

=====
*** Basic Information ***
=====

[Create date] 2017/10/19

[Program Name] Language Install

[Version] 1.08

[PCB No.]

[Interchangeability] X / O

[Other Firmware Requirements] None

[PCB Requirements] None

[Software category] Normal Release

[Release category] Normal Release

[Program category] Firmware

Exported to(language) GEN(ja,en,gb,f,e,d,i,nl,s,n,dk,sf,p,pl,h,cz,ru,tr,ca)

[Firmware No.] D0191496

[File Information]

File Name D0191496.fwu

File Type Module for Service

Size 11.91 MB (12486876 byte)

[Availability of RFU] No

[Production reflection] 1st Mass Production

=====
*** Note ***
=====

[Note]

=====
*** Important Notes ***
=====

[Important Notes]

=====
*** Modification History ***
=====

[Modifications made:]

Language firmware for R-C5.5 was released to the firmware download list.

[Modification history]

Version 1.08
1st mass production

=====
*** Basic Information ***
=====

[Create date] 2018/05/21

[Program Name] System/Copy

[Version] 1.23

[PCB No.]

[Interchangeability] X / O

[Other Firmware Requirements] None

[PCB Requirements] None

[Software category] Normal Release

[Release category] Normal Release

[Program category] Firmware

Exported to(language) GEN(all)

[Firmware No.] D0195331W

[File Information]

File Name D0195331W.fwu

File Type Module for Service

Size 16.59 MB (17393780 byte)

[File Information]

File Name D0195331W.rfu

File Type Module for Remote Upgrade

Size 16.59 MB (17400064 byte)

[Availability of RFU] Yes

[Production reflection] 2018/05

=====
*** Note ***
=====

[Note]

=====
*** Important Notes ***
=====

[Important Notes]

=====
*** Modification History ***
=====

[Modifications made:]

Rank C

Other Changes:

Newly added SMBv2/v3 support.

This firmware is dependent on the following firmware modules.

Please be sure to update all of them:

- System/Copy v1.23 (D0195331W)
- Network Support v7.39 (D0205334M)
- Web Support v1.55 (D0205335H)
- Scanner v01.14 (D0195333G)

Please refer to the RTB(No.RGene095) for details.

[Modification history]

Version 1.22

Symptom Corrected:

- .SC 817, SC 819, SC 878-03 occur.

Version 1.21

Symptom corrected:

1. If the Auto Logout timer is On, there will be a memory leak occurring everytime a user logs in to the device.
2. Repeated failures to login with an IC card will lock the entire account instead of just locking out the access of that card (PIN lock).
3. The timer used for the "Access Violation" setting's time interval does not properly compensate for changes to the device timer.
4. If User Code authentication is enabled or if "External Optional Counter Type" != 0, accounts locked by the "Lock out" setting (SP-5413-1) are not locked out of WIM.
5. Although the "Logout Using Card" function of Card Authentication Package v2 is turned on, the user cannot log out when he or she swipes the card.
6. Cannot scan to shared folders in Mac OS X 10.7 or Mac OS X 10.8.
This firmware is dependent on the following firmware modules.
Please be sure to update all of them:
Network Support firmware v7.38 or later
7. Cannot communicate with the @Remote Center if embedded RC Gate is enabled.

Version 1.20

Minor change applied.

Version 1.19

Symptom corrected:

Data stored in the NAND Flash ROM on the controller board is corrupted.

Version 1.18

Symptom corrected:

1. Stored jobs (Locked Print, Sample Print, etc.) might not be shown in the operation panel if the DataOverwriteSecurity Unit is installed.
2. Pressing a Function Key that has been mapped to an SDK/J application might result in an SC997.
3. SC819 occurring during use of an SDK/J application under very specific conditions.
4. After an administrator (User, Network, or File) logs in and then out, unauthenticated users are unable to configure any of the settings in "Extended Feature Settings" even if the Machine Admin is disabled.
5. If the Machine Admin logs in before Java VM has finished starting up, it will not be possible to install SDK applications until the device has been rebooted.
6. Cannot move the HDD Encryption option to another SD card.

Version 1.17

Symptoms Corrected:

1. SC817 occurs after the firmware is updated via RFU.
2. The IPU test pattern cannot be printed out using SP4417-001.
3. Minor bug corrections.
4. The MFP operation panel might go black and not return until the power is cycled. This only occurred if User Authentication was enabled or the MFP had a Device Accounting Unit such as a coin collector or charge card reader.
5. An SC991 occurs and the Scanner cannot be used if the operation panel is turned back on within 60-120 seconds after the Auto Off Timer turns it off.
6. The MFP might stall if a document is scanned to SMB, E-mail or to the Document Server in jpeg format.

Other changes:

1. SC842 was newly added to indicate an RFU (remote firmware update) failure and to record contents which failed to be updated, and then RFU is retried.
2. Scan to Email now removes trailing dots (I.e. xxxx.com.) from destination email addresses.

Version 1.16

Symptom corrected:

1. The vendor code contained in the controller board Mac address was

- updated from "00-00-74" to "00-26-73" (all possible Mac addresses using the old vendor code have been exhausted).
2. MFPs with no HDD, stall with a SC955 error upon receiving any of the following type of job containing at least 1 blank page:
 - PS3 or PCL jobs with a resolution of 300dpi, fed LEF and the short edge of the LEF page is less than 173mm.
 - Any IPDS job.
 3. Might be unable to use the printer function if the MFP that installed VM card option, ELP and MFP Browser returns from energy saver mode.

Version 1.15

Symptom corrected:

1. Scan to NCP fails if all of the following conditions met:
 - The destination is specified using the IP address.
 - The Novell server and the device are in different subnets.
 - The subnet routers filter SLP multicasts.

Note: Requires System firmware (version 1.12 or later) and Scanner firmware (version 01.06 or later).

2. Scan to NCP fails or takes long time to complete if the IPX protocol is used and there are more than 2 Novell Directory Services (NDS) servers in the network hierarchy.

Note: Requires System firmware (version 1.12 or later) and Scanner firmware (version 01.06 or later).

3. Jobs of more than 100 pages cannot be stored on the MFP (Locked Print, Stored Print, etc.) if another job is being stored from another source (Copier, Scanner, Fax) at the same time.
4. The submission of multiple jobs containing at least 50 pages each, might result in a reboot with an error message (SC990) displayed on the operation panel. This was a very infrequently occurring problem (~.01%).
5. The printer application will stall if any of the following situations are encountered:
 - A print job is submitted while another print job is already being processed by the device.
 - A print job is submitted while the TWAIN driver is scanning.
6. A scan initiated by TWAIN might fail if a print job is already being processed by the device.
7. When SMC output is operated in duplex at SP mode, output function stops after the 5th sheet is ejected.
8. SC995 occurs under the following conditions:
 - A file containing blank page(s) is saved to the Document Server from the printer driver.
 - "Print out blank pages" is selected.
 - A stamp or other character string/mark is added to the file, and the file is then printed out.
9. The machine reboots while performing a batch print job (printing does not resume after this).
10. Incoming FAX documents cannot be forwarded.
11. When paper is fed from the tandem tray (LCT), machine behavior does not conform to the setting (priority of "productivity" or "tray") of SP5-195-001: Limitless SW.

Version 1.14

Symptom corrected:

1. If the main power is turned off during a firmware update, "Please wait" is displayed and the machine cannot be rebooted.
2. Some "File Access Privilege Change" log's entries for the CSV file that downloaded via WebImageMonitor are occurred the following phenomena.
 - "User Entry ID" is always displayed as "0x00000000".
 - "User Code /User Name" is appeared as garbage characters.Note: To fix this problem, System firmware (version 1.14 or later), WebUapl firmware (version 1.10 or later) and Scanner firmware (version 01.11 or later) needs to be applied to the device.
3. If the Password Policy is enabled, "Target User Entry ID" and "Target User Code/User Name" are not logged in the CSV file that downloaded via WebImageMonitor and in the WebSmartDevice Monitor's Access Log List when a user tries and fails due to the password policy to change their password.
4. Sudden loss of wireless network connectivity with an error message on the operation panel: "Problems with the wireless card."
5. Firmware versions of the FAX and Finisher options are not recorded in Web Image Monitor > Access Log > "Firmware: Structure".
6. The device might stall when a large number of jobs (150 or more) are printed continuously.
7. The Job log will stop recording User ID, Username or Usercode in the Printer's Job log if WIM is accessed more than 300 times using authentication.
8. If a new UserCode is added to the addressbook via WIM, a password change is recorded (Web Image Monitor > Access Log > "Password Change"), even though UserCodes don't have passwords. This only occurred using either UserCode Authentication or no User Authentication whatsoever.
9. If a user logs in and out repeatedly to the device using an IC card (Card Authentication Package option) at the same time as the address book is being updated by a delivery server such as ScanRouter, the device might stall.
10. The destination of a scanned job sent to a destination in the device's address book, might not be recorded in the Job log. Note: Requires System firmware (version 1.14 or later) and Scanner firmware (version 01.11 or later).

Other changes:

1. Global Scan NX now supports High Compression PDF files. Note: Requires Global Scan NX version 1.2 (SDK application), System firmware (version 1.14 or later), and Embedded Software Architecture SD card Ver.4.14 (SDK/J SDcard Ver.4.14 or later).
2. Global Scan NX now supports a preview function. Note: Requires Global Scan NX version 1.2 (SDK application), System firmware (version 1.14 or later), and Embedded Software Architecture SD card Ver.4.14 (SDK/J SDcard Ver.4.14 or later).
3. Scan to Email now removes trailing dots (I.e. xxxx.com.) from destination email addresses.
4. Multiple stored jobs submitted for printing simultaneously will

now be recorded individually in the Job log instead of only the first job being recorded. This change only applies to non-print jobs that have been stored. Prior to this change, the printing of stored print jobs were already recorded individually in the Job log.

Note: Requires the following firmware versions (or later):
System (version 1.14), Websys (version 1.52), Scanner (version 01.11), Web Uapl (version 1.10), and either of NFA (version 1.10M).

5. The device is able to log the downloading (using WIM or DeskTopBinder) of scanned documents from the MFP HDD.
Note: Requires System firmware (version 1.14 or later) and NFA firmware (Ver.1.10M or later).

Version 1.13

Symptom corrected:

1. Continuous printing of IPDS jobs for 5-6 hours results in the error message "Functional problem detected." being displayed on the operation panel. This is recorded in the error log as an SC687 error.
2. If a user tries to logout at the same time as another user is trying to retrieve UserCodes via WebIMageMonitor or Web SmartDeviceMonitor Ver 2, the device might stall with the message "Logging out.... Please wait".
3. If a user fails to login from the operation panel, subsequent logins/logouts might not be logged.
4. Some Lockout entries in the Access log are missing information when viewed in Web SmartDeviceMonitor Ver 2.
5. Web Smart DeviceMonitor > Access Log > "Machine Data Encryption Key Change" > "Start Date/Time" and "End Date/Time" fields are blank.
6. The printing of any SMC report including the following will be recorded in the Access Log as "Machine Data Encryption Key Change"
 - Operation panel > User Tools > Administrator Tools > "Display/Print Counter" > Counter List
 - Operation panel > User Tools > Interface Settings > Print List
7. Mismatched Entry ID and User Name in Web Smart DeviceMonitor > Access Log > "Machine Data Encryption Key Change" log.
8. Fixed: If both SNTP and Date/Time settings are configured in WIM, WIM might not be accessible. This happened very infrequently (about 1% of the time).
Note: The fix requires that NCS firmware version 7.23 or later be applied to the device.
9. Firmware updates using an SD card might fail. This was an infrequently occurring problem and could often be overcome by simply trying the update again.
10. If the login name or password used for LDAP Authentication contain extended ASCII characters (Ie. umlaut), authentication will fail.
11. If a user logs back in after their session has timed out, the device might stall with the message "Authenticating... Please wait".

Version 1.12

Symptom corrected:

1. An application might not be able to load from an SD card (Printer/Scanner unit, SDK application etc) if either of the WIM settings, Permit Firmware Update or Permit Firmware Structure Change are enabled.
2. If the device receives a large number of jobs via LPR, one of the following might happen:
 - The device will cancel some or all of the jobs.
 - The device will not be able to access the network.
3. The Scanner application will stall if the privileges of a Stored File (Scanner application function) are changed. This only occurs if the Access Log is enabled.
4. The Access Log records a password change if the Program/Change Administrator screen is opened via WIM and the OK button is pressed.
5. An admin login/logout will be logged everytime the administrator accesses a new WIM page.
Note: To fix this problems, System firmware (version 1.12 or later), Websys firmware (version 1.50 or later), Web Uapl firmware (version 1.09 or later) and Printer firmware (version 1.02 or later) needs to be applied to the device.
6. An admin login/logout will be logged everytime an Auto Email Notification or On-demand Email Notification is sent.
Note: To fix this problems, System firmware (version 1.12 or later), Websys firmware (version 1.50 or later), Web Uapl firmware (version 1.09 or later) and Printer firmware (version 1.02 or later) needs to be applied to the device.
7. Devices using an IPv6 linklocal address, might not be able to use IPsec.

Other changes:

1. The speed of switching between SDK applications is faster than before.
Note: To use this, "Embedded Software Architecture SD card Ver.4.08 (SDK/J SDcard Ver.4.08 or later)" and system firmware (version 1.06 or later) needs to be applied to the device.
2. The Card Authentication Package (SDK application) is now available.
3. The version numbers of some hardware security components called the "Ic Key" and "Ic Hdd" are displayed in the operation panel's firmware version menu.

@Remote related issue:

1. Some counter values acquired by Auto Discovery (MIB counter data) was incorrect. If the device is managed as HTTPS device, all acquired counters are correct and same as on the SMC report.
2. RFU from @ remote may not be reported to the center.

Version 1.11

Symptom corrected:

1. When connecting to an LDAP server, the device ignores all Kerberos Realms except the first field (up to 5 can be configured).
This will cause authentication to fail on any LDAP

server outside the first Kereberos Realm.

2. The E-mail address that searched by LDAP server is not displayed in "Prg.Dest".(GFPR#RA08030001)
3. 64 failed attempts to login to Simplified LDAP Authentication will cause all subsequent attempts to fail. This could be resolved by cycling the power.
4. WebImageMonitor is inaccessible if SDK applications are installed.
5. Date/Time print function on copied paper does not function correctly. The time zone setting is ignored and printed with GMT only.
6. Minor bugs related to @Remote.
7. SC828 occur or machine stalls when performing the Detailed Self-diagnostic mode.

Other changes:

1. The IPDS option is now available.
To use this option, System firmware (version 1.11 or later),
NCS firmware (version 7.14 or later),
Websys firmware (version 1.09 or later)
and Printer firmware (version 1.01 or later)
needs to be applied to the device.

Version 1.10

Symptom corrected:

- 1.The PS option will not start if it was originally installed on the same SD-card as the Printer/Scanner option (SP5-873-001) and then the Printer/Scanner option was uninstalled (SP5-873-002).
- 2.SC866 (SD Card Error 1: Confirmation) occurs when installing an SD card option.

Other changes:

- 1.The version numbers of some hardware security components called the "Ic Key" and "Ic Hdd" are displayed in the operation panel's firmware version menu.

Version 1.09

Symptom corrected:

- 1.If a USB device is removed while the MFP is in use, an SC 819 error will be shown on the operation panel.

Other changes:

- 1.The new features of "Embedded Software Architecture SD card Ver.4.03 (SDK/J SDcard Ver.4.03)" are now supported. For the details of these features, please refer to the release notes for "Embedded Software Architecture SD card Ver.4.03 (SDK/J SDcard Ver.4.03)".
- 2.Two SSP modes and UP modes have been added for Extend Certification function.
SSP mode: SP5-401-160, -161

Version 1.08

Minor bug correction.

Version 1.01.3
1st mass production

=====
*** Basic Information ***
=====

[Create date] 2018/05/21

[Program Name] Scanner

[Version] 01.14

[PCB No.]

[Interchangeability] X / O

[Other Firmware Requirements] None

[PCB Requirements] None

[Software category] Normal Release

[Release category] Normal Release

[Program category] Firmware

Exported to(language) GEN(all)

[Firmware No.] D0195333G

[File Information]

File Name D0195333G.fwu

File Type Module for Service

Size 0.98 MB (1025000 byte)

[File Information]

File Name D0195333G.rfu

File Type Module for Remote Upgrade

Size 0.98 MB (1032448 byte)

[Availability of RFU] Yes

[Production reflection] 2018/05

=====
*** Note ***
=====

[Note]

=====
*** Important Notes ***
=====

[Important Notes]

=====
*** Modification History ***
=====

[Modifications made:]

Rank C

Other changes:

Newly added SMBv2/v3 support.

This firmware is dependent on the following firmware modules.

Please be sure to update all of them:

- System/Copy v1.23 (D0195331W)
- Network Support v7.39 (D0205334M)
- Web Support v1.55 (D0205335H)
- Scanner v01.14 (D0195333G)

Please refer to the RTB(No.RGene095) for details.

[Modification history]

Version 01.13

Symptom corrected:

1. The MFP operation panel might go black and not return until the power is cycled. This only occurred if User Authentication was enabled or the MFP had a Device Accounting Unit such as a coin collector or charge card reader.
2. A scan configured to output a Multi-page TIFF might have actually output a PDF. This only occurred if both of the following conditions were met:
 - Scanner operation panel > Send Settings > Compression (Gray Scale/Full Color) > OFF
 - Scanner operation panel > Scan Settings > Scan Type > Auto Color Select
3. The scanner will stall "Updating the destination List. Please wait..." will be displayed on the operation panel. This occurs if the device's address book is updated via ScanRouter while the device is in Sleep Mode.

Version 01.12

Symptom corrected:

1. Scan to NCP fails if all of the following conditions met:
 - The destination is specified using the IP address.
 - The Novell server and the device are in different subnets.
 - The subnet routers filter SLP multicasts.

Note: Requires System firmware (version 1.15 or later) and Scanner firmware (version 01.12 or later).

1. Scan to NCP fails or takes long time to complete if the IPX protocol is used and there are more than 2 Novell Directory Services (NDS) servers in the network hierarchy.

Note: Requires System firmware (version 1.15 or later) and Scanner firmware (version 01.12 or later).

Version 01.11

Symptom corrected:

1. Some "File Access Privilege Change" log's entries for the CSV file that downloaded via WebImageMonitor are occurred the following phenomena.
 - "User Entry ID" is always displayed as "0x00000000".
 - "User Code /User Name" is appeared as garbage characters.

Note: To fix this problem, System firmware (version 1.14 or later), WebUapl firmware (version 1.10 or later) and Scanner firmware (version 01.11 or later) needs to be applied to the device.
2. Job log CSV file contains the wrong "User Entry ID" for scanner jobs that were sent from the document server. This only occurred using either UserCode Authentication or Basic Authentication
3. The Job log displayed by WSDM contains the wrong "User Code/User Name", "User Entry ID" and "User display name" for scanner jobs that were sent from the document server. This only occurred using either UserCode Authentication or Basic Authentication.
4. The destination of a scanned job sent to a destination in the device's address book, might not be recorded in the Job log.

Note: To fix this problem, System firmware (version 1.14 or later) and Scanner firmware (version 01.11 or later) needs to be applied to the device.

Other changes:

1. Multiple stored jobs submitted for printing simultaneously will now be recorded individually in the Job log instead of only the first job being recorded. This change only applies to non-print jobs that have been stored. Prior to this change, the printing of stored print jobs were already recorded individually in the Job log.

Note: Requires the following firmware versions (or later):
System (version 1.14), Websys (version 1.52), Scanner (version 01.11), WebUapl (version 1.10), and either of NFA (version 1.10M).

Version 01.10

1st mass production

=====
*** Basic Information ***
=====

[Create date] 2018/05/21

[Program Name] System/Copy

[Version] 1.23

[PCB No.]

[Interchangeability] X / O

[Other Firmware Requirements] None

[PCB Requirements] None

[Software category] Normal Release

[Release category] Normal Release

[Program category] Firmware

Exported to(language) GEN(all)

[Firmware No.] D0205331V

[File Information]

File Name D0205331V.fwu

File Type Module for Service

Size 16.65 MB (17454260 byte)

[File Information]

File Name D0205331V.rfu

File Type Module for Remote Upgrade

Size 16.65 MB (17461504 byte)

[Availability of RFU] Yes

[Production reflection] 2018/05

=====
*** Note ***
=====

[Note]

=====
*** Important Notes ***
=====

[Important Notes]

=====
*** Modification History ***
=====

[Modifications made:]

Rank C

Other Changes:

Newly added SMBv2/v3 support.

This firmware is dependent on the following firmware modules.

Please be sure to update all of them:

- System/Copy v1.23 (D0205331V)
- Network Support v7.39 (D0205334M)
- Web Support v1.55 (D0205335H)
- Scanner v01.14 (D0205343G)

Please refer to the RTB(No.RGene095) for details.

[Modification history]

Version 1.22

Symptom Corrected:

- .SC 817, SC 819, SC 878-03 occur.

Version 1.21

Symptom corrected:

1. If the Auto Logout timer is On, there will be a memory leak occurring everytime a user logs in to the device.
2. Repeated failures to login with an IC card will lock the entire account instead of just locking out the access of that card (PIN lock).
3. The timer used for the "Access Violation" setting's time interval does not properly compensate for changes to the device timer.
4. If User Code authentication is enabled or if "External Optional Counter Type" != 0, accounts locked by the "Lock out" setting (SP-5413-1) are not locked out of WIM.
5. Although the "Logout Using Card" function of Card Authentication Package v2 is turned on, the user cannot log out when he or she swipes the card.
6. Cannot scan to shared folders in Mac OS X 10.7 or Mac OS X 10.8.
This firmware is dependent on the following firmware modules.
Please be sure to update all of them:
Network Support firmware v7.38 or later
7. Cannot communicate with the @Remote Center if embedded RC Gate is enabled.

Version 1.20

Minor change applied.

Version 1.18

Symptom corrected:

1. Stored jobs (Locked Print, Sample Print, etc.) might not be shown in the operation panel if the DataOverwriteSecurity Unit is installed.
2. Pressing a Function Key that has been mapped to an SDK/J application might result in an SC997.
3. SC819 occurring during use of an SDK/J application under very specific conditions.
4. After an administrator (User, Network, or File) logs in and then out, unauthenticated users are unable to configure any of the settings in "Extended Feature Settings" even if the Machine Admin is disabled.
5. If the Machine Admin logs in before Java VM has finished starting up, it will not be possible to install SDK applications until the device has been rebooted.
6. Cannot move the HDD Encryption option to another SD card.

Version 1.17

Symptoms Corrected:

1. SC817 occurs after the firmware is updated via RFU.
2. The IPU test pattern cannot be printed out using SP4417-001.
3. Minor bug corrections.
4. The MFP operation panel might go black and not return until the power is cycled. This only occurred if User Authentication was enabled or the MFP had a Device Accounting Unit such as a coin collector or charge card reader.
5. An SC991 occurs and the Scanner cannot be used if the operation panel is turned back on within 60-120 seconds after the Auto Off Timer turns it off.
6. The MFP might stall if a document is scanned to SMB, E-mail or to the Document Server in jpeg format.

Other changes:

1. SC842 was newly added to indicate an RFU (remote firmware update) failure and to record contents which failed to be updated, and then RFU is retried.
2. Scan to Email now removes trailing dots (I.e. xxxx.com.) from destination email addresses.

Version 1.16

Symptom corrected:

1. The vendor code contained in the controller board Mac address was updated from "00-00-74" to "00-26-73" (all possible Mac addresses using the old vendor code have been exhausted).
2. MFPs with no HDD, stall with a SC955 error upon receiving any of the following type of job containing at least 1 blank page:
 - PS3 or PCL jobs with a resolution of 300dpi, fed LEF and the short edge of the LEF page is less than 173mm.
 - Any IPDS job.
3. Might be unable to use the printer function if the MFP that

installed VM card option, ELP and MFP Browser returns from energy saver mode.

Version 1.15

Symptom corrected:

1. Scan to NCP fails if all of the following conditions met:

- The destination is specified using the IP address.
- The Novell server and the device are in different subnets.
- The subnet routers filter SLP multicasts.

Note: Requires System firmware (version 1.12 or later) and Scanner firmware (version 01.06 or later).

2. Scan to NCP fails or takes long time to complete if the IPX protocol is used and there are more than 2 Novell Directory Services (NDS) servers in the network hierarchy.

Note: Requires System firmware (version 1.12 or later) and Scanner firmware (version 01.06 or later).

3. Jobs of more than 100 pages cannot be stored on the MFP (Locked Print, Stored Print, etc.) if another job is being stored from another source (Copier, Scanner, Fax) at the same time.

4. The submission of multiple jobs containing at least 50 pages each, might result in a reboot with an error message (SC990) displayed on the operation panel. This was a very infrequently occurring problem (~.01%).

5. The printer application will stall if any of the following situations are encountered:

- A print job is submitted while another print job is already being processed by the device.
- A print job is submitted while the TWAIN driver is scanning.

6. A scan initiated by TWAIN might fail if a print job is already being processed by the device.

7. When SMC output is operated in duplex at SP mode, output function stops after the 5th sheet is ejected.

8. SC995 occurs under the following conditions:

- A file containing blank page(s) is saved to the Document Server from the printer driver.
- "Print out blank pages" is selected.
- A stamp or other character string/mark is added to the file, and the file is then printed out.

9. The machine reboots while performing a batch print job (printing does not resume after this).

10. Incoming FAX documents cannot be forwarded.

11. When paper is fed from the tandem tray (LCT), machine behavior does not conform to the setting (priority of "productivity" or "tray") of SP5-195-001: Limitless SW.

Version 1.14

Symptom corrected:

1. If the main power is turned off during a firmware update, @ "Please wait" is displayed and the machine cannot be rebooted.

2. Some "File Access Privilege Change" log's entries for the CSV file that downloaded via WebImageMonitor are occurred the following phenomena.

- "User Entry ID" is always displayed as "0x00000000".
 - "User Code /User Name" is appeared as garbage characters.
- Note: To fix this problem, System firmware (version 1.14 or later), WebUapl firmware (version 1.10 or later) and Scanner firmware (version 01.11 or later) needs to be applied to the device.

3. If the Password Policy is enabled, "Target User Entry ID" and "Target User Code/User Name" are not logged in the CSV file that downloaded via WebImageMonitor and in the WebSmartDeviceMonitor's Access Log List when a user tries and fails due to the password policy to change their password.
4. Sudden loss of wireless network connectivity with an error message on the operation panel: "Problems with the wireless card."
5. Firmware versions of the FAX and Finisher options are not recorded in Web Image Monitor > Access Log > "Firmware: Structure".
6. The device might stall when a large number of jobs (150 or more) are printed continuously.
7. The Job log will stop recording User ID, Username or Usercode in the Printer's Job log if WIM is accessed more than 300 times using authentication.
8. If a new UserCode is added to the addressbook via WIM, a password change is recorded (Web Image Monitor > Access Log > "Password Change"), even though UserCodes don't have passwords. This only occurred using either UserCode Authentication or no User Authentication whatsoever.
9. If a user logs in and out repeatedly to the device using an IC card (Card Authentication Package option) at the same time as the address book is being updated by a delivery server such as ScanRouter, the device might stall.
10. The destination of a scanned job sent to a destination in the device's address book, might not be recorded in the Job log.
Note: Requires System firmware (version 1.14 or later) and Scanner firmware (version 01.11 or later).

Other changes:

1. Global Scan NX now supports High Compression PDF files.
Note: Requires Global Scan NX version 1.2 (SDK application), System firmware (version 1.14 or later), and Embedded Software Architecture SD card Ver.4.14 (SDK/J SDcard Ver.4.14 or later).
2. Global Scan NX now supports a preview function.
Note: Requires Global Scan NX version 1.2 (SDK application), System firmware (version 1.14 or later), and Embedded Software Architecture SD card Ver.4.14 (SDK/J SDcard Ver.4.14 or later).
3. Scan to Email now removes trailing dots (I.e. xxxx.com.) from destination email addresses.
4. Multiple stored jobs submitted for printing simultaneously will now be recorded individually in the Job log instead of only the first job being recorded. This change only applies to non-print jobs that have been stored. Prior to this change, the printing of stored print jobs were already recorded individually in the Job log.
Note: Requires the following firmware versions (or later):
System (version 1.14), Websys (version 1.52), Scanner (version 01.11), Web Uapl (version 1.10), and either of NFA (version

1.10M).

5. The device is able to log the downloading (using WIM or DeskTopBinder) of scanned documents from the MFP HDD.

Note: Requires System firmware (version 1.14 or later) and NFA firmware (Ver.1.10M or later).

Version 1.13

Symptom corrected:

1. Continuous printing of IPDS jobs for 5-6 hours results in the error message "Functional problem detected." being displayed on the operation panel. This is recorded in the error log as an SC687 error.
2. If a user tries to logout at the same time as another user is trying to retrieve UserCodes via WebIMageMonitor or Web SmartDeviceMonitor Ver 2, the device might stall with the message "Logging out.... Please wait".
3. If a user fails to login from the operation panel, subsequent logins/logouts might not be logged.
4. Some Lockout entries in the Access log are missing information when viewed in Web SmartDeviceMonitor Ver 2.
5. Web Smart DeviceMonitor > Access Log > "Machine Data Encryption Key Change" > "Start Date/Time" and "End Date/Time" fields are blank.
6. The printing of any SMC report including the following will be recorded in the Access Log as "Machine Data Encryption Key Change"
 - Operation panel > User Tools > Administrator Tools > "Display/Print Counter" > Counter List
 - Operation panel > User Tools > Interface Settings > Print List
7. Mismatched Entry ID and User Name in Web Smart DeviceMonitor > Access Log > "Machine Data Encryption Key Change" log.
8. Fixed: If both SNTP and Date/Time settings are configured in WIM, WIM might not be accessible. This happened very infrequently (about 1% of the time).
Note: The fix requires that NCS firmware version 7.23 or later be applied to the device.
9. Firmware updates using an SD card might fail. This was an infrequently occurring problem and could often be overcome by simply trying the update again.
10. If the login name or password used for LDAP Authentication contain extended ASCII characters (I.e. umlaut), authentication will fail.
11. If a user logs back in after their session has timed out, the device might stall with the message "Authenticating... Please wait".

Version 1.12

Symptom corrected:

1. An application might not be able to load from an SD card (Printer/Scanner unit, SDK application etc) if either of the WIM settings, Permit Firmware Update or Permit Firmware Structure Change are enabled.
2. If the device receives a large number of jobs via LPR, one of the

following might happen:

- The device will cancel some or all of the jobs.
- The device will not be able to access the network.
- 3.The Scanner application will stall if the privileges of a Stored File (Scanner application function) are changed. This only occurs if the Access Log is enabled.
- 4.The Access Log records a password change if the Program/Change Administrator screen is opened via WIM and the OK button is pressed.
- 5.An admin login/logout will be logged everytime the administrator accesses a new WIM page.
- 6.Note: To fix this problems, System firmware (version 1.12 or later), Websys firmware (version 1.50 or later), Web Uapl firmware (version 1.09 or later) and Printer firmware (version 1.02 or later) needs to be applied to the device.
- 7.An admin login/logout will be logged everytime an Auto Email Notification or On-demand Email Notification is sent.
- 8.Note: To fix this problems, System firmware (version 1.12 or later), Websys firmware (version 1.50 or later), Web Uapl firmware (version 1.09 or later) and Printer firmware (version 1.02 or later) needs to be applied to the device.
- 9.Devices using an IPv6 linklocal address, might not be able to use IPsec.

Other changes:

- 1.The speed of switching between SDK applications is faster than before.
Note: To use this, "Embedded Software Architecture SD card Ver.4.08 (SDK/J SDcard Ver.4.08 or later)"and system firmware (version 1.06 or later) needs to be applied to the device.
- 2.The Card Authentication Package (SDK application) is now available.
- 3.The version numbers of some hardware security components called the "Ic Key" and "Ic Hdd" are displayed in the operation panel's firmware version menu.

@Remote related issue:

- 1.Some counter values acquired by Auto Discovery (MIB counter data) was incorrect. If the device is managed as HTTPS device, all acquired counters are correct and same as on the SMC report.
- 2.RFU from @ remote may not be reported to the center.

Version 1.11

Symptom corrected:

- 1. When connecting to an LDAP server, the device ignores all Kerberos Realms except the first field (up to 5 can be configured). This will cause authentication to fail on any LDAP server outside the first Kerberos Realm.
- 2. The E-mail address that searched by LDAP server is not displayed in "Prg.Dest".(GFPR#RA08030001)
- 3. 64 failed attempts to login to Simplified LDAP Authentication will cause all subsequent attempts to fail.
This could be resolved by cycling the power.
- 4. WebImageMonitor is inaccessible if SDK applications are installed.
- 5. Date/Time print function on copied paper does not function correctly. The time zone setting is ignored and printed with GMT only.

6. Minor bugs related to @Remote.
7. SC828 occur or machine stalls when performing the Detailed Self-diagnostic mode.

Other changes:

1. The IPDS option is now available.

To use this option, System firmware (version 1.11 or later),
NCS firmware (version 7.14 or later),
Websys firmware (version 1.09 or later) and
Printer firmware (version 1.01 or later)
needs to be applied to the device.

Version 1.10

Symptom corrected:

- 1.The PS option will not start if it was originally installed on the same SD-card as the Printer/Scanner option (SP5-873-001) and then the Printer/Scanner option was uninstalled (SP5-873-002).
- 2.SC866 (SD Card Error 1: Confirmation) occurs when installing an SD card option.

Other changes:

- 1.The version numbers of some hardware security components called the "Ic Key" and "Ic Hdd" are displayed in the operation panel's firmware version menu.

Version 1.09

Symptom corrected:

- 1.If a USB device is removed while the MFP is in use, an SC 819 error will be shown on the operation panel.

Other changes:

- 1.The new features of "Embedded Software Architecture SD card Ver.4.03 (SDK/J SDcard Ver.4.03)" are now supported. For the details of these features, please refer to the release notes for "Embedded Software Architecture SD card Ver.4.03 (SDK/J SDcard Ver.4.03)".
- 2.Two SSP modes and UP modes have been added for Extend Certification function.
SSP mode: SP5-401-160, -161

Version 1.08

Minor bug correction.

Version 1.01.3

1st mass production

=====
*** Basic Information ***
=====

[Create date] 2018/05/21

[Program Name] Network Support

[Version] 7.39

[PCB No.]

[Interchangeability] X / O

[Other Firmware Requirements] None

[PCB Requirements] None

[Software category] Normal Release

[Release category] Normal Release

[Program category] Firmware

Exported to(language) GEN(all)

[Firmware No.] D0205334M

[File Information]

File Name D0205334M.fwu

File Type Module for Service

Size 6.68 MB (7004568 byte)

[File Information]

File Name D0205334M.rfu

File Type Module for Remote Upgrade

Size 6.69 MB (7012608 byte)

[Availability of RFU] No

[Production reflection] 2018/05

=====
*** Note ***
=====

[Note]

=====
*** Important Notes ***
=====

[Important Notes]

=====
*** Modification History ***
=====

[Modifications made:]

Rank C

Other Changes:

Newly added SMBv2/v3 support.

This firmware is dependent on the following firmware modules.

Please be sure to update all of them:

Color Scanner:

- System/Copy v1.23 (D0205331V)
- Network Support v7.39 (D0205334M)
- Web Support v1.55 (D0205335H)
- Scanner v01.14 (D0205343G)

Monochrome Scanner:

- System/Copy v1.23 (D0195331W)
- Network Support v7.39 (D0205334M)
- Web Support v1.55 (D0205335H)
- Scanner v01.14 (D0195333G)

Please refer to the RTB(No.RGene095) for details.

[Modification history]

Version 7.38

Symptom corrected:

1. If the device's IPP Authentication setting is enabled, the driver cannot be installed on Windows 2008 R2 SP1 or 7 SP1 using an IPP port.
 2. Scan to SMB fails if the both of the following conditions are met.
 - Either the device has NBT disabled or it is enabled but the device is unable to resolve the destination's NetBIOS name.
 - One or more octets in the destination's IPv4 address contain leading zeros.
 3. Symptom corrected: SC991 might occur and network functions could not be used. This occurs if DHCP and DDNS are both enabled in the device and if the DHCP server distributes to the device an FQDN that is more than 127 byte in length.
 4. Symptom corrected: Device applications or services that use any of port 80, 443, 7443 or 7444 could not be used. This occurs if the illegal packet is sent after SSL negotiation handshake to any of the device's TCP ports 443, 7443 or 7444. Affected applications include Web Image Monitor, IPP Printing and @Remote.
 5. If "CNAME" is specified as the destination folder, ScanTo Folder will abort.
 6. If NBT is disabled, the destination for Scan to Folder might not be displayed and Windows authentication might fail.
 7. Cannot scan to shared folders in Windows 8 and Windows Server 2012.
 8. Cannot scan to shared folders in Mac OS X 10.7 or Mac OS X 10.8.
- This firmware is dependent on the following firmware modules.

Please be sure to update all of them:
System/Copy firmware v1.21 or later.

Version 7.37

Symptom corrected:

1. Chunk Transfer Encoding over an IPP port might results in print jobs being reset.
2. If SSDP = Active (Web ImageMonitor > Configuration > Network Security), a high load on the CPU might result in Web ImageMonitor locking up.
3. MFP with an external controller will lose network connectivity. This only occurred if the network settings were changed repeatedly and the MFP's "NetWare" setting was already "Active" (before the network settings were changed).
4. The MFP icon might not be shown in the Windows "Network" dialogue if SSDP is enabled. This affected Windows Vista, 2008/R2, and 7.
5. The device might lose network connectivity if SSDP is enabled. Network connectivity could be temporarily restored after a power cycle.
6. Under very specific combinations of IP address, Subnet Mask, and Gateway address, some of the MFP's network configuration settings might revert to defaults.
7. Use of an IP address to send a Scan to SMB might result in the scanned document not being sent.

Version 7.35

Symptom corrected:

1. An httpd timeout has been implemented to prevent Web ImageMonitor lockups that sometimes occurred when applications accessed the MFP by http.
2. Scan to SMB fails if the file submitted to the DFS folder in the destination and the file of the same name exist in the DFS folder.
3. If Windows Authentication is enabled, printing a large number of copies of a job might take longer than might typically be expected.

Version 7.34

Symptom corrected:

1. If the MFP/LP has a statically configured IP address and domain, it always sends a HELO using just its hostname. SMTP servers that require client HELOs to include the client's FQDN will close the connection. The result of this was that the MFP/LP was unable to send emails.
2. Unable to Scan to SMB to Windows 7 or Windows Server 2008 R2 destinations that have Windows Live ID Sign-in assistant installed.
3. Trying and failing to login to a Scan destination three times might result in the Scanner application stalling.

4. Unable to Scan to SMB to Windows 98/98SE/Me/NT 4.0 destinations specified using an IP address.
5. Unable to retrieve the Windows group name from a Windows 2008 R2 server during Windows Authentication. Because of this, logged in users will only be granted the "Available Functions" specified for them in the Address book.
6. The device is unable to assign group privileges to a logged in user if that group has a name consisting of more than 20 bytes. To address this issue, the supported group name length will be increased to 40 bytes.
7. The MFP's Windows Authentication function is unable to use Kerberos when being authenticated on a Windows 2008 or Windows 2008 R2 server. The MFP will still be successfully authenticated because it is able to fail back to NTLMv2.
8. After changing the MFP's DNS server address or Domain name, Scan to SMB destinations specified using a hostname might not be found.
9. The Scan to SMB "Connection Test" fails if performed on directory located directly below a DFS root. Only the "Connection Test" failed, scanning was successful and even the "Connection Test" worked if performed on any sub-directory.
10. The device might return an SC 819 error when browsing the network using SMB. This only occurred if SMB was browsed frequently and the device was not rebooted.
11. If the MFP's IP address is changed to an IP address of another subnet, users will not be able to browse the network (using Scan to SMB) until the MFP is rebooted.

Other changes:

SSL-related changes:

Note: The new field will only appear if Web Support firmware version 1.54 or later has also been applied to the device.

1. When the device creates a certificate request, it is now able to specify which algorithm (SHA1 or MD5) it wants used to sign the certificate. This has been implemented by adding a field "Algorithm Signature" to the certificate request form.
2. Web Image Monitor now shows the certificate's key length in:
 - Configuration > Security > Device Certificate > Details
3. Specific versions of SSL or TLS (SSLv2, SSLv3, or TLSv1) can now be enabled/disabled using Web Image Monitor. The setting can be configured from either of the following locations:
 - Configuration > Security > Network Security
 - Configuration > Security > SSL/TLS
4. The encryption strength used for SSL can now be configured. This can be done using either of the following settings in Web Image Monitor:
 - Configuration > Security > Network Security
 - Configuration > Security > SSL/TLS
5. Unable to Scan to SMB to a destination that is not specified using an FQDN.
6. Unable to Scan to SMB to destinations that are using both LM Authentication and Samba v2.x.
7. The SMB retry function fails to retry the sending of failed SMB transfers (Scan to SMB or Fax delivery).

8. The device's SMB timeout was too short (1sec). This caused problems when being used across subnets. For this reason, it has been increased to 10 sec.
9. For security reasons, the device will no longer accept SSL incoming, or establish outgoing, connections that use NULL or ADH ciphers.
10. Windows Authentication fails if the username or password includes lower-case European characters.

Version 7.30

Symptom corrected:

1. If either of the WSD Printer or Netware functions are enabled, the following problems might occur. If these problems occur, they typically last for about 2.5 hours.
 - 1) The network might become unresponsive.
 - 2) User Tools can be accessed but configuration changes will not be applied.
 - 3) Application buttons on the operation panel might become unresponsive.
2. Scan to SMB is unable to send documents to a hostname containing 2byte characters.
3. Windows authentication might fail on a domain controller whose hostname contains 2 byte characters.
4. SDK/J applications might not be able to recognize some supported USB devices.
5. When the device IP address and DNS server location are obtained from DHCP, the domain specified by the device setting "IPv4 > Domain Name > Specify" will be overwritten by the domain obtained from DHCP.

Other changes:

1. Scan to Folder destinations located on Windows 7 or Windows Server 2008 R2 can now be selected by browsing.
2. The MFP now supports CIFS, DFS and NTLM v2.

Version 7.27

Symptom corrected:

The MFP's IP address lease renewal request is incorrectly formatted and rejected by DHCP relay agents. This will result in a loss of connectivity that lasts until the MFP reinitializes the network connection (10 seconds).

Version 7.26

Symptom corrected:

1. When jobs are submitted to the device's lpr port repeatedly, some of the jobs might not be printed.
2. If IPP authentication is enabled, printing through an IPP port from a Windows Vista/Server 2008 client might result in printing failure.
3. Multiple Windows Vista/Server 2008 PCs might not be able to access the device through IPsec.

4.

- Connecting to a Scan to SMB destination might cause the device to stall.
- Scan to SMB documents might not be sent to their destination.

Version 7.23

Other changes:

- 1.Kerberos authentication support for Windows Server 2008.

Symptom corrected:

- 1.If the device fails to establish a WPA or WPA2 connection once, it will not try again until rebooted.
- 2.The device is unable to roam between access points using different versions of the IEEE 802.11 standard (a, b, or g).
- 3.LPR jobs submitted by an HP-UX, AIX or Netware 6.5 (SP6 or SP7) host will be cancelled, resulting in an error.
Note: This problem will not affect Netware 6.5 SP7 if the patch "iprntnw65sp7b.zip" has been installed.
<http://download.novell.com/Download?buildid=HsQQ9fMHax0~>
- 4.The device doesn't advertise its hostname via DHCP option 12.
The DNS server might not be updated by DHCP.
- 5.IPP print jobs are cancelled. This happened very infrequently.
- 6.After a job consisting of a multiple of exactly 8KB (8192 bytes) is submitted via IPP, the device will no longer accept any more jobs until rebooted.
- 7.If both SNTP and Date/Time settings are configured in WIM, WIM might not be accessible. This happened very infrequently (about 1% of the time).
Note: The fix requires that System firmware version 1.13 or later be applied to the device.

Version 7.17

Symptom corrected:

- 1.Jobs submitted using the IE ftp client result in an SC991 error.
This only occurs using Windows XP x64.
- 2.Sending a PJI readback (or ustatus) will result in an SC997.
This only occurs if diprint's bidirect is on from telnet.
- 3.SNMP events (Access Violation or Lockout), are not recorded in the Access Log.
- 4.If the sending of a Scan to Email using SMIME is interrupted (Ie. A job is submitted to the printer or the device application is switched before the email has been sent), an SC997 error will occur.
- 5.When a WSD client boots, the device's WSD service might be stopped.
- 6."Date/Time" changes initiated by an SNTP server are not recorded in the Access Log.
- 7.The device might not be able to access the network once the Log collection tool is run (TechMail#TS080441).

Version 7.14

Symptom corrected:

1. The device might not be able to reboot via WIM after the device's

- date/time is decremented to an earlier date/time using WIM.
2. An SSL2.0 client code fails to properly check for NULL (CVE-2006-4343). (TechMail#OTS-2008-185)
 3. Multiple RSA implementations fail to properly handle signatures (CVE-2006-4339). (TechMail#OTS-2008-276).
 4. Web SmartDeviceMonitor shows the IP addresses of TWAIN clients in reverse.
Example: 192.168.1.10 ==> 10.1.168.192
 5. If an LPR job is submitted to the device followed by an AppleTalk job, the device will stall.
 6. An SC819 error might be shown on the operation panel if the device is accessed via IPsec repeatedly without a power cycle.
 7. An SC997 will be displayed on the Operation Panel of EFI controller based devices if IPv6 network settings are changed.
 8. Excessive time lag when the device rejoins the network after exiting Energy Saver Mode.
This will occur under either one of the following conditions:
 - The device is connected to a hub that uses the spanning tree protocol.
 - The device is connected via Wireless LAN.
 9. If WPA2 is configured for a device, the Access Log List in Web SmartDeviceMonitor ver 2.x will always show the WPA Encryption Method as TKIP and never as CCMP (AES), regardless of actual settings.

Other changes:

1. The IPDS option is now available.
To use this option, System firmware (version 1.11 or later), NCS firmware (version 7.14 or later), Websys firmware (version 1.09 or later) and Printer firmware (version 1.01 or later) needs to be applied to the device.
2. The device supports Windows server 2008 DHCPv6 server.

Version 7.05
Minor bug correction.

Version 7.03
1st mass production

=====
*** Basic Information ***
=====

[Create date] 2018/05/21

[Program Name] Web Support

[Version] 1.55

[PCB No.]

[Interchangeability] X / O

[Other Firmware Requirements] None

[PCB Requirements] None

[Software category] Normal Release

[Release category] Normal Release

[Program category] Firmware

Exported to(language) GEN(all)

[Firmware No.] D0205335H

[File Information]

File Name D0205335H.fwu

File Type Module for Service

Size 3.73 MB (3916188 byte)

[File Information]

File Name D0205335H.rfu

File Type Module for Remote Upgrade

Size 3.74 MB (3924224 byte)

[Availability of RFU] No

[Production reflection] 2018/05

=====
*** Note ***
=====

[Note]

=====
*** Important Notes ***
=====

[Important Notes]

=====
*** Modification History ***
=====

[Modifications made:]

Rank C

Other Changes:

Newly added SMBv2/v3 support.

This firmware is dependent on the following firmware modules.

Please be sure to update all of them:

Color Scanner:

- System/Copy v1.23 (D0205331V)
- Network Support v7.39 (D0205334M)
- Web Support v1.55 (D0205335H)
- Scanner v01.14 (D0205343G)

Monochrome Scanner:

- System/Copy v1.23 (D0195331W)
- Network Support v7.39 (D0205334M)
- Web Support v1.55 (D0205335H)
- Scanner v01.14 (D0195333G)

Please refer to the RTB(No.RGene095) for details.

[Modification history]

Version 1.54

Other changes:

SSL-related changes:

Note: The new fields will only appear if Network Support firmware version 7.34 or later has also been applied to the device.

No1. When the device creates a certificate request, it is now able to specify which algorithm (SHA1 or MD5) it wants used to sign the certificate. This has been implemented by adding a field "Algorithm Signature" to the certificate request form.

No2. Web Image Monitor now shows the certificate's key length in:

- Configuration > Security > Device Certificate > Details

No3. Specific versions of SSL or TLS (SSLv2, SSLv3, or TLSv1) can now be enabled/disabled using Web Image Monitor . The setting can be configured from either of the following locations:

- Configuration > Security > Network Security
- Configuration > Security > SSL/TLS

No4. The encryption strength used for SSL can now be configured. This can be done using either of the following settings in Web Image Monitor :

- Configuration > Security > Network Security
- Configuration > Security > SSL/TLS

Version 1.53

Symptom corrected:

1. If the maximum number of log entries has been reached, then logs downloaded via WIM might have some incorrect log IDs or missing fields.

Maximum number of entries:

Access Log (with HDD): 6000

Access Log (without HDD): 500

Job Log (with HDD): 2000

Job Log (without HDD): 500

Other changes:

1. Authentication errors resulting from the changing of the username or password of a user currently logged into WIM, are now logged.

Note: Requires the following firmware versions (or later):

Websys(version 1.53), Printer(version 1.06e) and

WebUapl(version 1.11).

Version 1.52

Symptom corrected:

1. Some specific events will cause the User Entry ID to be missing from logs downloaded via WIM.
2. Miscellaneous wording errors in logs downloaded via WIM.
3. The names of files stored in the device (File Name) are not recorded in logs downloaded from WIM.
4. Destination Addresses appears garbled in logs downloaded via WIM. This might cause all subsequently recorded fields to also exhibit problems.
5. User Entry IDs in logs downloaded via WIM are 0. This occurred if the status of the Lockout function was changed for the user associated with the User Entry ID.

Other changes:

1. Some new items have been added to the Access Log.
2. Multiple stored jobs submitted for printing simultaneously will now be recorded individually in the Job log instead of only the first job being recorded. This change only applies to non-print jobs that have been stored. Prior to this change, the printing of stored print jobs were already recorded individually in the Job log.

Note: Requires the following firmware versions (or later):

System (version 1.14), Websys (version 1.52), Scanner (version 01.11), Webapl (version 1.10), and either of NFA (version 1.10C (Color scanner model)) or (1.10M(B/W scanner model)).

3.
 - Unfinished jobs (ie. those in the processing state) are now recorded in logs downloaded via WIM.
 - Log entries with future dates (as the result of a change of the device clock) are now recorded in logs downloaded via WIM.
 - The overwriting of a log entry is now logged. Old entries are overwritten if the maximum number of entries has been reached.
- Maximum number of entries:

Access Log (with HDD): 6000
Access Log (without HDD): 500
Job Log (with HDD): 2000
Job Log (without HDD): 500

4. Entries in the Result column of logs downloaded via WIM, are now worded differently.

Version 1.51.1

Some of the Device Settings menu items are not displayed correctly in WIM.

Instances of WIM configured to display English and Japanese were unaffected.

Version 1.50

Symptom corrected:

1. An admin login/logout will be logged everytime the administrator accesses a new WIM page.
2. An admin login/logout will be logged everytime an Auto Email Notification or On-demand Email Notification is sent.

Note: To fix these problems, System firmware (version 1.12 or later), Websys firmware (version 1.50 or later), Web Uapl firmware (version 1.09 or later) and Printer firmware (version 1.02 or later) needs to be applied to the device.

Other changes:

1. Logs can be downloaded from WIM (Configuration > Download Logs).
2. The following operations are logged in the Access log.
 - a. Web Image Monitor Auto Logout
 - b. File Access Privilege Change
 - c. Administrator Change
 - d. Address Book Change

These can be displayed in the Access Log menu.

Note: In order to display b-d in WIM, System firmware (ver 1.12 or later) and Websys firmware (version 1.50 or later) are required.

Version 1.09

Symptom corrected:

1. WebImageMonitor contained wrong wording or message.
 - a. Wrong error message for S/MIME: Configuration > Security > Device Certificate
(Wrong) E-mail address of certificate does not match Administrator E-mail address
(Correct) E-mail address of certificate is not entered or does not match Administrator E-mail address
 - b. Wrong wording for Access Log: Configuration > Device Settings > Logs
(Wrong) All Logs Deletion
(Correct) HDD format
2. WIM displays "This device is currently in use by other functions. Please try again later". A reboot of the device is needed to use WIM again.

- 3.If the device is accessed from WIM and then it goes into Energy Saver Mode for at least 30 minutes, the web service might stall if the Document Server is accessed again.
Note: To fix this issue, Websys firmware ver 1.09 or later, WebUapl firmware ver 1.08 or later and Printer firmware ver 1.01 or later needs to be applied.
- 4.The web service might stall if the IPsec menu is accessed and the Encryption Algorithm setting = "Cleartext".
- 5.Configuration > Security > IPsec > Encryption Key Auto Exchange Settings are not saved if configured via WIM.
- 6.The web service will stall if more than 130 User Certificates are stored in the Address Book without a powercycle.
- 7.At the @Remote installation, SC819 occur when select SP5-985-01 to "1".
Note: To fix this issue, Netfile firmware ver.1.07M/1.06C or later WebUapl firmware ver.1.08 or later and Web Support firmware ver.1.09 needs to be applied.

Other changes:

- 1.The IPDS option is now available.
To use this option, System firmware (version 1.11 or later), NCS firmware (version 7.14 or later), Websys firmware (version 1.09 or later) and Printer firmware (version 1.01 or later) needs to be applied to the device.

Version 1.05
Minor bug correction.

Version 1.02
1st mass production

=====
*** Basic Information ***
=====

[Create date] 2018/05/21

[Program Name] Scanner

[Version] 01.14

[PCB No.]

[Interchangeability] X / O

[Other Firmware Requirements] None

[PCB Requirements] None

[Software category] Normal Release

[Release category] Normal Release

[Program category] Firmware

Exported to(language) GEN(all)

[Firmware No.] D0205343G

[File Information]

File Name D0205343G.fwu

File Type Module for Service

Size 1.00 MB (1043772 byte)

[File Information]

File Name D0205343G.rfu

File Type Module for Remote Upgrade

Size 1.00 MB (1048832 byte)

[Availability of RFU] Yes

[Production reflection] 2018/05

=====
*** Note ***
=====

[Note]

=====
*** Important Notes ***
=====

[Important Notes]

=====
*** Modification History ***
=====

[Modifications made:]

Rank C

Other Changes:

Newly added SMBv2/v3 support.

This firmware is dependent on the following firmware modules.

Please be sure to update all of them:

- System/Copy v1.23 (D0205331V)
- Network Support v7.39 (D0205334M)
- Web Support v1.55 (D0205335H)
- Scanner v01.14 (D0205343G)

Please refer to the RTB(No.RGene095) for details.

[Modification history]

Version 01.13

Symptom corrected:

1. The MFP operation panel might go black and not return until the power is cycled. This only occurred if User Authentication was enabled or the MFP had a Device Accounting Unit such as a coin collector or charge card reader.
2. A scan configured to output a Multi-page TIFF might have actually output a PDF. This only occurred if both of the following conditions were met:
 - Scanner operation panel > Send Settings > Compression (Gray Scale/Full Color) > OFF
 - Scanner operation panel > Scan Settings > Scan Type > Auto Color Select
3. The scanner will stall "Updating the destination List. Please wait..." will be displayed on the operation panel. This occurs if the device's address book is updated via ScanRouter while the device is in Sleep Mode.

Version 01.12

Symptom corrected:

1. Scan to NCP fails if all of the following conditions met:
 - The destination is specified using the IP address.
 - The Novell server and the device are in different subnets.
 - The subnet routers filter SLP multicasts.

Note: Requires System firmware (version 1.15 or later) and Scanner firmware (version 01.12 or later).

1. Scan to NCP fails or takes long time to complete if the IPX protocol is used and there are more than 2 Novell Directory Services (NDS) servers in the network hierarchy.

Note: Requires System firmware (version 1.15 or later) and Scanner firmware (version 01.12 or later).

Version 01.11

Symptom corrected:

1. Some "File Access Privilege Change" log's entries for the CSV file that downloaded via WebImageMonitor are occurred the following phenomena.
 - "User Entry ID" is always displayed as "0x00000000".
 - "User Code /User Name" is appeared as garbage characters.

Note: To fix this problem, System firmware (version 1.14 or later), WebUapl firmware (version 1.10 or later) and Scanner firmware (version 01.11 or later) needs to be applied to the device.
2. Job log CSV file contains the wrong "User Entry ID" for scanner jobs that were sent from the document server. This only occurred using either UserCode Authentication or Basic Authentication
3. The Job log displayed by WSDM contains the wrong "User Code/User Name", "User Entry ID" and "User display name" for scanner jobs that were sent from the document server. This only occurred using either UserCode Authentication or Basic Authentication.
4. The destination of a scanned job sent to a destination in the device's address book, might not be recorded in the Job log.

Note: To fix this problem, System firmware (version 1.14 or later) and Scanner firmware (version 01.11 or later) needs to be applied to the device.

Other changes:

1. Multiple stored jobs submitted for printing simultaneously will now be recorded individually in the Job log instead of only the first job being recorded. This change only applies to non-print jobs that have been stored. Prior to this change, the printing of stored print jobs were already recorded individually in the Job log.

Note: Requires the following firmware versions (or later):
System (version 1.14), Websys (version 1.52), Scanner (version 01.11), WebUapl (version 1.10), and either of NFA (version 1.10C).

Version 01.10

1st mass production