Secure Installation and Operation of Your ColorQube™ 9201/9202/9203

Purpose and Audience
This document provides information on the secure installation and operation of a ColorQube™ 9201/9202/9203 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™ 9201/9202/9203 Multifunction System is operated and maintained in a secure manner.

Background
The ColorQube™ 9201/9202/9203 Multifunction System is currently undergoing Common Criteria evaluation. The information provided here is consistent with the security functional claims made in the Security Target. 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 or from your Xerox representative.

1. Please follow the guidelines below for secure installation, setup and operation of the evaluated configuration for a ColorQube™ 9201/9202/9203 Multifunction System:
   a). The security functions in the evaluated configuration of the ColorQube™ 9201/9202/9203 that should be set up by the System Administrator are:
      • Immediate Image Overwrite
      • On Demand Image Overwrite
      • Disk Encryption
      • IP Filtering
      • Audit Log
      • SSL (for protection of management data)
      • IPSec
      • SNMP v3
      • Trusted Certificate Authorities
      • Authentication, Authorization and Personalization
      • 802.1x Device Authentication
      • Session Inactivity Timeout

   The System Administrator login is required when accessing the security features of a ColorQube™ 9201/9202/9203 machine via the Web User Interface (Web UI). To log in to the Web UI as an authenticated System Administrator, follow the instructions under “CentreWare Internet Services” located on page 2-6 in the SAG.

   To log in to the Local User Interface (Local UI) as an authenticated System Administrator, follow the “Administrator Access” instructions located on page 2-4 in the SAG.

   Follow the instructions located in the System Administrator Guide (SAG) in Chapter 8, Security to set up these security functions except as noted in the items below.

   b). The following services of the ColorQube™ 9201/9202/9203 are also considered part of the evaluated configuration and should be enabled when needed by the System Administrator - Copy, Embedded Fax, Scan to E-mail, Workflow Scanning, Internet Fax and Reprint Saved Jobs.

   c). Secure acceptance of the ColorQube™ 9201/9202/9203, once device delivery and installation is completed, should be done by:
      • Printing out a Configuration Report by following the “How to Print a Configuration Report” instructions located on page 3-2 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™ 9201/9202/9203 Multifunction Systems Security Target, Version 1.0 and make sure that they are the same in all cases.


---

2. Xerox Common Access Card Xerox ColorQube™ 9201/9202/9203, Version 1.0, 09/09, 604E53830
For customers concerned about document files on the hard disk drive(s) or Embedded Fax card memory the Immediate Image Overwrite and On Demand Image Overwrite security features, which comes installed on the ColorQube™ 9201/9202/9203 Multifunction System, must be properly configured and enabled. Please follow the “Immediate Image Overwrite” instructions starting on page 8-17 in the SAG and the “On Demand Overwrite” instructions starting on page 8-19 in the SAG for proper enablement, setup and initiation of Immediate Image Overwrite and On Demand Image Overwrite, 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.

• 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. Follow the instructions starting on page 8-19 the SAG for invoking a Standard or Full On Demand Image Overwrite from either the Local UI or the Web UI.

• Once an On Demand Image Overwrite has been initiated by the System Administrator from either the Local UI or Web UI 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 instructions starting on page 8-21 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).
  • 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 Image 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, Xerox recommends that first a system reboot or software reset 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 reboot 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

---

3 The ColorQube™ 9201/9202/9203 Multifunction System comes in two configurations – a multi-board configuration with separate Network Controller and Copy Controller boards and separate hard disk drives and a single board configuration with one board containing both the Network and Copy Controllers and with a single hard disk drive.
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 a ColorQube™ 9201/9202/9203 Multifunction System is decommissioned, returned, sold or disposed of.

f). The ColorQube™ 9201/9202/9203 Multifunction System supports the use of SSLv2.0, SSLv3.0, RC4 and MD5. However, customers are advised to set the crypto policy of their clients to request either SSLv3.1 or TLSv1.0 and to disallow the use of RC4 and MD5.

g). For SSL to work properly the machine must be assigned a valid, fully qualified machine name and domain. To set the machine name and domain:
- Follow the “Access Internet Services” instructions on page 2-6 of the SAG to access the Web UI.
- At the Web UI, select the Properties tab.
- Select the following entries from the Properties ‘Content menu’: Connectivity → Protocols → IP (Internet Protocol).
- Enter the domain name in the ‘Domain Name’ text box and the machine name in the ‘Host Name’ text box inside the General group box.
- Select the [Apply] button to save the domain and host names entered.

h). Xerox recommends the following when utilizing Secure Sockets Layer (SSL) on a ColorQube™ 9201/9202/9203:
- Any self-signed digital certificate or digital certificate signed by a Trusted Certificate Authority should have a maximum validity of 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.

i). To enable HTTPS (SSL):
- At the Web UI, select the Properties tab.
- Follow the “Machine Digital Certificate Management” instructions starting on page 8-9 of the SAG to install on the device either a self-signed digital certificate or a digital certificate signed by a Certificate Authority (CA).
- Select the following entries from the Properties ‘Content menu’: Connectivity → Protocols → HTTP.
- Select the Secure HTTP (SSL) Enabled checkbox in the Configuration group box and enter the desired HTTPS port number in the Port Number text box.
- Select the [Apply] button. This will save the indicated settings. After saving the changes the Web UI will become disabled; the System Administrator will have to access the Web UI again.

j). Xerox recommends the following when utilizing Secure Sockets Layer (SSL) for secure scanning on a ColorQube™ 9201/9202/9203:
- SSL should be enabled and used for secure transmission of scan jobs from a ColorQube™ 9201/9202/9203.
- 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”.

k). 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.

---

4 Assumes that the Web UI has been accessed already by following the “Access Internet Services” instructions on page 2-6 of the SAG.
• 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.

l). 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. Note: IP Filtering is not available for either the AppleTalk protocol or the Novell protocol with the ‘IPX’ filing transport.

m). To enable disk encryption:
• At the Web UI³, select the Properties tab.
• Select the following entries from the Properties ‘Content menu’: Security → User Data Encryption.
• Select the Enabled checkbox in the User Data Encryption Enablement group box.
• Select the [Apply] button. This will save the indicated setting. After saving the changes the Network Controller will reboot; once this reboot is completed the System Administrator will have to access the Web UI again.

Xerox recommends that before enabling disk encryption the System Administrator should make sure that the ColorQube™ 9201/9202/9203 is not in diagnostics mode and that there are no active or pending scan jobs.

n). The system administration should ensure that the Embedded Fax Card and fax software is installed in accordance with the “Complete the Fax Setup Screens” instructions on page 15-2 in the SAG. 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 15-2 through 15-4 in the SAG³.

o). To enable and configure IPSec, follow the instructions starting on page 8-12 in the SAG³. Xerox strongly recommends that IPSec should be used for secure printing only; HTTPS (SSL) should be used to secure scanning. Note: IPSec is not available for either the AppleTalk protocol or the Novell protocol with the ‘IPX’ filing transport.

p). If the use of SNMPv3 is desired, it can be set up by following these instructions:
SNMPv3 cannot be enabled until SSL (Secure Sockets Layer) and HTTPS (SSL) are enabled on the machine.
• At the Web UI³, select the Properties tab.
• Select the following entries from the Properties ‘Content menu’: Connectivity → Protocols → SNMP. This will display the SNMP Configuration page.
• Select the “Enable SNMP v3 Protocol” checkbox inside the SNMP Properties group box.
• Select the [Edit SNMP v3 Properties] button inside the SNMP Properties group box. This will cause the Edit SNMP v3 Properties page to be displayed.
• On the Edit SNMP v3 Properties page:
  • Select the Account Enabled button inside the Administrator Account group box to create an administrator account.
  • Enter the desired Username and Authentication Password. The Authentication Password must be at least 8 alphanumeric characters.
  • Enter the desired Privacy Password of at least 8 alphanumeric characters.
  • Select the Account Enabled button inside the Print Drivers Account group box to create an account for bi-directional print drivers / Xerox remote clients.
  • Select the [Apply] button. This will create an administrator account and save the indicated settings/passwords. After saving the changes the SNMP Configuration page will be redisplayed.

Once SNMP v3 is enabled, SSL can be disabled and SNMP v3 will still function properly.

q). To enable the session inactivity timer (termination of an inactive session) for the Web UI:
• At the Web UI³, select the Properties tab.
• Select the following entries from the Properties ‘Content menu’: Security → System Timeout
• Enter the desired inactive session timeout interval in minutes.
• Select the [Apply] button. This will save the indicated Web UI inactivity timer setting. After saving the changes the System Timeout page will be redisplayed.

r). To enable the session inactivity timer (termination of an inactive session) for the Local UI:
• Select the [Machine Status] hard button on the device and then the [Tools] button to access the System Administrator Tool pathway.
• Select the following buttons from the Tools menu: [Device Settings] → [Timers] → [System Timeout…]
• Select the [Enabled] button and then enter the desired inactive session timeout interval in seconds in the text box.
s). Change the Administrator password as soon as possible. Reset the Tools password periodically.

Xerox recommends that you (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 “How to change the Administrator Password” instructions on page 3-1 in the SAG.

2. Xerox recommends that the System Administrator change the SNMP v1/v2c public/private community strings from their default string names to random string names.

3. Before upgrading software on a ColorQube™ 9201/9202/9203 Multifunction System 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. To maintain the certified configuration, it is recommended that acceptance of customer software upgrades via the network be turned off/disabled on the Web UI (Upgrade web page).

4. Xerox recommends that customers sign up for the RSS subscription service available only 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 that apply to the ColorQube™ 9201/9202/9203 Multifunction System.

5. The ColorQube™ 9201/9202/9203 Multifunction System 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).

6. Xerox recommends that the System Administrator continuously monitor the network that the ColorQube™ 9201/9202/9203 Multifunction System is connected to for unapproved activities and/or attempts to attack network resources, including the device itself. This should include monitoring of the number of logon tries to the Web UI.

7. Customers who encounter or suspect software problems against a ColorQube™ 9201/9202/9203 Multifunction System should immediately contact the Xerox Customer Support Center to report the suspected problem and initiate the SPAR (Software Problem Action Request) process for addressing problems found by Xerox customers.

8. A reboot of the system software for a ColorQube™ 9201/9202/9203 machine is necessary before a change made to the System Administrator password from the Local User Interface will be synced with and accepted by the Web User Interface. Until this system software reboot occurs, system administrator functions from the Web User Interface should not be accessed.

9. Caution: A ColorQube™ 9201/9202/9203 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 secure configuration is maintained.

10. Depending upon the configuration of the ColorQube™ 9201/9202/9203, two IPv4 addresses, a primary IPv4 address and a secondary IPv4 address, may be utilized. The System Administrator assigns the primary IPv4 address either statically or dynamically via DHCP from the IP (Internet Protocol) page on the Web UI. 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. Xerox recommends that the ‘Self Assigned Address’ option from the Web UI IP (Internet Protocol) page be disabled unless either APIPA is used or Apple Rendezvous/Bonjour support is required.

11. 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.

---

5 RDF Site Summary, or Rich Site Summary, or 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.

6 A SPAR is the software problem report form used internally within Xerox to document customer-reported software problems found in products in the field.

7 The primary IPv4 address can also be assigned dynamically via DHCP from the Dynamic Addressing screen on the Local UI.

8 The primary IPv4 address will always be displayed on the Configuration Report that can be printed for a WorkCentre™ 5632/5638/5645/5655/5665/5675/5687.
12. 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 the both the Local UI and Web UI show that IPv6 is enabled. IPv6 can be enabled again by first disabling it on the Web UI and then re-enabling it on the Web UI.

13. Xerox strongly recommends that users place documents scanned on a ColorQube™ 9201/9202/9203 using the Scan to Mailbox feature in private folders and not in public folders.

14. The following windows are available from the Local User Interface to a ColorQube™ 9201/9202/9203 with System Administrator login and authentication. These windows provide standard system configuration or job management capability:

   - **PagePack Passcode** - Allows the System Administrator to enter a 4 digit “PagePack PIN” to enable a PagePack device to work with metered supplies. Is accessible by selecting the following screens/buttons in order: [Machine Status] hard button → [Tools] button → [Device Settings] button → [Enter PagePack Passcode] button. Once the System Administrator accesses the PagePack Passcode screen and enters a valid PagePack PIN, the System Administrator can print out PagePack courtesy prints by selecting the [Skip] button; however, if the number of PagePack courtesy prints requested exceeds the allowable limit an appropriate error message will be displayed on the screen and the System Administrator will have to re-enter a valid PagePack PIN.

   - **Enter Cleaning Unit Passcode** - Allows the System Administrator to enter a 4 digit passcode to temporarily extend a Customer Replaceable Unit (CRU) when that CRU has reached its end of life. Is accessible by selecting the following screens/buttons in order: [Machine Status] hard button → [Tools] button → [Device Settings] button → [Enter Cleaning Unit Passcode] button.


   - **Service Plan** - Allows the System Administrator to set or change the Service Plan for the device. Is accessible by selecting the following screens/buttons in order: [Machine Status] hard button → [Tools] button → [Service Settings] button → [Service Plan] button.

   - **Network Logs** – Allows the System Administrator to download network logs to a USB drive for troubleshooting purposes. Is accessible by selecting the following screens/buttons in order: [Machine Status] hard button → [Tools] button → [Network Settings] button → [Advanced Settings] button → [Network Logs] button. The System Administrator can download either a basic or an enhanced level of network log information, and a separate screen will provide information on the completion status of the download.


   - **Supply Counter Reset** – Allows the System Administrator to manually reset the supply counter for a CRU on a ColorQube™ 9201/9202/9203 back to 100% when that CRU is replaced. Is accessible by selecting the following screens/buttons in order: [Machine Status] hard button → [Tools] button → [Troubleshooting] button → [Resets] button → [Supply Counter Reset] button.

15. The following windows are available to any authenticated and authorized user from the Local User Interface to a ColorQube™ 9201/9202/9203. 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.

   - **Workflow Scanning Authentication Required** – Allows a user to enter the proper user credentials for a workflow scanning job being sent to a network destination that requires user login. Is accessible by selecting the following screens/buttons in order: [Services Home] hard button → [Workflow Scanning] button → [Start] hard button when a user is submitting a workflow scanning job to a network destination that requires user login → [OK] 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 by the ColorQube™ 9201/9202/9203. 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...
17. **Authentication.** These pages provide additional system configuration capability:

- **Overwrite Security Failure** – Automatically provides an error message to the user if an Immediate Image Overwrite of a copy, print, workflow scanning, scan to email, Internet 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.

- **System Administrator Password Reset** – Allows any user to manually reset the System Administrator password back to the default value. Is accessible when the System Administrator has enabled this feature on the Web UI, the user has obtained from the Xerox Support Center the 12-digit alphanumeric reset code that is unique for each ColorQube™ 9201/9202/9203 device, and the user presses and holds down the proper 3-button sequence on the machine keypad.

- **Custom Services** – Provides access to any custom services (Third Party applications developed with a common API to run on a Xerox device) that are installed in the device. Is accessible by selecting the following screens/buttons in order: [Services Home] hard button ➔ [Custom Services] button. The user then selects any of the installed services listed on the Custom Services screen which will cause that service to be run. The user should be aware of the following:
  - A screen will be displayed with the appropriate error message when the device encounters an error while attempting to access a custom service installed on the device.
  - If the [Access] hard button is selected after selecting an installed custom service , a screen will be displayed that will allow the user to exit the Custom Services service.

- **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.

- **Automatic Maintenance** – Provides a notice to a user when automatic maintenance of the Internal Marking Engine on the device to perform print quality diagnostics and calibration is being performed. Applicable screens will be displayed to indicate when this automatic maintenance is about to start and is in progress; the user has the option to cancel the automatic maintenance by selecting the [Cancel] button on the screen that appears when automatic maintenance is about to start.

16. The following page is available from the Web UI on the ColorQube™ 9201/9202/9203 to any logged in and authenticated user. This page provides workflow scanning configuration capability:

- **Scan Compression Capability Page** – Allows a user to set compression capability for Workflow Scanning. Is accessible by selecting the following items in order: Scan tab ➔ selecting a template from the Template List in the Scan content menu ➔ [Edit] button in the Compression Capability group box.

17. The following pages are available from the Web UI on the ColorQube™ 9201/9202/9203 with System Administrator login and authentication. These pages provide additional system configuration capability:

- **Public Address Book** – Allows the System Administrator to set up the contents and access rights for the Public Address Book. Is accessible by selecting the Public Address Book tab. From the Public Address Book tab content menu the System Administrator can access the following pages to setup the Public Address Book:
  - **View All Names** – Displays the Public Address Book page and provides access to all names in the Public Address Book.
  - **Edit** – Edits a Public Address Book name selected from the Public Address Book page.
  - **Add New Name** – Accesses the Add New Name page to add a new name to the Public Address Book.
  - **Import** – Accesses the Import page to import of names from a file that will be added to the Public Address Book. A Next button on the Import page allows the System Administrator to set options on how the names are to be imported.
  - **Export** – Accesses pages to export the Public Address Book to a user-defined file.
  - **Download Sample** – Allows the System Administrator to download a sample Public Address Book into a user-defined file where names can be added at a later time.
  - **Delete All Names** – Allows the System Administrator to delete all names from the Public Address Book.
  - **Access Rights** – Allows the System Administrator to set the access rights to the Public Address Book.

- **Entry Screen Defaults** – Allows the System Administrator to set the default entry screens (also called the “default walkup screens”) for the Local UI. Is accessible by selecting the Properties tab and then selecting General Setup ➔ Entry Screen Defaults from the Properties tab content menu.

- **Date and Time** – Allows the System Administrator to set the date and time for the device. Is accessible by selecting the Properties tab and then selecting General Setup ➔ Date and Time from the Properties tab content menu.

- **Sleep Mode Settings** – Allows the System Administrator to set the Network Controller sleep mode settings. Is accessible by selecting the Properties tab and then selecting General Setup ➔ Sleep Mode Settings from the Properties tab content menu.
menu. The System Administrator can also set up advanced Network Controller sleep mode settings by selecting the [Advanced Settings] button located on the Sleep Mode Settings page.

- **Network Logs** – Allows the System Administrator to download a detailed log file that contains printer diagnostic information that can be used for troubleshooting purposes. Is accessible by selecting the Properties tab and then selecting General Setup → Network Logs from the Properties tab content menu.

- **Ethernet** - Allows the System Administrator to set the Ethernet rated speed. Is accessible by selecting the Properties tab and then selecting Connectivity → Physical Connections → Ethernet from the Properties tab content menu.

- **USB Settings** - Allows the System Administrator to configure the USB Printing Port. Is accessible by selecting the Properties tab and then selecting Connectivity → Physical Connections → USB Settings from the Properties tab content menu.

- **FTP** – Allows the System Administrator to set the parameters for the FTP protocol used in network filing. Is accessible by selecting the Properties tab and then selecting Connectivity → Protocols → FTP from the Properties tab content menu.

- **Printing** – Allows the System Administrator to review and change the default settings for a print job submitted to the device using the Web UI. Is accessible by selecting the Properties tab and then selecting Services → Printing → General from the Properties tab content menu.

- **Printer Fonts** – Allows the System Administrator to view the types of printer fonts available for print jobs submitted to the device using the Web UI. Is accessible by selecting the Properties tab and then selecting Services → Printing → Printer Fonts from the Properties tab content menu.

- **Postscript®** – Allows the System Administrator to configure the Postscript® interpreter. Is accessible by selecting the Properties tab and then selecting Services → Printing → Postscript® from the Properties tab content menu.

- **PCL** – Allows the System Administrator to view and configure the device’s PCL printer language. Is accessible by selecting the Properties tab and then selecting Services → Printing → PCL from the Properties tab content menu.

- **TIFF** – Allows the System Administrator to view the device’s TIFF version information. Is accessible by selecting the Properties tab and then selecting Services → Printing → TIFF from the Properties tab content menu.

- **Scan Services File Extension Page** – Allows the System Administrator to set default file extensions for scan services to be created in either upper or lower case. Is accessible by selecting the Properties tab and then selecting Services → Scan Services → Defaults from the Properties tab content menu.

- **E-mail Defaults Security Page** – Allows the System Administrator to add or update Scan to E-mail security information. Is accessible by selecting the Properties tab and then selecting from the Properties tab content menu: Services → E-mail → Defaults → Edit from the Security group box on the E-mail Defaults page.

- **E-Mail Defaults File Extension Page** – Allows the System Administrator to set Scan to E-mail default file extensions to be created in either upper or lower case. Is accessible by selecting the Properties tab and then selecting from the Properties tab content menu: Services → E-mail → Defaults → Edit from the File Extension group box on the E-mail Defaults page.

- **Internet Fax Defaults Internet Fax Page** – Allows the System Administrator to add or update default Internet Fax job information. Is accessible by selecting the Properties tab and then selecting from the Properties tab content menu: Services → Internet Fax → Defaults → Edit from the Internet Fax group box on the Internet Fax Defaults page.

- **Internet Fax Defaults File Extension Page** – Allows the System Administrator to set Internet Fax default file extensions to be created in either upper or lower case. Is accessible by selecting the Properties tab and then selecting from the Properties tab content menu: Services → Internet Fax → Defaults → Edit from the File Extension group box on the Internet Fax Defaults page.

- **Validation Servers** – Allows the System Administrator to select and configure up to six Workflow Scanning validation servers. Is accessible by selecting the Properties tab and then selecting Services → Workflow Scanning → Validation Servers from the Properties tab content menu.

- **Scanning Web Services** – Allows the System Administrator to configure the HTTPS, Scan Template Management and Scan Extension scanning web services. Is accessible by selecting the Properties tab and then selecting Services → Workflow Scanning → Scanning Web Services from the Properties tab content menu.

- **Workflow Scanning Defaults File Extension Page** – Allows the System Administrator to set Workflow Scanning default file extensions to be created in either upper or lower case. Is accessible by selecting the Properties tab and then selecting from the Properties tab content menu: Services → Workflow Scanning → Default Template → Edit from the File Extension group box on the Workflow Scanning Default Template page.
• Workflow Scanning Display Settings Page – Allows the System Administrator to set up how the Workflow Scanning template list is displayed on the Local UI. Is accessible by selecting the Properties tab and then selecting from the Properties tab content menu Services → Workflow Scanning → Display Settings.

• Workflow Scanning Custom File Naming Page – Allows the System Administrator to set up automatic naming of Workflow Scanning generated files. Is accessible by selecting the Properties tab and then selecting from the Properties tab content menu Services → Workflow Scanning → Custom File Naming.

• System Timeout – Allows the System Administrator to set up the length of the Web UI inactivity timer. Is accessible by selecting the Properties tab and then selecting from the Properties tab content menu Security → System Timeout.

• 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]/diagnostics/index.dhtml and then selecting ‘Application Domain/Content 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.

• Grey Other Queue 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 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.

• 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.

• DLM Maker - Allows the System Administrator to create a DLM out of any file. Is accessible by typing http://[IP Address]/diagnostics/dlmMaker.php.

9 (IP Address) is the IPv4 address of the machine
• **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)](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)](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)](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)](http://{IP Address})/diagnostics/tree.php.

• **Color Copy Control Test Result** - Allows the System Administrator to view the Color Copy Control test results. Is accessible by typing [http://(IP Address)](http://{IP Address})/diagnostics/testResult.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)](http://{IP Address})/diagnostics/pclSetup.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)](http://{IP Address})/diagnostics/dl_pcl.php.

• **Download DLM Authentication Settings** - Allows the System Administrator to download the DLM authentication settings into the device. Is accessible by typing [http://(IP Address)](http://{IP Address})/diagnostics/dl_auth_settings.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)](http://{IP Address})/diagnostics/disableMultiplePages.php.

• **Print Behavior Settings** - Allows the System Administrator to configure/enable alternate media dimension settings for print jobs. Is accessible by typing [http://(IP Address)](http://{IP Address})/diagnostics/alternateMedia.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)](http://{IP Address})/diagnostics/ShowConfigPage.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)](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)](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)](http://{IP Address})/diagnostics/copiesPerPage.php.

• **Print Behavior Settings (Suppress Last Blank Page)** - Allows the System Administrator to suppress a last blank page for print jobs. Is accessible by typing [http://(IP Address)](http://{IP Address})/diagnostics/suppresslastblankpage.php.

• **Display CAC/PIV Feature** - Allows the System Administrator to enable the display of the CAC/PIV feature. Is accessible by typing [http://(IP Address)](http://{IP Address})/diagnostics/enableCAC.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)](http://{IP Address})/diagnostics/00022121.dhtml. The System Administrator should be aware that installing this Network Controller version will result in the ColorQube™ 9201/9202/9203 no longer being in the certified configuration.

18. The following pages are available from the Web User Interface to a ColorQube™ 9201/9202/9203 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 on a ColorQube™ 9201/9202/9203 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.

19. 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 certified 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 not allow the exclusion or limitation of liability for consequential damages so the foregoing limitation may not apply.