Suspends the file transfer being executed by JP1/Data Highway - AJE. The client executing the suspended file transfer ends the process in response to the corresponding exit code (ended by suspension). To resume the suspended file transfer process, use the command for resuming the suspended file transfer on the client side.
2	`CANCEL`	Cancels the file transfer being executed by JP1/Data Highway - AJE. The client executing the canceled file transfer ends the process in response to the corresponding exit code (ended by cancellation). The canceled file transfer cannot be resumed. If you cancel file transfer during their transmission, the delivery data in JP1/DH - Server is deleted. If you cancel file transfer during reception, the delivery data is not deleted. Note that you cannot cancel suspended file transfer.
3	`-deliveryid`	Specifies the delivery ID of the target file whose transfer is suspended or canceled. You can acquire the delivery ID by using the command for acquiring delivery information. If you omit specifying this option, all the files whose transfer is being executed by JP1/Data Highway - AJE are to be suspended or canceled.
4	`-property`	For details, see *7.3.2 Common options*.

(3) Description

The details of the command for suspending and canceling the active file transfer are described as follows:

(a) Time required for command execution

After this command is executed, it might take time for the instruction to reach the client.

(b) Storage expiration date

Delivery data of suspended file transfer is also deleted automatically when its storage period defined in the delivery policy expires. For that reason, we recommend setting a sufficiently long storage period.

(c) When the server stops

When the server stops, the ongoing file transfer processes are suspended.

(4) Execution example

```
DWAdminClient.bat SUSPEND
 -property "C:\DWCLient\property.xml"
 -deliveryid 00000001
```

7.4.2 Changing the delivery acceptance status for the file transfer function

This command changes the delivery acceptance status of the JP1/DH - Server file transfer function. Even when the server restarts, the delivery acceptance status is retained. By using this command, you can change the delivery acceptance status of every file transfer including the ones to be processed by using the JP1/DH - Server web window.

(1) Format

```
DWAdminClient.bat {STOPDELIVERY|STARTDELIVERY}
-property property-file
```

(2) Arguments

Table 7–11: Arguments of the command for changing the delivery acceptance status for the file transfer function

No.	Option	Description
1	`STOPDELIVERY`	Turns the delivery acceptance status for the JP1/DH - Server file transfer function to delivery denial. When this option is specified, it becomes impossible to start new file transfer or to resume suspended file transfer, and those file transfers are ended by delivery denial. However, if file transfer is in progress, the process is continued even when this option is specified.
2	`STARTDELIVERY`	Turns the delivery acceptance status for the JP1/DH - Server file transfer function to start delivery. When this option is specified, it becomes possible to start new file transfer and to resume suspended file transfer.
3	`-property`	For details, see *7.3.2 Common options*.

(3) Description

To resume the suspended file transfer, besides this command, use the command for resuming the suspended file transfer on the client side.

(4) Execution example

```
DWAdminClient.bat STOPDELIVERY
   -property "C:\DWCLient\property.xml"
```

7.4.3 Acquisition of server status

This command acquires the number of connections by the clients currently executing file transfer.

(1) Format

```
DWAdminClient.bat GETSERVERSTATUS
   -property property-file
   -result storage-destination-server-status-file
```

(2) Arguments

Table 7–12: Arguments of the command for acquiring server status

No.	Option	Description
1	`-result`	Specifies the path to the storage destination for the server status file. If the file does not exist in the specified location, a new server status file is created. If the file exists, the existing file is overwritten.

No.	Option	Description
2	`-property`	For details, see *7.3.2 Common options*.

(3) Description

(a) Format of the execution result file

The format of the execution result file is as follows:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<data>
    <server-status>
        <running-sockets>3</running-sockets>
    </server-status>
</data>
```

The following table describes the elements.

Table 7–13: Elements in the execution result file

Element/attribute	Number of elements	Description
`data` element	1	Fixed.
`server-status` element	1	Fixed.
`running-sockets` element	1	Indicates the number of connections by the clients currently executing file transfer.

(4) Execution example

```
DWAdminClient.bat GETSERVERSTATUS
   -property "C:\DWCLient\property.xml"
   -result C:\temp\result.xml
```

7.4.4 Dynamic management of the server settings

You can refer to or change the settings for the server without restarting JP1/DH - Server.

You can change the maximum number of TCP connections in the delivery rule settings (standard delivery policy) and the values for the following server parameters in the JP1/DH - Server configuration file (`digikatsuwide.xml`).

- Network bandwidth limit
- Maximum number of client connections (number of concurrent connections)

For details about the standard delivery policy, see the *Job Management Partner 1/Data Highway - Server System Administrator Guide*.

(1) Format

```
DWAdminClient.bat {GETCONFIG|SETCONFIG}
   -property property-file
   -config {server-parameter-file|-result storage-destination-server-
parameter-file}
```

(2) Arguments

Table 7–14: Arguments of the command for dynamic management of the server settings

No.	Option	Description
1	`-config`	When changing server parameters dynamically (`SETCONFIG`), specifies the server parameter file where the values after change are written. Specify this option when selecting `SETCONFIG`. You cannot specify it when selecting `GETCONFIG`.
2	`-result`	When obtaining the current server parameter file (`GETCONFIG`), specifies the path to the server parameter file at the storage destination. Specify this option when selecting `GETCONFIG`. You cannot specify it when selecting `SETCONFIG`.
3	`-property`	For details, see *7.3.2 Common options*.

(3) Description

(a) Format of the server parameter file

The format of the server parameter file is as follows:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<digivery-config>
  <digivery>
    <biz-connect id="bizconnect" >
      <service>
        <throughput-limit>
          <upload>maximum-transmission-bandwidth-for-uploading</upload>
          <download>maximum-transmission-bandwidth-for-downloading</
download>
        </throughput-limit>
        <service-task>
          <initial>maximum-number-of-client-connections-(initial-value)</
initial>
          <maximum>maximum-number-of-client-connections-(maximum-value)</
maximum>
        </service-task>
        <http-connection>
          <maximum>maximum-TCP-connections</maximum>
        </http-connection>
        </service>
    </biz-connect>
  </digivery>
</digivery-config>
```

The following table describes the elements.

Table 7–15: Elements in the server parameter file

Element/attribute	Number of elements	Description
digivery-config element	1	Fixed.
digivery element	1	Fixed.
biz-connect element	1	Fixed.
id attribute	1	Fixed. Specifies bizconnect.
service	1	Fixed.
throughput-limit	1	Fixed.
upload	1	Specifies the maximum transmission bandwidth for uploading in Mbps. You can specify a value in the range from 0 to 1,000. You cannot omit this value. When you specify 0, no limit is applied to the bandwidth.
download	1	Specifies the maximum transmission bandwidth for downloading in Mbps. You can specify a value in the range from 0 to 1,000. You cannot omit this value. When you specify 0, no limit is applied to the bandwidth.
service-task	1	Fixed.
initial	1	Specifies the initial value for the number of concurrent connections between JP1/DH - Server and clients. You can specify a value in the range from 1 to 64. You cannot omit this value.
maximum	1	Specifies the maximum value for the number of concurrent connections between JP1/DH - Server and clients. You can specify a value in the range from 1 to 64. You cannot omit this value.
http-connection	1	Fixed.
maximum	1	Specifies the maximum number of TCP connections during multiplex communication per connection between JP1/DH - Server and a client. You can specify a value in the range from 1 to 64. You cannot omit this value.

(b) Settings

- The changes made here are enabled from the first connection to be established after the settings have been changed. The communication at the point of command execution is not affected by these changes.
- The changes made by this command are enabled only for the settings of active JP1/DH - Server. When JP1/DH - Server is restarted, the changes made to the settings become disabled.

(4) Execution example

```
DWAdminClient.bat GETCONFIG
   -result C:\temp\result.xml
   -property "C:\DWCLient\property.xml"
```

7.4.5 Checking audit logs

You can acquire audit logs by domain. The audit logs you can acquire here are the same as the audit logs the representative user acquires on the web window.

(1) Format

```
DWAdminClient.bat GETAUDITLOG
   -property property-file
   -domain domain-name
   -fromdate YYYY/MM/DD
   -todate YYYY/MM/DD
   -result result-file-storage-destination
```

(2) Arguments

Table 7–16: Arguments of the command for checking audit log

No.	Option	Description
1	`-domain`	Specifies the target domain name.
2	`-fromdate`	Specifies the start date for audit logs to be acquired.
3	`-todate`	Specifies the end date for audit logs to be acquired.
4	`-result`	Specifies the path to the storage destination for the audit log file. If the file does not exist, a new audit log file is created. If the file exists, the existing file is overwritten.
5	`-property`	For details, see *7.3.2 Common options*.

(3) Description

For details about the output format for a command execution result audit log, see the *Job Management Partner 1/Data Highway - Server Administrator Guide*.

(4) Execution example

```
DWAdminClient.bat GETAUDITLOG
   -property "C:\DWCLient\property.xml"
   -domain hitachi
   -fromdate 2012/01/01
   -todate 2012/12/31
   -result C:\temp\audit.log
```

7.4.6 Acquiring delivery information

You can acquire a delivery information list containing information such as delivery IDs, files, sender/recipient user names, and dates and times.

(1) Format

```
DWAdminClient.bat GETDELIVERYINFO
   -property property-file
   [-sender sender-user-ID]
   [-receiver recipient-user-ID]
-result execution-result-file
```

(2) Arguments

Table 7–17: Arguments of the command for acquiring delivery information

No.	Option	Description
1	`-sender`	Used to acquire delivery information with a sender user ID specified. If you omit specifying this option, all sender users are set as targets for acquiring the delivery information.
2	`-receiver`	Used to acquire delivery information with a recipient user ID specified. If you omit specifying this option, all recipient users are set as targets for acquiring the delivery information.
3	`-result`	Specifies the path to the output destination of the execution result file.
4	`-property`	For details, see *7.3.2 Common options*.

(3) Description

(a) Specifying options

When the `-sender` option and the `-receiver` option are specified together, the result that is filtered with AND condition for both option is returned.

(b) Delivery with the approval route specified

You cannot check whether the approval route is specified or whether approval has been made, by using the execution result file.

(c) Format of the execution result file

An output example of the execution result file is as follows:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<data>
  <deliveries>
      <delivery id="123"
         send-status="in-progress | suspended | completed"
         send-date="2012-11-20T02:25:09+09:00"
         subject="xxx" message="Sending a document &#10;Taro Hitachi">
        <sender id="user1@domain1" email="user1@domain1.co.jp">
          <files>
                <file id="27" type="file" name="document for xx
meeting.txt" size="1024524"
                path="C\digikatsuwide\data\domain1\user1\123\27\a.dat" />
                <file id="28" type="file" name="xxstudyresult.doc"
size="3134562"
                  path="C\digikatsuwide\data\domain1\user1\123\28\a.dat" />
          </files>
        </sender>
        <receivers>
          <receiver id="user2@domain1" email="user2@domain1.co.jp">
            <files>
                  <file id="27" download-date="2012-11-21T10:15:33+09:00" />
                  <file id="28" download-date="" />
            </files>
          </receiver>
          <receiver id="user3@domain1" email="user3@domain1.co.jp">
            <files>
```

```
                  <file id="27" download-date="" />
                  <file id="28" download-date="" />
            </files>
          </receiver>
        </receivers>
      </delivery>
  </deliveries>
</data>
```

The following table describes the meanings of the elements of the execution result file.

Table 7–18: Meanings of the execution result file

Element/attribute	Number of elements	Description
`data` element	1	Always output.
`deliveries` element	1	Always output.
`delivery` element	0 or more	Output when delivery information exists. If there is no delivery information, no `delivery` element is included.
`id` attribute	1	The delivery ID is output.
`send-status` attribute	1	The following delivery (transfer) status is displayed: • For transfer being processed, not approved, or denied: `in-progress` • For transfer being suspended: `suspended` • For transfer already sent or approved: `completed`
`send-date` attribute	1	The date the delivery (transfer) was completed is displayed. If the delivery is not completed, empty double quotation marks (`""`) are displayed.
`subject` attribute	1	The subject of the delivery is output.
`message` attribute	1	The message included in the delivery is output.
`sender` element	1	The sender information is output.
`id` attribute	1	The user ID of the sender is output.
`email` attribute	1	The email address of the sender is output.
`files` element	1	A list of delivery files or folders is output.
`file` element	0 or more	Output when delivery file or folder information exists. If no delivery file or folder exists, this element is not output.
`id` attribute	1	The ID of the delivery file or folder is output.
`type` attribute	1	One of the following delivery type is output: • File: `"file"` • Folder: `"folder"`
`name` attribute	1	The name of the delivery file or folder is output.
`size` attribute	1	The size of the delivery file or folder is output in bytes. For a folder, the total number of bytes before archiving the contents of the folder is output.
`path` attribute	1	The actual file path of the delivery file or folder data stored on JP1/DH - Server is output in absolute file path format.

Element/attribute	Number of elements	Description
path attribute	1	If the type attribute is "folder", the delivery data is an archive file created by archiving the contents of the folder.
receivers element	1	A list of recipient information is output.
receiver element	1 or more	Recipient information is output. If there are multiple recipients, multiple receiver elements are output.
id attribute	1	The user ID of the recipient is output.
email attribute	1	The email address of the recipient is output.
files element	1	A list of delivery files or folders is output.
file element	0 or more	Output when delivery file or folder information exists. If no delivery file or folder exists, this element is not output.
download-date attribute	1	The date on which the delivery file or folder download completed is output. If the downloading is not completed, empty double quotation marks ("") are displayed.

Important note

- When the displayed send-status attribute is in-progress and the delivery is in progress, for the file element, only files being sent and files already sent are displayed. A file whose transfer has not started is not displayed. When you acquire information about files already sent, make sure that their send-status attribute are completed.
- When the sender user is deleted, the files sent by that user are also deleted. In this case, empty double quotation marks ("") are displayed for the id attribute of the sender element and for the path attribute of the file element.
- The send-status attribute is displayed as suspended only when a file transmission process is stopped by a suspension instruction from JP1/DH - Server generated through execution of the command for suspending the active file transfer. If a transmission process fails due to such a cause as a communication error, in-progress is displayed for the send-status attribute.

(4) Execution example

```
DWAdminClient.bat GETDELIVERYINFO
   -property "C:\DWCLient\property.xml"
   -sender hitachi01
   -result C:\temp\result.xml
```

7.4.7 Delivery deletion function

You can delete the specified delivery.

(1) Format

```
DWAdminClient.bat DELETEDELIVERY
   -property property-file
   -deliveryid deliver-ID
```

(2) Arguments

Table 7–19: Arguments of the command for delivery deletion

No.	Option	Description
1	`-deliveryid`	Specifies the delivery ID of the delivery to be deleted. You can acquire the delivery ID by using the delivery command for acquiring delivery information.
2	`-property`	For details, see *7.3.2 Common options*.

(3) Description

(a) Abnormal termination of the command

- If the `send-status` attribute is not `completed` (not sent or approved) in the acquired result of the delivery information acquisition command, the command is terminated abnormally because the system thinks the delivery is in progress.
- If the specified delivery ID cannot be deleted, the command is terminated abnormally.

(4) Execution example

```
DWAdminClient.bat DELETEDELIVERY
   -property "C:\DWCLient\property.xml"
   -deliveryid 00000001
```

7.4.8 Acquisition of user information

You can acquire (export) user information. The user information you can acquire here is the same as the information the representative user acquires on the web window by selecting a domain for exporting user settings.

(1) Format

```
DWAdminClient.bat EXPORTUSERINFO
   -property property-file
   -result execution-result-storage-destination
   -domain target-domain-name
```

(2) Arguments

Table 7–20: Arguments of the command for acquiring user information

No.	Option	Description
1	`-result`	Specifies the path to the storage destination of execution result file.

No.	Option	Description
1	`-result`	If the file does not exist, a new file is created. If the file exists, the existing file is overwritten.
2	`-domain`	Specifies the name of the target domain for acquiring user information list.
3	`-property`	For details, see *7.3.2 Common options*.

(3) Description

(a) Information to be output to the execution result file

For details about the format for user information to be output, see *3.5.2(2)(a) Format of a CSV file for import* in the *Job Management Partner 1/Data Highway - Server Administrator Guide*.

(b) User password information

For user password information in the execution result file, a string obfuscated in the format below is output. To specify an obfuscated user password in the command property file (`property.xml`), use a copy of the output string. An example of a string to be output is as follows:

Obfuscated string example

```
text:HEX:5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8
```

(4) Execution example

```
DWAdminClient.bat EXPORTUSERINFO
   -property "C:\DWCLient\property.xml"
   -result C:\temp\export_users.csv
   -domain HITACHI
```

7.4.9 Importing user information

You can import user information by using a CSV file.

(1) Format

```
DWAdminClient.bat IMPORTUSERINFO
   -property property-file
   -file import-file
   -result execution-result-storage-destination
```

(2) Arguments

Table 7–21: Arguments of the command for importing user information

No.	Option	Description
1	`-file`	Specifies the path to the CSV file to be imported. When a space is contained in a file path, surround that file path with double quotation marks (`""`).
2	`-result`	Specifies the path to the storage destination of execution result file.

No.	Option	Description
2	`-result`	If the file does not exist, a new file is created. If the file exists, the existing file is overwritten.
3	`-property`	For details, see *7.3.2 Common options*.

(3) Description

(a) Available user information for import

The following table describes available user information for import.

No.	User information	Create	View	Update	Delete
1	User	Y	Y	Y	Y
2	Domain	Y	Y	N	N
3	Group	Y	Y	Y	Y#
4	User's group	Y	Y	N	N
5	Representative user authority	Y	Y	N	N

#

The specified group cannot be deleted if a user or group exists directly below it. However, it can be deleted if those users all belong to another group.

Legend:

Y: Can be imported

N: Cannot be imported

(b) Example of creating an import CSV (import_users.csv) file

An example of creating an import CSV file is shown below. For details about notes on creating this file, see *3.5.2(1) Notes on creating the CSV file used for batch management* in the *Job Management Partner 1/Data Highway - Server Administrator Guide*.

```
[domains]
FUNCTION,NAME_EN,NAME_JA,PARENT_NAME_EN,FOR_GUEST,EXPIRE_DATE,QUOTA,
USE_USER_OPTION,USER_REGISTERABLE,MAX_DISK_SPACE,TRAFFIC_LIMIT,
LIMIT_USER_NUMBER,CUT_OFF_DAY,INPUT_ANY_ADDRESS,USE_UNREGISTERED_ADDRESS
CREATE,Hitachi xxxxxx,All Users,FALSE,,,,,51200,51200,100,31,TRUE,TRUE

[users]
FUNCTION,USER_ID,EMAIL,PASSWORD,NAME,NAME_EN,NAME_KANA,LANG,
MEMO,EXPIRE_DATE,QUOTA,USE_USER_OPTION,USE_GUEST_USERS,INPUT_ANY_ADDRESS
READ,u1@user,u1@xxx.com,passowrd,,,User1,,,en,,,2012/01/01,1024,,,
READ,u2@user,u2@xxx.com,passowrd,,,User2,,,en,,,2012/01/01,1024,,,

[groups]
FUNCTION,DOMAIN,NAME_EN,NAME_JA,PARENT_NAME_EN,FOR_GUEST,EXPIRE_DATE,QUOTA,U
SE_USER_OPTION,USER_REGISTERABLE,INPUT_ANY_ADDRESS
READ,domain1,Group1,group-1,Hitachi xxxxx

[binders]
USER_ID,GROUP_NAME_EN,FLAG_DELETE
u1@user,g1,FALSE
```

```
u2@user,g1,FALSE

[managers]
FUNCTION,USER_ID,GROUP_NAME_EN
```

Important note

If you want to specify only item names, and not the contents for the `[groups]` definition section, you can omit the item `DOMAIN`.

Description of each definition section is given in the following pages. The following table describes the items you can specify for the `[domains]` definition section.

Table 7–22: Setting items for the [domains] definition section

No.	Item	Meaning	Description	Omit
1	`FUNCTION`	Action type	Specify the type of action to be performed for the `[domains]` definition contents that is specified. • `CREATE`: Create the data • `READ`: Do nothing If you specify `READ`, the relevant record (line) is ignored. If no type is specified for `FUNCTION`, `CREATE` is used.	Allowed
2	`NAME_EN`	Group name (English)	Specify the group name (English). Note that the value specified here is used as a domain name with the spaces between words taken away. It is the same as the value after @ of the user ID.	Not allowed
	Rules for specifying a group name (English): • You can enter maximum of 200 single-byte alphanumeric characters and symbols. • You cannot use the following symbols: `/\?*:|"<>@^`. • You cannot use a value consisting only of spaces or periods (`.`).			
3	`NAME_JA`	Group name (Japanese/Chinese)	Specify the group name (Japanese/Chinese).	Not allowed
	Rules for specifying a group name (Japanese/Chinese): • You can enter maximum of 200 characters. • You cannot use the following symbols: `/\?*:|"<>@^`. • You cannot use a value consisting only of spaces or periods (`.`).			
4	`PARENT_NAME_EN`	Parent group name (English)	Specify the group name of the parent group (English). Specify `All Users` for this item.	Not allowed
5	`FOR_GUEST`	Group type	Specify the group type. This item is not case-sensitive. • `TRUE`: Guest group • `FALSE`: User group (used if the value is omitted) This item is not case-sensitive. You cannot specify a domain group as a guest group.	Allowed
6	`EXPIRE_DATE`	Account expiration date	Specify the account expiration date in *YYYY*/*MM*/*DD* or *YYYY*-*MM*-*DD* format. You can specify a date in the range from the current date (JST) to `2031/12/31` (Dec. 31, 2031).	Allowed

No.	Item	Meaning	Description	Omit
6	EXPIRE_DATE	Account expiration date	If you specify the string UNLIMITED, no limit is set for time. If you omit specifying a value, no limit is set for time. A single-byte space, line feed, and tab character in a string are ignored. Note that none of the above characters can be inserted between *YYYY*, *MM*, and *DD* items.	Allowed
7	QUOTA	Storage capacity	Specify the storage capacity in MB. If you omit specifying a value, the amount of 1 GB is applied. You can specify a value in the range from 0 to 8796093022207.	Allowed
8	USE_USER_OPTION	Permission for the use of the Options function	Specify whether to permit the use of the Options function. This item is not case-sensitive. • TRUE: Permitted (used if the value is omitted) • FALSE: Not permitted This item is not case-sensitive.	Allowed
9	USER_REGISTERABLE	Permission for the use of the Guest Users function	Specify whether to permit the use of the Guest Users function. This item is not case-sensitive. • TRUE: Permitted • FALSE: Not permitted (used if the value is omitted) This item is not case-sensitive. If you specify TRUE for FOR_GUEST, specify FALSE for this item. If you specify TRUE, an error occurs.	Allowed
10	MAX_DISK_SPACE	Disk capacity	Specify the total disk capacity in MB. You can specify a value in the range from 0 to 8796093022207.	Not allowed
11	TRAFFIC_LIMIT	Download limit	Specify the download limit in MB per month. You can specify a value in the range from 0 to 8796093022207.	Not allowed
12	LIMIT_USER_NUMBER	Maximum number of users	Specify the maximum number of users. You can specify a value in the range from 1 to 1,000,000.	Not allowed
13	CUT_OFF_DAY	Reset date for download limit measurement	Specify the reset date for download limit measurement. You can specify a value in the range from 1 to 31.	Not allowed
14	INPUT_ANY_ADDRESS	Address input permission	Specify whether to permit inputting address by selecting either of the values below. This item is not case-sensitive. • TRUE: Permitted • FALSE: Not permitted (used if the value is omitted)	Allowed
15	USE_UNREGISTERED_ADDRESS	Address input permission	Specify whether to permit inputting address by selecting either of the values below. This item is not case-sensitive. • TRUE: Permitted • FALSE: Not permitted (used if the value is omitted)	Allowed

The following table describes the items you can specify for the [users] definition section.

Table 7–23: Setting items of the [users] definition section

<table>
<tr><th>No.</th><th>Item</th><th>Meaning</th><th>Description</th><th>Omit</th></tr>
<tr><td>1</td><td>FUNCTION</td><td>Action type</td><td>Specify the type of action to be performed for the [users] definition contents that is specified.
• CREATE: Create the data (used if the value is omitted)
• READ: Do nothing
• UPDATE: Update the data
• DELETE: Delete the data
If you specify READ, the relevant record (line) is ignored.
If you specify DELETE, the items after EMAIL are ignored. In addition, an error occurs if a non-existing value is specified for USER_ID, or for users specified for an approval route, if there is only one user specified for that approval route.</td><td>Allowed</td></tr>
<tr><td rowspan="2">2</td><td>USER_ID</td><td>User ID</td><td>Specify the user ID.</td><td rowspan="2">Not allowed</td></tr>
<tr><td colspan="3">Rules for specifying a user ID:
• You cannot specify the same user ID for multiple records (lines).
• Write a user name in the following format: <i>any-string</i> + @ + <i>domain-name</i>.
• The domain name is the same as that of the representative user.
• An error occurs if input string for the part after @ does not exist or if the domain does not match the domain of the representative user.
• The user ID must be unique in a domain.
• In Windows, a maximum of 100 single-byte alphanumeric characters and symbols can be entered, and in Linux, a maximum of 256 single-byte alphanumeric characters and symbols can be entered, both including an ID assigned to a domain.
• You cannot specify the same user ID as the existing user ID.
• You cannot use a space character or the following symbols: /\?*:|"<>#@^[]$.
• You cannot use a value consisting only of periods (.).</td></tr>
<tr><td rowspan="2">3</td><td>EMAIL</td><td>Email address</td><td>Specify the email address.
If you specify CREATE for FUNCTION, you cannot omit specifying this item.
If you specify UPDATE for FUNCTION, and omit specifying this item, the email address is not changed.</td><td rowspan="2">Not allowed at the time of creation</td></tr>
<tr><td colspan="3">Rules for specifying an email address:
• You cannot specify the same email address as the existing email address.
• You can enter maximum of 256 single-byte alphanumeric characters and symbols.
• You cannot use a space character or the following symbols: /\?*:|"<>^.</td></tr>
<tr><td rowspan="2">4</td><td>PASSWORD</td><td>Password</td><td>Specify the password with a string.
If you specify CREATE for FUNCTION, you cannot omit specifying this item. If you specify UPDATE for FUNCTION, and omit specifying this item, the password is not changed.
To specify a password by using digest authentication, enter a 40-character digest string after text:HEX. The digest string portion is not case-sensitive.
For a digest string, you can use what is output in the password field of the exported file.
Note that you cannot specify a string starting with text:HEX for an unencrypted password string.</td><td rowspan="2">Not allowed at the time of creation</td></tr>
<tr><td colspan="3">Rules for specifying a password:</td></tr>
</table>

<table>
<tr><th>No.</th><th>Item</th><th>Meaning</th><th>Description</th><th>Omit</th></tr>
<tr><td>4</td><td colspan="3">• You can use alphanumeric characters and symbols in a given length as defined by authentication rules. You can use the following symbols: `!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~`.<br>• Digest authentication is a method that JP1/DH - Server uses to store a password in the database. When this method is used, the actual password string cannot be restored from the value output for digest authentication.<br>Example of a password used for digest authentication: `text:HEX:5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8`</td><td>Not allowed at the time of creation</td></tr>
<tr><td rowspan="2">5</td><td>NAME</td><td>Name
(Japanese/Chinese)</td><td>Specify the name (Japanese/Chinese).
If you specify UPDATE for FUNCTION, and omit specifying this item, the name is not changed.</td><td rowspan="2">Allowed</td></tr>
<tr><td colspan="3">Rules for specifying a name (Japanese/Chinese):
• You can enter maximum of 256 characters.
• You cannot use the following symbols: /\?*:|"<>#@^[]$.
• You cannot use a value consisting only of spaces or periods (.).</td></tr>
<tr><td rowspan="2">6</td><td>NAME_EN</td><td>Name (English)</td><td>Specify the name (English).
If you specify UPDATE for FUNCTION, and omit specifying this item, the name (English) is not changed.</td><td rowspan="2">Allowed</td></tr>
<tr><td colspan="3">Rules for specifying a name (English):
• In Windows, a maximum of 100 single-byte alphanumeric characters and symbols can be entered, and in Linux, a maximum of 256 single-byte alphanumeric characters and symbols can be entered.
• You cannot use the following symbols: /\?*:|"<>#@^[]$.
• You cannot use a value consisting only of spaces or periods (.).</td></tr>
<tr><td rowspan="2">7</td><td>NAME_KANA</td><td>Name (<i>kana</i>)</td><td>Specify the name (<i>kana</i>).
If you specify UPDATE for FUNCTION, and omit specifying this item, the name (<i>kana</i>) is not changed.</td><td rowspan="2">Allowed</td></tr>
<tr><td colspan="3">Rules for specifying a name (<i>kana</i>):
• You can enter maximum of 256 characters.
• You cannot use the following symbols: /\?*:|"<>#@^[]$.
• You cannot use a value consisting only of spaces or periods (.).</td></tr>
<tr><td>8</td><td>LANG</td><td>User language</td><td>Specify the user language.
• ja: Japanese (used if the value is omitted)
• en: English
• zh: Chinese
If you specify UPDATE for FUNCTION, and omit specifying this item, the user language is not changed.</td><td>Allowed</td></tr>
<tr><td>9</td><td>MEMO</td><td>Memo</td><td>Specify the memo.
If you omit specifying a value, registration is made without any information for this item. You can enter maximum of 4,096 characters.
If you specify UPDATE for FUNCTION, and omit specifying this item, the contents of the memo are not changed.</td><td>Allowed</td></tr>
<tr><td>10</td><td>EXPIRE_DATE</td><td>Account expiration date</td><td>Specify the account expiration date in <i>YYYY</i>/<i>MM</i>/<i>DD</i> or <i>YYYY</i>-<i>MM</i>-<i>DD</i> format. You can specify a date in the range from the current date to 2031/12/31 (Dec. 31, 2031).
If you omit specifying a value, depending on the type of the first group the user belongs to (specified in [binders] definition section), one of the following applies:</td><td>Allowed</td></tr>
</table>

No.	Item	Meaning	Description	Omit
10	EXPIRE_DATE	Account expiration date	• The user belongs to a user group: Inherits the property of the group. • The user belongs to a guest group: The account is valid within the day the import process is executed. If you specify UPDATE for FUNCTION, and omit specifying this item, the account expiration date is not changed. If you specify the string UNLIMITED, no limit is set for time. However, if the user belongs to the guest group (specified in the [binders] definition section), the same rule applies as when the value is omitted. A single-byte space, line feed, and tab character in a string are ignored. Note that none of the above characters can be inserted between *YYYY*, *MM*, and *DD* items.	Allowe d
11	QUOTA	Storage capacity	Specify the storage capacity in MB. You can specify a value in the range from 0 to 8796093022207. If you specify UPDATE for FUNCTION, and omit specifying this item, the storage capacity is not changed. If you omit specifying a value, the property of the first group the user belongs to (specified in [binders] definition section) is inherited.	Allowe d
12	USE_USER_OPTION	Permission for the use of the Options function	Specify whether to permit the use of the Options function. This item is not case-sensitive. • TRUE: Permitted • FALSE: Not permitted If you specify UPDATE for FUNCTION, and omit specifying this item, the storage capacity is not changed. If you omit specifying a value, the property of the first group the user belongs to (specified in [binders] definition section) is inherited.	Allowe d
13	USE_GUEST_USERS	Permission for the use of the Guest Users function	Specify whether to permit the use of the Guest Users function. This item is not case-sensitive. • TRUE: Permitted • FALSE: Not permitted If you specify UPDATE for FUNCTION, and omit specifying this item, the storage capacity is not changed. If you omit specifying a value, the property of the first group the user belongs to (specified in [binders] definition section) is inherited.	Allowe d
14	INPUT_ANY_ADDRESS	Address input permission	Specify whether to permit inputting address. This item is not case-sensitive. • TRUE: Permitted • FALSE: Not permitted If you specify UPDATE for FUNCTION, and omit specifying this item, the storage capacity is not changed. If you omit specifying a value, the property of the first group the user belongs to (specified in [binders] definition section) is inherited. You can omit the item itself.	Allowe d

The table below describes the items you can specify for the `[groups]` definition section. Note that to register a parent group and a child group together, you must register a parent group first.

Table 7–24: Setting items of the [groups] definition section

No.	Item	Meaning	Description	Omit
1	`FUNCTION`	Action type	Specify the type of action to be performed for the `[groups]` definition contents that is specified. • `CREATE`: Create the data • `READ`: Do nothing • `UPDATE`: Update the data • `DELETE`: Delete the data If you specify `READ`, the relevant record (line) is ignored. If no type is specified for `FUNCTION`, `CREATE` is used. If you specify `DELETE`, the specified group cannot be deleted if a user or group exists directly below it. However, it can be deleted if those users all belong to another group. In case the group deleted in this section is specified in the `[binders]` section, an error occurs during the process for `[binders]` section.	Allowed
2	`DOMAIN`	Domain name	Specify the domain name. Specify the domain name (the value after @ of the user ID) or the group name of the domain (the value of `NAME_EN` for registration of the items in `[domains]` section). This item is not case-sensitive.	Not allowed
3	`NAME_EN`	Group name (English)	Specify the group name (English).	Not allowed at the time of creation
	Rules for specifying a group name (English): • In Windows, a maximum of 100 single-byte alphanumeric characters and symbols can be entered, and in Linux, a maximum of 256 single-byte alphanumeric characters and symbols can be entered. • You cannot use the following symbols: `/\?*:|"<>@^`. • You cannot use a value consisting only of spaces or periods (`.`). • You cannot specify the name of the same group in the same domain for multiple records (lines). • If you register the value with only the lower case and upper case changed when you update this item, the value is not changed because this item is not case-sensitive.			
4	`NAME_JA`	Group name (Japanese/Chinese)	Specify the group name (Japanese/Chinese).	Not allowed at the time of creation
	Rules for specifying a group name (Japanese/Chinese): • You can enter maximum of 200 characters. • You cannot use the following symbols: `/\?*:|"<>@^`. • You cannot use a value consisting only of spaces or periods (`.`).			
5	`PARENT_NAME_EN`	Parent group name (English)	Specify the group name of the parent group (English). You cannot specify `All Users` for the value. The rules for specifying this item are the same as the rules for specifying a value for `NAME_EN`.	Not allowed at the time of creation
6	`FOR_GUEST`	Group type	Specify the group type. This item is not case-sensitive. • `TRUE`: Guest group • `FALSE`: User group (used if the value is omitted)	Allowed

No.	Item	Meaning	Description	Omit
6	FOR_GUEST	Group type	This item is not case-sensitive. You cannot specify a domain group as a guest group. If you specify UPDATE for FUNCTION, and a value different from the registered group type, an error occurs. Also in the above case, if you omit specifying this item, the group type is not changed.	Allowe d
7	EXPIRE_DATE	Account expiration date	Specify the account expiration date in *YYYY*/*MM*/*DD* or *YYYY*-*MM*-*DD* format. You can specify a date in the range from the current date (JST) to 2031/12/31 (Dec. 31, 2031). If you specify the string UNLIMITED, no limit is set for time. If you omit specifying a value, no limit is set for time. A single-byte space, line feed, and tab character in a string are ignored. Note that none of the above characters can be inserted between *YYYY*, *MM*, and *DD* items. If you specify UPDATE for FUNCTION, and omit specifying this item, the account expiration date is not changed.	Allowe d
8	QUOTA	Storage capacity	Specify the storage capacity in MB. If you omit specifying a value, the amount of 1 GB is applied. You can specify a value in the range from 0 to 8796093022207. If you specify UPDATE for FUNCTION, and omit specifying this item, the storage capacity is not changed.	Allowe d
9	USE_USER_OPTION	Permission for the use of the Options function	Specify whether to permit the use of the Options function. This item is not case-sensitive. • TRUE: Permitted (used if the value is omitted) • FALSE: Not permitted This item is not case-sensitive. If you specify UPDATE for FUNCTION, and omit specifying this item, the permission setting for the use of the Options function is not changed.	Allowe d
10	USER_REGISTERABLE	Permission for the use of the Guest Users function	Specify whether to permit the use of the Guest Users function. This item is not case-sensitive. • TRUE: Permitted • FALSE: Not permitted (used if the value is omitted) This item is not case-sensitive. If you specify TRUE for FOR_GUEST, specify FALSE for this item. If you specify TRUE at the time of group creation, an error occurs. When the setting for guest group is updated, regardless of the entered value, FALSE is forcibly applied to this item. If you specify UPDATE for FUNCTION, and omit specifying this item, the permission setting for the use of the Guest Users function is not changed.	Allowe d
11	INPUT_ANY_ADDRESS	Address input permission	Specify whether to permit inputting address by selecting either of the values below. This item is not case-sensitive. • TRUE: Permitted • FALSE: Not permitted (used if the value is omitted)	Allowe d

No.	Item	Meaning	Description	Omit
11	`INPUT_ANY_ADDRESS`	Address input permission	If you specify `UPDATE` for `FUNCTION`, and omit specifying this item, the setting for the address input permission is not changed.	Allowed

The following table describes the items you can specify in the `[binders]` definition section.

Table 7–25: Setting items of the [binders] definition section

No.	Item	Meaning	Description	Omit
1	`USER_ID`	User ID	Specify the user ID of the user whose group you want to change. Example: `user1@company` • In Windows, a maximum of 100 single-byte alphanumeric characters and symbols can be entered, and in Linux, a maximum of 256 single-byte alphanumeric characters and symbols can be entered. • You cannot use a space character or the following symbols: `/\?*:|"<>#@^[]$`. • You cannot use a value consisting only of periods (`.`).	Not allowed
2	`GROUP_NAME_EN`	Group name (English)	Specify the name (English) of the group to include the user into or to exclude the user from. You cannot include a user belonging to the guest group to the user group. You cannot include a user belonging to the user group in the guest group. • You can enter maximum of 200 single-byte alphanumeric characters and symbols. • You cannot use the following symbols: `/\?*:|"<>@^`. • You cannot use a value consisting only of spaces or periods (`.`).	Not allowed
3	`FLAG_DELETE`	Delete flag	Specify whether to include the user in the group or exclude the user from the group. • `TRUE`: Exclude the user from the group • `FALSE`: Include the user in the group If you omit specifying a value, the user is included.	Allowed

The following table describes the items you can specify in the `[managers]` definition section.

Table 7–26: Setting items of the [managers] definition section

No.	Item	Meaning	Description	Omit
1	`FUNCTION`	Action type	Specify the type of operation to be performed for the `[managers]` definition section. • `CREATE`: Appoint the user as a group manager (used if the value is omitted) • `READ`: Do nothing If the batch process is executed by the system administrator, a representative user is created by specifying `CREATE`. If you specify `READ`, the relevant record (line) is ignored.	Allowed

<table>
<tr><th>No.</th><th>Item</th><th>Meaning</th><th>Description</th><th>Omit</th></tr>
<tr><td rowspan="2">2</td><td>USER_ID</td><td>User ID</td><td>Specify the user ID of the user to be set as a representative user or group manager.
The user to be specified as a group manager must belong to the affiliated group. Note that you cannot specify one user as group managers for multiple groups.</td><td rowspan="2">Not allowed</td></tr>
<tr><td colspan="3">Rules for specifying a user ID:
• In Windows, a maximum of 100 single-byte alphanumeric characters and symbols can be entered, and in Linux, a maximum of 256 single-byte alphanumeric characters and symbols can be entered, both including an ID assigned to a domain.
• You cannot use a space character or the following symbols: /\?*:|"<>#@^[]$.
• You cannot use a value consisting only of periods (.).</td></tr>
<tr><td rowspan="2">3</td><td>GROUP_NAME_EN</td><td>Group name (English)</td><td>Specify the name (English) of the target group for managing.</td><td rowspan="2">Not allowed</td></tr>
<tr><td colspan="3">Rules for specifying a group name (English):
• You can enter maximum of 200 single-byte alphanumeric characters and symbols.
• You cannot use the following symbols: /\?*:|"<>@^.
• You cannot use a value consisting only of spaces or periods (.).</td></tr>
</table>

Important note

- If you specify a domain group for GROUP_NAME_EN, the user specified for USER_ID is created as a representative user.
- If the batch process is executed by the system administrator, the target group is identified with the domain name (the part after @ in the specified user ID) and the group name looked up as keywords.

(c) Format of the execution result file

For details, see *3.5.2(2)(a) Format of a CSV file for import* in the *Job Management Partner 1/Data Highway - Server Administrator Guide*.

(4) Execution example

```
DWAdminClient.bat GETSERVERSTATUS
   -property "C:\DWCLient\property.xml"
   -result C:\temp\result.xml
```

7.5 List of messages

The following table describes a list of messages.

Table 7–27: List of messages

Message ID	Message details	Description
DWCO1001_I	Command start.	Notifies that the command process is started.
DWCO1002_I	Command finished.	Notifies that the command process is completed.
DWCO1101_E	An option [{0}] must be specified only once.	Indicates that multiple options with the same name are specified for the argument of the command. Do not specify multiple options with same name. The option specified multiple times is output to *{0}*.
DWCO1102_E	Arguments must be a pair of an option key and its value.	Indicates that only the key for an option or only a value is specified for the argument of the command. Specify a key and value pair.
DWCO1103_E	Option [{0}] is invalid.	Indicates that an invalid option was specified for the argument of the command. See *7.4 List of administrator commands* and specify a valid option. The specified invalid option is output to *{0}*.
DWCO1104_E	Please specify option [{1}].	Indicates that a mandatory option is not specified. Specify the mandatory option. The mandatory option is output to *{1}*.
DWCO1105_E	Please specify option [{1}] within [{0}] characters.	Indicates that the number of characters specified for the option value exceeds the maximum characters that can be specified. Specify the value for the option in the number of characters equal to or less than the allowed number of characters.
DWCO1109_E	The specified files/folders do not exist or cannot be read. (Path:{0})	The certificate file does not exist in the specified file or folder or cannot be read. Check if the certificate file exists in the specified file or folder, you have read permission, or the character code for the file is proper. The path to the specified file or folder is output to *{0}*.
DWCO1110_E	Please specify an integer number between [{1}] to [{2}] for option [{3}]. (Value:{0})	A value other than an integer in the preset range was specified for the option. Specify an integer in the specifiable range for the option. The value specified for the option is output to *{0}*. The smallest integer that can be specified for the option is output to *{1}*, the largest integer that can be specified for the option is output to *{2}*, and the option is output to *{3}*.
DWCO1112_E	The settings of Command Property File is wrong. (Setting:{0}, Value:{1})	There is an error in the command property file (`property.xml`). Confirm the following: • Either `PASSWORD` or `CERTIFICATION` is specified for the authentication method. • When the electronic certificate authentication is used as the authentication method, the path to the certificate file is specified. • When the electronic certificate authentication is used as the authentication method, the password for the certificate file is specified. Correct the data in the item with an error, and then try again. The setting item name is output to *{0}*, and the set value is output to *{1}*.
DWCO1113_E	The selected files/folders do not exist or cannot be written. (Path:{0})	The specified file or folder does not exist or data cannot be written to it. Check if the specified file or folder exists, or if you have write permission. The path to the specified file or folder is output to *{0}*.

Message ID	Message details	Description
DWCO1141_E	Please specify "now" in the [-downloaddate] option.	Specify `now` for the option `-downloaddate`.
DWCO1201_E	User authentication failed.	User authentication for JP1/DH - Server failed. Check the authentication information defined in the command property file.
DWCO1203_E	This user cannot use delivery because the user's password expired.	Unable to send or receive data because the password has expired. Set a new password.
DWCO1206_E	You do not have authority to execute.	The user does not have authority to execute the commands for system administrators.
DWCO1501_I	Log files which expires have been deleted. (File name:{0})	Notifies that the log file has been deleted. The file name is output to *{0}*.
DWCO1502_I	Failed to delete log files which expires. (File name:{0})	Notifies that the deletion of the log file failed. The file name is output to *{0}*.
DWCO1701_I	Got server status.	Notifies that the server status has been acquired successfully.
DWCO1702_I	Got server parameter.	Notifies that the server parameter has been acquired successfully.
DWCO1703_I	Set server parameter.	Notifies that the server parameter has been set successfully.
DWCO1704_E	Failed to read server parameter file. (Details:{0})	Check if the server parameter file exists, or if reading of the file is permitted. The detailed reason is output to *{0}*.
DWCO1705_E	Failed to parse an XML. (Details:{0})	The format of the server parameter file is invalid. Check and revise the format. The detailed reason is output to *{0}*.
DWCO1706_E	Failed to generate an XML. (Details:{0})	Check the detailed reason output to *{0}* and take necessary action.
DWCO1707_E	The XML format is invalid. (Details:{0})	The format of the server parameter file is invalid. Check and revise the format. The detailed reason is output to *{0}*.
DWCO1708_E	A setting is wrong. (Setting:{0}, Value:{1})	There is an error in the setting items in the server parameter file. Check and review the settings. The setting item name is output to *{0}*, and the set item is output to *{1}*.
DWCO1720_I	Got user information.	Notifies that the user information has been acquired successfully.
DWCO1721_E	The specified domain does not exist. (Domain:{0})	The specified domain does not exist. Check if an existing domain is specified. The domain name is output to *{0}*.
DWCO1722_E	Failed to get user information. (Details:{0})	Check if writing to the user information export file is permitted. The detailed reason is output to *{0}*.
DWCO1723_I	Imported user information.	Notifies that the user information has been imported successfully.
DWCO1724_E	Failed to import user information. (Details:{0})	Check the detailed reason output to *{0}* and try again.
DWCO1725_E	Failed to import user information. Please refer to the results file for details of the error. (Results file:{0})	Import of user information failed. Based on the detailed information output to the result file, correct the user information import file and try again. The result file name is output to *{0}*.
DWCO1726_W	Failed to write a results file. (Details:{0})	Check if writing to the result file is permitted. The detailed reason is output to *{0}*.
DWCO1730_I	Got audit log.	Notifies that the audit log has been acquired successfully.

Message ID	Message details	Description
DWCO1731_E	Failed to get audit log. (Details:{0})	Acquisition of the audit log failed. See the detailed reason output to *{0}*, confirm that writing to the audit log file is permitted, and then try again.
DWCO1732_E	The specified date is wrong. (Date:{0})	Check that the date format is *YYYY/MM/DD*, and if the date is correct. The date is output to *{0}*.
DWCO1801_I	Got delivery information.	Notifies that the delivery information has been acquired successfully.
DWCO1802_E	Failed to get delivery information. (Details:{0})	Acquisition of the delivery information failed. Check and review the settings based on the detailed reason, and then try again. The detailed reason is output to *{0}*.
DWCO1803_E	Failed to output delivery information to an XML file. (Path:{0})	Check if you have write permission for the specified file. The path to the XML file is displayed in {0}.
DWCO1821_I	Updated delivery status. (Delivery ID:{0}, File ID:{1})	Notifies that the delivery status has been updated successfully. The delivery ID is output to *{0}*, and the file ID is output to *{1}*.
DWCO1822_E	Failed to update delivery status. It might be caused by the following reasons: The delivery does not exist. The delivery expired. Uploading is not completed. The delivery was not approved. (Delivery ID:{0}, File ID:{1}, Details:{2})	Update of the delivery status failed. Check if the relevant delivery exists, if its data storage period has expired, if its transmission was completed, and if its approval process has completed. The delivery ID is output to *{0}*, the file ID is output to *{1}*, and the detailed reason is output to *{2}*.
DWCO1841_I	Deleted a delivery. (Delivery ID:{0})	Notifies that the delivery has been deleted successfully. The delivery ID is output to *{0}*.
DWCO1842_E	Failed to delete a delivery. It might be caused by the following reasons: The delivery does not exist. Uploading is not completed. The delivery was not approved. (Delivery ID:{0}, Details:{1})	A non-existing delivery cannot be deleted. A delivery whose transfer is not completed cannot be deleted. For an unapproved delivery, try again after it is approved. The delivery ID is output to *{0}*, and the detailed reason is output to *{1}*.
DWCO1843_E	Failed to delete a delivery. The delivery might be sending or downloading. (Delivery ID:{0}, Details:{1})	A delivery being in progress of transmission or reception cannot be deleted. The delivery ID is output to *{0}*, and the detailed reason is output to *{1}*.
DWCO1901_E	An unexpected error occurred.	An unexpected exception occurred. Load might be concentrated on the server. Try again after a while. If the same error keeps occurring even after some retries, contact our sales representative or support contact. Also, it is possible that the user executing the process might have been deleted in the middle of execution. Contact the representative user or a group manager.
DWCO1902_E	Unable to start the application because initialization of logs failed.	The settings for the log files are invalid. This problem could be solved by re-installation.
DWCO1903_E	Unable to start the application because reading message files failed.	The settings for the configuration file are invalid. This problem could be solved by re-installation.
DWCO1904_E	Unable to start the application because reading setting files failed.	The settings for the configuration file are invalid. This problem could be solved by re-installation.
DWCO1906_E	Failed to connect to the server. (Details:{0})	See the detailed reason, and then check and review the execution environment such as the network environment again. The detailed reason is output to *{0}*.
DWCO1907_E	The server is busy. Please try again later.	The server is currently busy, and the HTTP status code 503 (Service Unavailable) is returned. Try again after a while.
DWCO1908_E	The session has timed out. Please try again.	The session is timed out. Log in again.

Message ID	Message details	Description
DWCO1909_E	The server returned an error. (Details:{0})	See the detailed reason, and then check and review the settings for the user, group, and delivery rules again. The detailed reason is output to *{0}*.
DWCO1911_E	The operation of getting a lock for concurrent control timed out.	A command is already running in the same computer. Because more than one command cannot be executed simultaneously, try again after the active command ends. If this error message frequently appears, the problem might be solved by setting a longer timeout time. Also, the user might not have the write permission to the Windows temporary folder. Check that the temporary folder is set correctly.
DWCO1999_E	Unable to start the application.	The server is busy, and the service cannot be started. Try again after a while.
DWCO2002_I	Suspended running file transfers. (Delivery ID:{0})	Notifies that the file transfer process has been suspended. The delivery ID is output to *{0}*.
DWCO2005_W	Running file transfers do not exist.	Notifies that there was no file transfer process.
DWCO2006_W	Running file transfers do not exist. (Delivery ID:{0})	Notifies that there was no file transfer process. The delivery ID is output to *{0}*.
DWCO2007_I	The specified delivery was already suspended. (Delivery ID:{0})	Notified that the delivery you tried to suspend had already been suspended. The delivery ID is output to *{0}*.
DWCO2008_E	Failed to suspend the specified delivery because it was already canceled. (Delivery ID:{0})	You cannot suspend a delivery that has been canceled. The delivery ID is output to *{0}*.
DWCO2009_E	The specified delivery did not exist. (Delivery ID:{0})	Notifies that the specified delivery does not exist. Check if the specified delivery ID is correct. The delivery ID is output to *{0}*.
DWCO2010_E	The specified delivery cannot be suspended. (Delivery ID:{0})	The specified delivery cannot be suspended because the delivery might already have been sent in the web window. The delivery ID is output to *{0}*.
DWCO2022_I	Canceled running file transfers. (Delivery ID:{0})	Notifies that the file transfer process was canceled. The delivery ID is output to *{0}*.
DWCO2025_I	The specified delivery was already canceled. (Delivery ID:{0})	Notified that the delivery you attempted to cancel has already been canceled. The delivery ID is output to *{0}*.
DWCO2026_E	Failed to cancel the specified delivery because it was already suspended. (Delivery ID:{0})	You cannot cancel a delivery that has been suspended. The delivery ID is output to *{0}*.
DWCO2027_E	The specified delivery cannot be canceled. (Delivery ID:{0})	The specified delivery cannot be canceled because the delivery might already have been sent in the web window. The delivery ID is output to *{0}*.
DWCO2041_I	Set acceptance of the file transfer function to deny.	The delivery acceptance status of the file transfer function has been set to delivery denial.
DWCO2061_I	Set acceptance of the file transfer function to allow.	The delivery acceptance status of the file transfer function has been set to start delivery.

7.6 List of CSV error messages

The following table describes a list of CSV error messages. For details about CSV error messages other than those described below, see the *Job Management Partner 1/Data Highway - Server Administrator Guide*.

Table 7–28: List of CSV error messages

No.	Error message	Description
1	You cannot delete this group (XXX) because some users belong to it. (DOMAIN, NAME_EN)	Output when users (including a child group) exist within the target group for deletion. Delete all the users in the group. The group name (English) is output to *XXX*.
2	A group name (XXX) was delete in the input csv data.,Joint verification failures exist.	Output when you attempt to include a user in the group to be deleted. To make the user belong to a group, specify a group that is not a deletion target. The group name (English) is output to *XXX*.

8 Operation and Failure Corrective Actions

This chapter describes the commands used for operation of and failure corrective actions for JP1/DH - Server.

8.1 List of commands

The following tables describe commands for acquiring failure information acquisition and operations management provided by JP1/DH - Server.

Table 8–1: Commands for acquiring failure information provided by JP1/DH - Server

No.	Command name		Function
1	In Windows	`getlog_server.bat`	Acquires the failure information without the database backup from the server.
	In Linux	`getlog_server.sh`	
2	In Windows	`getdetaillog_server.bat`	Acquires the failure information with the database backup from the server.
	In Linux	`getdetaillog_server.sh`	
3	In Windows	`getlog_client.bat`	Acquires the failure information from a client.
	In Linux	`getlog_client.sh`	

Table 8–2: Commands for operations management provided by JP1/DH - Server

No.	Command name		Function
1	In Windows	`dbbackup.bat`	Backs up the database.
	In Linux	`dbbackup.sh`	
2	In Windows	`dbrestore.bat`	Restores the database.
	In Linux	`dbrestore.sh`	
3	In Windows	`dbchangepassword.bat`	Changes the database password.
	In Linux	`dbchangepassword.sh`	
4	In Windows	`regist_users_number.bat`	Registers the number of purchased user licenses.
	In Linux	`regist_users_number.sh`	
5	In Windows	`selfsignedkeygen.bat`	Creates a secret key.
	In Linux	`selfsignedkeygen.sh`	
6	In Windows	`selfsignedcertreq.bat`	Creates a CSR (certificate signing request).
	In Linux	`selfsignedcertreq.sh`	
7	In Windows	`selfsigned.bat`	Creates a self-signed server certificate.
	In Linux	`selfsigned.sh`	

The save location for the commands is as follows:

```
installation-folder#\bin\
```

#: In Linux, change *installation-folder* to `/opt/jp1dh/server`.

8.2 Commands for acquiring failure information

This section describes the commands for acquiring the failure information of JP1/DH - Server.

8.2.1 getlog_server.bat (acquiring the failure information without the database backup from the server)/getdetaillog_server.bat (acquiring the failure information with the database backup from the server)/ getlog_client.bat (acquiring failure information from a client)

(1) Function

Acquire failure information of JP1/DH - Server from the server or client machine. These commands enable you to acquire the following information in the machine environment where JP1/DH - Server operates:

- OS information
- Hardware information
- Running process
- Network configuration
- Installed application
- Event logs (For applications and system)
- Setting information for Internet Explorer
- Setting information for Java
- Log information for linked products
- Configuration files for JP1/DH - Server
- Database information

Before using the `getlog_client.bat` command, change the following item in the batch file:

```
rem ----------------------------
rem  User-set items
rem ----------------------------
set SERVERNAME=FQDN-of-JP1/DH-Server-machine
```

Example:

```
rem ----------------------------
rem  User-set items
rem ----------------------------
set SERVERNAME= jp1dhserver.foo1.foo2,co.jp
```

(2) Executor

A user with a built-in Administrator account or with Administrator permissions executes the command from the command prompt.#

#

Do not execute a command directly. Use the command prompt to execute a command.

(3) Format

- To acquire failure information from the server machine:

```
getlog_server.bat or getdetaillog_server.bat DB-password
```

- To acquire failure information from a client machine:

```
getlog_client.bat
```

(4) Arguments

DB-password

Specify the database password.

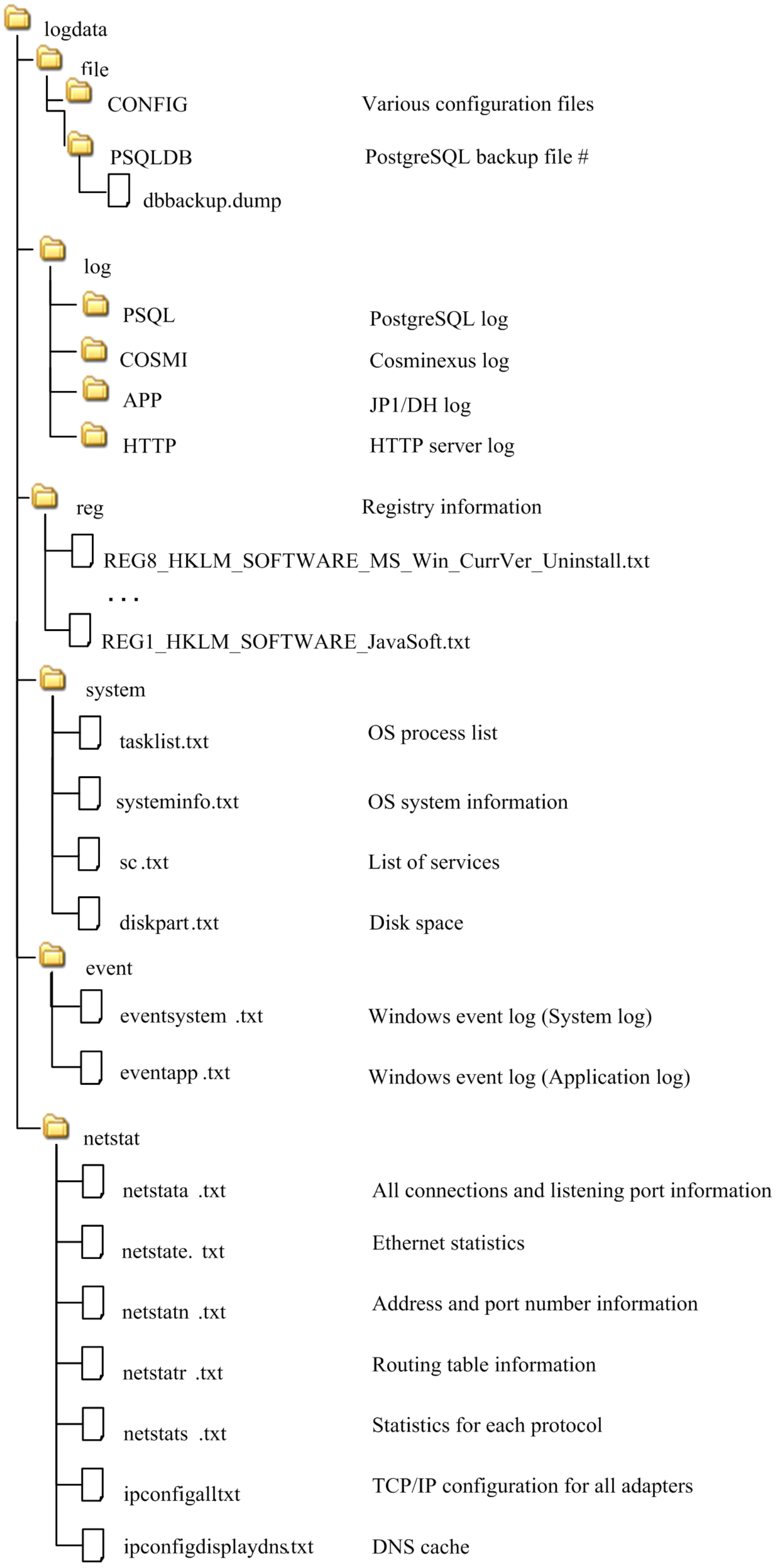
The default value for the database password is set to `p@ssw0rd`.

(5) Execution results

The files with the command execution results are stored in the `logdata` folder created immediately below the current directory where the command is executed.

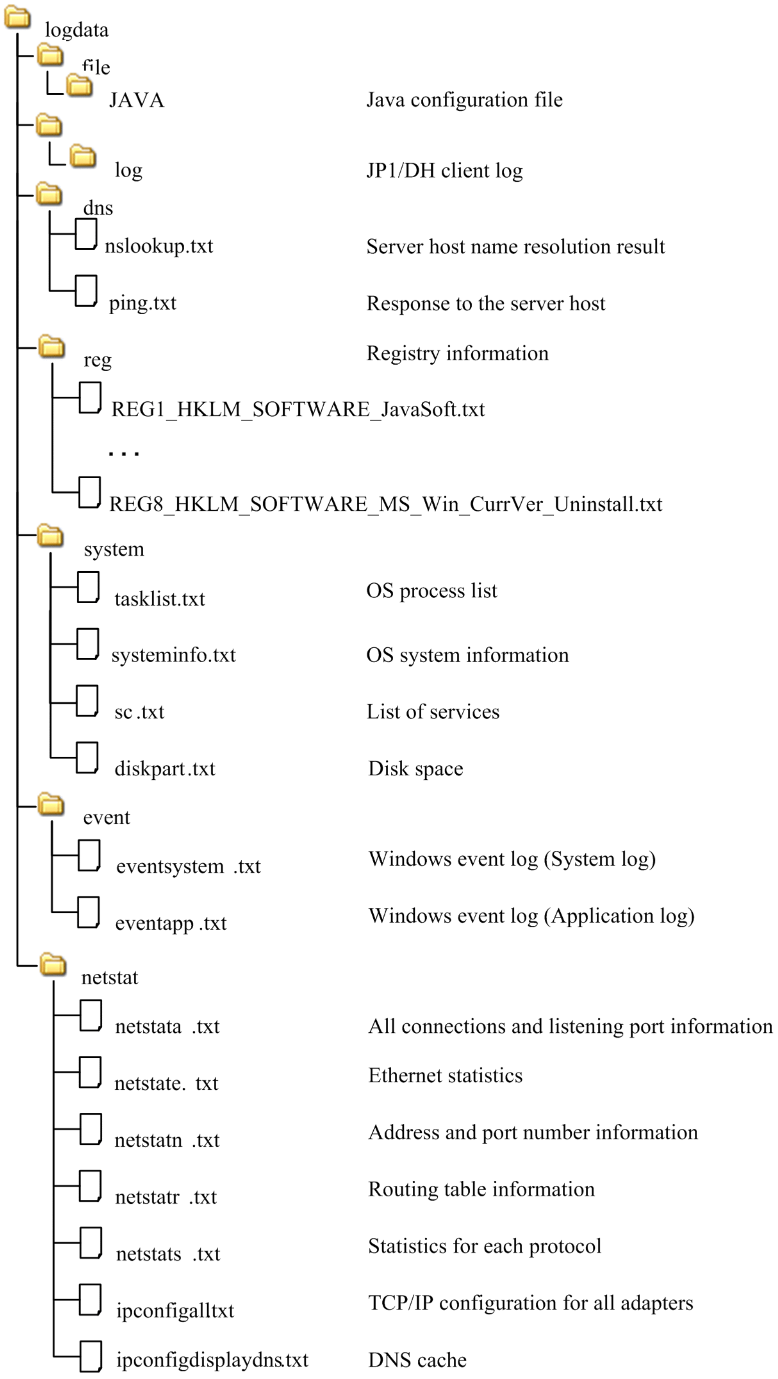
The following figures show the configuration of output files.

Figure 8–1: Example of the output files (When the command is executed on the server)



#: This is only output when getdetaillog_server.bat is executed.

Figure 8–2: Example of the output files (When the command is executed on a client)



Note that some of the files to be output in Linux are different from those in Windows. Files with differences are as follows:

- Output destination of registry information
  `logdata/reg/.HTC_`*xxxx*`.inf`
  Note: *xxxx* represents a value output differently depending on your product.
- Output destination of `\logdata\netstat\ipconfigall.txt` (a file that includes TCP/IP configuration for all adapters)
  `logdata/reg/ifconfiga.txt`
- `\logdata\netstat\ipconfigdisplaydns.txt` (a file that includes DNS cache) is not output.

- Output destination of the event log data
  `logdata/event/messages`
  `logdata/event/messages-`*yyyymmdd*
  In Linux, corresponding system log data is acquired.

(6) Return codes

Return code	Description	Operation after an event occurrence	Occurrence condition
`0`	Normal	--	Information is collected successfully.
`4`	Warning (information level)	Interrupts command processing.	• Execution of command is canceled during permission confirmation response for collecting information. • Execution of command is canceled during folder deletion confirmation response.
`8`	Error	Interrupts command processing.	Information collection failed.
`16`	Error	Interrupts command processing.	• A command is executed without the database password specified as the argument. • The backup of the database by using the backup command failed (only when the `getdetaillog_server.bat` command is executed).

(7) Output message (Output destination: stdout)

No.	Message	Return code	Operation after an event occurrence	Action to be taken by the operator	Occurrence condition
1	Failure information will be collected.	--	Starts command execution.	None	When a command is executed
2	Successfully collected the failure information. Press any key.	`0`	Terminates command execution.	None	When information is collected successfully
3	Did not successfully collect the failure information. Check the following items: • Does the user who executed the command have Administrator permissions? • Does the user who executed the command have write permission for the output folder?	`8`	Terminates command execution.	Check the following and re-execute the command: • The user executing the command has Administrator permissions. • The user executing the command has write permission to the output destination folder.	When collecting information failed
4	Did not successfully collect the failure information. Could not find the configuration file to be copied.	`8`	Terminates command execution.	Make sure that the collection target file exists.	When the collection target configuration file is not found
5	An output folder for the collected information exists.	--	Waits for user response.	Select **y** to continue execution, or **n** to cancel execution.	When a log output destination folder already exists

No.	Message	Return code	Operation after an event occurrence	Action to be taken by the operator	Occurrence condition
5	Overwrite the output information? (y/n)	--	Waits for user response.	Select **y** to continue execution, or **n** to cancel execution.	When a log output destination folder already exists
6	Canceled command execution. Press any key.	`4`	Terminates command execution.	If you selected **n** in No. 5, delete or move the log output destination folder, and then re-execute the command.	When **n** is selected in No. 5
7	Specify the DB password in the argument. Press any key and try again.	`16`	Terminates command execution.	Specify the database password as the argument, and then re-execute the command.	When a command is executed without the database password specified as the argument
8	Did not successfully collect the failure information. Press any key and try again.	`16`	Terminates command execution.	Check the following and re-execute the command: • The database service (`JP1_DH_DATABASE_SVR`) is running. • The password specified in the command is correct. • The content of the database error message that was output immediately before this message is checked and the cause of the error is removed.	When backing up the database with the backup command failed (Only when the `getdetaillog_server.bat` command is executed)

Note: If an error occurs within the database, the error message described above is output after an error message is output by the database.

(8) Notes on using the command

Do not execute a command directly. Use the command prompt to execute a command.

If you have enabled UAC (User Account Control) in the operating system, use one of the following ways to execute a command:

- Log in as a built-in Administrator user, start the command prompt, and then execute a command.
- Log in as a user with Administrator permissions, start the command prompt by clicking **Run as Administrator**, and then execute a command.
- Execute a command from a shortcut for the command prompt with the elevated privileges created at the time of JP1/DH - Server installation.#

  #

  If you use a command prompt in this way in Windows Server 2012 or Windows Server 2012 R2, you need to install Microsoft .NET Framework 3.5. For details about how to install Microsoft .NET Framework 3.5, see *D. Installing .NET Framework 3.5*.

If the command is interrupted due to an error in the database, a backup file with a size of 0 bytes is created.

In an execution environment such as the ones described below, acquiring failure information might take a while.

- Where there are many connections to the network

  If the machine has many definitions of network connections, acquiring network configuration information might take time.

- Where there are many output logs

If you execute the `getlog_client.bat` command in the 32-bit command prompt on a client with a 64-bit operating system, you cannot acquire the information about the 64-bit application. Make sure that you execute the command in the 64-bit command prompt.

Simultaneous executions of commands on the same machine are not supported.

8.3 Commands for operations management

This section describes the commands for operations management of JP1/DH - Server.

Note that the default value for the database password is set to `p@ssw0rd`.

8.3.1 dbbackup.bat (backing up the database)

(1) Function

Logically backs up the database used by JP1/DH - Server.

(2) Executor

A user with a built-in Administrator account or with Administrator permissions executes the command from the command prompt.#

#

Do not execute a command directly. Use the command prompt to execute a command.

(3) Format

```
dbbackup.bat DB-password backup-destination-folder [backup-file-name]
```

(4) Arguments

DB-password

Specify the database password.

backup-destination-folder

Specify the destination folder to output the database backup file with an absolute path.

Specify the absolute path length no more than 200 bytes.

backup-file-name (optional)

Specify the name of the database backup file with an absolute path.

If you omit this argument, the backup file is created with the name of `dbbackup.dump`.

(5) Execution results

A backup file is output in the specified destination folder.

(6) Return codes

Return code	Description	Operation after an event occurrence	Occurrence condition
0	Normal	--	Backup succeeded.
4	Warning	Interrupts command processing.	Execution of command is canceled during overwrite-confirmation response.

Return code	Description	Operation after an event occurrence	Occurrence condition
8	Warning	Interrupts command processing.	• A command is executed without the argument specified. • A command is executed without the database password specified. • The folder specified as the argument does not exist.
16	Error	Interrupts command processing.	Backup failed.

(7) Output message (Output destination: stdout)

No.	Message	Return code	Operation after an event occurrence	Action to be taken by the operator	Occurrence condition
1	The backup will start.	--	Starts command execution.	None	When a command is executed
2	Successfully finished the backup. Press any key.	0	Terminates command execution.	None	When backup succeeded
3	Specify the DB password in the argument. Press any key and try again.	8	Terminates command execution.	Specify the database password as the argument, and then re-execute the command.	When a command is executed without the database password specified as the argument
4	Specify the backup folder in the argument.	8	Terminates command execution.	Specify the backup destination folder as the argument, and then execute the command.	When a command is executed without the argument specified
5	The specified folder does not exist. Press any key and try again.	8	Terminates command execution.	Make sure that the specified backup destination folder is correct.	When an incorrect folder is specified as the argument
6	Did not successfully finish the backup. Press any key and try again.#	16	Terminates command execution.	Check the following and re-execute the command: • The database service (`JP1_DH_DATABASE_SVR`) is running. • The password specified in the command is correct. • The content of the database error message that was output immediately before this message is checked and the cause of the error is removed.	When backup failed
7	******* exists in the backup folder. Overwrite the output information? (y/n)	--	Waits for user response.	Select **y** to continue execution, or **n** to cancel execution.	When a backup file already exists in the backup destination folder
8	Canceled command execution. Press any key.	4	Terminates command execution.	If you selected **n** in No. 7, agree to the confirmation item and then press any key.	When **n** is selected in No. 7

#: If an error occurs within the database, this error message is output after an error message is output by the database.

(8) Notes on using the command

Do not execute a command directly. Use the command prompt to execute a command.

If you have enabled UAC (User Account Control) in the operating system, use one of the following ways to execute a command:

- Log in as a built-in Administrator user, start the command prompt, and then execute a command.
- Log in as a user with Administrator permissions, start the command prompt by clicking **Run as Administrator**, and then execute a command.
- Execute a command from a shortcut for the command prompt with the elevated privileges created at the time of JP1/DH - Server installation.#

  #

  If you use a command prompt in this way in Windows Server 2012 or Windows Server 2012 R2, you need to install Microsoft .NET Framework 3.5. For details about how to install Microsoft .NET Framework 3.5, see *D. Installing .NET Framework 3.5*.

If the command is interrupted due to an error in the database, a backup file with a size of 0 bytes is created.

Simultaneous executions of commands on the same machine are not supported.

8.3.2 dbrestore.bat (restoring the database)

(1) Function

Restores the database used by JP1/DH - Server from the backup file. Before executing this command, shut down the JP1/DH Web application server (Cosminexus J2EE server).

(2) Executor

A user with a built-in Administrator account or with Administrator permissions executes the command from the command prompt.#

#

Do not execute a command directly. Use the command prompt to execute a command.

(3) Format

```
dbrestore.bat DB-password restore-source-folder [restore-file-name]
```

(4) Arguments

DB-password

Specify the database password.

restore-source-folder

Specify the destination folder where the database backup file is stored with an absolute path.

Specify the absolute path length no more than 200 bytes.

restore-file-name (optional)

Specify the name of the backup file to be used for restoring the database.

If you omit this argument, `dbbackup.dump` is used for restoration.

(5) Execution results

The data in the specified backup file is restored to the database.

(6) Return codes

Return code	Description	Operation after an event occurrence	Occurrence condition
`0`	Normal	--	Restoration succeeded.
`4`	Warning	Interrupts command processing.	• A command is executed without the argument specified. • A command is executed without the database password specified. • The folder specified as the argument does not exist.
`8`	Error	Interrupts command processing.	Restoration failed.
`16`	Warning	Interrupts command processing.	Execution of the command is canceled during confirmation response for shutting down the JP1/DH Web application server (Cosminexus J2EE server).

(7) Output message (Output destination: stdout)

No.	Message	Return code	Operation after an event occurrence	Action to be taken by the operator	Occurrence condition
1	The restoration will start.	--	Starts command execution.	None	When a command is executed
2	Successfully finished the restoration. Press any key.	`0`	Terminates command execution.	None	When restoration succeeded
3	Specify the DB password in the argument. Press any key and try again.	`4`	Terminates command execution.	Specify the database password as the argument, and then re-execute the command.	When a command is executed without the database password specified as the argument
4	Specify the restore source folder in the argument.	`4`	Terminates command execution.	Specify the restore source folder as the argument, and then re-execute the command.	When a command is executed without the argument specified
5	The specified folder does not exist. Press any key and try again.	`8`	Terminates command execution.	Make sure that the specified restore source folder is correct.	When an incorrect folder is specified as the argument
6	******* does not exist in the specified folder.	`8`	Terminates command execution.	Make sure that the specified restore source folder and restore file name are correct.	When an incorrect folder or restore file name is specified as the argument
7	Did not successfully finish the restoration. Press any key and try again.#	`8`	Terminates command execution.	Check the content of the output error message, remove the cause of the error, and then re-execute the command.	When restoration failed

No.	Message	Return code	Operation after an event occurrence	Action to be taken by the operator	Occurrence condition
8	Confirm that the DH Web application server is suspended before continuing. Continue? (y/n)	--	Waits for user response.	Select **y** to continue execution, or **n** to cancel execution.	When a command is executed
9	Canceled command execution. Press any key.	`16`	Terminates command execution.	If you selected **n** in No. 8, agree to the confirmation item and then press any key.	When **n** is selected in No. 8

#: If an error occurs within the database, this error message is output after an error message is output by the database.

(8) Notes on using the command

Do not execute a command directly. Use the command prompt to execute a command.

If you have enabled UAC (User Account Control) in the operating system, use one of the following ways to execute a command:

- Log in as a built-in Administrator user, start the command prompt, and then execute a command.
- Log in as a user with Administrator permissions, start the command prompt by clicking **Run as Administrator**, and then execute a command.
- Execute a command from a shortcut for the command prompt with the elevated privileges created at the time of JP1/DH - Server installation.#

  #

  If you use a command prompt in this way in Windows Server 2012 or Windows Server 2012 R2, you need to install Microsoft .NET Framework 3.5. For details about how to install Microsoft .NET Framework 3.5, see *D. Installing .NET Framework 3.5*.

Simultaneous executions of commands on the same machine are not supported.

8.3.3 dbchangepassword.bat (changing the database password)

(1) Function

Changes the password for the database that is used by JP1/DH - Server.

You can use alphanumeric characters and the following symbols in this command:#

```
& | < > ( ) % ^ ; , ' \ ! ? # $ ~ - = @ + * . /
```

#

Do not use any characters or symbols except the ones described above in a password. If you use any characters or symbols other than the ones described above, you might not be able to change the password any more.

Also, make sure that you make changes to the following configuration file and batch file after changing the password:

- `digikatsuwide.xml`

File path

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

Description of changes

```
<persistence>
      <database>
            <password>password-after-change</password>
      </database>
```

Example:

```
<persistence>
      <database>
            <password>Dh8%7uK0(z$a</password>
      </database>
```

- dbcreate.bat

  File path

  installation-folder\setup_util\dbcreate.bat

  Description of changes

```
set PGPASSWORD=password-after-change
```

Example:

```
set PGPASSWORD=Dh8%7uK0(z$a
```

(2) Executor

A user with a built-in Administrator account or with Administrator permissions executes the command from the command prompt.#

#

Do not execute a command directly. Use the command prompt to execute a command.

(3) Format

```
dbchangepassword.bat password-before-change password-after-change
```

(4) Arguments

password-before-change

Specify the current password.

If you use any of the following symbols, append a caret (^) escape character to the symbol, and then enclose the caret and symbol in double quotation marks:

```
& | < > ( ) % ^ ; , ' \
```

password-after-change

Specify a new password.

If you use any of the following symbols, append a caret (^) escape character to the symbol, and then enclose the caret and symbol in double quotation marks:

```
& | < > ( ) % ^ ; ,
```

In addition, if you use one of the following symbols, append a backslash (\) escape character to the symbol:

```
' \
```

(5) Execution results

The database password is changed.

(6) Return codes

Return code	Description	Operation after an event occurrence	Occurrence condition
0	Normal	--	The password is changed successfully.
4	Warning	Interrupts command processing.	Execution of the command is canceled during password change confirmation response.
8	Warning	Interrupts command processing.	No argument is specified.
16	Warning	Interrupts command processing.	The number of specified arguments is incorrect.
32	Error	Interrupts command processing.	The password change failed.

(7) Output message (Output destination: stdout)

No.	Message	Return code	Operation after an event occurrence	Action to be taken by the operator	Occurrence condition
1	The DB password will be changed to ******. Are you sure? (y/n)	--	Waits for user response.	Select **y** to continue execution, or **n** to cancel execution.	When a command is executed
2	The password will be changed.	--	Starts command execution.	None	When **y** is selected in No. 1
3	Successfully changed the password. Press any key.	0	Terminates command execution.	None	When the password is changed successfully
4	Specify an argument. Press any key and try again.	8	Terminates command execution.	Specify the current database password and new database password as the arguments, and then re-execute the command.	When no argument is specified
5	The number of arguments is invalid. Press any key and try again.	16	Terminates command execution.	Specify the current database password and new database password as the arguments, and then re-execute the command.	When the number of specified arguments is incorrect
6	Did not successfully change the password. Press any key and try again.#	32	Terminates command execution.	Check the content of the output error message, remove the cause of the error, and then re-execute the command.	When the password change failed

No.	Message	Return code	Operation after an event occurrence	Action to be taken by the operator	Occurrence condition
7	Canceled command execution. Press any key.	4	Terminates command execution.	If you selected **n** in No. 1, specify the new password, and then execute the command.	When **n** is selected in No. 1

#: If an error occurs within the database, this error message is output after an error message is output by the database.

(8) Notes on using the command

Do not execute a command directly. Use the command prompt to execute a command.

If you have enabled UAC (User Account Control) in the operating system, use one of the following ways to execute a command:

- Log in as a built-in Administrator user, start the command prompt, and then execute a command.
- Log in as a user with Administrator permissions, start the command prompt by clicking **Run as Administrator**, and then execute a command.
- Execute a command from a shortcut for the command prompt with the elevated privileges created at the time of JP1/DH - Server installation.#

  #

  If you use a command prompt in this way in Windows Server 2012 or Windows Server 2012 R2, you need to install Microsoft .NET Framework 3.5. For details about how to install Microsoft .NET Framework 3.5, see *D. Installing .NET Framework 3.5*.

Simultaneous executions of commands on the same machine are not supported.

8.3.4 regist_users_number.bat (registering the number of purchased user licenses)

(1) Function

Registers the number of purchased users of JP1/DH - Server.

(2) Executor

A user with a built-in Administrator account or with Administrator permissions executes the command from the command prompt.#

#

Do not execute a command directly. Use the command prompt to execute a command.

(3) Format

```
regist_users_number.bat DB-password number-of-purchased-users
```

(4) Arguments

DB-password

Specify the database password.

number-of-purchased-users

Specify the number of purchased users (a number from 0 to 2,147,483,647).

(5) Execution results

The number of purchased users is registered in the system.

(6) Return codes

Return code	Description	Operation after an event occurrence	Occurrence condition
`0`	Normal	--	The number of purchased users is registered successfully.
`4`	Warning	Interrupts command processing.	Execution of the command is canceled during confirmation response for registering the number of purchased users.
`8`	Warning	Interrupts command processing.	• No argument is specified. • The number of specified arguments is incorrect.
`16`	Error	Interrupts command processing.	The registration of the number of purchased users failed.

(7) Output message (Output destination: stdout)

No.	Message	Return code	Operation after an event occurrence	Action to be taken by the operator	Occurrence condition
1	The number of purchased users to be registered is ******. Are you sure? (y/n)	--	Waits for user response.	Select **y** to continue execution, or **n** to cancel execution.	When a command is executed
2	The number of purchased users will be registered.	--	Starts command execution.	None	When **y** is selected in No. 1
3	Successfully registered the number of purchased users. Press any key.	`0`	Terminates command execution.	None	When the number of purchased users is registered successfully
4	Specify an argument. Press any key and try again.	`8`	Terminates command execution.	Specify the database password and the number of purchased users as the arguments, and then re-execute the command.	• When no argument is specified • When the number of purchased users is specified with characters other than the single-byte numbers
5	The number of arguments is invalid. Press any key and try again.	`8`	Terminates command execution.	Specify the database password and the number of purchased users as the arguments, and then re-execute the command.	When the number of specified arguments is incorrect

No.	Message	Return code	Operation after an event occurrence	Action to be taken by the operator	Occurrence condition
6	Did not successfully register the number of purchased users. Press any key and try again.#	`16`	Terminates command execution.	Check the content of the output error message, remove the cause of the error, and then re-execute the command.	When the registration of the number of purchased users failed
7	Canceled command execution. Press any key.	`4`	Terminates command execution.	If you selected **n** in No. 1, specify the number of purchased users to be registered, and then execute the command.	When **n** is selected in No. 1

#: If an error occurs within the database, this error message is output after an error message is output by the database.

(8) Notes on using the command

Do not execute a command directly. Use the command prompt to execute a command.

If you have enabled UAC (User Account Control) in the operating system, use one of the following ways to execute a command:

- Log in as a built-in Administrator user, start the command prompt, and then execute a command.
- Log in as a user with Administrator permissions, start the command prompt by clicking **Run as Administrator**, and then execute a command.
- Execute a command from a shortcut for the command prompt with the elevated privileges created at the time of JP1/DH - Server installation.#

  #

  If you use a command prompt in this way in Windows Server 2012 or Windows Server 2012 R2, you need to install Microsoft .NET Framework 3.5. For details about how to install Microsoft .NET Framework 3.5, see *D. Installing .NET Framework 3.5*.

Simultaneous executions of commands on the same machine are not supported.

8.3.5 selfsignedkeygen.bat (creating a secret key)

(1) Function

Creates a secret key to be used for immediate use of JP1/DH - Server for purposes such as testing and evaluation.

(2) Executor

A user with a built-in Administrator account or with Administrator permissions executes the command from the command prompt.#

#

Do not execute a command directly. Use the command prompt to execute a command.

(3) Format

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

(4) Arguments

`-out` *secret-key-file*

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

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

Specify the bit length of a secret key to be created. The values that you can specify are as follows:

`512`, `1024`, `2048`, `4096`

If you omit this argument, `1024` is used.

(5) Execution results

A secret key file is created in the folder specified for `-out`.

(6) Notes on using the command

Do not execute a command directly. Use the command prompt to execute a command.

If you have enabled UAC (User Account Control) in the operating system, use one of the following ways to execute a command:

- Log in as a built-in Administrator user, start the command prompt, and then execute a command.
- Log in as a user with Administrator permissions, start the command prompt by clicking **Run as Administrator**, and then execute a command.
- Execute a command from a shortcut for the command prompt with the elevated privileges created at the time of JP1/DH - Server installation.#

  #

  If you use a command prompt in this way in Windows Server 2012 or Windows Server 2012 R2, you need to install Microsoft .NET Framework 3.5. For details about how to install Microsoft .NET Framework 3.5, see *D. Installing .NET Framework 3.5*.

Simultaneous executions of commands on the same machine are not supported.

8.3.6 selfsignedcertreq.bat (creating a CSR (certificate signing request))

(1) Function

Creates a CSR (certificate signing request) file to be used for immediate use of JP1/DH - Server for the purposes such as testing and evaluation.

(2) Executor

A user with a built-in Administrator account or with Administrator permissions executes the command from the command prompt.#

#

Do not execute a command directly. Use the command prompt to execute a command.

(3) Format

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

(4) Arguments

`-key` *key-file*

Specify the secret key created in *8.3.5 selfsignedkeygen.bat (creating a secret key)*.

`-out` *CSR-file*

Specify the name of the CSR (certificate signing request) file to be created.

`-subject "`*subject*`"`

Specify the subject name of the certificate in the format described below. The values that you can specify are as follows:

```
"C=2-character-country-code(JP for Japan),ST=state-or-province-
name,L=city-or-area-name,O=organization-name,OU=organization-unit-
name,CN=FQDN-of-the-server-host"
```

An example of specification is as follows:

```
"C=JP,ST=Tokyo,L=Shinagawa-ku,O=Hitachi Ltd.,OU=Software
Development,CN=p1dhserver.foo1.foo2.co.jp"
```

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

space, period (`.`), hyphen (`-`), and forward slash (`/`)

You cannot use a comma.

(5) Execution results

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

(6) Notes on using the command

Do not execute a command directly. Use the command prompt to execute a command.

If you have enabled UAC (User Account Control) in the operating system, use one of the following ways to execute a command:

- Log in as a built-in Administrator user, start the command prompt, and then execute a command.

- Log in as a user with Administrator permissions, start the command prompt by clicking **Run as Administrator**, and then execute a command.
- Execute a command from a shortcut for the command prompt with the elevated privileges created at the time of JP1/DH - Server installation.#

  #

  If you use a command prompt in this way in Windows Server 2012 or Windows Server 2012 R2, you need to install Microsoft .NET Framework 3.5. For details about how to install Microsoft .NET Framework 3.5, see *D. Installing .NET Framework 3.5*.

Simultaneous executions of commands on the same machine are not supported.

8.3.7 selfsigned.bat (creating a self-signed server certificate)

(1) Function

Creates a self-signed server certificate to be used for immediate use of JP1/DH - Server for the purposes such as testing and evaluation.

(2) Executor

A user with a built-in Administrator account or with Administrator permissions executes the command from the command prompt.#

#

Do not execute a command directly. Use the command prompt to execute a command.

(3) Format

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

(4) Arguments

`-in` *CSR-file*

Specify the CSR file created in *8.3.6 selfsignedcertreq.bat (creating a CSR (certificate signing request))*.

`-out` *certificate-file*

Specify the name of the self-signed server certificate file to be created.

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

Specify the signature algorithm. You can specify the following algorithms:

`MD5`, `SHA1`, `SHA224`, `SHA256`, `SHA384`, `SHA512`

If you omit this argument, `SHA1` is used.

`-signkey` *key-file*

Specify the secret key created in *8.3.5 selfsignedkeygen.bat (creating a secret key)*.

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

Specify the period for which the created certificate is valid in units of days. Note that the command execution day is automatically set as the starting day of the valid period and you cannot change the starting day.

(5) Execution results

A self-signed server certificate is created in the following folder:

installation-folder`\bin\`

(6) Notes on using the command

Do not execute a command directly. Use the command prompt to execute a command.

If you have enabled UAC (User Account Control) in the operating system, use one of the following ways to execute a command:

- Log in as a built-in Administrator user, start the command prompt, and then execute a command.
- Log in as a user with Administrator permissions, start the command prompt by clicking **Run as Administrator**, and then execute a command.
- Execute a command from a shortcut for the command prompt with the elevated privileges created at the time of JP1/DH - Server installation.#

  #

  If you use a command prompt in this way in Windows Server 2012 or Windows Server 2012 R2, you need to install Microsoft .NET Framework 3.5. For details about how to install Microsoft .NET Framework 3.5, see *D. Installing .NET Framework 3.5*.

Simultaneous executions of commands on the same machine are not supported.

9 Troubleshooting

This chapter describes troubleshooting for JP1/DH - Server.

9.1 Troubleshooting

The following table describes problems that can occur and actions to be taken for these problems.

Table 9–1: List of troubleshooting tips

No.	Problem	Possible cause	Action to be taken
1	The login window is not displayed during the operation check described in *5.5.1(1) Checking the operation of JP1/DH Web application server*.	The IP address of the machine with JP1/DH - Server or the sender email address specified in the JP1/DH Web application server settings might be incorrect.	See *5.3 Setting up the JP1/DH Web application server environment* and confirm that the IP address of the server and the sender email address specified in the mail server settings are specified correctly. Neither of these settings can be omitted.
2	When you attempt to access the login window of JP1/DH - Server, the window is not displayed, and the message `Page cannot be displayed. The session may have been timed-out.` is displayed.	IPv6 protocol might be given priority to be selected or used in the configuration settings for the operating system of the computer where JP1/DH - Server is installed.	In an operating system that supports both IPv6 protocol and IPv4 protocol, if the IPv6 protocol is given priority, the problem described to the left might occur. In such a case, see the support information for your operating system and change the configuration settings so that IPv4 protocol has priority to be used.
3	The login window is not displayed when you attempt to access JP1/DH - Server via the URL, `https://`*FQDN-of-the-server-host*`/`, described in *5.5.1(2) Checking access to JP1/DH - Server*. If you access JP1/DH - Server via the URL, `https://`*FQDN-of-the-server-host*`/index.html`, the login window is displayed.	The JP1/DH Web server settings might be incorrect.	See *5.4.4 Editing the settings for the JP1/DH Web server* and confirm that the host name of the server is entered in lower case for the setting items `ProxyPass` and `ProxyPassReverse` in the `httpsd.conf` configuration file.

10 Messages

This chapter describes the messages output when errors occur during installation and setup of JP1/DH - Server, and how to respond to these errors.

10.1 Message format

The format of a message to be output by JP1/DH - Server when an error occurs during installation and setup of JP1/DH - Server is described in the following subsection.

10.1.1 Output format of a message

A message to be output consists of a message ID and message text.

- KJDH*nnnn*-*Z* *message-text*

Each element of a message ID indicates the following items:

K

Indicates the system identifier.

JDH

Indicates that the message is output by JP1/DH - Server.

nnnn

Indicates the serial number of the message.

Z

Indicates one of the following message types:

- E: Error
  The processing is interrupted after the message is output.
- W: Warning
  The processing is continued after the message is output.
- I: Information
  The user is notified of the information.

10.1.2 Description format of a message

This subsection describes the description format of a message in this manual. Italic characters indicate a placeholder for some actual text to be provided by the system when a message is displayed. Also, messages are listed in ascending order of message IDs. An example of the description format of a message is as follows:

message-ID

message-text

Message description

(S) Indicates how the system handles the error.

(O) Indicates the actions to be taken by the operator when the message is output.

10.2 List of messages

The list of messages output by JP1/DH - Server when errors occur during installation and setup of JP1/DH - Server is as follows:

KJDH5000-W

> This platform is not supported. Installation is canceled.

Installation is interrupted because an attempt to install the product to a platform that does not satisfy the prerequisites for the OS was made.

(S) Interrupts the installation.

(O) Check the prerequisites for the OS, and then install the product to a machine with the requisite OS.

KJDH5001-W

> The login account does not have the permissions needed for installation or uninstallation. Use the Administrator account.

Installation is interrupted because the user performing installation or uninstallation does not have administrator rights.

(S) Interrupts the installation.

(O) Install or uninstall the product by using the user account with administrator rights.

KJDH5002-W

> The path for the installation folder is too long. Re-specify the installation folder.

The path to the installation folder is too long. Change the installation folder.

(S) Waits for user action.

(O) Change the installation destination.

KJDH5003-W

> There is not enough free space for installation. At least 2 GB of free space is required for setup.

Installation is interrupted because there is not sufficient free space on the installation drive.

(S) Interrupts the installation.

(O) Secure enough free space on the installation drive, and then install the product again.

KJDH5004-E

> Failed to set up the database. Installation is canceled.

Installation is interrupted because the database setup failed.

(S) Interrupts the installation, and rolls back the system to the state at the start of installation.

(O) Check the Hitachi Integrated Installer log#, remove the problem according to the output error information, and then install the product again.

#: A log file for Hitachi Integrated Installer is output in the following location: `C:\Windows\Temp\HCDINST`

KJDH5005-E

Failed to configure the database. Installation is canceled.

Installation is interrupted because the database construction failed.

(S) Interrupts the installation, and rolls back the system to the state at the start of installation.

(O) Check the Hitachi Integrated Installer log#, remove the problem according to the output error information, and then install the product again.

#: A log file for Hitachi Integrated Installer is output in the following location: `C:\Windows\Temp\HCDINST`

KJDH5006-E

Failed to set up the application server. Installation is canceled.

Installation is interrupted because the application server setup failed.

(S) Interrupts the installation, and rolls back the system to the state at the start of installation.

(O) Check the Hitachi Integrated Installer log#, remove the problem according to the output error information, and then install the product again.

#: A log file for Hitachi Integrated Installer is output in the following location: `C:\Windows\Temp\HCDINST`

KJDH5007-E

Failed to install the application configuration file. Installation is canceled.

Installation is interrupted because the installation of the application configuration file failed.

(S) Interrupts the installation, and rolls back the system to the state at the start of installation.

(O) Check the Hitachi Integrated Installer log#, remove the problem according to the output error information, and then install the product again.

#: A log file for Hitachi Integrated Installer is output in the following location: `C:\Windows\Temp\HCDINST`

KJDH5008-E

Could not install the product because the latest version %s is already installed.

Installation is interrupted because a newer version of the product is already installed.

(S) Interrupts the installation.

(O) Uninstall the installed version, and then install the desired version of the product again.

KJDH5009-E

Failed to overwrite install the application server. Could not suspend the application server. Installation is canceled.

Overwrite installation is interrupted because the overwrite installation of the application server failed.

(S) Interrupts the overwrite installation, and rolls back the system to the state at the start of the overwrite installation.

(O) Manually stop the services of the JP1/DH Web application server and JP1/DH Web server. If you can stop the services, perform the overwrite installation again.

KJDH5010-E

Failed to overwrite install the database. Could not suspend the database. Installation is canceled.

Overwrite installation is interrupted because the overwrite installation of the database failed.

(S) Interrupts the overwrite installation, and rolls back the system to the state at the start of the overwrite installation.

(O) Manually stop the database service (`JP1_DH_DATABASE_SVR`). If you can stop the service, perform the overwrite installation again.

KJDH5011-E

Failed to overwrite install the application server. Installation is canceled.

Overwrite installation is interrupted because the overwrite installation of the application server failed.

(S) Interrupts the overwrite installation, and rolls back the system to the state at the start of the overwrite installation.

(O) Check the Hitachi Integrated Installer log#, remove the problem according to the output error information, and then perform the overwrite installation again.

#: A log file for Hitachi Integrated Installer is output in the following location: `C:\Windows\Temp\HCDINST`

KJDH5012-E

Failed to overwrite install the database. Installation is canceled.

Overwrite installation is interrupted because the overwrite installation of the database failed.

(S) Interrupts the overwrite installation, and rolls back the system to the state at the start of the overwrite installation.

(O) Check the Hitachi Integrated Installer log#, remove the problem according to the output error information, and then perform the overwrite installation again.

#: A log file for Hitachi Integrated Installer is output in the following location: `C:\Windows\Temp\HCDINST`

KJDH5013-E

Failed to overwrite install the application configuration file. Installation is canceled.

Overwrite installation is interrupted because the overwrite installation of the application configuration file failed.

(S) Interrupts the overwrite installation, and rolls back the system to the state at the start of the overwrite installation.

(O) Check the Hitachi Integrated Installer log$^{\#}$, remove the problem according to the output error information, and then perform the overwrite installation again.

#: A log file for Hitachi Integrated Installer is output in the following location: `C:\Windows\Temp\HCDINST`

KJDH5014-E

Failed to overwrite install the application server. Could not start the application server. Installation is canceled.

Overwrite installation is interrupted because the overwrite installation of the application server failed.

(S) Interrupts the overwrite installation, and rolls back the system to the state at the start of the overwrite installation.

(O) Check the Hitachi Integrated Installer log$^{\#}$, remove the problem according to the output error information, and then perform the overwrite installation again.

#: A log file for Hitachi Integrated Installer is output in the following location: `C:\Windows\Temp\HCDINST`

KJDH5015-E

Failed to overwrite install the database. Could not start the database. Installation is canceled.

Overwrite installation is interrupted because the overwrite installation of the database failed.

(S) Interrupts the overwrite installation, and rolls back the system to the state at the start of the overwrite installation.

(O) Check the Hitachi Integrated Installer log$^{\#}$, remove the problem according to the output error information, and then perform the overwrite installation again.

#: A log file for Hitachi Integrated Installer is output in the following location: `C:\Windows\Temp\HCDINST`

KJDH5016-E

Failed to uninstall the application server. Uninstallation is canceled.

Uninstallation is interrupted because the uninstallation of the application server failed.

(S) Interrupts the uninstallation, and rolls back the system to the state at the start of the uninstallation.

(O) Check the Hitachi Integrated Installer log$^{\#}$, remove the problem according to the output error information, and then uninstall the product again.

#: A log file for Hitachi Integrated Installer is output in the following location: `C:\Windows\Temp\HCDINST`

KJDH5017-E

Failed to uninstall the database. Uninstallation is canceled.

Uninstallation is interrupted because the uninstallation of the database failed.

(S) Interrupts the uninstallation, and rolls back the system to the state at the start of the uninstallation.

(O) Check the Hitachi Integrated Installer log$^{\#}$, remove the problem according to the output error information, and then uninstall the product again.

#: A log file for Hitachi Integrated Installer is output in the following location: `C:\Windows\Temp\HCDINST`

KJDH5018-E

> Failed to uninstall the application configuration file. Uninstallation is canceled.

Uninstallation is interrupted because the uninstallation of the application configuration file failed.

(S) Interrupts the uninstallation, and rolls back the system to the state at the start of the uninstallation.

(O) Check the Hitachi Integrated Installer log#, remove the problem according to the output error information, and then uninstall the product again.

#: A log file for Hitachi Integrated Installer is output in the following location: `C:\Windows\Temp\HCDINST`

KJDH5019-E

> You cannot install this product in an environment where PostgreSQL is already installed. Uninstall PostgreSQL to proceed.

Installation is interrupted because PostgreSQL is already installed in the installation destination environment.

(S) Interrupts the installation.

(O) Uninstall PostgreSQL existing in the installation destination, and then install JP1/DH - Server again.

KJDH5020-E

> You cannot install this product in an environment where Windows user "postgres" already exists. Delete that user to proceed.

Installation is interrupted because the Windows user, `postgres`, already exists in the installation destination environment.

(S) Interrupts the installation.

(O) Delete the Windows user, `postgres`, and then install the product again.

KJDH5021-E

> Could not install the database because folder %1 exists. Delete or move %1 to proceed.

Installation is interrupted because the folder *%1*# already exists in the installation destination environment.

(S) Interrupts the installation.

(O) Delete the folder *%1*#, and then install the product again.

#: The PostgreSQL database folder that was created in the previous installation of the product

KJDH5022-E

> You cannot specify a path that includes '#' for the installation folder name.

Installation is interrupted because a path to the installation folder including # is specified for the installation folder name.

(S) Interrupts the installation.

(O) Change the installation folder name, and then install the product again.

KJDH5023-E

> Failed to uninstall the application server. Could not suspend the application server. Uninstallation is canceled.

Uninstallation is interrupted because the uninstallation of the application server failed.

(S) Interrupts the uninstallation, and rolls back the system to the state at the start of the uninstallation.

(O) Manually stop the following services in the Windows Service Manager, and then uninstall the product again:

- `JP1_DH_WEB SVR`
- `JP1_DH_WEB CONTAINER`

KJDH5024-E

> Failed to uninstall the database. Could not suspend the database. Uninstallation is canceled.

Uninstallation is interrupted because the uninstallation of the database failed.

(S) Interrupts the uninstallation, and rolls back the system to the state at the start of the uninstallation.

(O) Manually stop the following service in the Windows Service Manager, and then uninstall the product again:

- `postgresql-`*`x.x`* (*`x.x`*: PostgreSQL version number)

KJDH5025-E

> Failed to overwrite install the application server. Could not start the application server. Overwrite installation is canceled.

Overwrite installation is interrupted because the overwrite installation of the application server failed.

(S) Interrupts the overwrite installation, and rolls back the system to the state at the start of the overwrite installation.

(O) Check the Hitachi Integrated Installer log#, remove the problem according to the output error information, and then perform the overwrite installation again.

#: A log file for Hitachi Integrated Installer is output in the following location: `C:\Windows\Temp\HCDINST`

KJDH5026-E

> Failed to overwrite install the database. Could not start the database. Overwrite installation is canceled.

Overwrite installation is interrupted because the overwrite installation of the database failed.

(S) Interrupts the overwrite installation, and rolls back the system to the state at the start of the overwrite installation.

(O) Check the Hitachi Integrated Installer log#, remove the problem according to the output error information, and then perform the overwrite installation again.

#: A log file for Hitachi Integrated Installer is output in the following location: `C:\Windows\Temp\HCDINST`

KJDH5027-E

Could not install the product because %s is already installed.

Installation is interrupted because %s is already installed.

(S) Interrupts the installation.

(O) Uninstall the installed %s, and then install the desired version of the product again.

Appendixes

A. List of Files and Folders

The following table lists files and folders used in JP1/DH - Server.

Table A–1: List of files and folders

File or folder	Path to the file or folder
Log file for the new fixing patch#	*DH_Path*`\PATCHLOG.TXT`
Backup folder for the new fixing patch#	*DH_Path*`\patch_backup_dir`
Batch file for collecting failure information from the servers (except for the database)	*DH_Path*`\bin\getlog_server.bat`
Batch file for collecting failure information from the servers (including the database)	*DH_Path*`\bin\getdetaillog_server.bat`
Batch file for collecting failure information from a client	*DH_Path*`\bin\getlog_client.bat`
Batch file for backing up the database	*DH_Path*`\bin\dbbackup.bat`
Batch file for restoring the database	*DH_Path*`\bin\dbrestore.bat`
Batch file for changing the database password	*DH_Path*`\bin\dbchangepass.bat`
Batch file to register the number of purchased users	*DH_Path*`\bin\regist_users_number.bat`
Batch file to update What's new information	*DH_Path*`\bin\reload_app.bat`
Storage folder for delivery file	*DH_Path*`\data`
Folder containing some shortcuts to manuals	*DH_Path*`\doc`
Storage folder for containing documents and manuals	*DH_Path*`\uCPSB\CC\web\containers\jp1dh\webapps\digikatsuwide\pdf`
JDBC driver for database access	*DH_Path*`\lib\postgresql-9.2-1003.jdbc4.jar`
Logs output destination folder	*DH_Path*`\log`
Temporary folder for the application configuration file	*DH_Path*`\misc`
Installation folder for the database	*DH_Path*`\PostgreSQL`
Data folder for the database	*DH_Path*`\PostgreSQL\9.2\data`
Storage folder for system commands and utilities	*DH_Path*`\sbin`
Storage folder for batch files for building the system	*DH_Path*`\setup_utl`
Storage folder for JP1/DH - Server configuration template files	*DH_Path*`\template`
Installation folder for the JP1/DH Web application server and JP1/DH Web server	*DH_Path*`\uCPSB`
Configuration file	*DH_Path*`\uCPSB\CC\web\containers\jp1dh\webapps\digikatsuwide\digikatsuwide.xml`
Definition file for the JP1/DH Web server	*DH_Path*`\uCPSB\httpsd\conf\httpsd.conf`

Legend:

DH_Path: Installation folder for JP1/DH - Server

#

This file or folder is created when a fixing patch is applied.

B. Changing the Database Communication Port Number

This appendix describes how to change the database communication port number.

Before performing the following steps, you must log in to the JP1/DH - Server machine as a built-in Administrator user (for Windows) or a root user (for Linux).

1. Stop JP1/DH - Server.

   Stop the services of the JP1/DH Web application server and database, as described in *6. Starting and Stopping*.

2. Change the communication port number that the database uses.

   File path

   ```
   installation-folder#\PostgreSQL\9.2\data\postgresql.conf
   ```

   #

   In Linux, change *installation-folder* to `/opt/jp1dh/server`.

   - Setting database communication port number

     Change the communication port number that the database uses.

     ```
     port = port-number           # (change requires restart)
     ```

     Example: To set the port number to 56789

     ```
     port = 56789                 # (change requires restart)
     ```

3. Start the database.

   Start the database, as described in *6. Starting and Stopping*.

4. Change the environment configuration of the JP1/DH Web application server.

   Edit the configuration file of the JP1/DH Web application server to change the port number that the application server uses to communicate with the database.

   File path

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

   #

   In Linux, change *installation-folder* to `/opt/jp1dh/server`.

   - Setting the port number that is used to communicate with the database

     Change the port number used by the application server to communicate with the database.

     ```
     <biz-connect id="bizconnect">
         <persistence>
             <database >
                 ...
                 <url>jdbc:postgresql://localhost:communication-port-number/
     bcdb</url>
             </database>
         </persistence>
     </biz-connect>
     ```

     Example: To set the port number to 56789

```
<biz-connect id="bizconnect">
    <persistence>
        <database >
            ...
            <url>jdbc:postgresql://localhost:56789/bcdb</url>
        </database>
    </persistence>
</biz-connect>
```

5. Start the JP1/DH Web application server.
   Follow the steps in *5.3.2(1) Starting the JP1/DH Web application server*.
6. Prepare for changing the application configuration.
   Follow the steps in *5.3.2(2) Preparing to change the application configuration*.
7. Restart the JP1/DH Web application server.
   Follow the steps in *5.3.2(3) Restarting the JP1/DH Web application server*.
8. Change the configuration of the application.
   Start the command prompt (in Windows) or console (in Linux), and then perform the following:
   - In Windows:

   ```
   set PGPORT=database-communication-port-number
   installation-folder\setup_util\deploy_app.bat
   ```

   - In Linux (if tcsh is used as a login shell):

   ```
   setenv PGPORT=database-communication-port-number
   /opt/jp1dh/server/setup_util/deploy_app.sh
   ```

   - In Linux (if bash
   - is used as a login shell):

   ```
   export PGPORT=database-communication-port-number
   /opt/jp1dh/server/setup_util/deploy_app.sh
   ```

   Follow the given instructions.
9. Stop the JP1/DH Web application server.
   Follow the steps in *5.3.2(5) Stopping the JP1/DH Web application server*.
10. Start the service of the JP1/DH Web application server.
    Start the service of the JP1/DH Web application server, as described in *6. Starting and Stopping*.

Important note

If you change the database communication port number from the initial value, you must set the new database communication port number in the environment variable before executing the following commands:

- *installation-folder*/setup_util/deploy_app.bat
- *installation-folder*/bin/dbbackup.bat
- *installation-folder*/bin/dbchangepassword.bat
- *installation-folder*/bin/dbrestore.bat
- *installation-folder*/bin/getdetaillog_server.bat

- *installation-folder*/bin/regist_users_number.bat

Important note

In Linux, change *installation-folder* to /opt/jp1dh/server and the extension .bat to .sh.

C. Configurations for Clustered System Operations

This appendix provides information about configurations necessary for operations of a clustered JP1/DH - Server system.

C.1 Overview of a cluster system

A cluster system consists of multiple server systems that work together so that they can operate as a single system. If one server fails in a cluster, another can take over the task.

The cluster system is made of one host that processes tasks and another that is waiting so that it can take over in the event of failure. The former host is called an active node, and the latter, a standby node. If a failure occurs on the active node, the standby node takes over the processing to continue tasks. This takeover action is called failover.

A failover is performed based on a logical node, which is a logical host. Applications in a cluster system must run within a logical host environment in order to fail over to continue tasks. When the applications run on a logical host, they are independent of a physical server machine, allowing them to run on any server machine.

A logical host consists of three components: applications running as a service or daemon, shared disk, and a logical IP address. The applications, such as JP1/DH - Server services, store their data in the shared disk and use the logical IP address to communicate with other applications.

The following table lists and describes each component of the logical host.

Table C–1: Components of a logical host

No.	Logical host component	Description
1	Service or daemon	JP1/DH - Server applications running in a cluster system. If an active logical host fails, a standby logical host starts the services or daemons with the same name and takes over.
2	Shared disk	Disk unit connected to both the active and standby systems. It contains information for failover operations, such as definitions and operating status. In the event of a failure in an active logical host, the standby logical host is connected to the shared disk as the active host.
3	Logical IP address	An IP address allocated to a running logical host. If the active node fails, then the same logical IP address is allocated to the standby node. Therefore, clients can continue access via the same IP address as if only one node is always running.

C.2 Supported clustering software

To run the JP1/DH - Server system in a cluster environment, you must use a specific clustering software product for each operating system on which the system runs.

The following table lists clustering software supported by JP1/DH - Server.

Table C–2: Clustering software supported by JP1/DH - Server

No.	OS	Clustering software
1	Windows Server 2008 R2 Standard (Service Pack 1)	Not supported
2	Windows Server 2008 R2 Enterprise (Service Pack 1)	WSFC#
3	Windows Server 2008 R2 Datacenter (Service Pack 1)	WSFC#

No.	OS	Clustering software
4	Windows Server 2012 Standard	WSFC#
5	Windows Server 2012 Datacenter	WSFC#
6	Windows Server 2012 R2 Standard	WSFC#
7	Windows Server 2012 R2 Datacenter	WSFC#
8	Red Hat Enterprise Linux 5	HA Monitor
9	Red Hat Enterprise Linux 6	HA Monitor

#

Every node must be running the same version of Windows Server and be a member of the same Active Directory domain.

We recommend that you have a different server machine to run Active Directory, instead of using a clustered JP1/DH - Server machine. For details, see the documentation provided by your clustering software product.

C.3 Prerequisites for the cluster system

To run the JP1/DH - Server system in a cluster environment, two or more server machines with the shared disk connected must be configured to form a cluster. The following table lists and describes the prerequisites for the cluster system.

Table C–3: Prerequisites for the cluster system

No.	Item	Description
1	System configuration	• The system must consist of two or more server machines that share a disk. • A JP1/DH - Server machine in the cluster must be accessible to clients via a logical IP address, which must be able to be shared between servers. • The shared disk must be set up with common data. For details about data stored in the shared disk, see *C.6 Data stored on the shared disk*.
2	Shared disk	• The shared disk must be shared between the active and standby system nodes. • The shared disk must be under exclusive control so that it cannot be concurrently accessed by multiple servers. • Data written to files must be consistent and inherited by the standby node during a failover. • If the shared disk is in use by a process during a failover, the failover must be forced to be completed. • The shared disk must meet the hardware requirements.
3	Hardware	• The hardware must comply with the hardware requirements for your clustering software. For details about the clustering software supported by JP1/DH - Server, see *C.2 Supported clustering software*.
4	Software	• The software must comply with the software requirements for your clustering software. • For details about the clustering software supported by JP1/DH - Server, see *C.2 Supported clustering software*.
5	Setup	• JP1/DH -Server cluster setup instructions must be followed to set up your JP1/DH - Server environment.

C.4 Redundant components in a cluster

The following table lists and describes redundant components in the JP1/DH - Server cluster configuration.

Table C–4: Redundant components in the cluster

No.	Component	Description	Clustered
1	NIC	Used to provide a host address and an IP address for accepting service requests.	Yes
2	NIC (for heartbeats)	Used for the alive monitoring of the machine.	No
3	Clustering software	Clustering software that provides redundancy. For details about the clustering software supported by JP1/DH - Server, see *C.2 Supported clustering software*.	Yes
4	IP address for accepting service requests	An IP address, which is allocated to a clustered JP1/DH - Server environment, accessible to clients. Service requests reach the NIC on the machine running the clustering software.	Yes
5	Runtime libraries for managed applications	A set of files necessary to run applications managed by your clustering software. In a Windows environment, these are mainly services.	Yes
6	Managed applications	Applications managed by your clustering software. In a Windows environment, these are mainly services.	Yes
7	Other non-managed applications	A set of applications installed in your operating system by default.	No
8	Shared disk (for application data)	A shared disk that stores application data, specified by the runtime libraries for the managed applications.	--
9	Shared disk (for cluster management)	A set of files for managing the cluster configuration used by your clustering software (WSFC-specific).	--
10	Domain controller	A domain controller used for managing an account that your clustering software uses (WSFC-specific).	No

Legend:

Yes: It is included in the cluster.

No: It is not included in the cluster.

--: It is not supported by the clustering software.

C.5 Licenses

The following table lists and describes licenses required to run your JP1/DH - Server system in the cluster.

Table C–5: Licenses

No.	Item	Description
1	OS	The operating system must comply with licensing structure of your operating system.
2	Clustering software	The clustering software must comply with the licensing structure of your clustering software. For any use of software that the clustering software requires, the software must comply with the licensing structure of your clustering software.
3	JP1/DH - Server	The active and standby systems must have their own full package licenses. Also, the number of user licenses that comes with the full package license (100 licenses) will be invalid. You must purchase as many additional user licenses as you use in your cluster environment.

C.6 Data stored on the shared disk

In the cluster configuration, the information that needs to be shared by every cluster node must be stored on the shared disk. The following table lists and describes data to be stored on the shared disk in the JP1/DH - Server cluster configuration.

Table C–6: Data to be stored on the shared disk

No.	Item	Description
1	Storage folder for delivery data	A folder to store data sent and received by JP1/DH - Server. The `<directory></directory>` element in the configuration file `digikatsuwide.xml` specifies this folder.
2	Audit log folder	A folder to store the JP1/DH - Server audit log file. The `log.file` directive in the configuration file `ROOT_SERVICE.srv` specifies this folder.
3	Data area in the database	Data area in the database. The startup option D of the database service specifies this value.
4	A complete set of certificates and keystore	Certificates and keystores used in the JP1/DH - Server system over SSL connections.

C.7 How to access the cluster environment

When WSFC is used, clients must access the cluster environment via a logical IP address managed by your clustering software. The clustering software converts the logical IP address into a physical server address so that the clients do not need to be aware of the physical address.

When HA Monitor is used, multiple IP addresses are allocated to a single physical NIC.

C.8 Failover limitation

In the cluster configuration, your clustering software detects any failed application and resource failure. When the clustering software detects the failure, it provides failover. However, different clustering software can detect different ranges and types of failures. This means that a user operation upon the failure cannot always be continued after the failover process.

C.9 Use of WSFC

(1) Accounts used in the cluster configuration

For WSFC, you can use a Local System account for services even in the cluster configuration. The account of each service is not changed in this configuration. The following table lists and describes accounts used in the JP1/DH - Server system.

Table C–7: Accounts used in the cluster configuration

No.	Account	Description
1	Local System (or System)	Used as an account to run the JP1/DH - Server application and reverse proxy processes.

No.	Account	Description
1	Local System (or System)	This account must have full control permissions for the installation folder and shared disk.
2	User account used to create a cluster	Used when a WSFC cluster is set up. This account must belong to the Domain Admins group.
3	Cluster account	Computer account for the cluster itself.
4	Computer account for clustered services or applications	Computer account used for clustered services or applications.
5	postgres	Used as an account to run the database. This account must have read or write permission for the shared disk.

(2) Registry key used in the cluster configuration

In the default JP1/DH - Server configuration, the startup option D of the database is stored in the registry key. You must change the value of the following registry key from the installation drive to the shared disk:

```
\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\JP1_DH_DATABASE_SVR
\ImagePath
```

An example is shown as follows:

From

```
C:/Program Files/Hitachi/jp1dh/server/PostgreSQL/9.2/bin/pg_ctl.exe
runservice -N "JP1_DH_DATABASE_SVR" -D " C:/Program Files/Hitachi/jp1dh/
server/PostgreSQL/9.2/data" -w
```

To

```
C:/Program Files/Hitachi/jp1dh/server/PostgreSQL/9.2/bin/pg_ctl.exe
runservice -N "JP1_DH_DATABASE_SVR" -D "I:/PostgreSQL/9.2/data" -w
```

(3) Settings for each generic service

All JP1/DH - Server applications are installed as Windows services. The following tables list and describe the settings for each service.

Table C–8: Database service settings

No.	Category	Item	Value
1	General	Resource Name	JP1_DH_DATABASE_SVR
2		Resource type	Generic Service
3		Service name	JP1_DH_DATABASE_SVR
4		Startup parameters	*JP1/DH-Server-installation-folder*`\PostgreSQL\9.2\bin\pg_ctl.exe" runservice -w -N "pgsql-9.2" -D "I:\PostgreSQL\9.2\data\`
5		Use Network Name for computer name	Selected
6	Dependencies	Service name and conditions	Cluster disk name AND cluster network name

No.	Category	Item	Value
7	Policies	Response to resource failure	If resource fails, attempt restart on current node
8		Period for restarts (mm:ss)	15:00 (default)
9		Maximum restarts in the specified period	1 (default)
10		If restart is unsuccessful, fail over all resources in this service or application	Selected (default)
11		If all the restart attempts fail, begin restarting again after the specified period (hh:mm)	01:00 (default)
12		Pending timeout (mm:ss)	03:00 (default)
13	Advanced Policies	Possible Owners	Node 001 Node 002
14		Basic resource health check interval	Use standard time period for the resource type
15		Thorough resource health check interval	Use standard time period for the resource type
16		Run this resource in a separate Resource Monitor	Not selected
17	Registry Replication		Not specified

Table C–9: Service settings for the JP1/DH Web application server

No.	Category	Item	Value
1	General	Resource Name	JP1_DH_WEB CONTAINER
2		Resource type	Generic Service
3		Service name	JP1_DH_WEBCON
4		Startup parameters	*JP1/DH-Server-installation-folder*`\sbin\jp1dhwebcon.exe" -start`
5		Use Network Name for computer name	Not selected
6	Dependencies	Service name and conditions	JP1_DH_DATABASE_SVR
7	Policies	Response to resource failure	If resource fails, attempt restart on current node
8		Period for restarts (mm:ss)	15:00 (default)
9		Maximum restarts in the specified period	1 (default)
10		If restart is unsuccessful, fail over all resources in this service or application	Selected (default)
11		If all the restart attempts fail, begin	01:00 (default)

No.	Category	Item	Value
11	Policies	restarting again after the specified period (hh:mm)	01:00 (default)
12		Pending timeout (mm:ss)	03:00 (default)
13	Advanced Policies	Possible Owners	Node 001 Node 002
14		Basic resource health check interval	Use standard time period for the resource type
15		Thorough resource health check interval	Use standard time period for the resource type
16		Run this resource in a separate Resource Monitor	Not selected
17	Registry Replication		Not specified

Table C–10: Service settings for the JP1/DH Web server

No.	Category	Item	Value
1	General	Resource Name	JP1_DH_WEB SVR
2		Resource type	Generic Service
3		Service name	JP1_DH_WEBSVR
4		Startup parameters	Not specified
5		Use Network Name for computer name	Not selected
6	Dependencies	Service name and conditions	JP1_DH_WEB CONTAINER
7	Policies	Response to resource failure	If resource fails, attempt restart on current node
8		Period for restarts (mm:ss)	15:00 (default)
9		Maximum restarts in the specified period	1 (default)
10		If restart is unsuccessful, fail over all resources in this service or application	Selected (default)
11		If all the restart attempts fail, begin restarting again after the specified period (hh:mm)	01:00 (default)
12		Pending timeout (mm:ss)	03:00 (default)
13	Advanced Policies	Possible Owners	Node 001 Node 002
14		Basic resource health check interval	Use standard time period for the resource type
15		Thorough resource health check interval	Use standard time period for the resource type

No.	Category	Item	Value
16	Advanced Policies	Run this resource in a separate Resource Monitor	Not selected
17	Registry Replication		Not specified

(4) Notes on the cluster configuration

- A cluster configuration managed by WSFC requires Active Directory.
- If your JP1/DH - Server applications run on Windows Server 2012 or Windows Server 2012 R2, a domain controller must be running on a separate machine.
- When you restart a clustered system, do not restart multiple machines at the same time. They must be restarted one by one.

(5) Setup

This subsection describes how to set up a WSFC cluster configuration.

For this configuration, every node must be running the same version of Windows Server and be a member of the same Active Directory domain.

1. Prepare a set of hardware components used to configure the cluster. The necessary set of components is as follows:
   - More than one machine
   - Shared disk (SCSI-connected)
   - Switch
   - Network interface card (NIC)

   Except for the shared disk, prepare as many hardware devices as the number of the machines. In addition, one machine requires two or more network interface cards.
2. Determine the Active Directory domain that your cluster belongs to.
   Consider joining the existing Active Directory domain if you have one. If the existing domain cannot be used, or if one does not exist, create a new Active Directory domain for your cluster configuration.
3. If you create a new Active Directory domain, determine where Active Directory will be installed.
   Prepare a dedicated machine for Active Directory and then install Active Directory.

   > **Important note**
   >
   > Although running Active Directory on a different node from the JP1/DH - Server node in the cluster configuration is possible, we do not recommend this.
4. Install the Failover Clustering feature in all nodes so that they can join the cluster configuration.
   For details about the Failover Clustering feature, see the *Windows Help*.

C.10 Using HA Monitor

(1) Failure detection

To detect server failures by using HA Monitor, you must write some monitoring commands in C language or shell language.

The commands are activated by HA Monitor, and they remain active while the server is up and running. When any of the commands terminates, HA Monitor assumes that a failure has occurred and starts a failover process.

An example monitoring command provided by HA Monitor is shown below. This example command checks for the process of the target program, and if no process exists, then you can assume that a failure occurred on the server.

```
#!/bin/sh
SERVER=/home/xxxx/yyyy   # Name of the program running on your server
while true                # Main loop
do
    # Use the ps command to check for the process of the program.
    CHECK=`ps -ef | grep $SERVER | grep -v grep`

    # If no process is found, exit the command.
    if [ "$CHECK" = "" ]
    then
        exit 0
    fi

    # If the process is found, keep monitoring.
done
```

JP1/DH - Server uses the Linux standard `ps` command to monitor daemons. It checks the output of the command to determine whether the daemons associated with the JP1/DH - Server system are running.

C.11 Non-redundant functions

The following table lists and describes functions that are not redundant even in the clustered JP1/DH - Server configuration.

Table C–11: Non-redundant functions

No.	Function	Description
1	What's new function	The same configuration is required for both the active and standby nodes.
2	Dynamic changes in system parameters	After every switchover between the active and standby nodes, system parameters must be set by using the dynamic change function.

C.12 Building the cluster system

(1) General procedure for installing JP1/DH - Server on the cluster system

After you make sure that the prerequisites are met, you can install JP1/DH - Server on each of the active and standby nodes.

1. Make sure that the installation prerequisites are met.
2. Install JP1/DH - Server.

(2) Installation prerequisites

To install JP1/DH - Server on the cluster system, you need to have the required installation environment, and the environment must be configured appropriately.

(a) Operating system and clustering software

- Your operating system and clustering software must match one of the clustering software products listed in *C.2 Supported clustering software*.
- Any patches, updates, and service packs that JP1/DH - Server and your clustering software require must be applied.

(b) Configuration

- Each node must have the same environment so that the standby node can take over the existing task after a failover.
- A cluster must contain two or more nodes.

(c) Disk

- Files must be protected by an appropriate means, such as a journaling file system, to avoid file loss due to a system down.

(d) Network

- IP addresses that correspond to host names (returned by the `hostname` command) must be used for communications. Your clustering software and any other software must not block traffic.
- Your clustering software and name server must not change the mapping of a host name to an IP address while the JP1/DH - Server system is running.
- The NIC corresponding to the host name must have the highest priority in the network binding setting. Other NICs, such as a NIC for heartbeats, must have a lower priority.

(e) Shared disk

- You need to make sure that all the criteria below are fulfilled, so that data written by the active node is not corrupted during failover. If they are not fulfilled, the JP1/DH - Server system might experience problems, such as an error, data loss, and failed startup, resulting in a malfunction of the system.
    - JP1/DH - Server must not be installed on the shared disk.
    - The shared disk must be shared between the active and standby nodes.
    - The shared disk must be allocated to the JP1/DH - Server system before the system starts.
    - The shared disk must not be unallocated while the JP1/DH - Server system is running.
    - The shared disk must be under exclusive control so that it cannot be concurrently accessed by multiple servers.

- Files must be protected by an appropriate means, such as a journaling file system, to avoid file loss due to a system down.
- Data written to files must be consistent and inherited by the standby node during a failover.
- If the shared disk is in use by a process during a failover, the failover must be forced to be completed.
- Your clustering software must have the ability to start and stop the JP1/DH - Server processes for recovery if necessary, when a failure is detected on the shared disk.

(f) Logical host name and IP address

- You need to make sure that the criteria below must be fulfilled, so that a recovery action is performed after one of the NICs is failed. If they are not fulfilled, a communication error occurs and the JP1/DH - Server system might malfunction until the NIC is switched over or the active node is failed over to the standby node by, for example, the clustering software.
  - The logical host name must contain only alphanumeric characters and hyphens (-).
  - A logical IP address that can be inherited by the standby node is available for communications.
  - A logical host name must have a one-to-one relationship with a logical IP address.
  - The logical host name must be in the `hosts` file or in the name server so that TCP/IP communication is possible.
  - The logical IP address must be allocated to JP1/DH - Server before the system starts.
  - The logical IP address must not be removed while the JP1/DH - Server system is running.
  - The mapping of the logical host name to the logical IP address must not be changed while the JP1/DH - Server system is running.
  - Your clustering software or other software must be responsible for a recovery action when a network failure is detected, and the JP1/DH - Server system does not have to be conscious about it. Also, the clustering software must have the ability to start and stop the JP1/DH - Server processes in the process of the recovery action, if necessary.

(g) Port management

The active and standby nodes must have the same port number configured for connecting to the Web server. If they have different port numbers set, a Web browser cannot display the JP1/DH - Server web windows after a failover. When you change the port number, set the same port number for both the active and standby nodes.

(3) Installing JP1/DH - Server on clustered nodes

The steps below describe how to install JP1/DH - Server on the active and standby nodes.

In conditional steps with "In WSFC" or "In HA Monitor", perform those steps only for your matching clustering software.

1. Make sure that JP1/DH - Server is *not* installed on the active and standby nodes. If the product is installed on any of the nodes, uninstall it.
2. Install JP1/DH - Server on the active and standby nodes.

   In WSFC:

      Log in to JP1/DH - Server as a built-in Administrator user.

   In HA Monitor:

      Log in as the root user.

   JP1/DH - Server must be installed to the same folder on the drive with the same name on each of the active and standby nodes.

To install JP1/DH - Server in the cluster system, you need to perform the new installation procedure. For details, see *5. Installation and Setup*.

3. On the active node, move the database data folder to the shared disk. If the database is up and running, shut down the database before moving the folder.

   From: *JP1/DH-Server-installation-folder*`\PostgreSQL\9.2\data`

   To: *shared-disk*`\PostgreSQL\9.2\data`

   After the data folder is moved, set permission to access the moved folder.

   In WSFC:

   Grant the full control permission to the `postgres` account.

   In HA Monitor:

   Use the following commands to change the owner and group to `postgres`:

   ```
   >chown -R postgres /shared-disk/PostgreSQL/9.2/data
   >chgrp -R postgres /shared-disk/PostgreSQL/9.2/data
   ```

4. Change the path to the data folder specified in the database startup option. The path must be changed on both the active and standby nodes. You need to perform different steps to change the startup option depending on your clustering software.

   In WSFC:

   The startup option is defined in the registry key. So you will change the value of the corresponding registry key. For details about the path to the registry key and changes to be made, see *C.9(2) Registry key used in the cluster configuration*.

   In HA Monitor:

   The startup option is defined in the `JP1_DH_DATABASE_SVR` script file to start and stop the service. In the cluster configuration, a separate file, with the shared disk specified in the startup option, is used to start and stop the service.

   The file used in the cluster configuration is stored in the following folder:

   ```
   /opt/jp1dh/server/sbin/cluster/
   ```

   Change the value of the `PGSQLDIR_D` variable in the `JP1_DH_DATABASE_SVR` file to the path to the database data folder on the shared disk.

   After you changed the path, perform the following command on the active node:

   ```
   >/JP1/DH-Server-installation-folder/sbin/cluster/JP_DH_DATABASE_SVR
   start
   ```

   The database starts by using the modified `JP1_DH_DATABASE_SVR` file.

5. Configure the active and standby server environments. Follow the steps described in *5.3.1 Changing the configuration file*. In the cluster configuration, however, some of the configuration steps are different from those in the non-cluster configuration. You must be aware of the following:

   - Specify the logical IP address for the server IP address, instead of the IP address of the host machine. The element in the configuration file is `<ip>`.

   - Specify the FQDN corresponding to the logical address for the server FQDN, instead of the FQDN of the host machine. The elements in the configuration file are `<bind-hostname>`, `<bind-domainname>`, and `<bind-sub-domainname>`.

   - Specify the path on the shared disk for the storage folder for delivery data. The element in the configuration file is `<directory>`.

- Change the audit log output destination folder to the path on the shared disk. Define this folder in the following file:

  installation-folder`\misc\digikatsuwide\digikatsuwide\WEB-INF\services\ROOT_SERVICE.srv`

  Change the value of the `log.file` directive in the configuration file to the path on the shared disk.

  `log.file =` *shared-disk*`\log\jp1dh-audit.log`

6. On the active node, change the JP1/DH - Server application configuration. The configuration on the standby node will be changed in a later step. In this step, only change the configuration of the active node.

   In WSFC:

   In the **Start** menu for the Windows machine, right-click **Command Prompt** and select **Run as Administrator** in the context menu. Perform the steps described in *5.3.2 Changing the application configuration*.

   In HA Monitor:

   Perform the steps described in *5.3.2 Changing the application configuration*.

7. Before changing the application configuration on the standby node, change the current owner of resources, including the shared disk and network, from the active node to the standby node.

   In WSFC:

   As described in step 6, change the JP1/DH - Server application configuration on the standby node.

   After the change is done on the standby node, change the current owner of the resources from the standby node to the active node.

   In HA Monitor:

   On the active node, run the following command to shut down the database.

   ```
   >/JP1/DH-Server-installation-folder/sbin/cluster/JP_DH_DATABASE_SVR
   stop
   ```

   When the database is stopped, the shared disk needs to be mounted to the standby node so that the standby node can use the disk. To mount the disk to the standby node, use the `umount` command on the active node, and then use the `mount` command on the standby node.

   When the task is completed, run the following command on the standby node to start the database.

   ```
   >/JP1/DH-Server-installation-folder/sbin/cluster/JP_DH_DATABASE_SVR
   start
   ```

   When all the tasks are completed on the standby node, use the same command described above to shut down the database on the standby node. Then, unmount the shared disk from the standby node and mount it back to the active node. Finally, start the database on the active node.

8. On the active node, configure settings for the electronic certificate authentication function. Follow the steps described in *5.3.3 Specifying the settings for the electronic certificate authentication function*.

9. Register the root certificate in the active and standby nodes. Follow the steps described in *5.3.4 Registering a root certificate*.

   You need to perform this step to encrypt mail server traffic via SSL (SMTPS/STARTTLS) when the delivery notification function is used. Also, perform this step to encrypt directory server traffic via SSL when a directory server is used to authenticate users who try to log in to the system.

10. Edit the `hosts` file on the active and standby nodes. Follow the steps described in *5.3.5 Editing the hosts file*.

11. On the active node, create a certificate file used for SSL communication. Follow the steps described in *5.4.1 Creating a secret key file for SSL communication*, *5.4.2 Creating a password file*, and *5.4.3 Creating a certificate file for SSL communication*.

In the cluster configuration, however, some of the configuration steps are different from those in the non-cluster configuration. Specify the host name (FQDN) corresponding to the logical address for the server host name (FQDN), instead of the IP address of the host machine.

12. Store all the files created in step 10 in the shared disk.
13. Edit your JP1/DH Web server configuration files on the active and standby nodes. Follow the steps described in *5.4.4 Editing the settings for the JP1/DH Web server*.

    In the cluster configuration, however, some of the configuration steps are different from those in the non-cluster configuration. Specify the host name (FQDN) corresponding to the logical address for the server host name (FQDN), instead of the IP address of the host machine. Also, store the certificate in the shared folder, and set the path to the certificate folder to the path on the shared folder.

    In WSFC:

    To run the batch file `deploy_websvr.bat`, in the **Start** menu, find and right-click **Command Prompt**, select **Run as Administrator** in the context menu, and run the batch file in the displayed command prompt.

    In HA Monitor:

    Log in as the root user to edit the file.

C.13 Registering services to cluster software

Register the JP1/DH - Server services to your clustering software.

(1) In WSFC:

Register the following services by using the Failover Cluster Manager. All the services must be created as a Generic Service Resource.

- `JP1_DH_DATABASE_SVR`

  For details about the settings, see *Table C-8 Database service settings*.
- `JP1_DH_WEB_CONTAINER`

  For details about the settings, see *Table C-9 Service settings for the JP1/DH Web application server*.
- `JP1_DH_WEB SVR`

  For details about the settings, see *Table C-10 Service settings for the JP1/DH Web server*.

(2) In HA Monitor:

Specify the following paths to files used by HA Monitor in the server configuration file `servers`.

Each file can be found in the `/opt/jp1dh/server/sbin/cluster` directory.

- Server program (which is the startup command)

  Set the `name` directive in the `servers` file to `/opt/jp1dh/server/sbin/cluster/JP1_DH_CLUSTER_START`.
- Command to shut down the server

  Set the `termcommand` directive in the `servers` file to `/opt/jp1dh/server/sbin/cluster/JP1_DH_CLUSTER_STOP`.
- Monitoring command

Set the `patrolcommand` directive in the `servers` file to `/opt/jp1dh/server/sbin/cluster/JP1_DH_CLUSTER_PATROL`.

In the cluster configuration, HA Monitor starts and stops the services. Thus, the automatic service startup mechanism, which is used in the non-cluster configuration, must be turned off by executing the following commands:

```
>/JP1/DH-Server-installation-folder/sbin/chkconfig JP1_DH_DATABASE_SVR off
>/JP1/DH-Server-installation-folder/sbin/chkconfig JP1_DH_WEBCON off
```

C.14 JP1/DH - Server operations in the cluster

In a cluster system managed by clustering software, usually the software is responsible for detecting failure and switching the system.

What failures can be detected is determined by each clustering software and its settings. In this appendix, a failure is determined by checking whether service processes are running, as described in *C.9(3) Settings for each generic service* and *C.10(1) Failure detection*.

This approach might be a less accurate way of monitoring services. Sometimes an application cannot service its users even when its process is still running.

You can identify failures with higher accuracy by using the JP1/DH - Server commands.

To identify failures with higher accuracy, a system administrator must perform either of the following:

- Change how your clustering software identify failures.

  Customize monitoring scripts used by the clustering software for detecting failures. This means that JP1/DH - Server commands are used in the monitoring script. A successful command will allow processing to proceed, and a failed command will raise an error.

  Note that different clustering software have different monitoring script functions. For details, see the documentation of your clustering software.
- Monitoring and detecting failures separately of the monitoring functionality of the clustering software.

  Use the JP1/DH - Server commands to create scripts. These scripts can execute the JP1/DH - Server commands, and send an email notification to a system administrator if the script fails. The scripts must be run on a regular basis by using, for example, a task scheduler.

The major difference between the two approaches above is whether the clustering software switches the system when a JP1/DH - Server command fails.

In the first approach, the software switches the system immediately after the JP1/DH - Server command fails. However, even if the command fails, the application might be able to provide its service (including changing the configuration for authentication rules and delivery rules). Any operation during system switchover causes an error, which might result in a shorter service time.

In the second approach, the software does not switch the system. Thus, when receiving the notification, a system administrator must check what type of error exists, and manually switch the system if a failure actually occurs. This procedure takes some time to switch the system, but the switchover can be performed only when the service is unavailable.

However, the system administrator is unaware of a failure occurring, without email notifications sent by a script or some other means. If you employ the second approach, make sure that the system administrator is notified of any failure in a way such as email notification.

For the first approach, the system administrator must be familiar with the specifications of monitoring scripts provided by the clustering software. Therefore, we recommend the second approach in a clustered JP1/DH - Server configuration if you need a higher accuracy of failure detection.

In a cluster configuration described in this appendix, the clustering software detects a failure by checking whether JP1/DH - Server application processes are running. What is necessary for failure detection depends on how you operate your system. See the documentation of your clustering software to configure failure detection suitable for your operations.

D. Installing .NET Framework 3.5

If you are using Windows Server 2012 or Windows Server 2012 R2, you must install Microsoft .NET Framework 3.5 to open a command prompt with the elevated privileges. You can use **Add Roles and Features Wizard** to install .NET Framework 3.5 Features.

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 System Administrator Guide* (3021-3-359(E))
- *Job Management Partner 1 Version 10 Job Management Partner 1/Data Highway - Server Administrator Guide* (3021-3-360(E))
- *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 following abbreviations for product names:

Full name or meaning	Abbreviation
Job Management Partner 1/Automatic Job Management System 3	JP1/AJS3
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
DB	Database
DMZ	De-Militarized Zone
FQDN	Fully Qualified Domain Name
JDK	Java Development Kit
NIC	Network Interface Card
OS	Operating System
SQL	Structured Query Language
SSL	Secure Socket Layer

Acronym	Full name or meaning
RPM	Redhat Package Manager
SCSI	Small Computer System Interface
WSFC	Windows Server Failover Clustering
WSH	Windows Script Host

E.4 Default installation folder

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

In Windows:

```
system-drive:\Program Files\Hitachi\jp1dh\server
```

In Linux:

```
/opt/jp1dh/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.

Index