**SHARP**

# Audit Log Reference Guide

# Contents

Sharp Corporation

# Preface

Thank you for selecting our product.

This guide describes the overview of the audit log and the content recorded in the audit log for the system administrator. Before using the machine, please read this manual thoroughly. Be sure to keep this manual for future reference.

The guide assumes that you are familiar with a personal computer and that you are knowledgeable of computer networks. When you need additional information, refer to the manuals provided with the personal computer, operating system, and network products.

Sharp Corporation

Important
1. This manual may not be edited, modified or copied in whole or part without the written consent of the publisher.
2. Some parts of this manual are subject to change without prior notice.
3. The screen shots and the illustrations in this manual are used as examples. They may differ from yours depending on the model, the software, or the OS.

All product and company names are registered trademarks or trademarks of their respective owners.

# Using This Guide

The guide describes the functions and format of the audit log.

## Organization of This Guide

This guide consists of the following chapters:

### 1 Overview of Audit Log

Describes the overview and functions of the audit log.

### 2 Items Stored in Audit Log

Describes the items recorded in the audit log.

## Conventions

- The following terms are used in this guide:

  **Important**
  - Indicates important information you have to know or be reminded before operations.

  **Note**
  - Indicates supplemental information useful for operations.

  **Refer**
  - Indicates reference destinations.

- The following symbols are used in this guide:

  " " 
  - A cross-reference included in this guide.
  - Names of media, features, and touch screen messages and input text.

  [ ]
  - Names of buttons and menus displayed on the touch screen.

- The items or format of the audit log to be saved may vary depending on the model.

# 1    Overview of Audit Log

## 1.1    Audit Log

Audit logs are the time-series records of important events (hereafter referred to as "audit event") that occurred in device, such as trouble, configuration change, and user operation, in which "who", "what", "when", and "result" are described.

The audit-log function is used for security audit for detecting the user's illicit usage.

## 1.2    Function of the Audit Log

### Storing the audit log

The device stores audit events that occur on the device as the audit logs.

Up to 15,000 audit logs can be saved in the device and when the number reaches 15,000, the device overwrites the logs in chronological order.

When no storage is installed on the device, a maximum of 50 logs can be stored.

To store the audit logs, enable the audit log settings on the device or Internet Services.

### Exporting the audit log

The audit logs stored in the device can be exported from Internet Services in text file format.

### Sending the audit log to the Syslog server

The audit logs stored in the device can be sent by Syslog transfer (transferred to the other computers on the network in the Syslog protocol).

The Syslog transfer setting is available on device.

> **Refer**
> - For information on the setting on the device, refer to the manual of the device.
> - For information on the setting on Internet Services, refer to the help of Internet Services.

# 1.3　Format of the Exported Audit Log

## Header information

| Item | Format | Description |
|---|---|---|
| Format Version | Integer | The setting value is "3" |
| Device's IP Address | Character string that consists of half-size alphanumeric characters (a to z, 0 to 9), dot(.), colon(:) | Displays the IP address (IPv4 or IPv6) |
| Coding Method | String | Fixed to UTF-8 |
| Time Zone | -720 to 720 | Displays time difference based on GMT The unit is minute, and the value is negative if the time zone is west of Meridian. |
| Date Format | YYYY/MM/DD, MM/DD/YYYY, or DD/MM/YYYY | |

## Audit log information

| Item | Format | Description |
|---|---|---|
| Log ID | Integer (1 to 60000) | ID that is assigned when audit event occurs is exported |
| Date | String | Date of audit-event occurrence is exported |
| Time | hh:mm:ss | Time of audit-event occurrence (hour, minute, and second) is exported |
| Audit Event ID | Hexadecimal integer (0x0000 to 0xffff) | ID that corresponds to audit event is exported |
| Logged Events | String | A string representing the type of the audit event is exported |
| User Name | String | A string* representing the user who caused the audit event is exported |
| Description | String | A string that describes the details of the audit event is exported |
| Status | String | Character string that represents the status or processing result of occurred audit-event is exported |
| Optionally Logged Items | String | Optionally logged information of audit event is exported |

\*　:Default action: user ID
　　When the user ID is unknown: user name
　　When both the user ID and user name are unknown: -
　　System administrator: KO
　　Customer engineer: CE
　　Unregistered user: Guest
　　When system internal operation triggered the event: System
　　When the event is triggered via NMP: SNMP: admin

# 1.4 Message Format for Syslog Transfer of Audit Log

| Item | Format | Description |
|---|---|---|
| Priority | Integer | Integer calculated with the following expression<br>Facility << 3 \| Severity<br><br>**Note**<br>• Facility can be set in the device.<br>• Severity is fixed to "6". |
| Version | 1 | Fixed to "1" |
| Date/Time | yyyy-mm-ddThh:mm:ssZ | Date and Time (hour, minute, and second) of audit-event occurrence<br>The time zone is UTC. |
| Device Information | For FQDN and host name:<br>String<br>For IPv4 address:<br>nnn.nnn.nnn.nnn | - |
| App-Name | - | Fixed to "-" |
| ProcId | - | Fixed to "-" |
| MsgId | - | Fixed to "-" |
| Structured-Data | - | Fixed to "-" |
| Audit-log ID | ID=nnnnnn | ID that is assigned when audit event occurs is exported |
| User Name | UserName=String | A string representing the user who caused the audit event is exported<br><br>**Refer**<br>• Audit log information (P.5) |
| Logged Events | Event=String | ID that corresponds to audit event is exported |
| Logged Event Description | Description=String | A string that describes the details of the audit event is exported |
| Status | Status=String | Character string that represents the status or processing result of occurred audit-event is exported |
| Optionally Logged Item | OptItems=String | Optionally logged information of the audit event is exported |

# 2 Items Stored in Audit Log

## 2.1 Change of Device Status

| Item | Description |
|---|---|
| Audit Event ID | 0x0101 |
| Logged Events | "System Status" |

## Start/stop of Device Operation

### Normal cold-booting

| Item | Description |
|---|---|
| Date/Time | When device status becomes "Ready" |
| User Name | "-" |
| Description | "Started normally (cold boot)" |
| Status | "-" |
| Optionally Logged Items | "-" |

### Normal warm-booting

| Item | Description |
|---|---|
| Date/Time | When device status becomes "Ready" |
| User Name | "-" |
| Description | "Started normally (warm boot)" |
| Status | "-" |
| Optionally Logged Items | "-" |

### Booting due to forced initialization of the log

| Item | Description |
|---|---|
| Date/Time | When device status becomes "Ready" |
| User Name | "-" |
| Description | "Started (NVM initialized)" |
| Status | "-" |
| Optionally Logged Items | "-" |

### Booting due to forced initialization of the storage

| Item | Description |
| --- | --- |
| Date/Time | When device status becomes "Ready" |
| User Name | "-" |
| Description | "Started (Storage initialized)" |
| Status | "-" |
| Optionally Logged Items | "-" |

### Shutdown

| Item | Description |
| --- | --- |
| Date/Time | When device detects a request to turn off the power |
| User Name | "-" |
| Description | "Shutdown requested" |
| Status | "-" |
| Optionally Logged Items | **Action**<br>Up to 64 bytes, excluding the null-terminated string<br>When failure recovery is done, describe as "Recovered from failures"<br>Otherwise, describe as "-" |

# Self Test

### Result of Self Test

| Item | Description |
| --- | --- |
| Date/Time | Just before the device becomes "Ready" |
| User Name | "-" |
| Description | "Self Test" |
| Status | "Successful" or "Failed" |
| Optionally Logged Items | **Checksum of ROM Image1**<br>**Checksum of ROM Image2** |

# 2.2 Login/Logout

| Item | Description |
|---|---|
| Audit Event ID | 0x0201 |
| Logged Events | "Login/Logout" |

## User authentication

### Login

| Item | Description |
|---|---|
| Date/Time | When user-authentication result is fixed |
| User Name | User ID of the corresponding login |
| Description | "Login" |
| Status | "Successful", "Failed(Invalid UserID)", "Failed(Invalid Password)" or "Failed" |
| Optionally Logged Items | **Access method**<br>"Local", "Web User Interface" or "Printer Driver"<br><br>**Host name**<br>Up to 45 bytes, excluding the null-terminated string<br>IP address<br><br>Note<br>• When the IP address is unknown, it is a local access, or Private Charge Print authentication fails, describe as "-".<br><br>**Authentication method**<br>"Local", "Remote" or "Custom"<br><br>**Role**<br>"System Administrator", "Accounting Administrator", "Customer Engineer", "Customer Engineer (Unlimited Operation)", "Casual Operator" or "-"<br><br>Note<br>• When login fails, describe as "-".<br>For the system administrator, describe as "System Administrator"; for the customer engineer, describe as "Customer Engineer"; and for local users and unregistered users, describe as "Casual Operator". |

Note
- When Private Charge Print authentication fails, an audit log is recorded only when the following all conditions are satisfied.

    - Private Charge Print is enabled and [Charge / Private Print Settings] is set as follows:

        -[Receive Control]          :[Control by Job Login Results]
        -[Job Login Success]        :[Save as Private Charge Print Job]
        -[Job Login Failure]        :[Delete Job]
        -[Job Without User ID]      :[Delete Job]

    - The type of the print job is either one of the following:

        - User authentication for the user information attached to the print job fails

        - Print job with no user information attached

## Logout

| Item | Description |
|---|---|
| Date/Time | When user's logout request is detected |
| User Name | User ID of the corresponding login |
| Description | "Logout" |
| Status | "Successful" or "Failed" |
| Optionally Logged Items | **Access method**<br>"Local" or "Web User Interface"<br><br>**Host name**<br>Up to 45 bytes, excluding the null-terminated string<br>IP address<br><br>Note<br>• When the IP address is unknown or it is a local access, describe as "-". |

## Access denial due to authentication failures

Note
• Due to timing, access denial can be recorded before the corresponding authentication failure by the system administrator is recorded.

| Item | Description |
|---|---|
| Date/Time | When the number of successive authentication failure reaches the number set in the system |
| User Name | User ID of the corresponding login |
| Description | "Locked Authentication" |
| Status | "-" |
| Optionally Logged Items | Number of authentication failures before access denial |

## Detection of unauthorized access

Note
• Due to timing, access denial can be recorded before the corresponding authentication failure by the system administrator is recorded.

| Item | Description |
|---|---|
| Date/Time | When the number of successive authentication failure within the specified time reaches the number set in the system |
| User Name | User ID of the corresponding login |
| Description | "Detected continuous Authentication Fail" |
| Status | "-" |
| Optionally Logged Items | **Detection means (protocol)**<br>"SNMPv3", "Web User Interface" or "-"<br><br>**Number of successive authentication failures before detected as an unauthorized access** |

## 2.3　　Change of Audit Policy

| Item | Description |
|------|-------------|
| Audit Event ID | 0x0301 |
| Logged Events | "Audit Policy" |

## Access to important data

### Enabling of audit-log management function

| Item | Description |
|------|-------------|
| Date/Time | When setting the specified item is complete |
| User Name | User ID |
| Description | "Audit Log" |
| Status | "Enabled" |
| Optionally Logged Items | "–" |

### Disabling of audit-log management function

| Item | Description |
|------|-------------|
| Date/Time | When setting the specified item is complete |
| User Name | User ID |
| Description | "Audit Log" |
| Status | "Disabled" |
| Optionally Logged Items | "–" |

## 2.4　　Job Completion

| Item | Description |
|------|-------------|
| Audit Event ID | 0x0401 |
| Logged Events | "Job Status" |

## Job

### Print

| Item | Description |
|------|-------------|
| Date/Time | When job is completed |
| User Name | User ID or user name of the user who executed the job |
| Description | "Print" |
| Status | "Completed", "Completed with Warnings", "Canceled by User", "Canceled by Shutdown", "Aborted" or "Unknown" |

| Item | Description |
|---|---|
| Optionally Logged Items | **Root job UUID**<br>Up to 36 bytes, excluding the null-terminated string<br><br>**Relation between root job UUID and the corresponding job**<br>"Related" or "Owned"<br><br>**Job Account ID**<br>Up to 32 bytes, excluding the null-terminated string<br>When the value is not set, describe as "-"<br><br>**Action**<br>Up to 64 bytes, excluding the null-terminated string<br>When the forced printing is suspended, describe as "Released forced output"<br>Otherwise, describe as "-"<br><br>**Host name**<br>Up to 45 bytes, excluding the null-terminated string<br><br>Note<br>• When the host name is unknown, the IP address is recorded, and when both the host name and IP address are unknown, describe as "-".<br><br>**File Name**<br>Up to 64 bytes, excluding the null-terminated string<br>When the value is not set, describe as "-"<br><br>**Job Type**<br>Up to 16 bytes, excluding the null-terminated string<br>When the value is not set, describe as "-" |

## Copy

| Item | Description |
|---|---|
| Date/Time | When job is completed |
| User Name | User ID or user name of the user who executed the job |
| Description | "Copy" |
| Status | "Completed", "Completed with Warnings", "Canceled by User", "Canceled by Shutdown", "Aborted" or "Unknown" |
| Optionally Logged Items | **Root job UUID**<br>Up to 36 bytes, excluding the null-terminated string<br><br>**Relation between root job UUID and the corresponding job**<br>"Related" or "Owned"<br><br>**Job Account ID**<br>Up to 32 bytes, excluding the null-terminated string<br>When the value is not set, describe as "-"<br><br>**Action**<br>Up to 64 bytes, excluding the null-terminated string<br>When the forced printing is suspended, describe as "Released forced output"<br>When detection of scan-job inhibition code is suspended, describe as "Ignored inhibited code"<br>Otherwise, describe as "-" |

## Scan

| Item | Description |
|---|---|
| Date/Time | When job is completed |
| User Name | User ID or user name of the user who executed the job |
| Description | "Scan" |
| Status | "Completed", "Completed with Warnings", "Canceled by User", "Canceled by Shutdown", "Aborted" or "Unknown" |
| Optionally Logged Items | **Root job UUID**<br>Up to 36 bytes, excluding the null-terminated string<br><br>**Relation between root job UUID and the corresponding job**<br>"Related" or "Owned"<br><br>**Job Account ID**<br>Up to 32 bytes, excluding the null-terminated string<br>When the value is not set, describe as "-"<br><br>**Action**<br>Up to 64 bytes, excluding the null-terminated string<br>When detection of scan-job inhibition code is suspended, describe as "Ignored inhibited code"<br>When encryption is used, describe as "Encrypted"<br>When the signature is applied, describe as "Signed"<br>Other than the above, describe as "-"<br><br>**Destination Name (to)**<br>Up to 64 bytes, excluding the null-terminated string<br>When the value is not set, describe as "-"<br><br>Note<br>• Only e-mail address can be set.<br><br>**Sender Name (from)**<br>Up to 64 bytes, excluding the null-terminated string<br>When the value is not set, describe as "-"<br><br>Note<br>• Only e-mail address can be set.<br><br>**Document ID for URL send**<br>Up to 10 bytes, excluding the null-terminated string<br>When the value is not set, describe as "-" |

## Folder

| Item | Description |
|---|---|
| Date/Time | When job is completed |
| User Name | User ID or user name of the user who executed the job |
| Description | "Mailbox" |
| Status | "Completed", "Completed with Warnings", "Canceled by User", "Canceled by Shutdown", "Aborted" or "Unknown" |

| Item | Description |
|---|---|
| Optionally Logged Items | **Root job UUID**<br>Up to 36 bytes, excluding the null-terminated string |
| | **Relation between root job UUID and the corresponding job**<br>"Related" or "Owned" |
| | **Job Account ID**<br>Up to 32 bytes, excluding the null-terminated string<br>When the value is not set, describe as "-" |
| | **Action**<br>Up to 64 bytes, excluding the null-terminated string<br>When the forced printing is suspended, describe as "Released forced output"<br>Otherwise, describe as "-" |

## Report

| Item | Description |
|---|---|
| Date/Time | When job is completed |
| User Name | User ID or user name of the user who executed the job |
| Description | "Print Reports" |
| Status | "Completed", "Completed with Warnings", "Canceled by User", "Canceled by Shutdown", "Aborted" or "Unknown" |
| Optionally Logged Items | **Root job UUID**<br>Up to 36 bytes, excluding the null-terminated string |
| | **Relation between root job UUID and the corresponding job**<br>"Related" or "Owned" |
| | **Job Account ID**<br>Up to 32 bytes, excluding the null-terminated string<br>When the value is not set, describe as "-" |

## Job Flow

| Item | Description |
|---|---|
| Date/Time | When job is completed |
| User Name | User ID or user name of the user who executed the job |
| Description | "Job Flow Service" |
| Status | "Completed", "Completed with Warnings", "Canceled by User", "Canceled by Shutdown", "Aborted" or "Unknown" |
| Optionally Logged Items | **Root job UUID**<br>Up to 36 bytes, excluding the null-terminated string |
| | **Relation between root job UUID and the corresponding job**<br>"Related" or "Owned" |
| | **Job Account ID**<br>Up to 32 bytes, excluding the null-terminated string<br>When the value is not set, describe as "-" |

### Others

| Item | Description |
|---|---|
| Date/Time | When job is completed |
| User Name | User ID or user name of the user who executed the job |
| Description | "-" |
| Status | "Completed", "Completed with Warnings", "Canceled by User", "Canceled by Shutdown", "Aborted" or "Unknown" |
| Optionally Logged Items | **Root job UUID**<br>Up to 36 bytes, excluding the null-terminated string<br>**Relation between root job UUID and the corresponding job**<br>"Related" or "Owned"<br>**Job Account ID**<br>Up to 32 bytes, excluding the null-terminated string<br>When the value is not set, describe as "-" |

# 2.5 Change/view of Device Setting

| Item | Description |
|---|---|
| Audit Event ID | 0x0501 |
| Logged Events | "Device Settings" |

## Date & time setting

### Change of date & time setting (local time)

| Item | Description |
|---|---|
| Date/Time | When the result of setting change is fixed |
| User Name | User ID of the user who executed the job |
| Description | "Adjust Time" |
| Status | "Successful" or "Failed" |

| Item | Description |
|---|---|
| Optionally Logged Items | **Previous Date and Time**<br>Date and Time (hour, minute, and second) of audit-event occurrence |
| | **Mean**<br>When the time is changed by the service, one of the following strings is recorded<br>"Time change by system."<br>"Time change by EPBB."<br>"Time change by NTP."<br>"Time change by SNMP."<br>"Time change by XPJL."<br>"Time change by SSMM."<br>"Time change by unknown service."<br>When the time is changed by the user, describe as "Time change by user" |
| | **Host name or IP address**<br>If the service that has changed the time is NTP Server, the host name or IP address will be added to the record |

# User information

## User registration

| Item | Description |
|---|---|
| Date/Time | When the result of user information registration is fixed |
| User Name | User ID |
| Description | "Add User" |
| Status | "Successful" or "Failed" |
| Optionally Logged Items | **User ID of the corresponding user**<br><br>**Role of the corresponding user**<br>"System Administrator", "Accounting Administrator" or "Casual Operator"<br><br>⎡Note⎤<br>• For unregistered users, describe as "Casual Operator". |

## Change of registered user information

⎡Note⎤
• An audit log is recorded only when the authentication mode is set to [Local]. However, when the system administrator information is changed, an audit log is recorded even when the authentication mode is set to other than [Local].

| Item | Description |
|---|---|
| Date/Time | When the result of user information change is fixed |
| User Name | User ID |
| Description | "Edit  User" |
| Status | "Successful" or "Failed" |

| Item | Description |
|---|---|
| Optionally Logged Items | **User ID of the corresponding user**<br>When the user ID itself is changed, the new user ID is recorded |
| | **Role of the corresponding user**<br>"System Administrator", "Accounting Administrator", "Casual Operator" or "-"<br><br>Note<br>• When the role itself is changed, the new role is recorded. For local users and unregistered users, describe as "Casual Operator". |
| | **Attributes of the corresponding user**<br>"ID", "Password", "CardID", "Name", "Permission", "Role", "ICCardID" and "Other" |

## Deletion of registered user information

| Item | Description |
|---|---|
| Date/Time | When the result of user information deletion is fixed |
| User Name | User ID |
| Description | "Delete  User" |
| Status | "Successful" or "Failed" |
| Optionally Logged Items | **User ID of the corresponding user**<br>When the user ID itself is changed, the new user ID is recorded |
| | **Role of the corresponding user**<br>"System Administrator", "Accounting Administrator" or "Casual Operator" |

## Used user name management table full

| Item | Description |
|---|---|
| Date/Time | When it is detected that the used user name management table is full |
| User Name | "-" |
| Description | "Deleted Username Queue Overflow" |
| Status | "Successful" |
| Optionally Logged Items | "-" |

# Folder

## Folder creation

| Item | Description |
|---|---|
| Date/Time | When the folder creation is determined |
| User Name | User ID |
| Description | "Create Mailbox" |
| Status | "Successful" or "Failed" |

| Item | Description |
|---|---|
| Optionally Logged Items | **Host Name**<br>Up to 45 bytes, excluding the null-terminated string<br><br>**Note**<br>• When the host name is unknown, the IP address is recorded. When both the host name and IP address are unknown, describe as "-". When the operation is conducted from the control panel, describe as "Local".<br><br>**Folder Number**<br>Left-aligned half-width numerals (3 digits at maximum. When the most significant digit is "0", omit the "0".) |

### Folder deletion

| Item | Description |
|---|---|
| Date/Time | When the result of folder deletion is fixed |
| User Name | User ID |
| Description | "Delete Mailbox" |
| Status | "Successful" or "Failed" |
| Optionally Logged Items | **Host Name**<br>Up to 45 bytes, excluding the null-terminated string<br><br>**Note**<br>• When the host name is unknown, the IP address is recorded. When both the host name and IP address are unknown, describe as "-". When the operation is conducted from the control panel, describe as "Local".<br><br>**Folder Number**<br>Left-aligned half-width numerals (3 digits at maximum. When the most significant digit is "0", omit the "0".) |

# Authentication mode

### Change

| Item | Description |
|---|---|
| Date/Time | When setting the specified item is complete |
| User Name | User ID |
| Description | "Switch Authentication Mode" |
| Status | "Successful" |
| Optionally Logged Items | **New Setting Value**<br>"Local is enabled", "Network is enabled", "Custom is enabled" or "OFF is enabled"<br><br>**Previous Setting Value**<br>"Local is enabled", "Network is enabled", "Custom is enabled" or "OFF is enabled" |

# Security setting

## Change

| Item | Description |
| --- | --- |
| Date/Time | When setting the specified item is complete<br>Even if the setting is changed after rebooting, the storage timing is the time when the value is changed |
| User Name | User ID |
| Description | "Change Security Setting" |
| Status | "Successful" |
| Optionally Logged Items | **Items**<br>"Authentication"<br>"Authorization"<br>"Accounting"<br>"Image Overwrite"<br><br>Note<br>• If changed from "Off" to "3 Overwrites", two pieces of Audit Log will be recorded.<br>"Storage Encryption"<br>"S/MIME"<br>"IPSEC"<br>"SNMPv1/v2"<br>"SNMPv1/v2 (Read Only)"<br>"SNMPv3"<br>"SNMPv3 (Read Only)"<br>"802.1x"<br>"Certificate Verify Mode"<br>"Maintainer Password"<br>"IntelligentCard"<br>"FIPS140"<br>"Self Test"<br>"Auto Clear Timer"<br>"Service Rep. Restricted Operation"<br>"Print Reports Button"<br>"External Code Integrity Check"<br>"No Encrypt Ext App Install"<br>"CORS"<br>"ThinPrint" |

| Item | Description |
|---|---|
| Optionally Logged Items | "HTTP SSL/TLS"<br>"HTTP SSL/TLS Forced"<br>"IPP SSL/TLS Forced"<br>"SMTP SSL/TLS"<br>"LDAP SSL/TLS"<br>"ThinPrint SSL/TLS"<br>"Session Lock Timer"<br>"Authentication Operation Message"<br>"USB Port Management"<br>"Front USB-A"<br>"Rear USB-A"<br>"PC USB-B"<br>"Deleted User Account Names Days of Restriction"<br>"Maximum Number of Reusable Sequential Characters"<br>"Number of Password Generations Required"<br>"ID Token Validation (Microsoft Entra ID)"<br>"Certificate Verify Mode (Microsoft Entra ID)"<br>"Invalid User Deletion (Microsoft Entra ID)"<br>"Syslog"<br>"Download Disable Flag"<br>"Firmware Download via Network"<br>"Web UI Timer"<br>"SSL Protocol Information"<br>"CSRF Check"<br>"Runtime System Protection"<br>"Device Ceritificate Enrollment"<br>"Startup Integrity Check"<br>"POP3 with OAuth Authentication"<br>"Common Criteria Function"<br>"Universal Print"<br>"Tls Security Level"<br><br>**Change description**<br>When the enabled/disabled setting is changed, describe as "is enabled" or "is disabled" respectively<br>When the setting other than enabled/disabled is changed, describe as "is configured" |

## View

| Item | Description |
|---|---|
| Date/Time | View from Internet Services: When the HTML including the data to be referred to is obtained<br>View from panel UI: When the [Device] screen is accessed |
| User Name | User ID |
| Description | "View Security Setting" |
| Status | "Successful" |
| Optionally Logged Items | **Access method**<br>"Local" or "Web User Interface"<br><br>**Host name**<br>Up to 45 bytes, excluding the null-terminated string<br><br>⏐ Note ⏐<br>• When the host name is unknown, the IP address is recorded. When both the host name and IP address are unknown or when it is a local access, describe as "-". |

# Job-related

## Change

| Item | Description |
|---|---|
| Date/Time | When setting the specified item is complete |
| User Name | "CE" |
| Description | "Change Job Setting" |
| Status | "Successful" |
| Optionally Logged Items | **Function Name**<br>"Delay Print" or "Private Print" |

# XCP plugin

## Start/stop of XCP plugin

| Item | Description |
|---|---|
| Date/Time | When the XCP plugin starts and stops |
| User Name | "-" |
| Description | "Activate Embedded Plug-in" or "Deactivate Embedded Plug-in" |
| Status | "Successful" or "Failed" |
| Optionally Logged Items | **XCP plugin name and host information of the request source** |

# 2.6　Access to Data Stored in Device

| Item | Description |
|---|---|
| Audit Event ID | 0x0601 |
| Logged Events | "Device Data" |

# Certificate

## Certificate registration

| Item | Description |
|---|---|
| Date/Time | When the result of registering one certificate is fixed |
| User Name | User ID |
| Description | "Import Certificate" |
| Status | "Successful" or "Failed" |

| Item | Description |
| --- | --- |
| Optionally Logged Items | **Category**<br>"RootCA", "DeviceEE" or "SSCEE" |
| | **Key Size**<br>"512" to "2048" |
| | **Issuer DN**<br>Character string is 150 bytes at maximum |
| | **Serial Number**<br>40 bytes at maximum |

## Certificate deletion

| Item | Description |
| --- | --- |
| Date/Time | When the result of deleting one certificate is fixed |
| User Name | User ID |
| Description | "Delete Certificate" |
| Status | "Successful" or "Failed" |
| Optionally Logged Items | **Category**<br>"RootCA", "DeviceEE" or "SSCEE" |
| | **Key Size**<br>"512" to "2048" |
| | **Issuer DN**<br>Character string is 150 bytes at maximum |
| | **Serial Number**<br>40 bytes at maximum |

## Certificate online registration

| Item | Description |
| --- | --- |
| Date/Time | Time when a certificate is registered online |
| User Name | "System" |
| Description | "Device Ceritificate Enrollment" |
| Status | "Successful" or "Failed" |
| Optionally Logged Items | **DN of the certificate owner** |

# Address book

## Address addition

| Item | Description |
| --- | --- |
| Date/Time | When the result of adding one address is fixed |
| User Name | User ID |
| Description | "Add Address Entry" |
| Status | "Successful" or "Failed" |

| Item | Description |
|---|---|
| Optionally Logged Items | **Host name**<br>Up to 45 bytes, excluding the null-terminated string<br><br>Note<br>• When the host name is unknown, the IP address is recorded. When both the host name and IP address are unknown, describe as "-". When the operation is conducted from the control panel, describe as "Local".<br><br>**Registration Number**<br>Left-aligned half-width numerals (4 digits at maximum. When the most significant digit is "0", omit the "0".) |

## Address deletion

| Item | Description |
|---|---|
| Date/Time | When the result of deleting one certificate is fixed |
| User Name | User ID |
| Description | "Delete Address Entry" |
| Status | "Successful" or "Failed" |
| Optionally Logged Items | **Host name**<br>Up to 45 bytes, excluding the null-terminated string<br><br>Note<br>• When the host name is unknown, the IP address is recorded. When both the host name and IP address are unknown, describe as "-". When the operation is conducted from the control panel, describe as "Local".<br><br>**Registration Number**<br>Left-aligned half-width numerals (4 digits at maximum. When the most significant digit is "0", omit the "0".) |

## Address change

| Item | Description |
|---|---|
| Date/Time | When the result of changing one address is fixed |
| User Name | User ID |
| Description | "Edit Address Entry" |
| Status | "Successful" or "Failed" |
| Optionally Logged Items | **Host name**<br>Up to 45 bytes, excluding the null-terminated string<br><br>Note<br>• When the host name is unknown, the IP address is recorded. When both the host name and IP address are unknown, describe as "-". When the operation is conducted from the control panel, describe as "Local".<br><br>**Registration Number**<br>Left-aligned half-width numerals (4 digits at maximum. When the most significant digit is "0", omit the "0".) |

## Uploading from remote client (Whole address book)

| Item | Description |
| --- | --- |
| Date/Time | When the result of uploading from remote client is fixed |
| User Name | User ID |
| Description | "Import Address Entry" |
| Status | "Successful" or "Failed" |
| Optionally Logged Items | **Host name**<br>Up to 45 bytes, excluding the null-terminated string<br><br>Note<br>• When the host name is unknown, the IP address is recorded, and when both the host name and IP address are unknown, describe as "-". |

## Downloading to remote client (Whole address book)

| Item | Description |
| --- | --- |
| Date/Time | When the result of downloading to remote client is fixed |
| User Name | User ID |
| Description | "Export Address Entry" |
| Status | "Successful" or "Failed" |
| Optionally Logged Items | **Host name**<br>Up to 45 bytes, excluding the null-terminated string<br><br>Note<br>• When the host name is unknown, the IP address is recorded, and when both the host name and IP address are unknown, describe as "-". |

## Deletion of all addresses

| Item | Description |
| --- | --- |
| Date/Time | When the result of deletion of all addresses is confirmed |
| User Name | User ID |
| Description | "Clear Address Entry" |
| Status | "Successful" or "Failed" |
| Optionally Logged Items | **Host name**<br>Up to 45 bytes, excluding the null-terminated string<br><br>Note<br>• When the host name is unknown, the IP address is recorded, and when both the host name and IP address are unknown, describe as "-". |

# Audit log

### Downloading to remote client (Whole address book)

| Item | Description |
|------|-------------|
| Date/Time | When the result of downloading is fixed |
| User Name | User ID |
| Description | "Export Audit Log" |
| Status | "Successful" or "Failed" |
| Optionally Logged Items | **Host name**<br>Up to 45 bytes, excluding the null-terminated string<br><br>Note<br>• When the host name is unknown, the IP address is recorded, and when both the host name and IP address are unknown, describe as "-". |

# Document

### Sending scan documents to remote client

Note
• This applies only to documents stored by the Scan job.

| Item | Description |
|------|-------------|
| Date/Time | When the send result to the remote client is fixed |
| User Name | User ID |
| Description | "Retrieve scanned image" |
| Status | "Successful" or "Failed" |
| Optionally Logged Items | **Host name**<br>Up to 45 bytes, excluding the null-terminated string<br><br>Note<br>• When the host name is unknown, the IP address is recorded, and when both the host name and IP address are unknown, describe as "-".<br><br>**Stored & Send Link document ID**<br>Up to 10 bytes, excluding the null-terminated string |

## Deletion

- An audit log is not recorded in the following cases:
  - When a folder is deleted (an audit log for "Folder Deletion" is recorded)
  - When deletion is executed from WebDAV or custom service content
  - When a document is deleted due to expiration (over time)
  - When a stored file other than a file in the folders or Private Charge Print, such as stored files for Delayed Print and Store Files for Polling, is deleted

| Item | Description |
|------|-------------|
| Date/Time | When the document deletion is determined |
| User Name | User ID |
| Description | "Delete Document" |
| Status | "Successful" or "Failed" |
| Optionally Logged Items | **Host name**<br>Up to 45 bytes, excluding the null-terminated string<br><br>```Note```<br>• When the host name is unknown, the IP address is recorded. When both the host name and IP address are unknown, describe as "-". When the operation is conducted from the control panel, describe as "Local".<br><br>**Folder number**<br>Can be up to 3 half-width numerals, in left-justified omitting leading zeros<br><br>**File number**<br>Can be up to 4 half-width numerals, in left-justified omitting leading zeros |

# Custom service

## Install

| Item | Description |
|------|-------------|
| Date/Time | When the Install process is ended |
| User Name | "-" |
| Description | "Install Custom Service" |
| Status | "Successful" or "Failed" |
| Optionally Logged Items | **Corresponding custom service content name (name)**<br>Example) "CS_RM_00108"<br>If unknown, described as "-"<br><br>**A string describing the reason of failure (recorded on failure)**<br>If the custom service name specified is already present on the device at the time of instance creation, the following is described: "Application already exists."<br>Other than the above: "RegApp regist failed to management service." |

### Custom service content registration that is not allowed

| Item | Description |
| --- | --- |
| Date/Time | When verification of the signature of the Custom service content file fails |
| User Name | User ID |
| Description | "Install Custom Service" |
| Status | "Failed" |
| Optionally Logged Items | **Host name**<br>Up to 45 bytes, excluding the null-terminated string<br><br>Note<br>• When the host name is unknown, the IP address is recorded, and when both the host name and IP address are unknown, describe as "-". When the custom service content is registered via CPIM, the FQDN of the server from where the CPIM obtains the package is recorded.<br><br>**Custom service name**<br>Up to 63 bytes, excluding the null-terminated string<br>When it cannot be obtained (including retrieval error), describe as "-" |

### Uninstall

| Item | Description |
| --- | --- |
| Date/Time | When the Uninstall process is ended |
| User Name | "-" |
| Description | "Uninstall Custom Service" |
| Status | "Successful" or "Failed" |
| Optionally Logged Items | **Corresponding custom service content name (name)**<br>Example) "CS_RM_00108"<br>If unknown, described as "-"<br><br>**A string describing the reason of failure (recorded on failure)**<br>"Failed to delete RegApp from management service." |

# XCP plugin

### Install

| Item | Description |
| --- | --- |
| Date/Time | When the Install process is ended |
| User Name | "-" |
| Description | "Install Embedded Plug-in" |
| Status | "Successful" or "Failed" |
| Optionally Logged Items | **XCP plugin name**<br>If unknown, described as "-" |

### XCP plugin registration that is not allowed

| Item | Description |
| --- | --- |
| Date/Time | When verification of the signature of the XCP plugin file fails |
| User Name | User ID |
| Description | "Install Embedded Plug-in" |
| Status | "Failed" |
| Optionally Logged Items | **Host name**<br>Up to 45 bytes, excluding the null-terminated string<br><br>Note<br>• When the host name is unknown, the IP address is recorded, and when both the host name and IP address are unknown, describe as "-". When the custom service content is registered via CPIM, the FQDN of the server from where the CPIM obtains the package is recorded.<br><br>**Plugin file name**<br>If the registration is via CPIM, the download name of the downloaded file<br>Up to 63 bytes, excluding the null-terminated string<br>When it cannot be obtained (including retrieval error), describe as "-" |

### Uninstall

| Item | Description |
| --- | --- |
| Date/Time | When the uninstall process is ended |
| User Name | "-" |
| Description | "Uninstall Embedded Plug-in" |
| Status | "Successful" or "Failed" |
| Optionally Logged Items | **XCP plugin name**<br>If unknown, described as "-" |

# Cloning

### Export

| Item | Description |
| --- | --- |
| Date/Time | When the Export process is ended |
| User Name | User ID |
| Description | "Export Cloning Data" |
| Status | "Successful" or "Failed" |
| Optionally Logged Items | "-" |

### Import

| Item | Description |
| --- | --- |
| Date/Time | When the Import process is ended |

| Item | Description |
|---|---|
| User Name | User ID |
| Description | "Import Cloning Data" |
| Status | "Successful" or "Failed" |
| Optionally Logged Items | "–" |

# Falsification Detection

### Detecting access and execution of the files that is not allowed by whitelist

| Item | Description |
|---|---|
| Date/Time | When access or execution of the files that is not allowed by whitelist is detected |
| User Name | "System" |
| Description | "Illegal Access Detection" |
| Status | "Successful" |
| Optionally Logged Items | **Access type**<br>Example) "write"<br><br>**Accessed file name**<br><br>**Accessed program name** |

# Falsification detection and automatic correction upon activation

### Falsification detection upon activation

| Item | Description |
|---|---|
| Date/Time | When the falsification detection function is turned ON upon activation |
| User Name | "System" |
| Description | "Startup Integrity Check" |
| Status | "Successful" or "Failed" |
| Optionally Logged Items | **OS**<br><br>**Application** |

### Automatic software recovery

| Item | Description |
|---|---|
| Date/Time | When the automatic software recovery function is turned ON |
| User Name | "System" |
| Description | "System Software Recovery" |
| Status | "Successful" or "Failed" |

| Item | Description |
|---|---|
| Optionally Logged Items | "–" |

# 2.7     Change /Restoration of Device Configuration

| Item | Description |
|---|---|
| Audit Event ID | 0x0701 |
| Logged Events | "Device Config" |

## Important parts

### Replacement of important parts

| Item | Description |
|---|---|
| Date/Time | When replacement of the important part is detected |
| User Name | "–" |
| Description | "Important Parts" |
| Status | "Replaced" |
| Optionally Logged Items | "–" |

## Storage

### Detection of Storage replacement

| Item | Description |
|---|---|
| Date/Time | When system recognizes Storage |
| User Name | "–" |
| Description | "Storage" |
| Status | "Installed", "Removed" or "Replaced" |
| Optionally Logged Items | "–" |

## ROM

### Change of ROM version

| Item | Description |
|---|---|
| Date/Time | When difference between the ROM version at the previous activation and the version of ROM now being activated is detected<br><br>**Note**<br>• Timing of detecting the version varies per ROM.<br>• When NVM is initialized, change of ROM version is not recorded. |
| User Name | User ID |
| Description | "Software" |
| Status | "Updated" |
| Optionally Logged Items | **ROM Type**<br>Example) "Controller+PS"<br><br>**New Version**<br><br>**Previous Version** |

# 2.8     Communication Result

| Item | Description |
|---|---|
| Audit Event ID | 0x0801 |
| Logged Events | "Communication" |

## Reliability Communication

### Reliability Communication Error

| Item | Description |
|---|---|
| Date/Time | When Reliability Communication Error is detected at the periodical check |
| User Name | "-" |
| Description | "Trusted Communication" |
| Status | "Failed" |

| Item | Description |
|---|---|
| Optionally Logged Items | **Protocol name**<br>"SSL/TLS", "IPSEC" or "S/MIME"<br><br>**Other end of communication**<br>Up to 45 bytes, excluding the null-terminated string<br>Host name or IP address<br><br>⎿ Note ⏌<br>• When both the host name and IP address are unknown or when it is using S/MIME, describe as "-".<br>• The example of record in a communication destination is as follows:<br>  - IPv6:"[3ffe:0200:0000:010a:0000:0000:0000:0001]"<br>  - IPv4:"129.249.79.100"<br>  - Host name:"host.sharp.co.jp"<br>• A part exceeding 45 bytes is suppressed.<br><br>**Number of errors**<br><br>**Reason of errors**<br><br>⎿ Note ⏌<br>• The display example of Optionally Logged Items is as follows:<br>  - "SSL/TLS, [3ffe:0200:0000:010a:0000:0000:0000:0001],3,Certificate verification failed"<br>  - "IPSEC,[3ffe:0200:0000:010a:0000:0000:0000:0001],23,IKE negotiation failed"<br>• When multiple errors occur, they are recorded in one per line. A line cannot exceed 69 bytes.<br>• When more than 50 errors occur, the 51st and later errors are displayed as "+". |

# NTP

## Reliability Communication Error

| Item | Description |
|---|---|
| Date/Time | When the communication failure with the NTP server is detected |
| User Name | "System" |
| Description | "NTP Communication" |
| Status | "Failed" |

| Item | Description |
| --- | --- |
| Optionally Logged Items | **Communication destination**<br>Up to 45 bytes, excluding the null-terminated string<br>Host name (FQDN) or IP address<br><br>　**Note**<br>　• When both the host name and IP address are unknown, describe as "-". When host name resolution fails, the host name is recorded.<br>　• The example of record in a communication destination is as follows:<br>　　- IPv6:"[3ffe:0200:0000:010a:0000:0000:0000:0001]"<br>　　- IPv4:"129.249.79.100"<br>　　- Host name:"host.sharp.co.jp"<br>　• A part exceeding 45 bytes is suppressed.<br><br>**Reason of errors**<br>For server communication, describe as "NTP negotiation failed"<br>For DNS communication, describe as "jp,dns name resolution failed"<br><br>　**Note**<br>　• The display example of Optionally Logged Items is as follows:<br>　　- "[3ffe:0200:0000:010a:0000:0000:0000:0001],NTP negotiation failed"<br>　　- "ntp.sharp.co.jp,dns name resolution failed"<br>　• When multiple errors occur, they are recorded in one per line. A line cannot exceed 69 bytes.<br>　• When more than 50 errors occur, the 51st and later errors are displayed as "+". |

# EWB(Embedded Web Browser)

## Web access from EWB

| Item | Description |
| --- | --- |
| Date/Time | When accessed from EWB |
| User Name | User ID |
| Description | "Web Access" |
| Status | "Successful" |
| Optionally Logged Items | **Access URL** |

# SHARP

## SHARP CORPORATION