xerox

Version 1.0
Jan 16, 2012

Secure Installation and Operation of Your ColorQube™ 8700/8900

Secure Installation and Operation of Your ColorQube™ 8700/8900

Purpose and Audience

This document provides information on the secure installation and operation of a ColorQube™ 8700/8900 Multifunction System. All customers, but particularly those concerned with secure installation and operation of these machines, should follow these guidelines.

Overview

This document lists some important customer information and guidelines that will ensure that your ColorQube 8700/8900 Multifunction System is operated and maintained in a secure manner.

Background

The ColorQube 8700/8900 Multifunction System is currently undergoing Common Criteria evaluation. The information provided here is consistent with the security functional claims made in the Security Target[1]. Upon completion of the evaluation, the Security Target will be available from the Common Criteria Certified Product website (http://www.commoncriteriaportal.org/products.html) list of evaluated products, from the Xerox security website (http://www.xerox.com/information-security/common-criteria-certified/enus.html), or from your Xerox representative.

1. Please follow the guidelines below for secure installation, setup and operation of the evaluated configuration[2] for a ColorQube 8700/8900:

    a). The security functions in the evaluated configuration that should be set up by the System Administrator are:
    - Immediate Image Overwrite
    - On Demand Image Overwrite
    - Disk Encryption
    - FIPS 140-2 Encryption
    - IP Filtering
    - Audit Log
    - SSL
    - IPSec
    - Local, Remote or Smart Card Authentication
    - Local Authorization and Personalization
    - 802.1x Device Authentication
    - Session Inactivity Timeout

    System Administrator login is required when accessing the security features via the Web User Interface (Web UI) or when implementing the guidelines and recommendations specified in this document. To log in to the Web UI as an authenticated System Administrator, follow the instructions under "Initial Setup in CentreWare Information Services" located on page 19 in the System Administration Guide (SAG)[3].

    To log in to the Local User Interface (Local UI) as an authenticated System Administrator, follow the "System Administrator Access at the Control Panel" instructions located on page 18 in the SAG.

    Follow the instructions located in the SAG in Chapter 4, Security to set up these security functions except as noted in the items below. Note that whenever the SAG requires that the System Administrator provide an IPv4 address, IPv6 address or port number the values should be those that pertain to the particular device being configured.

    b). The following services are also considered part of the evaluated configuration and should be enabled when needed by the System Administrator - Copy, Embedded Fax, Fax Forwarding on Receive (for received Embedded Faxes), Scan to E-mail, Workflow Scanning, Scan to Mailbox, Scan to USB, Print from USB and Print from Mailbox.

    Secure acceptance of a ColorQube 8700/8900, once device delivery and installation is completed, should be done by:
    - Printing out a Configuration Report by following the "Configuration Report" instructions located on page 17 of the SAG.
    - Comparing the software/firmware versions listed on the Configuration Report with the Evaluated Software/Firmware versions listed in Table 2 of the Xerox ColorQube™ 8700/8900 Security Target, latest version issued and make sure that they are the same in all cases.

    c). Change the Administrator password as soon as possible. Reset the Tools password periodically.

---

[1] Xerox ColorQube™ 8700/8900 Security Target, Latest Version issued
[2] The term "evaluated configuration" will be used throughout this document to refer to the configuration of the ColorQube 7755/7765/7775 Multifunction System that is currently undergoing Common Criteria evaluation.
[3] Xerox® ColorQube® 8700 / 8900 System Administrator Guide, Version 1.0: February 2012

(1) Set the Administrator password to a minimum length of eight alphanumeric characters, (2) change the Administrator password once a month and (3) ensure that all passwords are strong passwords (e.g., passwords use a combination of alphanumeric and non-alphanumeric characters; passwords don't use common names or phrases, etc.).

For directions on how to change the Tools password, follow the "Changing the System Administrator Password" instructions on page 19 in the SAG.

The evaluated configuration assumes that the Admin Password Reset security feature will be disabled and not used. To disable this feature, perform the following:

- At the Web UI select the **Properties** tab.
- Select the following entries from the **Properties** '**Content** menu': **Security → Admin Password → Reset Policy**
- Select the [**Disable Password Reset**] option and then select the [**Apply**] button to save the option entered.

d). The System Administrator should establish or ensure that unique user accounts with appropriate privileges are created for all users who require access to the device, that no 'Guest' users are allowed to access any services on the device, and that local usernames established on the device match domain names and both map to the same individual. Follow the "User Database" instructions starting on page 60 in the SAG to set up local user accounts on the device.

The System Administrator should also ensure that authentication passwords for unique user accounts established for users should be set to a minimum length of 8 (alphanumeric) characters unless applicable internal procedures the System Administrator must comply with require a minimum password of a greater length. The 'Maximum Length' can be set to any value between 8 and 63 (alphanumeric) characters consistent with the same internal procedures.

Follow the "Specifying Password Requirements" instructions on page 61 in the SAG to set the minimum and maximum user authentication password lengths.

e). Xerox recommends the following passcodes be changed on a regular basis, chosen to be as random as possible and set to the indicated minimum lengths:

- Smart Card or CAC passcode – 8 characters (alphanumeric)
- Secure Print passcode – 6 digits
- Scan To Mailbox password – 8 characters (alphanumeric)

f). For establishing remote authentication access to network accounts follow the "Configuring Network Authentication Settings" instructions starting on page 61 of the SAG to set up an Authentication Server. Follow the "Configuring Smart Authentication Settings" instructions starting on page 64 of the SAG to set up user authentication via a Smart Card. Note that CAC is the only type of Smart Card supported in the evaluated configuration.

g). The System Administrator should ensure that no authenticated user is assigned the Accounting Administrator role.

h). In the evaluated configuration only the System Administrator should have the ability to delete a job. From the Local UI follow the instructions for "Setting Job Deletion Options at the Control Panel" on page 198 of the SAG to set job deletion to 'System Administrator Only'.

From the WebUI, set the permission for 'Delete Jobs' under the 'Job Status Pathway' to "Not Allowed" for all roles defined other than System Administrator. Follow the instructions for "Editing an Authenticated User Role" on page 74 of the SAG.

i). In the evaluated configuration the System Administrator should ensure that access to all pathways and services is set to "Not Allowed" for all defined roles so that they can be accessed only by authenticated users. Follow the instructions in the 'Editing Services and Tools Permissions for the Non-Logged In Users Role' section on page 72.

j). All print, copy, workflow scan, scan to email, LANFax and Embedded Fax jobs (both send and receive) are temporarily stored on the hard disk drive in the ColorQube 8700/8900. For customers concerned about these document files stored on the hard disk drive the Immediate Image Overwrite (IIO) and On Demand Image Overwrite (ODIO) security features, which come installed on the device, must be properly configured and enabled. Two forms of On Demand Image Overwrite are manually invoked – a Standard On Demand Image Overwrite that will overwrite all image data except data stored by the Reprint Save Job feature and data stored in Embedded Fax dial directories and mailboxes and a Full On Demand Image Overwrite that will overwrite all image data including data stored by the Reprint Save Job feature and data stored in Embedded Fax dial directories and mailboxes.

Please follow the "Manually Deleting Image Data" instructions starting on page 99 in the SAG for proper setup and initiation of On Demand Image Overwrite from the Web UI and the instructions under 'Manually Deleting Image Data at the Control Panel' on page 99 of the SAG for proper setup and initiation of On Demand Image Overwrite from the Local UI. Follow the "Scheduling Routine Deletion of Image Data" instructions starting on page 98 in the SAG for proper setup and initiation of a Scheduled On Demand Image Overwrite from the Web UI.

Ensure that the 'Confirmation Report' setting is set to "On" when setting up either a manual or scheduled ODIO so that a Confirmation Report will always print upon completion of an ODIO.

Follow the instructions under 'Enabling Immediate Image Overwrite the Control Panel' or 'Enabling Immediate Image Overwrite' on page 100 of the SAG to enable Immediate Image Overwrite from the control panel or the WebUI, respectively.

Notes:

- Immediate Image Overwrite of a delayed or secure print job will not occur until after the machine has printed the job.

- If an Immediate Image Overwrite fails, an error message will appear at the top of the screen indicating that there is an Immediate Image Overwrite error and that an On Demand Image Overwrite should be run. This error message will persist until an On Demand Image overwrite is initiated by the System Administrator. In the case that the copy controller is reset at the same time a copy job is being processed by the device, this same error message may also appear when the copy controller has completed its reset.

- If there is a power failure or system crash while a network scan job is being processed, an Immediate Overwrite of the residual data will occur upon job recovery. However, the network scan job may not appear in the Completed Job Log.

- If there is a power failure or system crash of the network controller while processing a print job, residual data might still reside on the hard disk drive(s). The System Administrator should immediately invoke an On Demand Image Overwrite once the machine has been restored.

- Once a manual or scheduled On Demand Image Overwrite has been initiated by the System Administrator from either the Local UI or Web UI, as applicable, it can not be aborted by the System Administrator.

  The System Administrator also has the option of scheduling either a Standard or Full On Demand Image Overwrite from the Web UI. Follow the "Scheduling Routine Deletion of Image Data" instructions on page 97 in the SAG to schedule an On Demand Image Overwrite.

- Before invoking an On Demand Image Overwrite verify that:
  - There are no active or pending print or scan jobs.
  - There are no new or unaccounted for Dynamic Loadable Modules (DLMs) or other software running on the machine.
  - There are no active processes that access the hard disk drive(s).
  - No user is logged into a session via network accounting, Xerox Standard Accounting, or the internal auditron, or into a session accessing a directory on the hard disk drive(s) [3].
  - After a power on of the machine all subsystems must be properly synced and, if printing of Configuration Reports is enabled on the device, the Configuration Report must have printed.
  - For any previously initiated On Demand Image Overwrite request the confirmation sheet must have printed.
  - The Embedded Fax card must have the correct software version and must be properly configured.

- When invoked from the Web UI the status of the completed On Demand Image Overwrite will not appear on the Local UI but can be ascertained from the On Demand Overwrite Confirmation Report that is printed after the Network Controller reboots.

- If an On Demand Image Overwrite fails to complete because of an error or system crash, a system reboot or software reset should be initiated by the System Administrator from either the Local UI or the Web UI and be allowed to complete; otherwise, the Local UI may become unavailable. If the Local UI does become unavailable the machine will have to be powered off and then powered on again to allow the system to properly resynchronize. Once the system reboots or software reset has completed the System Administrator should immediately perform another On Demand Image Overwrite.

- If there is a failure in the hard disk drive(s) a message recommending that an On Demand Image Overwrite be run will appear on the Local UI screen. An Immediate Image Overwrite Error Sheet will also be printed or may contain incomplete status information. The System Administrator should immediately perform the requested On Demand Image Overwrite.

- The time shown on the On Demand Overwrite progress screen displayed on the Local UI may not reflect Daylight Savings Time.

- If an On Demand Image Overwrite is successfully completed, the completion (finish) time shown on the printed On Demand Overwrite Confirmation Report will be the time that the system shuts down.

- The System Administrator should perform an On Demand Image Overwrite immediately before the device is decommissioned, returned, sold or disposed of.

k). The ColorQube 8700/8900 supports the use of SSLv2.0, SSLv3.0, RC4 and MD5. However, customers are advised to set the cyrpto policy of their clients to request either SSLv3.1 or TLSv1.0 and to disallow the use of RC4 and MD5. Security functions

in the evaluated configuration make use of cryptographic ciphers listed in Table 25 of the Security Target. The cryptographic module supports additional ciphers that may be called by other unevaluated functions.

l). For SSL to work properly the machine must be assigned a valid, fully qualified machine name and domain. Follow the instructions under 'DNS' on page 31 of the SAG for entering the host and domain names.

m). When utilizing Secure Sockets Layer (SSL):

- For the purposes of the evaluation, the maximum validity of digital certificates was set to 180 days.

- If a self-signed certificate is to be used the generic Xerox root CA certificate should be downloaded from the device and installed in the certificate store of the user's browser.

n). HTTPS is enabled in the evaluated configuration. To enable secure HTTPS follow the instructions in Steps 6 and 7 under 'Configuring HTTP Settings in CentreWare Internet Services" on page 50 of the SAG.

o). When utilizing Secure Sockets Layer (SSL) for secure scanning:

- SSL should be enabled and used for secure transmission of scan jobs.

- When storing scanned images to a remote repository using an https: connection, a Trusted Certificate Authority certificate should be uploaded to the device so the device can verify the certificate provided by the remote repository.

- When an SSL certificate for a remote SSL repository fails its validation checks the associated scan job will be deleted and not transferred to the remote SSL repository. The System Administrator should be aware that in this case the job status reported in the Completed Job Log for this job will read: "Job could not be sent as a connection to the server could not be established".

p). To be consistent with the evaluated configuration, the HTTPS protocol should be used to send scan jobs to a remote IT product.

q). SNMPv3 cannot be enabled until SSL (Secure Sockets Layer) and HTTPS (SSL) are enabled on the machine. To enable SNMPv3 follow the instructions starting on page 35 of the SAG. The System Administrator should be aware that in configuring SNMPv3 there is the option of resetting both the Privacy and Authentication passwords back to their default values. This option should only be used if necessary since if the default passwords are not known no one will be able to access the SNMP administrator account[4].

r). To be consistent with the evaluated configuration, protocol choices for remote authentication should be limited to [**Kerberos (Solaris)**], [**Kerberos (Windows)**] or [**LDAP**]. The device supports other protocol options. Choose the protocol option that best suits your needs. The System Administrator should be aware, however, that remote authentication using Kerberos will not work with Windows Server 2003.

In the case of LDAP/LDAPS the System Administrator should ensure that SSL is enabled as discussed in Step 3 under "Configuring LDAP Server Optional Information" on page 47 in the SAG. Make sure that [**Enable SSL**] under SSL is selected.

s). To be consistent with the evaluated configuration, the device should be set for local authorization. Remote authorization was not evaluated since that function is performed external to the system. Choose the authorization option that best suits your needs.

t). As part of the evaluated configuration, encryption of transmitted and stored data by the device must meet the FIPS 140-2 Standard. To enable the use of encryption in "FIPS 140 mode" and check for compliance of certificates stored on the device to the FIPS 140-2 Standard follow the instructions on page 76 of the SAG.

u). In viewing the Audit Log the System Administrator should note the following:

- Deletion of a file from Reprint Saved Job folders or deletion of a Reprint Saved Job folder itself is recorded in the Audit Log.

- Deletion of a print or scan job or deletion of a scan-to-mailbox job from its scan-to-mailbox folder may not be recorded in the Audit Log.

- Extraneous process termination events (Event 50) may be recorded in the Audit Log when the device is rebooted or upon a Power Down / Power Up. Extraneous security certificate completion status (Created/Uploaded/Downloaded) events (Event 38) may also be recorded.

v). The System Administrator should download and review the Audit Log on a daily basis. In downloading the Audit Log the System Administrator should ensure that Audit Log records are protected after they have been exported to an external trusted IT product and that the exported records are only accessible by authorized individuals.

---

[4]The SNMP administrator account is strictly for the purposes of accessing and modifying the MIB objects via SNMP; it is separate from the System Administrator "admin" user account or user accounts given SA privileges by the System Administrator "admin" user. The administrator account can not perform any System Administrator functions.

w). Be careful not to create an IP Filtering rule that rejects incoming TCP traffic from all addresses with source port set to 80; this will disable the Web UI. Also, the System Administrator should configure IP filtering so that traffic to open ports from external users (specified by subnet mask) is dropped and so that following ports for web services are closed: tcp ports 53202, 53303, 53404 and tcp/udp port 3702.

IP Filtering is not available for either the AppleTalk protocol or the Novell protocol with the 'IPX' filing transport. Also, IP Filtering will not work if IPv6 is used instead of IPv4.

x). To enable disk encryption follow the instructions under "Enabling Encryption of Stored Data" on page 78 of the SAG.

Before enabling disk encryption the System Administrator should make sure that the ColorQube™ 8700/8900 is not in diagnostics mode and that there are no active or pending scan jobs.

y). The System Administrator should ensure that the Embedded Fax Card and fax software is properly installed. The System Administrator can then set Embedded Fax parameters and options via the Local User Interface on the machine by following the instructions on pages 152 through 160 in the SAG.

z). To enable and configure IPSec, follow the instructions starting on page 83 of the SAG. IPSec should be used to secure printing jobs; HTTPS (SSL) should be used to secure scanning jobs.

Use the default values for IPSec parameters listed in the IPSec discussion starting on page 83 in the SAG whenever possible for secure IPSec setup.

aa). To enable the session inactivity timers (termination of an inactive session) from the Web UI follow the instructions on page 96 of the SAG.

bb). There is a software verification test feature that checks the integrity of the executable code by comparing a calculated hash value against a pre-stored value to ensure the value has not changed. To initiate this feature follow the instructions on page 105 of the SAG.

cc). To enable the Scan to Mailbox feature from the Web UI follow the instructions under 'Enabling or Disabling Scan to Mailbox' on page 126 of the SAG.

For the purposes of the evaluation, the Scan to Mailbox feature was set to store scanned documents only in private folders.

To set the scan policies for the Scan to Mailbox feature follow the instructions under 'Setting Scan Policies' starting on page 126 of the SAG. Public folders are not allowed in the evaluated configuration. The scan policies should therefore be set as follows:

- Deselect [**Allow Scanning to Default Public Folder**].
- Deselect [**Require per Job password to public folders**].
- Select [**Allow additional folders to be created**]
- Select [**Require password when creating additional folders**].
- Select [**Prompt for password when scanning to private folder**].
- Deselect [**Allow access to job log data**].

Passcodes for Scan-to-Mailbox mailboxes should be selected to be as random as possible and should be changed on a regular basis, consistent with applicable internal policies and procedures. Xerox recommends that the minimum length of a password assigned to a private Scan to Mailbox folder be 8 alphanumeric characters.

dd). To enable the Print from USB feature from the Web UI follow the instructions on page 119 of the SAG.

ee). To enable the Print from Mailbox feature from the Web UI follow the instructions on page 120 of the SAG.

ff). In the evaluated configuration the Embedded Fax Secure Receive option should be enabled[5] and the fax forwarding on receive feature should be enabled. The Local Polling option and embedded fax mailboxes should not be set up or used at any time.

To enable Secure Receive from the Local UI follow the instructions under 'Enabling or Disabling the Secure Fax Feature' on page 154 of the SAG. The System Administrator should ensure that the secure receive passcode, which is fixed at 4-digits, is changed every three days.

To enable Fax Forwarding on Receive and establish up to five fax forward rules from the WebUI follow the instructions for Fax Forwarding starting on page 158 of the SAG.

- The evaluation assumes that after normal business hours Fax Forwarding on Receive is enabled and secure receive is disabled.

---

[5] This will apply to any received fax, including faxes that are remotely polled to the device from another remote fax machine or remote device.

- The Mailbox and Polling Policy should be set to delete received faxes when they are printed. To set the Mailbox and Polling Policy follow the instructions under "Defining Mailbox and Polling Policies" on page 160 of the SAG. Makes sure the 'Delete on Print' option is selected for Received Documents.

gg). For best security print jobs (other than LANFax jobs) submitted to the device from a client or from the Web UI should be submitted as a secure print job. Once a secure print job has been submitted the authenticated user can release the job for printing at the Local UI following the directions under 'Releasing a Secure Print' on page 80 of the User Guide[6].

hh). In the evaluated configuration the Secure Print security function should be set to require the User ID for identification purposes to release a secure print job. The Secure Print security function can be accessed and configured by following the instructions under 'Configuring Secure Print Settings' on page 114 of the SAG.

ii). Before upgrading software on the device via the Manual/Automatic Customer Software Upgrade, please check for the latest certified software versions. Otherwise, the machine may not remain in its certified configuration.

jj). In the evaluated configuration, customer software upgrades via the network are not allowed.

kk). In the evaluated configuration the domain filtering option for E-mail was set to limit the domains to which Scan to E-mail jobs can be sent. To enable the domain filtering option follow the instructions under 'Edit Domain and Email Filter Settings' on page 134 of the SAG.

ll). In the evaluated configuration the Hold All Jobs function should be configured so that Enablement is set to 'Hold All Jobs in a Private Queue' and the Unidentified Jobs Policies is set to 'Hold Jobs; Only Administrators can Manage Jobs'. Follow the instructions for "Configuring the Hold All Jobs Feature" on page 115 of the SAG to access and configure the Hold All Jobs function.

mm). The following features and protocols are not included in the evaluation:
- Reprint from Saved Job
- SMart eSolutions
- Custom Services (Extensible Interface Platform or EIP)
- Network Accounting and Auxiliary Access
- Internet Fax
- Use of Embedded Fax mailboxes.
- NTP
- Direct USB Printing,
- AppleTalk and Novell protocols
- SFTP
- Web Services

2. The System Administrator should change the SNMPv1/v2c public/private community strings from their default string names to random un-guessable string names of at least 8 characters in length.

3. Customers should sign up for the RSS[7] subscription service available via the Xerox Security Web Site (Security@Xerox) at www.xerox.com/security that permits customers to view the latest Xerox Product Security Information and receive timely reporting of security information about Xerox products, including the latest security patches.

4. The device should be installed in a standard office environment. Office personnel should be made aware of authorized service calls (for example through appropriate signage) in order to discourage unauthorized physical attacks such as attempts to remove the internal hard disk drive(s). The System Administrator should also ensure that office personnel are made aware to pick up the outputs of print and copy jobs in a timely manner.

5. Customers who encounter or suspect software problems should immediately contact the Xerox Customer Support Center to report the suspected problem and initiate the SPAR (Software Problem Action Request)[8] process for addressing problems found by Xerox customers.

---

[6] Xerox® ColorQube® 8700 / 8900 User Guide, Version 1.0: February 2012
[7] Really Simple Syndication – A lightweight XML format for distributing news headlines and other content on the Web. Details for signing up for this RSS Service are provided in the **Security@Xerox RSS Subscription Service guide posted on the Security@Xerox site at http://www.xerox.com/go/xrx/template/009.jsp?view=Feature&ed_name=RSS_Security_at_Xerox&Xcntry=USA&Xlang=en_US**.
[8] A SPAR is the software problem report form used internally within Xerox to document customer-reported software problems found in products in the field.

6. Caution: A ColorQube 8700/8900 allows an authenticated System Administrator to disable functions like Image Overwrite Security that are necessary for secure operation. System Administrators are advised to periodically review the configuration of all installed machines in their environment to verify that the proper evaluated configuration is maintained.

7. Depending upon the configuration of the device, two IPv4 addresses, a primary IPv4 address and a secondary IPv4 address, may be utilized. The System Administrator selects whether the primary IPv4 address will be obtained statically or dynamically via DHCP from the *IP (Internet Protocol)* page on the Web UI[9]. The second IPv4 address is assigned via APIPA when the System Administrator enables the 'Self Assigned Address' option from the *IP (Internet Protocol)* page on the Web UI. If the 'Self Assigned Address' option is enabled (which is the default case), this secondary IPv4 address will not be visible to the SA[10]. The 'Self Assigned Address' option from the Web UI *IP (Internet Protocol)* page should be disabled unless either APIPA is used or Apple Rendezvous/Bonjour support is required.

8. If a system interruption such as power loss occurs a job in process may not be fully written to the hard disk drive(s). In that case any temporary data created will be overwritten during job recovery but a corresponding record for the job may not be recorded in the completed job log or audit log.

9. If IPv6 is disabled and then a software upgrade is performed by a Xerox Service Technician using an AltBoot, IPv6 will be disabled even though both the Local UI and Web UI show that IPv6 is enabled. IPv6 can be enabled again via the Web UI by first disabling and then re-enabling it.

10. A unique Scan-to-Mailbox mailbox should be established for each authenticated user.

11. Remote Polling should only be used by the System Administrator.

12. Printing of Embedded Fax confirmation reports is not included in the evaluation. The Embedded Fax cover sheets should not be printed with an Embedded Fax job.

13. Users should be aware that correct remote repository document pathnames for the receipt of workflow scanning jobs should start with one '\' as opposed to the two '\'s shown in the SAG (e.g., page 140).

14. Users should be provided with appropriate training on how to use the ColorQube 8700/8900 in a secure manner before being assigned user accounts to access the device.

15. The following windows are available to any authenticated and authorized user from the Local User Interface. These windows provide standard machine services or job management capability:

   - **Embedded Fax Batch Send Confirmation** – Allows a user to either send an Embedded Fax job to a remote destination immediately or include the job as part of a "batch" of Embedded Fax jobs sent to the same destination. Is accessible by selecting the following screens/buttons in order: [**Services Home**] hard button → [**Fax**] feature button → [**Start**] hard button when a user is submitting an Embedded Fax Send job to the same destination as a previously submitted "delayed send" Embedded Fax job.

   - **Releasing All Secure Receive Jobs** – An authenticated user with the secure receive passcode number can release all received Embedded Faxes as follows:
     - At the control panel, press Job Status button.
     - From the **Active Jobs** tab touch any one of the incoming received Embedded Fax listed.
     - Touch the [**Release All**] button .
     - Use the keypad to enter the secure receive passcode number and then touch the [**Enter**] button.

   - **Pausing an active job being processed by the device** – Allows the user to pause an active copy, print, workflow scanning, scan to email, Internet Fax or Embedded Fax job while it is being processed. Is accessible by selecting the [**Stop**] machine hard button while a job is being processed by the device. Depending on the type of jobs being processed by the device when the [**Stop**] button is selected, one of the following **Pause** windows will be displayed as appropriate to allow the user to determine whether to delete or continue processing of the job: **Scanning Pause** window, **Printing Pause** window, **Copy Only (Scanning and Printing) Pause** window, **Scanning/Printing (Simultaneous Jobs) Pause** window, **Scanning Build Job Segment (No Printing) Pause** window, **Printing Build Job Segment (No Scanning) Pause** window or **Scanning Build Job Segment/Printing Another Job Pause** window.

   - **Overwrite Security Failure** – Automatically provides an error message to the user is case an Immediate Image Overwrite of a copy, print, workflow scanning, scan to email, LAN Fax or Embedded Fax job fails. The error message informs the user to notify the System Administrator that an On Demand Overwrite should be run and persists on the Local UI screen until either a manual or a scheduled On Demand Overwrite is initiated.

---

[9] The primary IPv4 address can also be assigned dynamically via DHCP from the Dynamic Addressing screen on the Local UI.
[10] The primary IPv4 address will always be displayed on the Configuration Report that can be printed for a ColorQube 8700/8900.

- **User Interface Diagnostics** - Allows the user to run diagnostics on the User Interface software. Is accessible by pressing the machine hard buttons '**Dial Pause**' + '*****' + '**#**' in that order.

16. The Web UI provides a set of on-line help pages that provide guidance on most of the Web UI pages. These on-line help pages can be accessed from the Web UI by selecting the [**Help**] button on the upper right hand corner of every Web UI page; the on-line help page corresponding to the Web UI page being viewed will be displayed. There is also a 'TOC' contents list of all Web UI help pages to the left of each help page; scrolling through the content list and selecting the desired page will also cause the applicable on-line help page to be displayed.

The following pages are available from the Web UI with System Administrator login and authentication but are not documented in the SAG, User's Guides or the on-line help:

- **LDAP Policy** - Allows the System Administrator to set the use of Simple Authentication and Security Layer (SASL) to authenticate and encrypt LDAP. Is accessible by selecting the **Properties** tab and then selecting the following entries from the Properties 'Content menu': { Either **Connectivity** → **Protocols** → **LDAP** or **Security** → **Authentication** → **Setup** → Edit hyperlink under 'Actions' from the **LDAP Servers** line } → [**LDAP Policies**].

- **Application Domain/Content Query -** Allows the configuration of the system to perform an LDAP query for the logged-in user's authentication domain prior to authenticating the server. Is accessible by typing **http://{IP Address}[11]/diagnostics/index.dhtml** and then selecting '**Authentication Domain/Context Query**' from the **Diagnostics** Content Menu.

- **Scanning Lock Files -** Allows bypassing the filename locking feature. Is accessible by typing **http://{IP Address}/diagnostics/index.dhtml** and then selecting '**Scanning Lock Files**' from the **Diagnostics** Content Menu or by typing **http://{IP Address}/diagnostics/lockFiles.dhtml**.

- **Gray Other Queues Button -** Allows the System Administrator to grey out the 'Other Queue' button on the Local UI. Is accessible by typing **http://{IP Address}/diagnostics/index.dhtml** and then selecting '**Grey Other Queues Button**' from the **Diagnostics** Content Menu or by typing **http://{IP Address}/diagnostics/hideotherqueuesbutton.php**.

- **Secure Print Alphanumeric PIN -** Allows the System Administrator to set the secure print PIN to be alphanumeric characters instead of just digits. Is accessible by typing either **http://{IP Address}/diagnostics/index.dhtml** and then selecting '**Secure Print Alphanumeric PIN**' from the **Diagnostics** Content Menu or by typing **http://{IP Address}/diagnostics/secureprintalphanumericpin.php**.

- **Secure Attribute Editor -** Allows the user to change some system attributes related to PDLs (e.g., memory usage, copies per page, etc.). Is accessible by typing **http://{IP Address}/diagnostics/secureattr.dhtml**.

- **Suppress Job Name -** Allows the System Administrator to suppress displaying the job name on the Banner Page when submitting a print job. Is accessible by typing **http://{IP Address}/diagnostics/jobNameSuppress.dhtml**.

- **Job Log File Format -** Allows the System Administrator to set the XML job log file format. Is accessible by typing **http://{IP Address}/diagnostics/jobLog.dhtml**.

- **File Extension Case -** Allows the System Administrator to select all file extensions to be created in either lower or upper case. Is accessible by typing **http://{IP Address}/diagnostics/fileExtensionCase.dhtml**.

- **Email Security -** Allows the System Administrator to secure the device's email service. Is accessible by typing **http://{IP Address}/diagnostics/emailSecurity.php**.

- **Binary Printing Support -** Allows the device to accept printing jobs that are identified as binary files. Is accessible by typing **http://{IP Address}/diagnostics/binaryAllow.php.**

- **XSA Reports with User IDs -** Allows the device to generate Xerox Standard Accounting reports with User IDs. Is accessible by typing **http://{IP Address}/diagnostics/enableUserID.php**.

- **Postscript Filter PDL Guessing Policy -** Allows the System Administrator to select whether the Postscript Filter guess algorithm will use a strict or loose interpretation. Is accessible by typing **http://{IP Address}/diagnostics/postScriptTokens.php**.

- **Web Services IP Lockout Reset -** Allows the System Administrator to clear the Web Services IP Address Lockout cache. Is accessible by typing **http://{IP Address}/diagnostics/ipLockout.php**.

- **Service Registry Reset -** Allows the System Administrator to reset the device's Service Registry to its default values. Is accessible by typing **http://{IP Address}/diagnostics/registryReset.php**.

---

[11] {IP Address} is the IPv4 address of the machine

- **Job Queue Limit -** Allows the System Administrator to set the maximum number of jobs that can be listed in the device's job queues. Is accessible by typing **http://{IP Address}/diagnostics/jobLimit.php**.

- **Barcode Space Character Interpretation -** Allows the System Administrator to choose how the device renders space characters within barcode fonts. Is accessible by typing **http://{IP Address}/diagnostics/barcodeSpaceToggle.php**.

- **DHCP v6 -** Allows the System Administrator to choose which compliance option will be followed when DHCP v6 is used. Is accessible by typing **http://{IP Address}/diagnostics/ dhcpv6Options.php**.

- **View Service Registry Contents -** Allows the System Administrator to view the contents of the device's Service Registry. Is accessible by typing **http://{IP Address}/diagnostics/viewRegistry.php**.

- **Diagnostics Tree -** Allows the System Administrator to view the selectable list of diagnostics Special Purpose Pages. Is accessible by typing **http://{IP Address}/diagnostics/tree.php**.

- **PCL Advanced Configuration -** Allows the System Administrator to enter the desired PCL advanced configuration paper size code. Is accessible by typing **http://{IP Address}/diagnostics/pclSetup.php**.

- **Control Kerberos Settings –** Allows the System Administrator to control how the device performs Kerberos authentication with a domain controller, LDAP server and other kerberized services as they are developed. Is accessible by typing **http://{IP Address}/diagnostics/kerberosSettings.php**.

- **Download DLM PCL Forms -** Allows the System Administrator to download the DLM PCL forms into the device. Is accessible by typing **http://{IP Address}/diagnostics/dl_pcl.php**.

- **Multiple Pages per JBIG2 Dictionary -** Allows the System Administrator to enable the multiple pages per JBIG2 dictionary feature (for PDF and PDF/A only). Is accessible by typing **http://{IP Address}/diagnostics/disableMultiplePages.php**.

- **Show WebUI Configuration Page -** Allows the System Administrator to enable users who are not authenticated administrators to view the WebUI Configuration Page. Is accessible by typing **http://{IP Address}/diagnostics/ShowConfigSheet.php**.

- **NTLM v2 Response -** Allows the System Administrator to enable the device to send only the NT Lan Manager (NTLM) Version 2 protocol (and refuse the LM & NTLM versions). Is accessible by typing **http://{IP Address}/diagnostics/NTLMSecurity.php**.

- **Custom Size Allowed -** Allows the System Administrator to allow custom size paper to be used for print jobs. Is accessible by typing **http://{IP Address}/diagnostics/customSizeAllowed.php**.

- **Copies Per Page Print Setting -** Allows the System Administrator to permit the use of the copies per page setting for print jobs. Is accessible by typing **http://{IP Address}/diagnostics/copiesPerPage.php**.

- **HTTP SSL Cipher Encryption Strength -** Allows the System Administrator to control the set of supported ciphers when using SSL (e.g., to enforce 128 bit or higher encryption keys). Is accessible by typing **http://{IP Address}/diagnostics/SSLCiphers.php**.

- **Port 9100 Print Stream Filtering -** Allows the System Administrator to enable/disable the filtering of the RAW IP print stream for the occurrence of the PostScript control-T character. Is accessible by typing **http://{IP Address}/diagnostics/Port9100PrintStreamFiltering.php**.

- **Color Preset Screen -** Allows the System Administrator to enable/disable the "Color Preset Screen" feature before a copy job. Is accessible by typing **http://{IP Address}/diagnostics/ColorPresetScreen.php**.

- **CRU Low/Reorder Message Suppression -** Allows the System Administrator to set whether the CRU Low/Reorder messages are enabled/disabled. Is accessible by typing **http://{IP Address}/diagnostics/CRULowReorderMessageSuppression.php**.

- **Install Software (View Scan Templates Created by WIA Driver) -** Allows the System Administrator to install the #00022121 Network Controller version to view templates created by the Microsoft Windows Image Acquisition (WIA) driver. Is accessible by typing **http://{IP Address}/diagnostics/00022121.dhtml**. The System Administrator should be aware that installing this Network Controller version will result in the device no longer being in the evaluated configuration.

- **Cost Control Enablement and Receipt Printing Setup -** Allows the System Administrator to enable the Cost Control feature when Secure Access and network accounting are enabled. Is accessible by typing **http://{IP Address}/diagnostics/CostControl.php**.

- **Scan Image Compression -** Allows the System Administrator to manage the asymmetric sub sampling options of scan image processing. Is accessible by typing **http://{IP Address}/diagnostics/asymmetricSubSample.php**.

17. The following pages are available from the Web User Interface with no user login and authentication required:

- **Site Map** - Provides the user with hyperlink pointers to each Web User Interface screen organized by Web UI tab. Is accessible by selecting the [**Site Map**] button in the upper right hand corner of every Web User Interface page.

- **Exit from Sleep Mode** – Automatically informs the user, when the Network Controller is in 'Sleep Mode' at the time the user attempts to make a change to current settings on a Web User Interface web page, that the Network Controller needs to be taken out of 'Sleep Mode' before the requested changes can be made.

18. Customers who required specialized changes to support unique workflows in their environment may request specific changes to normal behavior. Xerox will supply these SPAR releases to the specific customers requesting the change. Please note that in general enabling a specialized customer-specific feature will take the system out of the evaluated configuration.

Contact
For additional information or clarification on any of the product information given here, contact Xerox support.

Disclaimer
The information provided in this Xerox Product Response is provided "as is" without warranty of any kind. Xerox Corporation disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Xerox Corporation be liable for any damages whatsoever resulting from user's use or disregard of the information provided in this Xerox Product Response including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Xerox Corporation has been advised of the possibility of such damages. Some states do no allow the exclusion or limitation of liability for consequential damages so the foregoing limitation may not apply.