End User Guide to Establishing and Maintaining Connectivity

End User Tips for Remote Services Offerings

Table of Contents

Introduction

There is a wide range of root causes associated with a failure to establish or preserve uninterrupted communication between equipment in a customer's site and the Xerox Communication server (Edge).

This document is intended to be an evergreen collection of "Hints & Tips" that serves as a point of reference for those driving adoption of connectivity and those attempting to resolve connectivity issues at customer sites.

Loss of Communications after Service Action

Connection Method(s) Affected

- ✓ Device Direct
- ✓ Proxy: XDA Lite (rarely)
- ✓ Proxy: CentreWare Web (rarely)

Current Situation

The customer equipment has been communicating with the Edge server, but after a service action the communication ceases.

Root Causes

If the service action includes an Alt Boot process or a software update, the device's connectivity settings are not captured by the clone file used as part of an upgrade process. The clone file may not automatically restore device settings/configuration resulting in a communication drop-off.

Also, there are occasions when FX devices (i.e. WC73XX, WC74XX, etc.) must be reset to factory default settings to resolve performance issues. When this occurs a drop-off will result as well.

Corrective Action

After every service action, it is important to validate/test that the device is still communicating with the Edge server.

1. Follow the device direct setup instructions found in the System Administration Guide provided with your equipment to perform the test to perform the test. If you cannot located the documentation it can be viewed or downloaded from the Support and Drivers page on Xerox.com.
2. If the device cannot communicate with the Edge Server, check that all of the enablement settings for that particular device are correct as documented in the System Administration Guide.

Machine Time, Date & GMT Offset Settings

Connection Method(s) Affected

- ✓ Device Direct
- ✓ Proxy: XDA Lite
- ✓ Proxy: CentreWare Web

Current Situation

When the time, date and GMT offset settings are incorrect, regardless of whether they are in the past or the future, the device may not transmit data or the data may be rejected by the service sponsor systems.

Root Causes

Occasionally the correct time, date and GMT offset settings are not entered on a device when it is installed. When this happens, the default settings, instead of the correct settings, are included in the data set the device submits to Xerox.

Corrective Action

When you observe a communication loss, or data submissions that are not being used by the service sponsor systems to administer Remote Service offerings, confirm that the time, date and GMT offset settings in the device are accurate. Adjust them if necessary.

Transmission Time Settings

Connection Method(s) Affected

- ✓ Device Direct

Current Situation

The time of day at which data is transmitted to the Xerox Communications server (Edge) is randomly set when connectivity is initially established. Xerox devices and proxy applications are designed to recognize when a scheduled data transmission has been missed due to the device being powered off. Occasionally devices fail to communicate as expected when power is re-applied.

Root Causes

If a device that behaves in this manner is routinely powered off when the transmission time is scheduled to occur, the result could be intermittent or a general lack of communication.

Corrective Action

While it is difficult to detect if a device is exhibiting this behavior, if there is communication loss without an apparent root cause, consider changing the transmission time to occur during normal business hours. This is when the device is most likely to be powered on, maximizing the likelihood of transmissions occurring as scheduled. This setting is available on the device web UI using CentreWare Internet Services.

Customer Environment Impacts

Connection Method(s) Affected

- ✓ Device Direct
- ✓ Proxy: XDA Lite
- ✓ Proxy: CentreWare Web

Current Situation

There are interdependencies between security software applications and infrastructure configurations that run in customer environments which affect the ability of our devices and proxies to reliably connect and communicate with each other as well as with the Edge Server.

When you suspect communication issues exist at a customer location, you should check for the following possible root causes and take the necessary corrective actions.

Root Causes & Corrective Actions

Proxy Applications Turned Off
Data acquisition agent applications (proxies) are installed on customer workstations that routinely get turned off, perhaps for days at a time, resulting in loss of communication. Discuss with your customer where the proxy client software has been loaded. Recommend that, when possible, proxy applications be installed on a server that is expected to remain powered on 24/7 rather than on an individual's workstation or laptop.

Security Applications Blocking Communications
Some security applications that programmatically monitor network traffic are designed/configured to detect unauthorized communications, either from within the network or from outside of it, and to proactively block them. Check with the customer's IT System Administrator to determine if they are running any network traffic monitoring applications of this type and, if so, explore alternatives that may allow uninterrupted communications

between the customer's environment and Xerox communication servers (Edge) as well as between proxy installations and devices.

Security Software Updates
Security software updates in the customer's environment can cause data acquisition agent applications (proxies) to stop operating. Check with the customer to see if a MS Security update has recently taken place and, if so, validate that the proxy is running or if it requires restarting.

Proxy Server Configuration
Some proxy server configurations do not enable the auto proxy detection/auto registration functionality contained in our devices to successfully establish connectivity with Xerox communications servers (Edge). There is a dependency on WPD option 252 to be enabled. Many times this will be the case by default, but not always. Validate with your customer that WPD option 252 is enabled in their IT infrastructure.

PC Upgrades and Replacement
When customers re-image, update or replace a workstation or server upon which XDA Lite or CentreWare Web is installed, the software application could be deleted, uninstalled or rendered inoperable. If a communication failure is suspected, validate that the software application is still installed and working properly. Engage the local System Administrator if necessary.

PC / Server Administrative Rights
If a customer is having difficulty downloading or installing XDA Lite or CentreWare Web, they may need to request System Administrator rights to complete the installation. Alternatively, a System Administrator may need to perform the installation.

Multiple Installations of XDA Lite
Xerox Communication Servers may not capture data consistently if there are multiple installations of XDA Lite in a customer's environment. Customers should be informed that:

- There should only be one instance of XDA Lite installed within their environment.
- XDA Lite should not be installed on a PC/server where other SNMP-based applications or other Xerox printer management tools are installed.

Data Recovery Model Setting in CentreWare Web

Connection Method(s) Affected

- ✓ Proxy: CentreWare Web

Current Situation

There have been reports of CentreWare Web installations that stop running, causing the site's entire equipment inventory to drop off communications.

Upon investigation it was found that the server on which CWW was running had exhausted the free memory space available for the database and transaction log files that are created by CWW. This left insufficient system resources for CWW to continue its device management functionality.

The initial reaction by customers has been to increase the total memory in the server.

Root Causes

This issue can result from the data recovery model settings within CWW being modified to something other than the default value of "Simple." Unless the Simple model is employed it is possible for the database and transaction log file sizes to grow uncontrolled and eventually exhaust the available memory.

Corrective Action

The preferred data recovery model setting in CWW is the default (Simple). If you encounter an installation of CWW on a server that has run out of available memory, validate the data recovery model setting.

Further detail on Data Recovery Models and Transaction log Management can be found at http://msdn.microsoft.com/en-us/library/ms345583.aspx

An alternative to the use of the Simple Data Recovery is the use of an email alert when the database or transaction log exceeds an acceptable size. Further detail on establishing email alerts can be found at http://www.mssqltips.com/sqlservertip/1523/how-to-setup-sql-server-alerts-and-email-operator-notifications/

PC/Server Password Expiration Settings

Connection Method(s) Affected

- ✓ Proxy: XDA Lite
- ✓ Proxy: CentreWare Web

Current Situation

If one of the proxy applications (CentreWare Web or XDA Lite) is installed on a workstation or server that requires a regular password update, communication will be lost if the password is not updated as required.

Root Causes

If the workstation / server is one that is powered on continuously and not often used for other purposes, a drop off can go undetected for an extended period of time.

Corrective Action

1. Arrange for the workstation / server in question to not require a password or to not require that the password change.
2. Enable the CWW and XDA Lite option for an email alert or a pop-up to occur when there has been a communication failure between the proxy installation and the Edge. This will serve as a reminder to reset the password when it expires.

Limited Internet Access from the Customer's Environment

Connection Method(s) Affected

- ✓ Device Direct
- ✓ Proxy: XDA Lite (rarely)
- ✓ Proxy: CentreWare Web (rarely)

Current Situation

When Xerox equipment having the device direct auto-registration capability is installed in an environment that limits internet access for network connected equipment, the device may not be able to access the internet in order to connect with Edge.

Root Causes

It is becoming more common for customers to employ security techniques that limit internet access for equipment in their environment.

Corrective Action

If this condition exists in a customer's infrastructure, you can propose some alternatives that will maintain the security of their environment.

- Suggest that the IP address of the specific pieces of Xerox equipment be added to the list of network connected devices that are allowed internet access.
- Ensure that the customer's environment is allowed to access the URL for the Edge (NEVER use its IP address). The appropriate URL for Edge is https://dcs.support.xerox.com.

Physical Relocation of Equipment

Connection Method(s) Affected

- ✓ Device Direct (rarely)
- ✓ Proxy: Smart eSolutions Client
- ✓ Proxy: CentreWare Web

Current Situation

Customers who use legacy proxy applications (CentreWare Web and Smart eSolutions client) and who routinely relocate or reassign IP addresses for their Xerox equipment experience loss of communication and / or an absence of data submissions.

Root Causes

Devices that are connected to Edge via one of the proxy applications are discovered by the proxy through the use of Simple Network Management Protocol (SNMP) and located according to their IP address.

If a device is physically relocated or otherwise assigned a new IP address for any reason, the legacy proxy applications (CentreWare Web & Smart eSolutions client) require manual intervention to re-discover the equipment in order to maintain the connection.

Corrective Action

If a customer routinely relocates or reassigns IP addresses for their Xerox equipment, XDA Lite is recommended in place of legacy proxy applications. XDA Lite rediscovers previously connected devices and discovers / registers devices that have been newly installed in a customer's environment.

Proxy Reliability

Connection Method(s) Affected

- ✓ Proxy: Smart eSolutions Client (obsolete)
- ✓ Proxy: CentreWare Web

Current Situation

Customers using CentreWare Web or the Smart eSolutions client applications are experiencing an unacceptably high rate of communication loss.

Root Causes

The design of legacy versions of the data acquisition agents / proxy applications do not enable reliability enhancements that have been identified and as such they are inherently less reliable than the most recent version – XDA Lite

Corrective Action

XDA Lite rediscovers / discovers devices daily, improving a device's overall connectivity reliability. In addition, it retrieves application updates automatically and offers an improved local user interface providing a level of user value that has been extremely well received by customers.

It is highly recommended that, when provided the opportunity to replace the current installation of a legacy proxy application with XDA Lite, it be done to take advantage of its enhanced connectivity reliability.

Communication loss goes undetected

Connection Method(s) Affected

- ✓ Device Direct
- ✓ Proxy: XDA Lite
- ✓ Proxy: CentreWare Web

Current Situation

Communication failures between devices and proxy applications, proxy applications and Xerox communication servers (Edge) and between devices and Edge can go undetected for extended periods of time. Monitors in place on the Xerox Communication servers are inefficient in identifying specific customer devices and environments that are experiencing a communication loss.

Root Cause

There are a wide range of root causes that can lead to communication failure. Server monitors cannot identify specific root causes related to equipment performance, customer environment, customer behavior or proxy application issues.

Corrective Action

CentreWare Web, XDA Lite and some recently introduced devices have the ability to detect a loss of communication and issue an email alert or fault message indicating that a failure has occurred. It is highly recommended that these features be enabled on devices and proxy application installations. Customers, partners or Xerox representatives should receive these alerts and instructions on how to engage the required level of support to re-establish communications.

Incomplete Device Discovery during XDA Installation

Connection Method(s) Affected

- ✓ Proxy: XDA Lite

Current Situation:

When installing XDA Lite at times not all of the devices within the specified address range are discovered during the Device Discovery step.

Root Cause:

Usually this occurs when installing the proxy application in a complex environment that has, for example:

- A large equipment inventory
- A large number of subnets within the range to be scanned
- Many rules to be satisfied to enable communication within the environment

Corrective Action:

Perform Steps 1 and 2. If Step 2 is unsuccessful, go to Step 3.

1. Change the XDA Lite Communications Settings to increase the values for the Timeout and/or Retry. This will allow additional time for device discovery to occur.
2. Limit the address range(s) of the subnet(s) to be scanned by the application to those that are used strictly for connected office equipment.
3. Specify the IP address(s) of the equipment to be managed.

   NOTE: This step may limit the ability of the proxy application to re-discover equipment that has been moved or assigned a new IP address. This might cause a loss of connectivity between the device and the proxy installation.