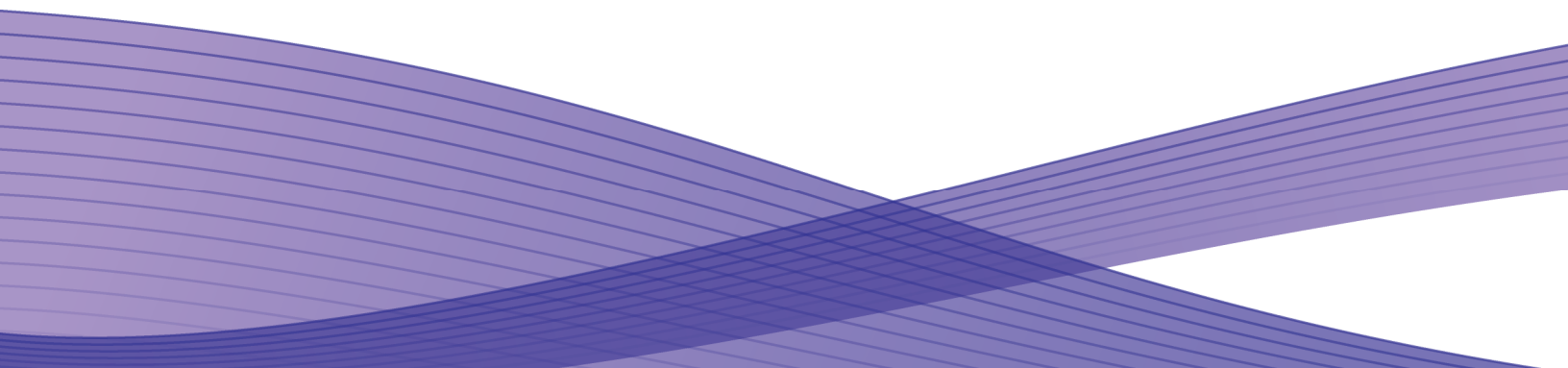
Version 1.1

Apr 29, 2011

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



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, 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[1] 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
   - Local, Remote or CAC/PIV Authentication
   - Local Authorization and Personalization
   - 802.1x Device Authentication
   - Session Inactivity Timeout

   System Administrator login is required when accessing the security features of a ColorQube™ 9201/9202/9203 machine 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 "CentreWare Internet Services" located on page 2-6 in the System Administration Guide (SAG)[2].

   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 SAG in Chapter 8, 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 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, Scan to Mailbox and Internet Fax.

   The following services of the ColorQube™ 9201/9202/9203 are to be disabled as part of the evaluated configuration - Network Accounting, Copy/Print Store and Reprint (may also called "Save for Reprint"/"Reprint Saved Jobs") and the Extensible Interface Platform (may also called "Extensible Services" or "Custom Services").

---

[1] The term "evaluated configuration" will be used throughout this document to refer to the configuration of the ColorQube™ 9201/9202/9203 Multifunction System that is currently undergoing Common Criteria evaluation.

[2] ColorQube™ 9201/9202/9203 System Administration Guide, Document Version : 1.0 (05/09)

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.

d). The System Administrator should establish or ensure that unique user accounts are established for all users of the ColorQube™ 9201/9202/9203 and that no 'Guest' users are allowed to access any services on the device. Follow the "User Information Database" instructions starting on page 8-2 in the SAG to set up local user accounts on the device.

   The System Administrator should also ensure that the 'Minimum Length' passwords for any unique user accounts established for all users of the ColorQube™ 9201/9202/9203 should be set to at least 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 "User Information Database Password Settings" instructions on page 8-3 in the SAG to set the minimum and maximum password lengths.

e). For establishing remote authentication access to network accounts follow the "Authentication Configuration" instructions located on page 7-3 of the SAG to set up an Authentication Server. Follow the "Configuring Common Access Card" instructions starting on page 14 of the Common Access Card (CAC) Guide[3] to set up user authentication via a Common Access Card.

f). For customers concerned about document files on the hard disk drive(s)[4] 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.

[3] Xerox Common Access Card Xerox ColorQube™ 9201/9202/9203, Version 1.0, 09/09, 604E53830

[4] 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 two hard disk drives.

- 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, 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 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 a ColorQube™ 9201/9202/9203 Multifunction System is decommissioned, returned, sold or disposed of.

g). 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 cyrpto policy of their clients to request either SSLv3.1 or TLSv1.0 and to disallow the use of RC4 and MD5.

h). 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.

i). 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.

j). Xerox recommends that HTTPS be enabled in the evaluated configuration. To enable HTTPS (SSL):

- At the Web UI[5], 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.

k). 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".

l). In the evaluated configuration for a ColorQube™ 9201/9202/9203, when 'Device User Interface Authentication" is set to [Remotely on the Network] the only authentication protocols options recommended to be used are [**Kerberos (Solaris)**], [**Kerberos (Windows 2000/2003)**] or [**LDAP**]. However, use of other authentication protocol options is allowable.

In the case of LDAP/LDAPS the System Administrator should ensure that SSL is enabled as discussed in Step 19 on page 7-9 in the SAG.

m). In the evaluated configuration for a ColorQube™ 9201/9202/9203, when setting up authorization only the [Locally on the Device (Internal Database)] option is recommended to be used. However, use of the [Remotely on the Network] authorization option is allowable.

n). 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 theAudit 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.

o). 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.

p). 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.

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.

q). To enable disk encryption:

- At the Web UI, 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.

[5] From here on the directions assume that the Web UI has been accessed already by following the "Access Internet Services" instructions on page 2-6 of the SAG.

r). The System Administrator 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 SAG.

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

Xerox also recommends that the default values for IPSec parameters listed in the IPSec section in the SAG be used whenever possible for secure IPSec setup. The following default values not listed in the SAG should also be used for secure IPSec setup:

- For defining policies the options listed for 'Hosts', 'Protocols' and 'Action' are all defaults; the System Administrator should choose the particular option that pertains to whether the hosts and protocols in each case are to be allowed or discarded and the corresponding desired action.
- The Host Group address type defaults to 'Specific'.
- Protocol Group Custom Protocol defaults to being disabled. If Custom Protocol is enabled then the protocol defaults to 'TCP' and the Device Is type defaults to 'Server'.
- The IPSec New Actions keying method defaults to 'Internet Key Exchange (IKE)'.
    - If 'Manual Keying' is selected the IPSec security option defaults to 'ESP', the Security Parameter Index: IN defaults to '256', the Security Parameter Index: OUT defaults to '257', the hash method defaults to 'SHA-1', the encryption method defaults to '3DES' and the keys option defaults to '**ASCII format (System will automatically convert to hex value for you)**'. Also, "AH" alone should not be selected as the IPSec Security option.
    - If 'Internet Key Exchange (IKE)' is selected the IKE Phase 1 key lifetime defaults to '86,400 seconds', the DH Group defaults to '**DH Group 2 (1024-bit MODP)', the Encrypt/Hash pair defaults to 'SHA-1 and AES', the IPSec mode defaults to 'Transport Mode', the** IPSec security option defaults to 'ESP', the IKE Phase 2 key lifetime defaults to '28,800 seconds', the IKE Phase 2 hash method defaults to 'SHA1' and the IKE Phase 2encryption method defaults to '3DES'.

t). Xerox recommends that if SNMP is enabled SNMPv3 should be used. SNMPv3 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 UI, 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**[6] group box to create an administrator account.
- Enter the desired **Username** and **Authentication Password**. The **Authentication Password** must be at least 8 alphanumeric characters (the default value is '3tamAvUMEfeR84erar6z').
- Enter the desired **Privacy Password** of at least 8 alphanumeric characters (the default value is 'TRUDU27qumAspuswe4he').
- 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.

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.

[6]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.

u). To enable the session inactivity timers (termination of an inactive session) from the Web UI:

- At the Web UI, select the **Properties** tab.
- Select the following entries from the **Properties** '**Content** menu': **Security → System Timeout**
- Enter in the appropriate text box the desired inactive session timeout interval in minutes for the Web System Timer (i.e., the session timeout for the Web UI) and for the Touch User Interface System Timer (i.e., the session timeout for the Local User Interface).
- Select the [**Apply**] button. This will save the indicated inactivity timer settings. After saving the changes the *System Timeout* page will be redisplayed.

v). To enable the session inactivity timer (termination of an inactive session) for the Local UI from 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.
- Select the [**Save**] button. This will save the indicated Local UI inactivity timer setting. After saving the changes the *Timers* screen will be redisplayed.

w). The Saved Jobs for Reprint feature should be disabled to be consistent with the evaluated configuration. To disable this feature from the Web UI:

- Select the **Properties** tab.
- Select the following entries from the **Properties** '**Content** menu': **Services → Reprint Saved Jobs → Enablement**
- Select the [Disabled] button and then select the [Delete All Jobs] button.
- Select the [**Apply**] button. This will save the indicated settings and disable the Saved Jobs for Reprint feature.

x). The SMart eSolutions feature should be disabled to be consistent with the evaluated configuration. To disable this feature from the Web UI:

- Select the **Properties** tab.
- Select the following entries from the **Properties** '**Content** menu': **General Setup → SMart eSolutions**.
- Select the [Not Enrolled] button under 'SMart eSolutions Enrollment'.
- Select the [**Apply**] button. This will disable the SMart eSolutions feature.

y). To enable the Scan to Mailbox feature from the Web UI:

- Select the **Properties** tab.
- Select the following entries from the **Properties** '**Content** menu': **Services → Scan to Mailbox → Enablement**
- Select the [Enable Scan to Mailbox] button and then select the [On Scan tab, view Mailboxes by default] button.
- Select the [**Apply**] button. This will save the indicated settings.

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.

To set the scan policies for the Scan to Mailbox feature, select the following entries from the **Properties** '**Content** menu': **Services → Scan to Mailbox → Scan Policies.** 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].

z). The Admin Password Reset security feature should be disabled to be consistent with the evaluated configuration. To disable this feature from the Web UI:

- Select the **Properties** tab.
- Select the following entries from the **Properties** '**Content** menu': **Security → Admin Password → Reset Policy** tab.
- Select the [Disable Password Reset] button.

- Select the [**Apply**] button. This will disable the Admin Password Reset feature.

aa). The Custom Services (Extensible Interface Platform or EIP) feature should be disabled to be consistent with the evaluated configuration. To disable this feature from the Web UI:

- Select the **Properties** tab.
- Select the following entries from the **Properties** '**Content** menu': **Connectivity → Protocols → HTTP → Web Services** tab.
- Make sure that the [**Enable**] checkbox associated with the Extensible Service Registration entry under Remote System Management is not selected.
- Select the [**Apply**] button. This will ensure that Custom Services are disabled on the device.

bb). Network Accounting and Auxiliary Access should both be disabled to be consistent with the evaluated configuration. To disable Network Accounting and Auxiliary Access from the Local UI:

- Select the **[Machine Status**] tab and then the [**Tools**] button. This will access the Tools Pathway.
- Select the following buttons from the **Tools Pathway**: **Accounting Settings → Accounting Mode.**
- Make sure that neither the [Network Accounting] button nor the [**Auxiliary Access**] button is selected. From a security perspective it does not matter whether the [**None**] or the [**Xerox Standard Accounting**] option is selected.
- Select the [**Save**] button. This will ensure that Network Accounting and Auxiliary Access are both disabled on the device.

cc). For evaluated configuration of Embedded Fax Xerox strongly recommends that the Secure Receive option be enabled[7] and that the Local Polling option be disabled and that embedded fax mailboxes be used whenever practical to store fax jobs.

- To enable Secure Receive from the Local UI follow the instructions on page AdminstrationandAccounting-26 of the Admin and Accounting Guide[8]. Make sure that the [**Enable**] button is selected.
- Local Polling should be disabled in the evaluated configuration. To disable Local Polling from the Local UI follow the instructions on page FAX-24 of the Fax Guide[9]. Make sure that the Local Polling option is set to the [**Off**] (which is the default setting) on the Local Polling screen.
- To set up Embedded Fax mailboxes from the Local UI follow the instructions on page AdminstrationandAccounting-28 of the Admin and Accounting Guide. Make sure that passcode selected for a newly created mailbox is not the default value of '0000'.
- 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 on page AdminstrationandAccounting-28 of the Admin and Accounting Guide and select the 'Delete on Print' option.

dd). Xerox strongly recommends that any print job submitted to the device from a client or from the WebUI be submitted as a secure print job.

ee). To maintain the certified configuration, Xerox recommends that acceptance of customer software upgrades via the network be disabled. To disable software upgrades via the network from the WebUI:

- Select the **Properties** tab.
- Select the following entries from the **Properties** '**Content** menu': **General Setup → Machine Software → Upgrades**.
- Make sure that the [**Enable**] checkbox associated with the Upgrades entry is not selected.
- Select the [**Apply**] button. This will ensure that software upgrades via the network are disabled on the device.

ff). 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. If SNMP v3 is not enabled, Xerox recommends that the System Administrator change the SNMP v1/v2c public/private community strings from their default string names to random string names.

[7] This will apply to any received fax, including faxes that are remotely polled to the device from another remote fax machine or remote device.
[8] ColorQube™ 9201/9202/9303 Advanced Guide Administration and Accounting, Version 1.0 (05/09)
[9] ColorQube™ 9201/9202/9303 Advanced Guide Fax, Version 1.0 (05/09).

3. Xerox recommends that the System Administrator set the USB Settings to 'Direct Printing via Driver' mode to allow only direct printing and prohibit submittal of software upgrade files to the device from a USB Flash Drive. To set the USB Settings to 'Direct Printing via Driver' mode via the Web UI:
   - Select the **Properties** tab.
   - Select the following entries from the **Properties** '**Content** menu': **Connectivity → Physical Connections→ USB Port**.
   - Make sure the [Direct Printing via Driver] option under 'USB Connection Mode' is selected.
   - Select the [**Apply**] button. This will ensure that submittal of software upgrades to the device from a USB Flash Drive is prohibited.
4. 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.
5. Xerox recommends that customers sign up for the RSS[10] 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 that apply to the ColorQube™ 9201/9202/9203 Multifunction System.
6. 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).
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)[11] process for addressing problems found by Xerox customers.
8. 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 evaluated configuration is maintained.
9. 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 selects whether the primary IPv4 address will be obtained statically or dynamically via DHCP from the ***IP (Internet Protocol)*** page on the Web UI[12]. 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[13]. 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.
10. 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.
11. 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 by first disabling it on the Web UI and then re-enabling it on the Web UI.
12. Xerox recommends that a unique Embedded Fax or Scan-to-Mailbox mailbox is established for each authenticated user of the ColorQube™ 9201/9202/9203.
13. Xerox recommends that Remote Polling should only be used by the System Administrator.
14. Xerox recommends that passcodes for Embedded Fax and 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.
15. Xerox recommends that the System Administrator should disable (set to 'Off') both printing of Embedded Fax confirmation reports (see page AdminstrationandAccounting-29 of the Admin and Accounting Guide[8]) and Embedded Fax cover pages (see page FAX-11 of the Fax Guide[9]).
16. Xerox recommends that users of the ColorQube™ 9201/9202/9203 undergo appropriate training on how to use the ColorQube™ 9201/9202/9203 in a secure manner before being assigned user accounts to access the ColorQube™ 9201/9202/9203.

---

[10] 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**.

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

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

[13] The primary IPv4 address will always be displayed on the Configuration Report that can be printed for a ColorQube™ 9201/9202/9203.

17. Direct USB printing is not part of the evaluated configuration for a ColorQube™ 9201/9202/9203.

18. 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.

    - **Low Supply Warning** - Allows the System Administrator to set when to receive low supply warnings for the ColorQube Ink Sticks, Cleaning Unit, and Document Feed Roll. Is accessible by selecting the following screens/buttons in order: [**Machine Status**] hard button → [**Tools**] button → [**User Interface Settings**] button → [**General**] button → [**Low Supply Warning**] 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.

      Downloaded network logs are always encrypted and require Xerox personnel to decrypt the logs before they can be read by the System Administrator or other authorized persons.

    - **USB Settings** – Allows the System Administrator to enable/disable and set the configuration of the USB Printer Port connectivity. Is accessible by selecting the following screens/buttons in order: [**Machine Status**] hard button → [**Tools**] button → [**Network Settings**] button → [**Advanced Settings**] button → [**USB Settings**] button.

    - **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.

19. 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 (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, 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.

- **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.

20. 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 on the ColorQube™ 9201/9202/9203 with System Administrator login and authentication but are not documented in either the SAG or the on-line help:

    - **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.

    - **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.

    - **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. 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.

    - **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

    - **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}**[14]**/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**.

    - **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**.

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

- **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**.
- **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**.
- **Color Copy Control Test Result -** Allows the System Administrator to view the Color Copy Control test results. Is accessible by typing **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}/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}/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**.
- **Print Behavior Settings -** Allows the System Administrator to configure/enable alternate media dimension settings for print jobs. Is accessible by typing **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}/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}/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**.
- **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}/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}/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}/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.

21. 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.

22. 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 no allow the exclusion or limitation of liability for consequential damages so the foregoing limitation may not apply.