**SCC Software Requirement Specification Document**  
  
Table of Contents

[1. Scope of Application 7](#_Toc472603786)

[1.1. Related Documents 7](#_Toc472603787)

[1.2. Applicable Models 7](#_Toc472603788)

[2. Functional Outline 7](#_Toc472603789)

[2.1. Comparison with the Existing Functions 8](#_Toc472603790)

[3. Setting/Operation Conditions 10](#_Toc472603791)

[3.1. Settings 10](#_Toc472603792)

[3.1.1. Enabling/Disabling Setting of the SCC Function 10](#_Toc472603793)

[3.1.2. Measures for saturation communication 10](#_Toc472603794)

[3.1.3. SCC Proxy Server Setting 10](#_Toc472603795)

[3.1.4. SCC first registration URL 10](#_Toc472603796)

[3.1.5. URL forward setting 11](#_Toc472603797)

[3.2. Function List 11](#_Toc472603798)

[3.3. Top Access Setting Screen 11](#_Toc472603799)

[4. Functional Definition 12](#_Toc472603800)

[4.1. Enabling/Disabling of the SCC Function 12](#_Toc472603801)

[4.2. Installation Report Printing 12](#_Toc472603802)

[4.2.1. Print of the SCC Module Installation for the First Time 12](#_Toc472603803)

[4.2.2. SCC report print specification in V1.0 13](#_Toc472603804)

[4.3. Communication with Servers 13](#_Toc472603805)

[4.3.1. Communication Protocol 13](#_Toc472603806)

[4.3.2. Certificate of the SSL Communication 14](#_Toc472603807)

[4.3.3. Port Number and Proxy Authentication Settings 14](#_Toc472603808)

[4.3.4. Startup Mode 14](#_Toc472603809)

[4.3.5. Regular Communication Loop and Event Notification Loop 14](#_Toc472603810)

[4.3.6. URL setting 14](#_Toc472603811)

[4.4. Regular Communication Loop 15](#_Toc472603812)

[4.4.1. Communication Start Timing of Regular Communication Loop 15](#_Toc472603813)

[4.4.2. Communication Sequence of Regular Communication Loop 15](#_Toc472603814)

[4.4.3. Register Device 18](#_Toc472603815)

[4.4.4. Check for Updates 23](#_Toc472603816)

[4.4.5. Download Package 25](#_Toc472603817)

[4.4.6. Send Baseline Data 30](#_Toc472603818)

[4.4.7. Install Package 33](#_Toc472603819)

[4.4.8. Update Status 36](#_Toc472603820)

[4.4.9. Send Regular Data 38](#_Toc472603821)

[4.4.10. Send EOL Status 42](#_Toc472603822)

[4.4.11. EOL Report Print 42](#_Toc472603823)

[4.4.12. Send BOL Status 43](#_Toc472603824)

[4.4.13. GetRedirectURL 44](#_Toc472603825)

[4.4.14. Panel Message Display 44](#_Toc472603826)

[4.5. Event Notification Loop 46](#_Toc472603827)

[4.5.1. Communication Start Timing of Event Notification Loop 46](#_Toc472603828)

[4.5.2. Communication Sequence of Event Notification Loop 46](#_Toc472603829)

[4.5.3. Send Device Error 47](#_Toc472603830)

[4.5.4. Send Service File 50](#_Toc472603831)

[4.6. BOL, EOL 51](#_Toc472603832)

[4.7. Others 51](#_Toc472603833)

[4.7.1. Super Sleep 51](#_Toc472603834)

[4.7.2. Hibernation 52](#_Toc472603835)

[4.7.3. Persistent Policy 52](#_Toc472603836)

[4.7.4. Time-based Device State Data Values 53](#_Toc472603837)

[4.7.5. IP Redirect 54](#_Toc472603838)

[4.8. Definition of Boundary Threshold 55](#_Toc472603839)

[4.9. Error Handling 56](#_Toc472603840)

[4.9.1. Retry Processing at Communication Error 56](#_Toc472603841)

[4.9.2. Message Log 57](#_Toc472603842)

[4.10. Device Error Handling 59](#_Toc472603843)

[5. Performance Definition 59](#_Toc472603844)

[6. Restriction Definition 59](#_Toc472603845)

[6.1. Functional Restriction 59](#_Toc472603846)

[6.2. Input Restriction (Number of Digits, Prohibition) 59](#_Toc472603847)

[6.3. Exclusive Control 59](#_Toc472603848)

[6.4. Automatic Control 59](#_Toc472603849)

[7. Related Option (External OP and System OP) 59](#_Toc472603850)

# Scope of Application

This specification describes the SCC (b-Bridge CClient) Service Cloud supported by b-BridgeX L4.73.

## Related Documents

[02\_Requirement\SRS\JEA-03091\_SCC-Michigan](file:///\\tec-msga035\51-e-BridgeX\07-Requirement\Service%20Cloud\Requirement\PRD_2011) Project SaaS\_S2012 SRS.docx

02\_Requirement\SRS\JEA-03146\_SCC\_ExternalInterfaceSpecification.xlsx

02\_Requirement\SRS\JEA-03465\_Retrieved\_SCC\_Data\_selection.doc

02\_Requirement\SRS\JEA-03452\_DecommissionFunction\_Specifications.doc

02\_Requirement\SRS\JEA-03483\_Acquiring\_Resetting\_the\_DeptCounter\_via\_SCC\_Function

02\_Requirement\SRS\JEA-03687\_EmbAppInstallationEnhancement

02\_Requirement\SRS\JEA-03817\_ImprovementOfCollectionErrorCode\_Specifications.doc

02\_Requirement\SRS\JEA-03861\_PaperSensorLog(SCC)\_Specifications.doc

02\_Requirement\SRS\JEA-03815\_LicenseActivation\_Specifications\_JP.doc

## Applicable Models

Applicable models: EX series / EX-2 series later than L4.73, Baikal,

Reisshorn, St. Helens/Mosel,

Reisshorn-L(SSD), Reisshorn-LL

Drag/Phenix(TBD)

bBN series

# Functional Outline

SCC reduces the service cost and improves the service quality by realizing service without visiting, using the global cloud system for remote monitoring of the MFP and remote indication of the MFP operation.

The main functions provided by the global cloud system are as shown below:

1. Remote firmware update
2. Remote response to the device errors

・Acquisition or change of the MFP setting values (including the service settings)

・Monitoring of the MFP events

・Acquisition of logs

・Cloning

・Reboot

1. Remote support of the lease-expired MFP

・Data deletion

・Disabling of the function and network protocol

1. Remote installation of each data

・Customized data

・Application data

・License data

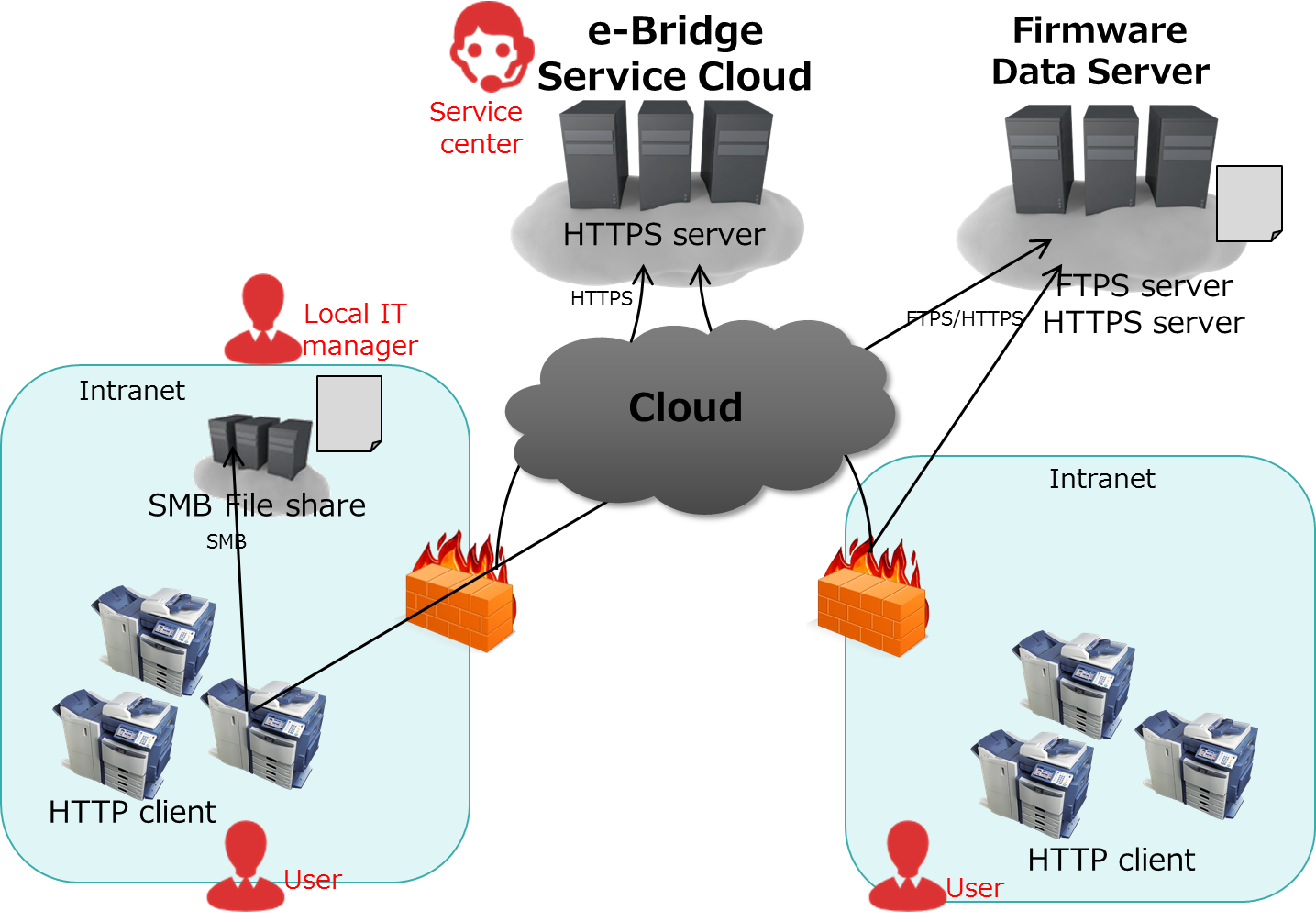


Fig. 1 System configuration of SCC

Each MFP is connected to the Service Cloud (server) via the firewall of the customers’ site.

## Comparison with the Existing Functions

The following is the comparison with the existing functions (RDMS and EFMS) which are similar to this:

Table 1 Comparison with the existing functions

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Classification | Function of the MFP | RDMS  (BBR2) | EFMS | SCC |
| Remote operation | Firmware update |  | ○ | ○ |
| 08/05/13 setting |  |  | ○ |
| TA setting |  |  | ○ |
| Cloning・Installation |  | ○ | ○ |
| Deletion of use data |  |  | ○ |
| Enabling/Disabling of the function |  |  | ○ |
| Reboot |  |  | ○ |
| Remote monitoring | Acquisition of all 08/05/13 settings | ○ |  | ○ |
| Acquisition of TA settings |  |  | ○ |
| Acquisition of service information (9S+300) |  |  | ○ |
| Acquisition of the function list・NIC setting list |  |  | ○ |
| Creation of a cloned file |  | ○ | ○ |
| Acquisition of the Job Log/ Message Log |  |  | ○ |
| Acquisition of the debug log |  | ○ | ○ |
| Detection・notification of abnormality | ○ | ○ | ○ |
| Acquisition of counters | ○  (Dept. Counter) | ○  (Total counter, Dept. counter) | △  (Dept. counter cannot be acquired.)  ->  Dept. counter was supported by L6.0, L4.9 and L4.733 version. |

# Setting/Operation Conditions

## Settings

### Enabling/Disabling Setting of the SCC Function

A service technician can set availability of the SCC function enable/disable from Self-diagnostic boot-up mode or service UI on panel.

An administrator cannot set the enable/disable from TA or via STAGE2 IF in normal boot-up mode (normal startup mode).

The default should be “Disable”. This shouldn’t be cloned. This will not be entered in the function list.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Public code** | **Set item name** | **Value description** | **Default** | **Public level** |
| 08-3820 | Enabling/Disabling of SCC function | 0: Disable 1: Enable | 0 | Maintenance  ~~Reiss-LL: Reservation~~  ~~Reiss-L-SSD: Inoperative~~ |

### Measures for saturation communication

TBD (Reserved)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Public code** | **Set item name** | **Value description** | **Default** | **Public level** |
| 08-3821 | Enabling/Disabling of Measures for saturation communication | 0: Disable 1: Enable | 0 | Maintenance  ~~Reiss-LL: Reservation~~  ~~Reiss-L-SSD: Inoperative~~ |

### SCC Proxy Server Setting

A service technician can set the SCC Proxy server from Self-diagnostic boot-up mode or service UI on panel.

An administrator cannot set the server in TA or via STGE2 I/F in normal boot-up mode (normal startup mode).

The default should be “Disable”. This shouldn’t be cloned. This will not be entered in the function list.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Public code** | **Set item name** | **Value description** | **Default** | **Public level** |
| 08-3822 | Enabling/Disabling of SCC Proxy Server | 0: Disable 1: Enable | 0 | Maintenance  ~~Reiss-LL: Reservation~~  ~~Reiss-L-SSD: Inoperative~~ |
| 08-3823 | SCC Proxy Server IP address setting | IP address or DNS name | 0.0.0.0 | ↑ (Same as above) |
| 08-3824 | SCC Proxy Server port number setting | 1-65535 | 80 | ↑ (Same as above) |
| 08-3825 | SCC Proxy Server account  ID setting | (Max. 30 characters)  Only US ASCII characters | (NULL) | ↑ (Same as above) |
| 08-3826 | SCC Proxy Server account  Password setting | (Max. 30 characters)  Only US ASCII characters | (NULL) | ↑ (Same as above) |

### SCC first registration URL

When service engineer wants for device to connect to special server (URL), this code is available.

The standard default value is NULL string and when this value is NULL, device connects edevice.Tprinters-solutions.com as current behavior.

This code is used only in first registration timing. Therefore, when the device isn’t registered on the server, device may be registered on other server. That is, device may not communicate the special server after first registration.

This behavior is prevented when the follows URL forward setting is ‘0’ (Disable).

(This function carries out the request that device shouldn’t connect foreign server and engineer sets up SCC in LAN.)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Public code** | **Set item name** | **Value description** | **Default** | **Public level** |
| 08-3827 | SCC first registration URL | 259 character ASCII | Refer below | Maintenance |

These diagnostic codes which are mentioned section 3.1.1, 3.1.2, 3.1.3 and 3.1.5 are saved on SRAM. But this code is saved on HDD. Hence, even if SRAM destination setting is changed, this value isn’t changed.

This shouldn’t be initialized by Factory Default. This should be initialized by HDD clear and Decommission. This shouldn’t be cloned. This will not be entered in the function list.

Default value of 08-3827

AUD: [https://gsidevice-ap.Tprinters-solutions.com:443](https://gsidevice-ap.toshiba-solutions.com:443)

Other: (NULL)

Refer to section 4.3.6 to get detail information.

### URL forward setting

When service engineer doesn’t want for device to connect a server which is specified by 08-3827, or default server (08-3827 is NULL string case), this value should be set as ‘0’ (Disable).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Public code** | **Set item name** | **Value description** | **Default** | **Public level** |
| 08-3828 | SCC URL forward setting | 0: Disable 1: Enable | AUD: 0  Other: 1 | Maintenance |

This shouldn’t be initialized by Factory Default. This should be initialized by Decommission. This shouldn’t be cloned. This will not be entered in the function list.

## Function List

No SCC-related additions in the function list.

## Top Access Setting Screen

No SCC-related additions on the setting screen of Top Access.

# Functional Definition

## Enabling/Disabling of the SCC Function

The SCC function operates by enabling 08-3820 (Enabling/Disabling of SCC function) and rebooting the MFP.

## Installation Report Printing

### Print of the SCC Module Installation for the First Time

The installation report is automatically printed when 08-3820 (Enabling/Disabling of SCC function) is changed from 0: Disable to 1: Enable, and after MFP registration processing is executed.

SCC installation report will be printed once if 08-3820 is changed from 0: OFF to 1: ON and never be printed anymore.

The following is printed:

Table 2 Printed items in the installation report

|  |  |
| --- | --- |
| Printed items | Description |
| Date and Time of Installation | Date the SCC module is installed  YYYY:MM:DD HH:MM:ssssssss |
| CC Plugin version | Version number of the SCC module |
| Registration status | MFP registered status to the cloud side |
| Serial Number | Serial number of the MFP  (Ex: C7H220662) |
| Model Number | Model number of the MFP  (Ex: TPRINTERS e-STUDIO2050C) |
| Firmware version | Firmware version number of the MFP  (Ex: T210SF0W1532) |
| Software version | Software version number of the MFP  (Ex: T569HD0W1532C) |
| IP address | IP address of the MFP  (Ex: 157.69.166.209) |
| Proxy Setting: URL | URL for Proxy |
| Proxy Setting: Port | Port number for Proxy |
| Ping | Result of connection to [http://www.google.com](http://www.google.com/)  (e.g. YES) |
| Port 80 | Result of connection to [http://www.microsoft.com](http://www.microsoft.com/)  (e.g. YES (0, 200) return value of Curl, HTTP Response ) |
| Port 443 | Result of connection to [http://www.microsoft.com](http://www.microsoft.com/)  (e.g. YES (0, 200) return value of Curl, HTTP Response ) |
| Primary URL connection result. | The URL which device connected at last.  When 08-3827 has invalid URL, that value is recorded.  (e.g.: “[https://edevice.Tprinters-solutions.com:443](https://edevice.toshiba-solutions.com:443)” (Regular sample)  “<ftp://test.local>” (Irregular sample 1)  “test.local” (Irregular sample 2)) |

Ex:

Device Installation Report

Date and Time of Installation: 2017:07:27 11:40:46240558

CC plugin version: 11.2.5.0

Registration status: REGISTERED

Serial Number: CFHE01508

Model Number: TPRINTERS e-STUDIO2505A

Firmware version: T373SF0W1050

Software version: T373HD0W1050

IP address: 157.69.166.123

Proxy Setting:

URL: 133.199.251.110

Port: 8080

Ping: NO

Port 80: YES (23, 200)

Port 443: YES (0, 200)

https://gsidevice-ap.Tprinters-solutions.com:443

### SCC report print specification in V1.0

Normal case:

Printed language is English only and is not localized.

SCC report printing is recorded in Job Log as network print

User counter for built-in Admin will be added after SCC report printing

Abnormal case:

The irregular scenarios of network print are applies to Installation Report printing.

(e.g.)

If power failure occurs during blinking LED (during RIP processing), SCC report is not printed after power-on recovery.

If 08-9344 (network print restriction mode) 1: only private, then SCC report is not printed with job log error record (error code = 4221) If the value is 2: only hold, job is registered as hold print.

If user authentication/ department code is enabled and quota given for built-in admin runs out, then SCC report is not printed with quota error.

If coin controller is equipped and external counter 08 code is enabled, then SCC report is not printed until coin is inserted.

If job full (1000 jobs are registered), then SCC report is not printed.

If print enabler is not equipped in monochrome machines then SCC report is not printed. (Depend on the destination: NAD, JPD etc)

Etc.

## Communication with Servers

### Communication Protocol

The MFP uses HTTPS for communication with servers.

The MFP is at the http client side and communication with the servers always starts from the MFP side (communication never start from the server side).

### Certificate of the SSL Communication

The server certificate for the SSL communication is previously installed to the MFP at SCC module installation.

Certificate issuing institution: Go Daddy

The client certificate for the SSL communication is not supported (not mutual authentication).

### Port Number and Proxy Authentication Settings

When the MFP is connected to the server via the proxy server, the setting is required for both MFP side and firewall side.

Setting for the MFP side:

Properly set from 08-3822 to 08-3826 (SCC Proxy Server setting group).

When the account ID is set to NULL, the MFP behaves as without the proxy authentication.

Setting for the firewall side:

For SCC, the setting to open the port number: 443 is required to be done for the firewall side.

If the port number: 443 is not available, the SCC module automatically uses the port number: 8443.

### Startup Mode

SCC process does not start up at the special startup.

While device is communicating with SCC server, we can’t use service UI.

### Regular Communication Loop and Event Notification Loop

Two loops operate inside the MFP by communicating with servers.

1. Regular communication loop
2. Event notification loop

“Regular communication loop” is a process loop to which the MFP periodically communicates with the server from the schedule setting.

“Event notification loop” is a process loop which notifies an event to the server immediately once the event is detected in the MFP.

“Regular communication loop” and “Event notification loop” operate separately.

“Regular communication loop” will be described in Section 4.4 and latter..

“Event notification loop” will be described in Section 4.5.

### URL setting

Device accesses a URL specified by 08-3827.

This value must start “http://” or “https://”. If service engineer wants to set port number of server, they need to use ‘;’ (colon) and set port number. When port number isn’t set, 80 (http) and 443 (https) are used.

[The sample of 08-3827

[https://edevice.Tprinters-solutions.com:443](https://edevice.toshiba-solutions.com:443)

Actual accessed URL is the followings.

[https://edevice.Tprinters-solutions.com:443](https://edevice.toshiba-solutions.com:443)/DeviceService.svc/device/\*\*\*

[Behavior based on 08-3827]

<NULL string case>

Device connects to NA server (edevice.Tprinters-solutions.com).

<Any values >

08-3827 value is used.

<Scenario>

1. 08-3827 value doesn’t start ”http://” and ”https://”.

Network error happens. Device doesn’t access NA server.

1. 08-3827 value is invalid.

Device accesses specified URL and network error happens. Device doesn’t access NA server.

1. 08-3827 is NULL string or valid URL and serial number of device is registered in the server.

Device accesses specified URL and it is registered to the server. After then device communicate the server.

1. 08-3827 value is NULL string or valid URL and serial number of device isn’t registered in the server.

4-1 Server returns error.

Registration error (STATUS\_FAILED) happens.

4-2 Server returns other URL

08-3828=’0’ (Disable) case, it’s registration error.

08-3828=’1’ (Enable) case, device accesses returned URL. After then device works same as current (L6.015 and before) behavior.

Device may be registered to other server instead of 08-3827 value’s one in above 4-2 scenario.

[Attention when service engineer uses HTTPS]

Device needs CA certification of server when HTTPS is used for communication.

CA certification can be imported by TA. When it isn’t done, communication fails. (Same as 08-3827 is invalid scenario.)

When actual SCC server URL (NA, EU and APAC) is used, they don’t need to import certification because it has been implemented in ROM data.

## Regular Communication Loop

### Communication Start Timing of Regular Communication Loop

The MFP communicates with the server at either one of the following timings after normal startup.

* SCC process startup
* Regular communication schedule
  + Specify time (every day or day of every week at the specified time)
  + Specify intervals from 5 min. to 60 min.

It is set to “every day at 0:00” by default.

### Communication Sequence of Regular Communication Loop

The MFP communicates in order of the following sequence at communication with the server (hereinafter, called “Communication cycle”.)

Table 3 Communication sequence with the server

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Communication name | Communication contents to the server | Server URL: (it is common up to the following.)  http:// Tprinters.cloudapp.net:8080/DeviceService.svc/ |
| 1 | GetRedirectURL | Get RedirectURL from Server | device/redirect/geturl |
| 2 | RegisterDevice | (The 1st time only) Register the MFP to the server.  (After the 2nd time) Authenticate the MFP. | device/register |
| 3 | CheckForUpdates | Check the update instruction from the server. | device/updates/check |
| 4 | Download Package | Download the update instruction from the server. | device/updates/download |
| 5 | SendBaselineData | Send the state before update from the server for rollback. | device/data/sendzip? (hash)&isBaseline=true |
| 6 | UpdateStatus | Notify the update application state to the server. | device/update/status/send |
| 7 | SendDeviceData | Send information of each MFP after update. | device/data/sendzip? (hash)&isBaseline=false |

The following is the state transition by SCC processing.

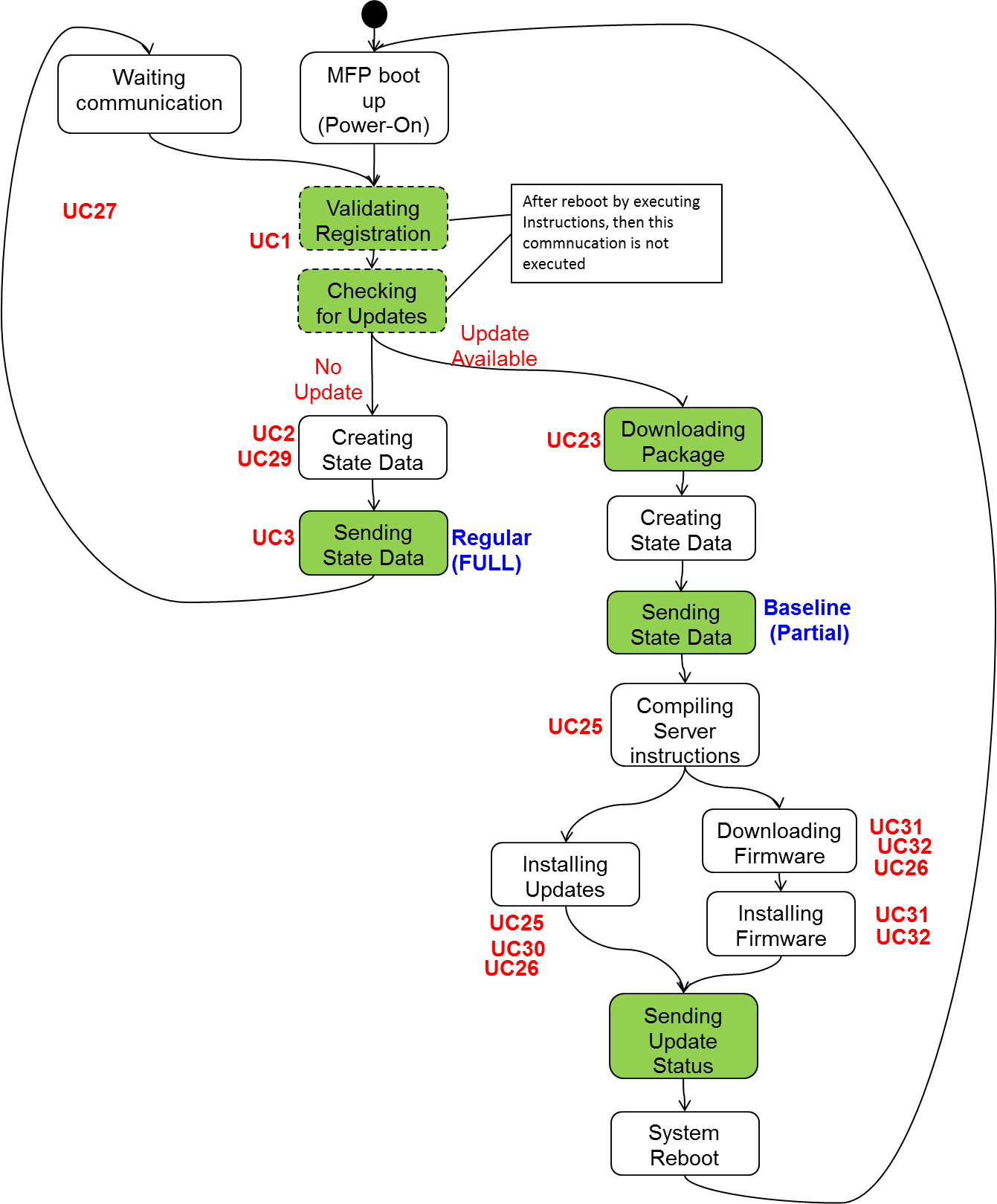


Fig. 2 State transition by SCC processing inside the MFP

### Register Device

The MFP is registered in the server by calling the interface, “Register Device”, at the server side.

The first call registers the MFP in the server.

The second or later call authenticates the MFP registered in the server.

#### Communication Parameter

The following is the information which is sent to the server from the MFP:

Table 4 Transmission parameter for the Register Device

|  |  |  |
| --- | --- | --- |
| No. | Information name | Description |
| 1 | Serial | Communication sequence number  (’1’ for the first request,’2’ for the reply to the following question) |
| 2 | Type | Communication type (Regular or Bootup) |
| 3 | RetryCount | Number of communication retry |
| 4 | Serial Number | MFP serial number (obtained by 08-9601)  \* This is used for check when the MFP is registered in the server side. |
| 5 | MACAddress | MAC address (Wired LAN) |
| 6 | Model | Model name  (Ex:： TPRINTERS e-STUDIO2540C) |
| 7 | ServiceCloudPluginVersion | SCC module version |
| 8 | FirmwareVersion | Firmware version (obtained by 08-9900) |
| 9 | Answer | Answer to the “secret question”.  (only when answering) |
| 10 | AccessToken | Token (only after it is issued from the server) |

The following is the information by which the MFP receives as the response from the server:

Table 5 Reception parameter for Register Device

|  |  |  |
| --- | --- | --- |
| No. | Information name | Description |
| 1 | Serial | Communication sequence number (Same as the one sent from the MFP) |
| 2 | Status | Status (Processing results at the server side)  STATUS\_REGISTERED … Registered normally.  STATUS\_UNREGISTERED … Failed in registration.  STATUS\_PENDING …Waiting for the answer to the secret question.  STATUS\_LOCKED …Exceeded the number of retry.  STATUS\_BUSY …The server side is in BUSY state.  STATUS\_FAILED …Fatal Error is occurred in Server. |
| 3 | AccessToken | Token  (Only when registration succeeded. Not applied to the communication after registration (2nd time or later)) |
| 4 | Challenge | Secret question (only at registration) |
| 5 | RetryTime | Retry intervals for the MFP to start connection next time (unit: minute)  (Only when Status= STATUS\_BUSY) |
| 6 | FrontPanelMsgOption | This value isn’t used. |
| 7 | SendDataConfig | This parameter represents which data should be sent.  \* Print Log  \* Scan Log  \* Message Log  \* Security　Setting  \* Default Setting  \* User Management Setting  \* Network and Print Service Setting  \* Address Book Data  (Please refer to JEA-03456 for L6.0 and later behavior.) |

[SendDataConfig parameter]

Default values are “off”. When server sets values to these parameters by response message, MFP applies them immediately. If the response message doesn’t have value, MFP uses previous values.

[Meaning of these parameters]

\* Print Log

Print job log

\* Scan Log

Scan job log

\* Message Log

Message log

\* Security Setting

Clone data which we can select by following screen.

TA > Administration > Maintenance > Create Clone File > Category Setting > Security

・Default Setting

(Same as above path) > Default Settings

・User Management Setting

(Same as above path) > User Management

・Network and Print Service Setting

(Same as above path) > Network/Print Service

・Address Book Data

(Same as above path) > Address Book and Address Book + Template > Mail Boxes

#### Normal Sequence

(First time: at MFP registration)

The server checks whether the MFP serial number is previously applied at the MFP registration. Then the server sends the secret question for the device authentication. The MFP answers the question and if the answer is correct, it is registered. The question is selected randomly from the list which is owned by the server.



Fig. 3 MFP registration sequence at the first time

(After registration: at the MFP authentication)

The MFP to which the registration is completed connects with the server using the token responded from the server at the registration.

When the server judges the token is invalid even after the MFP registration is completed, the registration sequence is performed.



Fig. 4 MFP authentication sequence

#### Abnormal Sequence

(The server is BUSY)

When the simultaneous processing of the clients by the server exceeds the limit, the server may request reconnection to the Register Device request. The MFP finishes connection with the server at this time, and connects again by adding 1 to the number of retry shown above after waiting for the period specified by the server.

The number of retry is returned to the initial value, 0, once the Register Device processing is completed normally.

The server inevitably receives the MFP request at the 3rd retry. If the 4th reconnection request is responded from the server, the MFP exits from the communication cycle and waits for the next communication schedule.



Fig. 5 Server BUSY

(The MFP registration fails)

When the MFP serial number is not registered to the server, failing in answering the question, or double registration is tried, the registration fails. When registration failure occurs consecutively 3 times, the server responds STATUS\_LOCK.

When either of failing in registration (STATUS\_UNREGISTERED) or STATUS\_LOCKED is returned, Installation Report is printed and the MFP exits from the communication cycle and waits for the next schedule. It does not go into the retry mode mentioned later.

(A communication error occurs in the Register Device)

Go to the retry processing mentioned later.

(Power failure occurs during the Register Device)

Communicate with the server at the next power on (No recovery processing is performed).

### Check for Updates

The MFP calls the interface, “Check for Updates”, at the server side to check whether update is specified after “Register Device”. If update is specified, download the updates. If no update is required, send information of each MFP to the server.

#### Communication Parameter

The following is the information sent to the server from the MFP:

Table 6 Transmission parameter for Check for Updates

|  |  |  |
| --- | --- | --- |
| No. | Information name | Description |
| 1 | Token | Token  The same token registered from the server at Register Device is set. |

The following is the information by which the MFP receives as the response from the server

Table 7 Reception parameter for Check for Updates

|  |  |  |
| --- | --- | --- |
| No. | Information name | Description |
| 1 | Status | Status (Processing result at the server side)  STATUS\_UPDATES\_AVAILABLE … with update  STATUS\_NO\_UPDATES\_AVAILABLE … without update  STATUS\_FAILED … A fatal error occurred.  STATUS\_INVALID\_TOKEN … Token is not correct. |
| 2 | PackageId | (Only when there is the update package)  The package ID of the update package  (It is used for the next Download Package.) |
| 3 | Hash | (Only when there is the update package)  The Hash value of the update package |

#### Normal Sequence



Fig. 6 Update check sequence

#### Abnormal Sequence

(STATUS\_FAILED or STATUS\_INVALID\_TOKEN)

When INVALID\_TOKEN is returned from the server, the MFP exit from the communication cycle and waits for the next communication schedule.

(A communication error occurs at Check For Updates)

Go to the retry processing mentioned later.

(Power failure occurs during Check For Updates)

Communicate with the server at the next power on (No recovery processing is performed).

### Download Package

The MFP downloads the update package (update instruction from the server) by calling the interface, “Download Package”, at the server side after “Check for Updates”.

There is one package per MFP (there are no 2 or more packages).

The following is the instructions from the server included in the package.

#### Communication Parameter

The following is the information sent to the server from the MFP:

Table 8 Transmission parameter for Download Package

|  |  |  |
| --- | --- | --- |
| No. | Information name | Description |
| 1 | Token | Token  The same token issued from the server at Register Device is set. |
| 2 | PackageId | Package ID  The same ID obtained from the server at Check for Updates is set. |

Information by which the MFP receives as the response from the server will be an updated package (ZIP file).

The followings are the Types of the instructions which come from Cloud server:

Table 9 Types of the instructions from the server

|  |  |  |
| --- | --- | --- |
| No. | Package Type | Description |
| 1 | EOL\_INSTRUCTIONS | Instruction which makes the user not to use the MFP and delete user data until the service technician goes to recover it due to the MFP lease period expiration. |
| 2 | FIRMWARE\_UPDATE | Instruction to execute software update of bBX/bBN. |
| 3 | POLICY\_VIOLATION\_DATA | Instruction to set the 05/08/13 settings and communication settings. |
| 4 | RESTORE\_DATA | Instruction to execute the Clone file installation. |
| 5 | SPECIAL\_INSTRUCTIONS | Instruction to perform other MFP execution.  Presently, only an instruction to send the debug log of the SCC module to the server. |
| 6 | SPECIAL\_INSTRUCTIONS\_DEVICE\_DEBUG\_FILE | Instruction to send bBX debug log. |
| 7 | CUSTOMIZED\_UI\_DATA | Instruction to install custom UI data. |
| 8 | APPLICATION\_OPERATION | Instruction to install and uninstall embedded application and license. Instruction to install language data. |
| 9 | CUSTOM\_USER\_PAPER\_TYPE | Instruction to install and uninstall user paper type. |
| 10 | LICENSE\_OPERATION | Instruction to install and uninstall license file which is supported from L6.11/L6.13 |

No. 1, 2, 7, 9 and 10 instructions can be executed individually. No. 3 through No.6 and 8 can be combined.

The package is an unencrypted ZIP file without a password.

A ZIP file includes the metadata file (Metadata.xml) and any of the one instruction from No. 1 through No. 10.

When No.2 and No. 7 through No. 10(firmware update, install of custom UI data, embedded application, license, localization data and user paper type), install data is not included in the package (ZIP file).

The MFP downloads the install data separately after Download Package.

When No. 6 (Clone file), the clone data is included in the package (ZIP file).

#### Metadata for Update Package

The following is the metadata (metadata.xml) of Update package (ZIP file): (element name = ‘UpdateMetadata’)

Table 10 metadata for Update Package

|  |  |  |
| --- | --- | --- |
| No. | Information name | Description |
| 1 | Device/id | Device ID |
| 2 | Device/Serial Number | MFP’s serial number  The value which is registered in Cloud server is sent to device. MFP must compare the value |
| 3 | Device/MACAddress | MFP’s MAC Address (Just Reference purpose: MFP does not have to compare) |
| 4 | Device/Model | MFP’s model name (Just reference purpose: MFP does not have to compare) |
| 5 | Packages/Package/Type | Type of Package:  EOL\_INSTRUCTIONS  POLICY\_VIOLATION\_DATA  RESTORE\_DATA  PLUGIN\_UPDATE  FIRMWARE\_UPDATE  SPECIAL\_INSTRUCTIONS  SPECIAL\_INSTRUCTIONS\_DEVICE\_DEBUG\_FILE  CUSTOMIZED\_UI\_DATA  APPLICATION\_OPERATION  CUSTOM\_USER\_PAPER\_TYPE  LICENSE\_OPERATION |
| 6 | Packages/Package/FileName | File name for Package |
| 7 | RestoreInstructions/ RestoreItems/Item | Type of Cloning Instruction  CLONE\_DATA  DEVICE\_CONFIG  Currently only ”CLONE\_DATA” is used |

#### EOL Instruction

The following is the update instruction from the server for EOL Instruction: (element name = ‘EOLInstructions’)

Table 11 Instruction parameter for EOL Instruction

|  |  |  |
| --- | --- | --- |
| No. | Information name | Description |
| 1 | Decommission Time | The time to start decommission. |

Refer to JEA-03452 document. Remote Decommission is this function.

#### Firmware Update Instruction

The following is the update instruction from the server for Firmware Update Instruction:

Table 12 Instruction parameter for Firmware Update Instruction

|  |  |  |
| --- | --- | --- |
| No. | Information name | Description |
| 1 | PolicyId | Policy ID |
| 2 | Location/URI | URI of the server which provides the firmware data  Maximum 2 can be defined for Primary server and secondary server. |
| 3 | Location/UserName | Account name to authenticate the server to the one which provides the firmware data  Maximum 2 can be defined for Primary server and secondary server. |
| 4 | Location/Password | Password to authenticate the server to the one which provides the firmware data.  Maximum 2 can be defined for Primary server and secondary server. |
| 5 | InstallTime | Specified time when installation is executed according to the schedule  Format: HH:MM AM/PM  e.g. 08:30 PM |
| 6 | Components/Component | Component to be updated  SystemFirmware  SystemSoftware  EngineFirmware  ScannerFirmware  DFFirmware  PFCFirmware  LaserFirmware (bBX model only)  PunchFirmware  FinisherFirmware  SaddleFirmware (bBX model only)  PU (bBX model only)  PU Loader (bBX model only)  SU (bBX model only)  SU Loader (bBX model only)  SU Recovery (bBX model only)  Tray (bBX model only)  LCF (bBX model only)  ADU (bBX model only)  FAXFirmware (bBN model only)  NICFirmware (bBN model only) |

#### Policy Violation Data Instruction

The following is the update instruction from the server for Policy Violation Data Instruction: (element name = ‘Policy’)

Table 13 Instruction parameter for Policy Violation Data Instruction

|  |  |  |
| --- | --- | --- |
| No. | Information name | Description |
| 1 | id | Policy ID |
| 2 | (Version)id | Format version for Policy  MFP must check this version and check capability itself to interpret the policy |
| 3 | Data/OtherSettings/ Parameter/Category | XPATH category to set. Select value from items below:  Network  SecurityConfiguration  VersionInfo  Device |
| 4 | Data/OtherSettings/ Parameter/Xpath | XPATH to set value |
| 5 | Data/OtherSettings/ Parameter/Value | XPATH value |
| 6 | Data/OtherSettings/ Parameter/TimeBasedvalue | Time based variable value  Format is consist of pairs: 24 hour time and values. e.g.  8,11;15,9:20,1  8:00 🡪 Value = 11  15:00 🡪 Value = 9  20:00 🡪 Value = 1 |
| 7 | Category-05/Code  MainCode  SubCode  Value | Violating the policy. Set 05 code and the value. |
| 8 | Category-08/Code  MainCode  SubCode  Value | Violating the policy. Set 08 code and the value. |
| 9 | Category-13/Code  MainCode  SubCode  Value | Violating the policy. Set 13 code and the value. |
| 10 | Control/PersistInterval | The polling interval (in minutes) for persistency.  Value can be from 1 hour to 24 hours.  (60min to 1440 min. Default = 300min (5 hours)) |
| 11 | Control/PersistExpiration | The period (in days) that persistency for the current policy is enforced since last communication. If regular sync cycle is shorter than the expiration setting, and the communication is normal without interruption, persistence never expires. A value of 0 will discontinue the persistency check. A very large number will practically keep the persistency check on. |

#### Restore Data Instruction

The following is the update instruction from the server for Restore Data Instruction: (element name = ‘Policy’)

Table 14 Instruction parameter for Restore Data Instruction

|  |  |  |
| --- | --- | --- |
| No. | Information name | Description |
| 1 | Item | Common to Device Config  CLONE\_DATA  DEVICE\_CONFIG |

#### Special Instruction

The following is the update instruction from the server for Special Instruction: (element name = ‘SpecialInstructions’)

Table 15 Instruction parameter for Special Instruction

|  |  |  |
| --- | --- | --- |
| No. | Information name | Description |
| 1 | SendDebugLog | Flag whether to send the SCC module debug log  Boolean value (true or false)  MFP will send SCC module’s debug log when value = true. |
| 2 | SendbBXDebugLog | (Added from V1.0)  Flag whether to send the bBX debug log  Boolean value (true or false)  MFP will send bBX Debug log when value = true. |

#### Customized UI Instructions

The following is the update instruction from the server for Customized UI Instructions: (element name = ’CustomizedUIInstructions’)

Table 16 Instruction parameter for Customized UI Instructions

|  |  |  |
| --- | --- | --- |
| No. | Information name | Description |
| 1 | PolicyId | Policy ID |
| 2 | Location/URI | URI of the server which provides the custom UI data.  Maximum 2 can be defined for Primary server and secondary server. |
| 3 | Location/UserName | Account name to authenticate the server to the one which provides the custom UI data  Maximum 2 can be defined for Primary server and secondary server. |
| 4 | Location/Password | Password to authenticate the server to the one which provides the custom UI data.  Maximum 2 can be defined for Primary server and secondary server. |

#### Application Instructions

The following is the update instruction from the server for Application Instructions: (element name = ’ApplicationInstructions’)

Table 17 Instruction parameter for Application Instructions

|  |  |  |
| --- | --- | --- |
| No. | Information name | Description |
| 1 | PolicyId | Policy ID |
| 2 | DataType | Application, license or language data. |
| 3 | Operation | Install, uninstall or delete all data. |
| 4 | Location/URI | URI of the server which provides the application data.  Maximum 2 can be defined for Primary server and secondary server. |
| 5 | Location/UserName | Account name to authenticate the server to the one which provides the application data  Maximum 2 can be defined for Primary server and secondary server. |
| 6 | Location/Password | Password to authenticate the server to the one which provides the application data.  Maximum 2 can be defined for Primary server and secondary server. |
| 7 | TargetApplicationID | ID which is applied this instruction. |

#### Custom User Paper Type Instructions

The following is the update instruction from the server for Custom User Paper Type Instructions: (element name = ’CustomUserPaperTypeInstructions’)

Table 18 Instruction parameter for Custom User Paper Type Instruction

|  |  |  |
| --- | --- | --- |
| No. | Information name | Description |
| 1 | PolicyId | Policy ID |
| 2 | Operation | Install or uninstall |
| 3 | UserPaperTypeNumber | User paper type number which is applied this policy. |
| 4 | Location/URI | URI of the server which provides the user paper type data.  Maximum 2 can be defined for Primary server and secondary server. |
| 5 | Location/UserName | Account name to authenticate the server to the one which provides the user paper type data  Maximum 2 can be defined for Primary server and secondary server. |
| 6 | Location/Password | Password to authenticate the server to the one which provides the user paper type data.  Maximum 2 can be defined for Primary server and secondary server. |

#### License　Instructions

The following is the update instruction from the server for License Instructions: (element name = ’LicenseInstructions’)

Table 19 Instruction parameter for License Instructions

|  |  |  |
| --- | --- | --- |
| No. | Information name | Description |
| 1 | PolicyId | Policy ID |
| 2 | Operation | Install or uninstall |
| 3 | Location/URI | URI of the server which provides the license data.  Maximum 2 can be defined for Primary server and secondary server. |
| 4 | Location/UserName | Account name to authenticate the server to the one which provides the license data  Maximum 2 can be defined for Primary server and secondary server. |
| 5 | Location/Password | Password to authenticate the server to the one which provides the license data.  Maximum 2 can be defined for Primary server and secondary server. |
| 6 | LicenseKey | License ID which is applied this instruction. |

#### Normal Sequence

When there is an update package, the MFP downloads the package (ZIP file) immediately using the Package ID responded at Check For Updates.

The package is downloaded as HTTPS.

As for the saved package, the hash value is calculated with MD5 and the value is compared with the one responded at Check For Updates.



Fig. 7 Download Package

#### Abnormal Sequence

(Communication error while downloading the package)

Delete the downloaded data and performs the retry processing mentioned later.

(Power failure while downloading the package)

Delete the downloaded data before the communication at the next start-up.

(HDD full)

Delete the downloaded data. Exit from the communication cycle. Wait until the next communication starts.

(Hash value mismatch)

Delete the downloaded data. Exit from the communication cycle. Wait until the next communication starts.

(unzip failure)

Delete the unzipped data. Exit from the communication cycle. Wait until the next communication starts.

### Send Baseline Data

The MFP sends each setting information to the server by calling the interface, “Send Zip (isBaseline=true)”, at the server side after “Download Package”.

The MFP creates send data by “SendDataConfig” setting which server notifies.

#### Communication Parameter

The following is the information sent to the server from the MFP:

These data are collected by “SendDataConfig” setting.

Table 20 MFP information included in the Baseline data

|  |  |  |
| --- | --- | --- |
| No. | Type | Description |
| 1 | Metadata | File which explains the contents of the Baseline data  (metadata.xml) |
| 2 | Setting value of the MFP | All 05/08/13 setting values, security setting value, network setting value, and MFP information, Installed embedded application information, installed user paper type information and installed license information.  (devicedata.xml)  (All 05/08/13 setting values are the value from 0000 through 9999 obtained by the GetList command. ~~It includes the design codes~~ It does not include the design codes, and information such as the password is masked with \*\*\*\*\* (asterisks), etc.) |
| 3 | Regular communication schedule setting | Regular communication schedule setting for the MFP to connect with the server  (devicedata.xml) |
| 4 | Clone file | Cloning data |
| 5 | Log information | Job log, message log and irregular log |
| 6 | Department counter | Department counter |

These are gathered in one ZIP file (devicedata.zip) and sent to the server.

The ZIP file is not encrypted and the password is not attached.

-> This should not apply because the server side cannot support it when the password is changed per model.

devicedata.xml includes Access Token.

As to the ZIP file, the hash value is calculated with MD5 and sent to the server side.

The following is the information by which the MFP receives as the response from the server:

Table 21 Reception parameter for Send Baseline data

|  |  |  |
| --- | --- | --- |
| No. | Information name | Description |
| 1 | Status | Status (Processing result of the server side)  STATUS\_OK … Data reception OK  STATUS\_FAILED … A fatal error occurred  STATUS\_FAILED\_DATAINTEGRITY … Hash value mismatch |
| 2 | Reconnect | (It is not used presently.)  Reconnection request flag (when the value is 1, the server requests reconnection.) |

#### Meta data

The following is the information for metadata (metadata.xml) in baseline data (ZIP file) which is sent from MFP to cloud server. (element name = ‘DeviceData’)

Table 22 metadata for Baseline data

|  |  |  |
| --- | --- | --- |
| No. | Information name | Description |
| 1 | id | ID for MFP data |
| 2 | DataType | Type of MFP data:  (They are created by “SendDataConfig” setting.)  DEVICE\_CONFIG  JOB\_LOG  ~~ERROR\_LOG~~  ACTIVITY\_LOG CLONE\_DATA  ~~SERVICE\_FILE~~  DEVICE\_DOM  MESSAGE\_LOG  DEVICE\_ERROR  DEPARTMENT\_COUNTERS  OTHER\_LOG |
| 3 | FileName | File name for MFP data |

#### devicedata.xml

The following is the information for configuration data (devicedata.xml) (element name = ‘SendDataRequest’)

Table 23 configuration data in Baseline data

|  |  |  |
| --- | --- | --- |
| No. | Information name | Description |
| 1 | AccessToken | Access Token which MFP got during RegisterDevice |
| 2 | Data/Cloned/ Parameter/Category | XPATH category. Select from items below:  Network  SecurityConfiguration  VersionInfo  Device  CloudSyncSchedule  Authentication  DeviceService |
| 3 | Data/Cloned/ Parameter/Xpath | XPATH |
| 4 | Data/Cloned/ Parameter/Value | XPATH value |
| 5 | Data/Cloned/ Parameter/TimeBasedvalue | Time based variable value  Format is consist of pairs: 24 hour time and values. e.g.  8,11;15,9:20,1  8:00 🡪 Value = 11  15:00 🡪 Value = 9  20:00 🡪 Value = 1 |
| 6 | Data/Category05/Code  MainCode  SubCode  Value  TimeBasedvalue | 05 code and value |
| 7 | Data/Category08/Code  MainCode  SubCode  Value  TimeBasedvalue | 08 code and value |
| 8 | Data/Category13/Code  MainCode  SubCode  Value  TimeBasedvalue | 13 code and value |
| 9 | Data/ApplicationList/  ApplicationInformation/  Id  ApplicationName  Version  LicenseStatus  VendorName | Information of installed embedded application |
| 10 | Data/UserPaperTypeInformation/ UserPaperType/  TypeNumber  TypeName  FileName  PaperType | Information of installed user paper type |
| 11 | Data/LicenseList/  Count  Entry/\* | Information of installed license |

#### Normal Sequence



Fig. 8 Send Baseline data

#### Abnormal Sequence

(Communication error during Baseline data transmission)

Delete the Baseline data and perform the retry processing mentioned later.

(Power failure during Baseline data transmission)

Delete the Baseline data before communication at the next start-up.

(Failing in obtaining the MFP setting value)

Execute the transmission processing to the server without performing any special error processing.

Only the setting value which could not be obtained is missed, and sent to the server without a file. In the worst case, a blank file is sent to the server.

(STATUS\_FAILED, STATUS\_FAILED\_DATAINTEGRITY)

Delete the created data. Exit the communication cycle and wait until the next communication starts.

### Install Package

The MFP installs the update package after “Send baseline data”.

When MFP receives applying cloning data instruction, it always applies the data.

(Even if SendDataConfig parameters are “off”, it should apply the data.)

#### Normal Sequence

(For other than firmware update)



Fig. 9 Installation of the update package

(For firmware update)



Fig. 10 Firmware update

#### Abnormal Sequence

(Power failure during installation)

Delete the update package data or the firmware data before communication at the next start-up.

(Power failure while waiting for the schedule)

From L6.15, firmware update will execute at the scheduled time. If the scheduled time is already passed when MFP comes up, firmware update will be scheduled to same time during next day.

Before L6.15, firmware update will be executed 1 hour after the reboot of device.

(Installation cannot start due to exclusion)

The processing is the same as when failing in installation.

(Failing in installation)

As with the normal sequence, notify the update result to the server. Regular communication is scheduled after 1 hour of installation failure. If device is powered off and on in between the regular schedule, boot up communication will happen. Once boot up communication is done, regular communication schedule is updated with usual regular communication time.

After that, since policy violation is continued, the server makes an instruction to update firmware. When it is repeated 3 times, the server stops sending the update instruction.

(Failing in one or more update upon receiving plural update instructions)

Update installation processing continues till it finishes even if there is an error. As with the normal sequence, notify the update results to the server and continue the regular cycle.

(SSD model)

Firmware update is impossible for SSD models. The operation should be the same as (Failing in installation) mentioned above.

### Update Status

The MFP notifies the installation status of the update package by calling the interface, “Update Status”, at the server side after “Install Package”.

#### Communication Parameter

The following is the information which is sent to the server from the MFP:

Table 24 Transmission parameter for Update Status

|  |  |  |
| --- | --- | --- |
| No. | Information name | Description |
| 1 | Token | Token  The same token issued from the server at Register Device is set. |
| 2 | PolicyId | Policy Id which is included in the package (ZIP file) received from the server at Download Package.  ID of the instruction (Policy) to which the installation results are notified. |
| 3 | UpdateStatus | Installation status notified to the server.  DOWNLOADING  DOWNLOADED  INSTALLED  FAILED  SCHEDULED  INSTALING  START  CLEARED (It’s not used.)  SYSTEMBUSY |
| 4 | UpdateType | Type of the instructions of the package (ZIP file) received from the server at Download Package  POLICY\_VIOLATION\_DATA  RESTORE\_DATA  ALL\_DATA (It’s not used.)  PLUGIN\_UPDATE (It’s not used.)  EOL\_INSTRUCTIONS  BOL\_INSTRUCTIONS (It’s not used.)  FIRMWARE\_UPDATE  SPECIAL\_INSTRUCTIONS  SPECIAL\_INSTRUCTIONS\_DEVICE\_DEBUG\_FILE  DEPT\_COUNTER\_INSTRUCTIONS (It’s not used.)  CUSTOMIZED\_UI\_DATA  APPLICATION\_OPERATION  APPLICATION\_LICENSE\_OPERATION  APPLICATION\_LOCALIZATION\_OPERATION  CUSTOM\_USER\_PAPER\_TYPE  LICENSE\_OPERATION |
| 5 | Progress | It is used only when downloading the firmware data.  Data size after downloaded. (KByte) |

State transition of the notification in No.3 UpdateStatus is as follows:

(Firmware update and other instruction which needs download data)

(SCHEDULED) → DOWNLOADING (download size) → DOWNLOADED → INSTALLING → INSTALLED

(Else)

DOWNLOADED → INSTALLED

The following is the information by which the MFP receives as the response from the server

Table 25 Reception parameter for Update Status

|  |  |  |
| --- | --- | --- |
| No. | Information name | Description |
| 1 | Status | Status (Processing result at the server side)  STATUS\_OK  STATUS\_FAILED … A fatal error occurred.  STATUS\_INVALID\_TOKEN … Token is not correct.  STATUS\_INVALID\_DATA … Data is invalid |

#### Normal Sequence



Fig. 11 Update Status sequence

The MFP reboots after receiving response from the server.

When only SPECIAL\_INSTRUCTION is sent, the MFP does not reboot and executes the next “Send Regular Data (Send Zip)” processing.

#### Abnormal Sequence

(Communication error during Update Status transmission)

It’s same behavior as 4.4.8.2.

(Power failure during Update Status transmission)

No special processing is required.

### Send Regular Data

The MFP sends each setting information to the server by calling the interface, “Send Zip (isBaseline= false)”, at the server side after “Update Status”. At this time, the MFP judges that it is a reboot after installation of the update package by the flag, and executes “Send Zip”, omitting the “Register Device” and “Check for Updates” processing.

The MFP creates send data by “SendDataConfig” setting which server notifies.

#### Communication Parameter

The following is the information sent to the server from the MFP:

These data are collected by “SendDataConfig” setting.

Table 26 MFP information included in Regular data

|  |  |  |
| --- | --- | --- |
| No. | Type | Description |
| 1 | Metadata | File which explains the contents of the Regular data  (metadata.xml) |
| 2 | Setting value of the MFP | All 05/08/13 setting values, security setting value, network setting value, and MFP information, Installed embedded application information, installed user paper type information and installed license information.  (devicedata.xml)  (All 05/08/13 setting values are the value from 0000 through 9999 obtained by the GetList command. It does not include the design codes, and information such as the password is masked with \*\*\*\*\* (asterisks), etc.) |
| 3 | Regular communication schedule setting | Regular communication schedule setting for the MFP to connect with the server  (devicedata.xml) |
| 4 | Clone file | Cloning data |
| 5 | Job Log | Print log, Scan log  (FAX transmission log and FAX receive log are supported L6.0 and later development.)  A csv file and its .schema are gathered in a ZIP file and sent. |
| 6 | Message Log | Presently, it is divided into 3 types of groups (messages, error, others).  A csv file and its .schema are gathered in a ZIP file and sent respectively. |
| 7 | CSV file group of 9S+300 | “Same as 9S+300” includes the following information:  ADJUSTMENT\_LIST (05 list)  SETTING\_LIST (08 list)  PM\_LIST  PIXEL\_TONER\_LIST  PIXEL\_SERVICE\_LIST  ERROR\_LOG (Error history)  FW\_UPGRADE\_LOG  POWER\_ONOFF\_LOG  VERSION\_LIST  ENG\_FW\_LOG (Some devices)  TOTAL\_COUNTER\_LIST  APPLICATION\_LIST (bBN only) |
| 8 | FUNCTION LIST | The same contents as the FUNCTION LIST executed by the administrator is sent as a postscript file from the [FUSER FUNCTION] screen on the panel. |
| 9 | NIC CONFIGURATION LIST | The same contents as the NIC CONFIGURATION LIST executed by the administrator is sent as a postscript file from the [FUSER FUNCTION] screen on the panel. |
| 10 | SCC module debug log | (Only when the server requests by SPECIAL\_INSTRUCTION)  SCC module debug log |
| 11 | bBX debug log | (Only when the server requests by  SPECIAL\_INSTRUCTIONS\_DEVICE\_DEBUG\_FILE)  bBX debug log (It’s an encrypted file which includes debug log, defunct log and power off log) |
| 12 | Paper sensor log | The log data of paper sensor  Maximum 2 files are gathered in a ZIP file and sent. |

These are gathered in one ZIP file (devicedata.zip) and sent to the server.

The ZIP file is not encrypted and the password is not attached.

-> This should not be applied because the server side cannot support it when the password is changed per model.

devicedata.xml includes Access Token.

As to the ZIP file, the hash value is calculated with MD5 and sent to the server side.

The following is the information by which the MFP receives as the response from the server:

Table 27 Reception parameter for Send Regular data

|  |  |  |
| --- | --- | --- |
| No. | Information name | Description |
| 1 | Status | Status (Processing result of the server side)  STATUS\_OK … Data reception OK  STATUS\_FAILED … A fatal error occurred  STATUS\_FAILED\_DATAINTEGRITY … Hash value mismatch |
| 2 | Reconnect | (It is not used presently.)  Reconnection request flag (when the value is 1, the server requests reconnection.) |

#### Meta data

The following is the information for metadata (metadata.xml) in regular data (ZIP file) which is sent from MFP to cloud server. (element name = ‘DeviceData’)

Table 28 metadata for Regular data

|  |  |  |
| --- | --- | --- |
| No. | Information name | Description |
| 1 | id | ID for MFP data |
| 2 | DataType | Type of MFP data:  (Included every time)  DEVICE\_CONFIG  (Collected by SendDataConfig setting)  JOB\_LOG  ~~ERROR\_LOG~~  ~~ACTIVITY\_LOG~~ CLONE\_DATA  ~~SERVICE\_FILE~~  DEVICE\_DOM  MESSAGE\_LOG  ~~DEVICE\_ERROR~~  DEPARTMENT\_COUNTERS  OTHER\_LOG  (Collected only when server sends “Special Instruction”)  DEBUG\_LOG |
| 3 | FileName | File name for MFP data |

#### devicedata.xml

The information for configuration data (devicedata.xml) which is included in regular data (ZIP file) is same contents as 4.4.6.3.

#### Normal Sequence



Fig. 12 Regular Data Transmission

#### Abnormal Sequence

(Communication error during Regular data transmission)

Delete the Regular data and perform the retry processing mentioned later.

(Power failure during Regular data transmission)

Delete the Regular data before communication at the next start-up.

(Failing in obtaining the MFP setting value)

Execute the transmission processing to the server without performing any special error processing.

Only the setting value which could not be obtained is missed, and sent to the server without a file. In the worst case, a blank file is sent to the server.

(STATUS\_FAILED, STATUS\_FAILED\_DATAINTEGRITY)

Delete the created data. Exit the communication cycle and waits until the next communication starts.

### Send EOL Status

The MFP notifies the status of the EOL processing results by calling the interface, “EOL Status”, at the server side after “Install Package” when the update package type is EOL\_INSTRUCTION.

This is unsupported function.

#### Communication Parameter

The following is the information sent to the server from the MFP:

Table 29 Transmission parameter of EOL Status

|  |  |  |
| --- | --- | --- |
| No. | Information name | Description |
| 1 | Token | Token  The same token issued from the server at Register Device is set. |
| 2 | Status | EOL processing results  SUCCESS  FAILED |
| 3 | EOLDate | Date EOL processing is completed  e.g. 04/24/2014 01:44:37 |
| 4 | Counter | MFP counter information |
| 5 | Contact | Contact information |

The information that the MFP receives as the response from the server is HTTP Response only, and there is no parameter which is to be defined as SCC.

### EOL Report Print

The MFP prints the EOL Report after “Send EOL Status”.

The following is the printed contents:

Same limitation happens as same as chapter: 4.2.2 SCC report print specification in V1.0

This is unsupported function.

Table 30 Items for EOL report

|  |  |
| --- | --- |
| Report Item | Description |
| Date and Time of Installation | EOL executed date & time  YYYY:MM:DD HH:MM:ssssssss |
| Serial Number | MFP’s serial number  (e.g. C7H220662) |
| Total Counters | Total counter value when EOL is executed  (e.g. 5357) |
| Service Locked | List for locked service by EOL |
| Protocol disabled | List for locked network protocols by EOL |
| Customer Data deleted | List for deleted user data by EOL |
| Job data deletion result | Result for job data secure erase by EOL |
| Contact Info | Contact information (email address etc) |

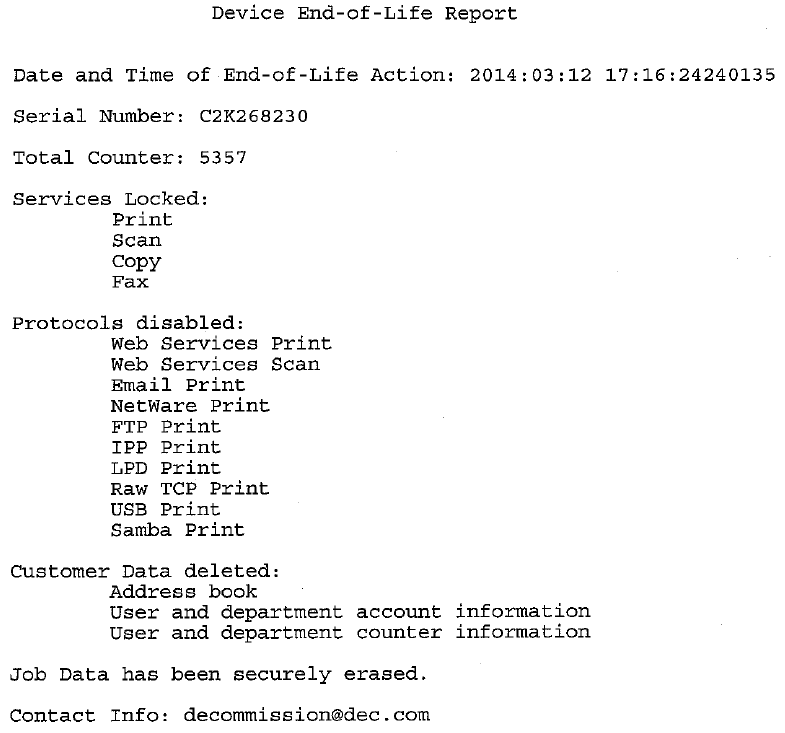


Figure 1 Example of EOL report

### Send BOL Status

The MFP notifies the status of the BOL processing results by calling the interface, “BOL Status”, at the server side after “Install Package” when the update package type is BOL\_INSTRUCTION.

This is unsupported function.

#### Communication Parameter

The following is the information sent to the server from the MFP:

Table 31 Transmission parameter for BOL Status

|  |  |  |
| --- | --- | --- |
| No. | Information name | Description |
| 1 | Token | Token  The same token issued from the server at Register Device is set. |
| 2 | Status | BOL processing results  SUCCESS  FAILED |

The information that the MFP receives as the response from the server is HTTP Response only, and there is no parameter which is to be defined as SCC.

### GetRedirectURL

The MFP will get Redirect URL information before Registration Device. MFP will redirect URL by using the URL and port number value which is acquired from Cloud server.

When URL forward setting is “Disable”, this function isn’t used.

#### Communication Parameter

The following is the information sent to the server from the MFP:

Table 32 Transmission parameter for GetRedirectURL

|  |  |  |
| --- | --- | --- |
| No. | Information name | Description |
| 1 | Counter | Counter of number of retries. Initial value is zero. Maximum number depends upon redirectable URLs. |

　The following is the information received from the server:

Table 33 Reception parameter for GetRedirectURL

|  |  |  |
| --- | --- | --- |
| No. | 情報名 | 説明 |
| 1 | Status | Received status from server  STATUS\_OK: a valid URL and port are returned  STATUS\_REDIRECTDISABLE: redirect is currently disabled  STATUS\_INVALIDIP: cloud cannot resolve IP to country. Device should keep retrying.  STATUS\_INVALIDREGION: cloud could not find a region for the resolved country. Device should keep retrying.  STATUS\_EXCEEDMAXTRY: cloud has attempted all regions. Device should stop retrying.  STATUS\_ERROR: certain internal cloud error occurs. Device should stop retrying. |
| 2 | RedirectURL | The URL to connect to |
| 3 | Port | The port to connect to |
| 4 | ClientIP | The IP address of the connecting device, for reference. |
| 5 | Region | The Region that the ClientIP maps to, for reference.  NA: North America  EU: Europe  AP: Asia-Pacific |

### Panel Message Display

The MFP displays a message that it is under SCC processing (Service in progress. Please do not turn off: %02d (%02d is a 2-digit numerical value)) on the status window of the panel (the left bottom) during the SCC regular communication cycle processing.



Service in progress. Please do not turn off:01

Table 34 Status and displayed numerical value during SCC processing

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Status during SCC processing | Description | Displayed numeric value |
| 1 | REGISTERINGDEVICE | Validating registration | 01 |
| 2 | CHECKINGFORUPDATES | Checking for updates | 02 |
| 3 | DOWNLOADINGUPDATES | Downloading updates | 03 |
| 4 | INSTALLINGUPDATES (\*1) | Installing updates | 04 |
| 5 | RESTORING (\*1) | Restoring configuration | 05 |
| 6-1 | GATHERINGDATA | Gathering device data | 06 |
| 6-2 | GATHERING9SDATA (\*1) | Gathering 9S-300 data | 06 |
| 7 | SENDINGDATA | Updating cloud data | 07 |
| 8 | DOWNLOADINGFIRMWARE | Downloading firmware | 08 |
| 9 | UPGRADINGFIRMWARE (\*2) | Upgrading firmware | 09 |
| 10 | SCHEDULEDFIRMWAREUPDATE | Scheduling firmware update | 10 |
| 11 | DEACTIVATING | Device has been decommissioned | 11 |
| 12 | REACTIVATING | Device has been activated | 12 |

(\*) While MFP is in these statuses, popup window is displayed. Popup window has sand clock picture.

(\*1) The title of the popup windows is “PROCEDSSING” and the message is same as it of status window.

(\*2) This popup window is same as current specification.

(While MFP is in “RESTORING” status, sand clock popup should be displayed and while it is in “UPGRADINGFIRMWARE” status, sand clock with progress bar should be displayed.)

Message Display Priority is the top of Pattern 2

04\_Design/AL/PanelUI/JEE-01607\_ScreenDefinition\_StatusWindow.doc

Please refer to attached excel file in page 10

## Event Notification Loop

### Communication Start Timing of Event Notification Loop

The MFP communicates with the server at the either one of the following timings after normal startup

* An event has occurred when going to see the MFP status at SCC process startup
* An event occurs

### Communication Sequence of Event Notification Loop

The MFP communicates in order of the following sequence at communication with the server (hereinafter, called “Communication cycle”.)

Table 35 Communication sequence with server

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Communication name | Communication contents to the server | Server URL: (it is common up to the following.)  http:// Tprinters.cloudapp.net:8080/DeviceService.svc/ |
| 1 | SendDeviceError | Notify the server of the event occurred in the MFP. | device/error |
| 2 | SendServiceFile | Transfer the Service File (9S-300 + LIST) to the server.  (only when it is requested from the server by the Send Device Error response)  (Only definition) | device/file/send |

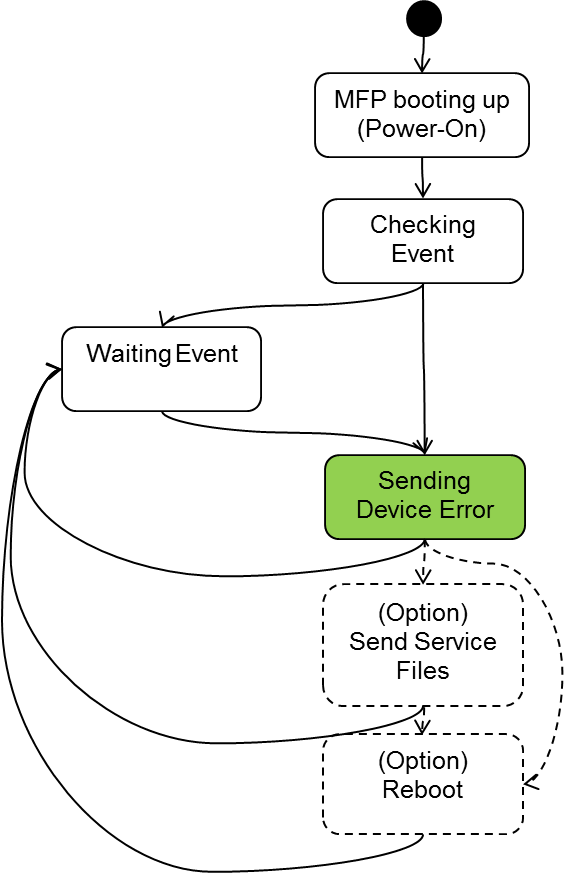


Fig. 13 Communication sequence for event notification loop

### Send Device Error

An event occurred in the MFP is notified with the thread which is different from the communication cycle mentioned in 4.4.2 in SCC. The event occurred in the MFP is notified to the server by calling the interface, “Send Device Error”, at the server side. Only errors which have error code are notified.

When any errors happen same error shouldn’t be sent to server unless they are removed.

When device detect errors removal without power off, they are notified to server with ‘-‘. (e.g. –D102).

#### Communication Parameter

The following is the information sent to the server from the MFP：

Table 36 Transmission parameter for Send Device Error

|  |  |  |
| --- | --- | --- |
| No. | Information name | Description |
| 1 | Token | Token  The same token issued from the server at Register Device is set. |
| 2 | Error/Level | Error level  It corresponds to the following of the MFP DOM (DeviceStatus.xsd):  /MFP/ErrorState/ErrorLevel |
| 4 | Error/Name | Error name  It corresponds to the following of the MFP DOM (DeviceStatus.xsd):  /MFP/ErrorState/Details/Name |
| 5 | Error/Code | Error code  It corresponds to the following of the MFP DOM (DeviceStatus.xsd).  /MFP/ErrorState/Details/Code |
| 7 | Error/Description | Error description  (Presently it is not used. Empty tag.) |
| 3 | Error/Jams/Jam/Location | Jam occurred location  (only when jam occurred.)  It corresponds to the following of the MFP DOM (DeviceStatus.xsd):  /MFP/ErrorState/JamLocation |

The following is the information by which the MFP receives as the response from the server：

Table 37 Reception parameter for Send Device Error

|  |  |  |
| --- | --- | --- |
| No. | Information name | Description |
| 1 | Status | Status (Processing results at the server side)  STATUS\_OK  STATUS\_INVALID\_TOKEN  STATUS\_FAILED |
| 2 | RebootRequired | Flag which is set when reboot is required for recovery from an error  Boolean value: true or false  The MFP reboots when this flag is ON.  Presently, due to “Auto Reboot of Fatal Error”, reboot is executed twice together with this flag. Thus, this flag will not be requested from the server as true, but false when the present pilot implementation is changed to L4.73 product implementation) |
| 3 | RequestServiceFiles | Flag which send 9S-300, FUNCTION LIST, and NIC CONFIGURATION LIST for error cause analysis.  Boolean value: true or false  The MFP transfers the file to the server when this flag is ON.  This parameter is only defined. It isn’t used. |

#### Normal Sequence



Fig. 14 Send Device Error sequence

#### Abnormal Sequence

(Communication error occurred at SendDeviceError)

The MFP executes the retry processing with the intervals of 60 min., but does not go into the retry mode.

(Power failure occurred during SendDeviceError)

No recovery processing is performed.

(Fxxx categoriezed error)

Because network isn’t available, device can’t send error to server.

### Send Service File

The MFP transfers the Service File (CSV file group of 9S+300, FUNCTION LIST, and postscript file of NIC CONFIGURATION LIST) to the server when it receives RequestServiceFiles=true as a response to “Send Device Error”. The MFP transfers a ZIP file in which the file group is gathered by calling the interface, “Send Service Files”, at the server side. (This parameter is only defined. It isn’t used.)

#### Communication Parameter

The following is the information sent to the server from the MFP：

Table 38 MFP information included in Service File data

|  |  |  |
| --- | --- | --- |
| No. | Type | Description |
| 1 | Metadata | File which explains the contents of the Service File data (ZIP file)  (metadata.xml)  Token factor is included. |
| 2 | CSV file group of 9S+300 | “Same as 9S+300” includes the following information:  ADJUSTMENT\_LIST (05 list)  SETTING\_LIST (08 list)  PM\_LIST  PIXEL\_TONER\_LIST  PIXEL\_SERVICE\_LIST  ERROR\_LOG (Error history)  FW\_UPGRADE\_LOG  POWER\_ONOFF\_LOG  VERSION\_LIST  ENG\_FW\_LOG (Some devices)  TOTAL\_COUNTER\_LIST  APPLICATION\_LIST |
| 3 | FUNCTION LIST | The same contents as the FUNCTION LIST executed by the administrator is sent as a postscript file from the [FUSER FUNCTION] screen on the panel. |
| 4 | NIC CONFIGURATION LIST | The same contents as the NIC CONFIGURATION LIST executed by the administrator is sent as a postscript file from the [FUSER FUNCTION] screen on the panel. |

These are gathered in one ZIP file (devicedata.zip) and sent to the server.

The ZIP file is not encrypted and the password is not attached.

(This will be changed to the ZIP file with a password when the present pilot implementation is changed to L4.73 product implementation. Use the self-diagnostic code 08-8715 for the password).

As to the ZIP file, the hash value is calculated with MD5 and sent to the server side.

The information that the MFP receives as the response from the server is HTTP Response only, and there is no parameter which is to be defined as SCC.

#### Normal Sequence

#### Abnormal Sequence

(Communication error occurred at SendServiceFile)

The MFP executes the retry processing with the intervals of 60 min., but does not go into the retry mode.

(Power failure occurred during SendServiceFile)

The created data is deleted before communication at the next start-up.

## BOL, EOL

BOL and EOL are unsupported function. EOL is implemented as remote decommission. Refer to JEA-03452.

The following is the status transition diagram for EOL (End Of Life: The MFP retires from SCC operation) and BOL (Begging Of Life: The MFP serves in SCC).



Fig. 15 State transition diagram for BOL and EOL

## Others

### Super Sleep

#### SCC is in process before going into Super Sleep

(The MFP starts communication with the server.)

When the MFP starts communication with the server, it does not go into Power save, Sleep and Super Sleep during the communication cycle period.

Except scheduling firmware update state.

#### SCC processing occurs during Super Sleep

(At regular communication with the server)

When the MFP is in the Super Sleep state at the time of the regular communication time with the server, the MFP recovers from the Super Sleep state (Wake up engine) and starts communication with the server. The MFP goes into the Super Sleep state after communication cycle processing.

(Waiting for an event)

The MFP cannot detect the events at the event loop side during Super Sleep.

(Wait of the retry mode)

When the MFP is in the Super Sleep state at the timing of exiting from 24-hours Wait, the MFP recovers from the Super Sleep state and starts communication with the server. The MFP goes into the Super Sleep state again after communication cycle processing.

### Hibernation

MFP doesn’t goes into hibernation during the communication cycle. Except scheduling firmware update state.

### Persistent Policy

**[Background]**

User Administrator may change 08/05/13 settings from Top Access locally during waiting the sync schedule to cloud server. But there is the case which service engineer wants to keep the 08/05/13 setting instructed by the policy from cloud.

**[Function]**

Persistent Policy check is executed to keep the 08/05/13 settings. Periodical check will be done based on the persistent interval set by Cloud server.

Persistent Expiration setting is available. If the duration is over persistent expiration then persistent policy check will be stopped.

**[Parameters from cloud server]**

2 parameters listed below are set in Policy schema.

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter name | Description | Max. value  Min. value | Default Value |
| PersistentInterval | Persistent Policy check duration | MAX: 1440 (min) 24hours  MIN: 60 (min) 1 hour | 300 (min) 5 hours |
| PersistentExpiration | Persistent Policy check expiration | MAX: -  MIN: 0 (day) | 7 days |

**[Behavior]**

Case1: No Persistent Check

Cloud server sets PersistentExpiration = 0

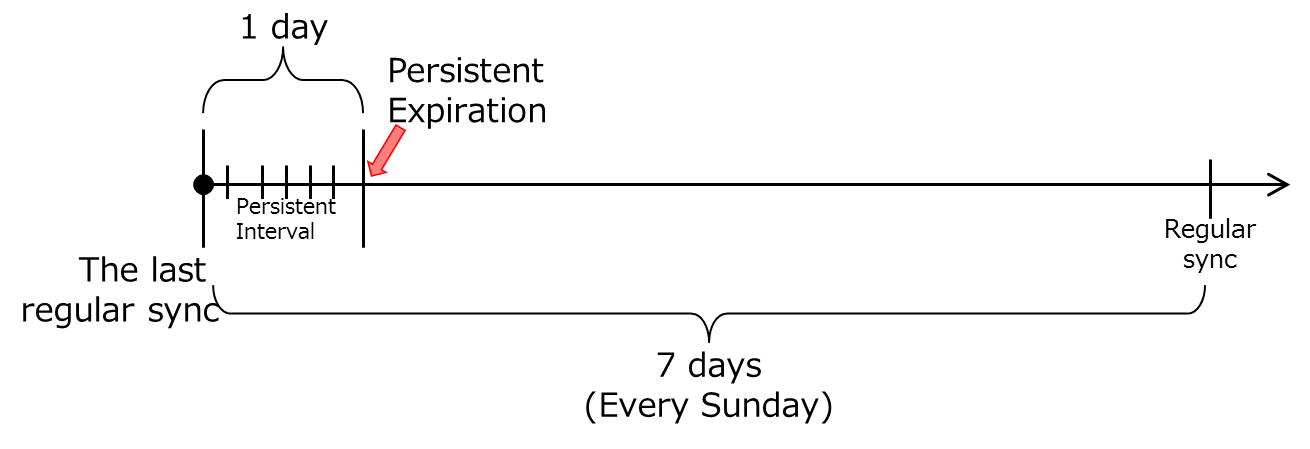
Case2: Sync communication schedule > Persistent Policy Check Expiration

If Persistent Policy check expiration is shorter then sync communication schedule:

Persistent Policy Check Expiration = 1 day

Sync communication schedule = 7 days

Persistent policy check will stop in case persistent policy check expiration is over from last sync communication.



Case3: Sync communication schedule < Persistent Policy check expiration

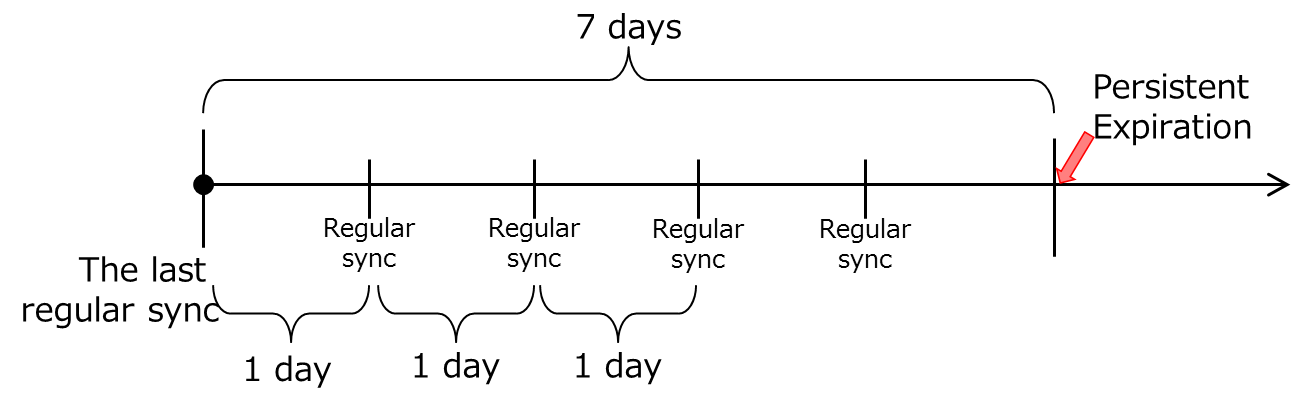
If Persistent Policy check expiration is longer then sync communication schedule:

Persistent Policy Check Expiration = 7 days

Sync communication schedule = 1 day

No expiration. Persistent Policy will be executed forever.

It’s because the timer is reset when every sync communication.



### Time-based Device State Data Values

**[Background]**

Time-based setting value change (08/05/13 code value) is required.

For example, energy save timer = 10 min in day time (MFP is frequently used in working time) but energy save timer = 1 min at night (MFP is not used).

**[Function]**

Time-based value can be set for 08/05/13 code value.

**[Parameters from cloud server]**

The listed items will be defined in Policy schema.

|  |  |  |
| --- | --- | --- |
| Parameter name | Description | Value |
| TimeBasedvalue | Time based value | Format is (time,value;)\*(time,value).  'time' is in 24 hour format, (0-23).  Sample:  '8,11;15,9;20,1'.  Value to 11 at 8am,  to 9 at 3pm,  to 1 at 8pm. |

### IP Redirect

**[Background]**

Now there are 3 sites for SCC cloud server in the world (North America, Europe, Asia-pacific). MFP must communicate with the appropriate region site.

**[Function]**

When the MFP is going to connect to the cloud server for the first time, MFP will ask the North American cloud server to get the appropriate URL (GetRedirectURLRequest).

North America cloud server detects the region from the MFP’s IP address and reply the best destination URL, (GetRedirectURLResponse). MFP sends a RegistrationRequest to the URL which it received.

#### Communication Parameter

The following is the information which is sent to the server from the MFP:

Table 39 Transmission parameter for the Get Redirect URL

|  |  |  |
| --- | --- | --- |
| No. | Information name | Description |
| 1 | Counter | Counter of number of retries. Initial vaue is zero. Maximum number depends upon redirectable URLs. |

The following is the information by which the MFP receives as the response from the server:

Table 40 Reception parameter for Get Redirect URL

|  |  |  |
| --- | --- | --- |
| No. | Information name | Description |
| 1 | Status | Response status  STATUS\_OK: a valid URL and port are returned  STATUS\_REDIRECTDISABLE: redirect is currently disabled  STATUS\_INVALIDIP: cloud cannot resolve IP to country. Device should keep retrying.  STATUS\_INVALIDREGION: cloud could not find a region for the resolved country. Device should keep retrying.  STATUS\_EXCEEDMAXTRY: cloud has attempted all regions. Device should stop retrying.  STATUS\_ERROR: certain internal cloud error occurs. Device should stop retrying. |
| 2 | RedirectURL | The URL connect to |
| 3 | Port | The port number to connect to |
| 4 | ClientIP | The IP address of the connecting device, for reference. |
| 5 | Region | The Region that the ClientIP maps to, for reference  Enumeration value:  NA : North America  EU : Europe  AP : Asia-Pacific |

## Definition of Boundary Threshold

(Max. size of the update package)

The maximum size of the update package which is downloaded and expanded from the server to the MFP is ○○MByte. (Present value of the build ○○)

(Max. size of the Baseline data and Regular data)

The maximum size of the Regular data transferred from the MFP to the server is ○○MByte. (Present value of the build ○○)

## Error Handling

### Retry Processing at Communication Error



Fig. 16 Retry processing at communication error

#### Connection Error

The MFP retries communication with the server in 60 seconds after detecting the error. When the first retry fails, the following Retry Mode processing is performed.

#### HTTP Error

When the server responds a HTTP error, the MFP retries communication in 60 seconds after detecting the error. When the second retry fails, the following Retry Mode processing is performed.

#### Retry Mode

The MFP goes into the retry mode even during communication of any messages when it fails in retry operation mentioned above. The retry mode continues until the MFP succeeds in communication.

The MFP tries to communicate with the server once a day during the retry mode. It starts communication in 24 hours after the previous failure, ignoring the schedule set by the regular communication. In the retry mode, communication starts from Register Device even if the previous failure occurred with any messages.

As for the interface of the event notification loop, “Send Device Error” and “Send Service File”, this operation does not apply.

When power failure occurs during the retry mode, the retry mode is cancelled, and the MFP starts the normal regular communication cycle after power on.

### Message Log

In SCC processing, the Message Logs are recorded in the following cases. Please refer to JEA-02123\_bBX\_ErrorCodeSpecification.xls.

Table 41 SCC error code list

|  |  |  |  |
| --- | --- | --- | --- |
| Error code | Error level | Notification  Category | Description |
| 0x5410 | Warning | - | **<Remote maintenance service error>**  The server returns STATUS\_UNREGISTERED.  (Failed to register the MFP) |
| 0x5411 | Warning | - | **<Remote maintenance service error>**  The server returns STATUS\_LOCKED.  (MFP registration is locked ) |
| 0x5412 | Warning | - | **<Remote maintenance service error>**  The server returns STATUS\_BUSY.  (Server BUSY occurred) |
| 0x5413 | Warning | - | **<Remote maintenance service error>**  The server returns STATUS\_FAILED.  (Fatal error occurred in the server) |
| 0x5414 | Warning | - | **<Remote maintenance service error>**  Integrity Check error of the ZIP file (baseline and regular data).  The server returns STATUS\_FAILED\_DATAINTEGRITY.  (Device file is not correct) |
| 0x5415 | Warning | - | **<Remote maintenance service error>**  Entered Retry Mode |
| 0x5416 | Warning | - | **<Remote maintenance service error>**  (Failed in installation of the update package) |
| 0x5417 | Warning | - | **<Remote maintenance service error>**  Integrity Check error of the ZIP file (Instructions from server)  (Update package is not correct) |
| 0x5418 | Warning | - | **<Remote maintenance service error>**  (Failed in installation of the file.)  This code isn’t used. Definition only. |
| 0x5419 | Warning | - | **<Remote maintenance service error>**  File is deleted because The file size is bigger than 200MB  (Delete file) |
| 0x5400 | Information | - | **<Succeeded in MFP registration>**  The server returns STATUS\_REGISTERED. |
| 0x71F2 | Information | Cloning  (existing category) | **<Successfully imported Clone File>** (existing message) |
| 0x7100 | Information | System Update  (existing category) | **<Successfully updated Copier Firmware>** (existing message) |
| 0x7182  0x7183  0x7184  0x7185 | Information | Change Settings  (existing category) | **<Edited Device Setting>** (existing message)  **<Edited Network Setting>** (existing message)  **<Edited Security Setting>** (existing message)  **<Edited Authentication Setting>** (existing message)  The setting value is changed in the background without noticing the user. |

## Device Error Handling

(The cases of power failure and HDD full are mentioned in each function description.)

# Performance Definition

The performance should not be degraded than the time in which time for executing the individual functions, such as 9S-300 acquisition, clone data application and firmware application, is accumulated.

Start-up time after power on should not be impacted.

# Restriction Definition

## Functional Restriction

When an event occurs and cancelled immediately when scc error notification process is in busy state,

the event may not be notified to the server.

Busy state means the following:

* Startup timing.
* Sending other event.

User cannot use SCC with RDMS (BBR2). If BBR2 function is enable, and if SCC function is enable, then BBR2 will not work.　(This limitation is removed from L6.02/L6.03 development.)

If self-diagnostic boot-up mode, then network will not work.

While device is communicating to server, service UI isn’t used. SCC function doesn’t work in special boot mode.

## Input Restriction (Number of Digits, Prohibition)

None

## Exclusive Control

See the attached file.

02\_Requirement/SRS/JEA-01891\_Relationship MFP status and Function execution.xls

## Automatic Control

None

# Related Option (External OP and System OP)

None