

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

[Create date] 2018/06/19

[Program Name] System/Copy

[Version] 3.06

[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.] D0465749F

[File Information]

File Name D0465749F.fwu

File Type Module for Service

Size 15.60 MB (16361136 byte)

[File Information]

File Name D0465749F.rfu

File Type Module for Remote Upgrade

Size 15.61 MB (16367872 byte)

[Availability of RFU] Yes

[Production reflection] 2018/06

=====
*** 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 v3.06 (D0465749F)
- Network Support v7.40 (D0465743M)
- Web Support v1.19 (D0465744E)
- Scanner v01.16 (D0475741F)

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

[Modification history]

Version 3.05

Rank C

Symptom corrected:

- The machine may fail to conduct encrypted communication.
- @remote communication with Cumin may be disconnected

Version 3.04

Symptom corrected:

The value of SP5045-02 automatically changes" to "0: Meter" when
@Remote connection is established.

SP5045-002

0: meter (default for EU and AP machines)

1: yard

2: feet

3: square meter

4: square yard

5: square feet (default for NA machines)

Version 3.03

Other changes:

A password screen is now displayed when the machine is booted up for
the first time at installation.

This firmware is dependent on the following firmware modules.

Please be sure to update all of them:

- Lcdc (OpePanel) firmware v1.07 or later.

- Language firmware v1.05 or later

Version 3.02

Symptom corrected:

1. A memory leak occurs (inter-thread messages).
2. Extended Security Settings can be changed by non-Administrators even when the Authentication Method inside these settings is set to "Do not".
3. The machine uses its own clock to judge the time/duration of an access attack event.
4. Administrators are able to login from WIM (via Administrator Authentication) even after the account has been locked out.
5. Scan to Folder job fails when sending to a folder on a Mac OS X 10.7 (Lion) or 10.8 (Mountain Lion).

Version 3.01

<Symptom corrected>

SC991 occurs when the @Remote Center connects to the machine.

Version 3.00.1

The firmware has been updated in accordance with the launch of the VM Card Type M (D56801).

Important:

Upgrade this firmware together with the Printer firmware ver.3.02 (D3965750).

<Symptom corrected>

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 1.11

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. If the PowerSavingSys firmware of the other model is saved to a f/w updated SD card, it is possible to install the firmware.

Version 1.10

Symptom corrected:

1. SC855 occurs even if the wireless LAN card is operating normally.
2. If the SMC report is printed out in duplex, the machine stops after exiting the fifth page.
3. 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.
4. The machine reboots while performing a batch print job (printing does not resume after this).
 5. SC816 occurs when the machine switches to Energy Saver mode.
 6. "Toner Order Failed" is displayed when the machine is disconnected from RC Gate (in cases where the machine is registered as an @Remote device).
 7. 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.
 8. A scan initiated by TWAIN might fail if a print job is already being processed by the device.
 9. 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.
 10. A problem in our implementation of AppleTalk affecting the ability of our devices to join an AppleTalk Zone through some Seed Routers.

Other changes:

1. The "External Charge Unit Management" button was added to the User Tools display (System Settings -> Administrator screen).
Note: This new button is not displayed when using the RW-7140 controller.

Version 1.09

Supported Printer Controller Type RW-7140 (first firmware version to support this controller).

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 1.09 or later) and Scanner firmware (version 01.13 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 1.09 or later) and Scanner firmware (version 01.13 or later).

Version 1.08

Symptom corrected:

1. 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 7.24 or later be applied to the device.

2. 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.
3. Web Smart DeviceMonitor > Access Log > "Machine Data Encryption Key Change" > "Start Date/Time" and "End Date/Time" fields are blank.
4. Mismatched Entry ID and User Name in Web Smart DeviceMonitor > Access Log > "Machine Data Encryption Key Change" log.
5. Firmware versions of the Finisher options are not recorded in Web Image Monitor > Access Log > "Firmware: Structure".
6. If the login name or password used for LDAP Authentication contain extended ASCII characters (i.e. umlaut), authentication will fail.
7. If a user logs back in after their session has timed out, the device might stall with the message "Authenticating... Please wait".

Other changes:

1. Scan to Email now removes trailing dots (i.e. xxxx.com.) from destination email addresses.
2. A display was added to the LCD that alerts the operator when Guide N6 on the FD6500A/B is opened.

Version 1.07

Symptom corrected:

1. Continuous printing of 50-150 page IPDS jobs, for 5 or 6 hours, results in an SC687 error.
2. SC819 errors, resulting in a stall, occur during printing or when the device is in Energy Saver mode. These errors occurred if the device power had not been cycled recently.
3. Printing a stored copier job results in an SC672 if all of the following conditions are met: -The BW copier job. -The page size of the printed job is changed from the stored job. -The device just returned from Energy Saver mode when the job was printed. -The MLB option is installed.

Other changes:

1. The default values and setting ranges for some engine SP modes were changed.

SP NO. Default values and setting ranges

1105 002 D046: 0to25/10/1 <C
 D049: 0to25/0/1 <C

1918 035 D046: -5to+5/-1.0/0.01%
 D049: -5to+5/-0.5/0.01%

035 D046: -5to+5/-1.0/0.01%
 D049: -5to+5/-0.5/0.01%

075 D046: -5to+5/-0.8/0.01%
 D049: -5to+5/-0.6/0.01%

2301 022 0to230/75/1uA

031 0to230/95/1uA

2. The function name were changed.

SP NO.

4901 002 Shading Correction: Target Level Setting

Version 1.06

1st Mass production.

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

[Create date] 2018/06/19

[Program Name] Network Support

[Version] 7.40

[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.] D0465743M

[File Information]

File Name D0465743M.fwu

File Type Module for Service

Size 6.44 MB (6749940 byte)

[File Information]

File Name D0465743M.rfu

File Type Module for Remote Upgrade

Size 6.44 MB (6754560 byte)

[Availability of RFU] No

[Production reflection] 2018/06

=====
*** 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 v3.06 (D0465749F)
- Network Support v7.40 (D0465743M)
- Web Support v1.19 (D0465744E)
- Scanner v01.16 (D0475741F)

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

[Modification history]

Version 7.39

Symptom corrected:

When simultaneously printing from AppleTalk on a Mac and a protocol other than AppleTalk in Windows, an SC899 error might occur.

Version 7.38

Symptom corrected:

1. An httpd timeout has been implemented to prevent Web Image Monitor lockups that sometimes occurred when applications accessed the MFP by http. (GFPR#RC10060010)
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.
4. Chunk Transfer Encoding over an IPP port might results in print jobs being reset.
5. If SSDP = Active (Web Image Monitor > Configuration > Network Security), a high load on the CPU might result in Web Image Monitor locking up.
6. 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).
7. The MFP icon might not be shown in the Windows "Network" dialogue if SSDP is enabled. This affected Windows Vista, 2008/R2, and 7.
8. Under very specific combinations of IP address, Subnet Mask, and Gateway address, some of the MFP's network configuration settings might revert to defaults.

9. Use of an IP address to send a Scan to SMB might result in the scanned document not being sent.
10. 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.
11. 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.
12. 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.
13. 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.
14. If "CNAME" is specified as the destination folder, ScanTo Folder will abort.
15. If NBT is disabled, the destination for Scan to Folder might not be displayed and Windows authentication might fail.
16. Cannot scan to shared folders in Windows 8 and Windows Server 2012.
17. 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 v3.02 or later.

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. The SMB retry function fails to retry the sending of failed SMB transfers (Scan to SMB or Fax delivery).
6. 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 Addressbook.
7. 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.

8. 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.
9. After changing the MFP's DNS server address or Domain name, Scan to SMB destinations specified using a hostname might not be found.
10. 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.
11. 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.
12. 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 1.18 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. For security reasons, the device will no longer accept SSL incoming, or establish outgoing, connections that use NULL or ADH ciphers.
6. Unable to Scan to SMB to a destination that is not specified using an FQDN.
7. Unable to Scan to SMB to destinations that are using both LM Authentication and Samba v2.x.
8. Windows Authentication fails if the username or password includes lower-case European characters.
9. 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.

Version 7.30

Symptom corrected:

1. The MFPs 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).
2. 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.
3. Scan to SMB is unable to send documents to a hostname containing 2byte characters.
4. Windows authentication might fail on a domain controller whose hostname contains 2 byte characters.
5. SDK/J applications might not be able to recognize some supported USB devices.
6. 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 7.25

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.

Version 7.24

Other changes:

1. Kerberos authentication support for Windows Server 2008.

Symptom corrected:

1. IPP print jobs are cancelled. This happened very infrequently.
2. 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.
3. 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 1.08 or later be applied to the device.

4. Device unable to exit Energy Saver mode without a reboot, if the NIC is disabled (SP5-985-001 = 0).

Version 7.20

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.

Version 7.18

1st Mass production.

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

[Create date] 2018/06/19

[Program Name] Web Support

[Version] 1.19

[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.] D0465744E

[File Information]

File Name D0465744E.fwu

File Type Module for Service

Size 2.59 MB (2717476 byte)

[File Information]

File Name D0465744E.rfu

File Type Module for Remote Upgrade

Size 2.60 MB (2724096 byte)

[Availability of RFU] Yes

[Production reflection] 2018/06

=====
*** 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 v3.06 (D0465749F)
- Network Support v7.40 (D0465743M)
- Web Support v1.19 (D0465744E)
- Scanner v01.16 (D0475741F)

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

[Modification history]

Version 1.18

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.

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

Version 1.16.1

Minor changes

Version 1.15
1st Mass production.

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

[Create date] 2018/06/19

[Program Name] Scanner

[Version] 01.16

[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.] D0475741F

[File Information]

File Name D0475741F.fwu

File Type Module for Service

Size 1.01 MB (1057632 byte)

[File Information]

File Name D0475741F.rfu

File Type Module for Remote Upgrade

Size 1.02 MB (1065216 byte)

[Availability of RFU] Yes

[Production reflection] 2018/06

=====
*** 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 v3.06 (D0465749F)
- Network Support v7.40 (D0465743M)
- Web Support v1.19 (D0465744E)
- Scanner v01.16 (D0475741F)

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

[Modification history]

Version 01.15

<Symptom corrected>

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 01.14

Symptom corrected:

1. 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.
2. 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.

Version 01.13

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 1.09 or later) and Scanner firmware (version 01.13 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 1.09 or later) and Scanner
firmware (version 01.13 or later).

Version 01.12
1st Mass production.