



CCX Technologies Inc.
700 - 1565 Carling Avenue
Ottawa, Ontario, Canada
K1Z 8R1

Release Notes

SystemX v1.8.2.1 Release Notes

CRN-0055.b

July 31, 2023

TABLE OF CONTENTS

Overview	2
New Features	2
Improvements	3
Bug Fixes	4
Upgrade File Info	5
Upgrade Process	6
Upgrading from CCX Technologies Upgrade Server	6
Upgrading with an Upgrade File	7

EXPORT CONTROL

An export permit is not required for the information contained in this document, as defined by the Canadian Export and Import Permits Act (R.S.C., 1985, c. E-19)

The information contained in this document is not subject to the International Traffic in Arms Regulations (ITAR). This document does not contain any Confidential, Secret, or Top Secret information or assets as defined by the Government of Canada or the North Atlantic Treaty Organization.

This document is proprietary and confidential.
It may not be disclosed in part or in whole without prior written consent from CCX Technologies Inc.

This document is revision-controlled and released. The latest version is accessible using CCX Technologies' PLM system. Copies not obtained through the PLM system may be out of date.

© 2023 CCX Technologies Inc.

This document is proprietary and confidential.
It may not be disclosed in part or in whole without prior written consent from CCX Technologies Inc.

Overview

This document outlines the updates made to the SystemX software platform for release 1.8.2 and provides upgrade instructions.

New Features

NF1: Added support for data collected from MIL-1553 data buses to the data collection system and the Avionics IDS.

NF2: Added support for reading avionics data from generic UDP packets.

NF3: Added a priority call list mode to handset groups, where the handsets are dialed in order if one handset doesn't answer in a certain amount of time.

NF4: Added a GUI ribbon history table, so that a user can view the content of message ribbons after they have been closed.

NF5: Added a GUI watchdog feature, so that a user will be informed if they have lost connectivity to the GUI, and/or if the system they are connected to has been rebooted.

NF6: A discretes tracker was added to the database service, so that a discrete can be activated based on the data in the latest rows of a data table. This feature can be used to activate an external indicator when an alert is generated.

NF7: Added local system state information to the data pushed to an external AHMS system.

NF8: Added support for filters to network bridge ports. They can be used to block or allow traffic based on ip properties on specific ports.

Improvements

IMP1: Options were added to limit the amount of data searched when performing a table search, based on timestamps and/or limit search to recent table partitions which improves the search experience when working with very large tables.

IMP2: ARINC-429 label update tools in GUI hide options for data types that aren't currently used in the label.

IMP3: Multiple database write and search performance improvements.

IMP4: Updated dashboard sparklines, improving performance and GUI clarity.

IMP5: Improved visibility for GUI dark mode to make statistic graphs easier to read.

IMP6: LXC decryption passwords have been hidden from configuration summary files.

IMP7: Added a new maintenance user type, which provides permissions required to load predefined overlay and template files on a system.

IMP8: Added a new remote user type, which provides permissions on a server required to access remotely connected routers and appliances.

IMP9: Added a "link up" status in the SBB radio monitor page to show link status in addition to the current "Active" status to have more visibility of the status of the whole system.

IMP10: Added SNMP Read Timeout indicator in GUI to have more visibility of system connectivity.

IMP11: Menu items will now dynamically update as objects are added and removed from the system.

IMP12: Added configurable registration periods to the Certus SIP Trunk.

Bug Fixes

BUG1: Resolved an issue with exporting builtin Avionics IDS algorithms where user modules were being exported which were set to read only. This was fixed so that builtin read only user modules were not exporting.

BUG2: Resolved an issue on the DataPHYs where if discretes were toggled at the exact same time the discrete state would lock-up and the unit would require a reboot to recover.

BUG3: Fixed an issue with the Falcon IDS Debug Mode, where error messages would appear in the logs when running on debug mode.

BUG4: Fixed an issue with incoming calls on Certus SIP trunks that were not completing due to the INVITE message format changes on the Certus terminal.

BUG5: Fixed issue where the PBX Handset Auto-attendant was not updated based on the availability of Handsets for incoming calls.

BUG6: Resolved an issue where a few specific WiFi channels in 5GHz mode on some router platforms would fail to come up on bootup.

BUG7: For release 1.8.2.1: resolved bug in release 1.8.2 where the value in integer pull-downs in the GUI (ie., PBX Handset Extensions) may not accurately reflect the system state.

Upgrade File Info

Name	SHA256 Checksum
systemx-dataphy_ng_rootfs-1.8.2.1-JUL31-14.46.14-2023.upgrade	9a5d85b39daaeaea75c792575152f21fdbae7ffd8194e96f9fe89e65fb334526
systemx-erouter_rootfs-1.8.2.1-JUL31-14.41.28-2023.upgrade	5ffecc86593d50b98c25bb6b21c474ec785ce42bdcb7aec49a8d650ae372e2a2
systemx-router_rootfs-1.8.2.1-JUL31-14.59.59-2023.upgrade	1d14e4508fb45837a7b3a95a3dc7d86d256da2746aae54ec27a22303ebceaacf
systemx-vm_appliance-1.8.2.1-JUL31-15.21.22-2023.upgrade	7123c80f9214fac274225b500cb922cb623d636d32a5e4630b2ed3520cebe17
systemx-vm_server-1.8.2.1-JUL31-15.10.26-2023.upgrade	df11bc5a54ad7b3cb90c2fac36950a0cdf38ffe812f7eb137cac64e2abd163d8

Upgrade Process

The system software can be upgraded from a file loaded directly from the CCX Technologies upgrade server or uploaded from a device connected to the SystemX Admin GUI.

Upgrading from CCX Technologies Upgrade Server

Internet access is required on the system for this upgrade method.

To upgrade the system software from an upgrade server:

1. Open the SystemX GUI and navigate to System -> System Upgrade
2. From Utilities, click on "Upgrade System from Server"

System Upgrade

Status

Current Version
1.6.0
Current version of the SystemX Software.

Upgrade Server Version
1.6.1
Version of SystemX Software available on the public upgrade server. Public Internet access is required to support upgrading from the Public Upgrade Server. To update this value either enable automatic upgrade checks or use the Check For Updates button in Utilities.

Upgrade Server Version is Newer
Indicates that the Version of SystemX Software on the Public Upgrade Server is newer and this system can be upgraded from it.

Upgrading
Indicates if the system is currently Upgrading.

Upgrade Status
None
Status of an Upgrade in Progress.

Valid Revert Snapshot
Indicates that there is a valid snapshot to revert to.

Last Filesystem Snapshot
2021-07-22T09:37:42.907684
Date/time that the last snapshot was taken, only valid if there is a valid snapshot.

Configuration

Maximum Revert Snapshot Age (Days)
8
The maximum revert snapshot age in days. If a snapshot is older than this it will be automatically deleted to free up space on the drive.

Enable Upgrade from USB
 Upgrade from server
Enable/disable auto-upgrades from a USB FLASH Drive

Enable Automatic Check for Upgrade

If enabled the system will automatically check with the Public Upgrade Server for Updates. The system will not automatically update from the server, but will provide an indicator to the user if a new upgrade is available.

Maximum Check For Upgrades WAN Cost
Extreme
The system will only check for upgrades from the Public Upgrade Server when the Active WAN Cost is equal to or less than this setting.

Maximum Download Upgrades WAN Cost
Low
The system will only permit the download of upgrade files from the Public Upgrade Server when the Active WAN Cost is equal to or less than this setting.

Save

Utilities

Check For Updates
Check the Public Upgrade Server for updates.

Upgrade System
Upgrade the System Software. If the upgrade is successful the system will reboot into the new version.

Upgrade System from Server
Upgrade the System Software from the Public Upgrade Server. If the upgrade is successful the system will reboot into the new version.

Revert
Revert the System Software. If the revert is successful the system will reboot into the new version.

Delete Last Snapshot
Delete the last snapshot. Deleting the last snapshot will free up space on the data drive, but you will no longer be able to revert the last upgrade.

Reboot System
Reboot the System Software. Reboot / Restart the system.

Advanced Configuration

Upgrade System from Server

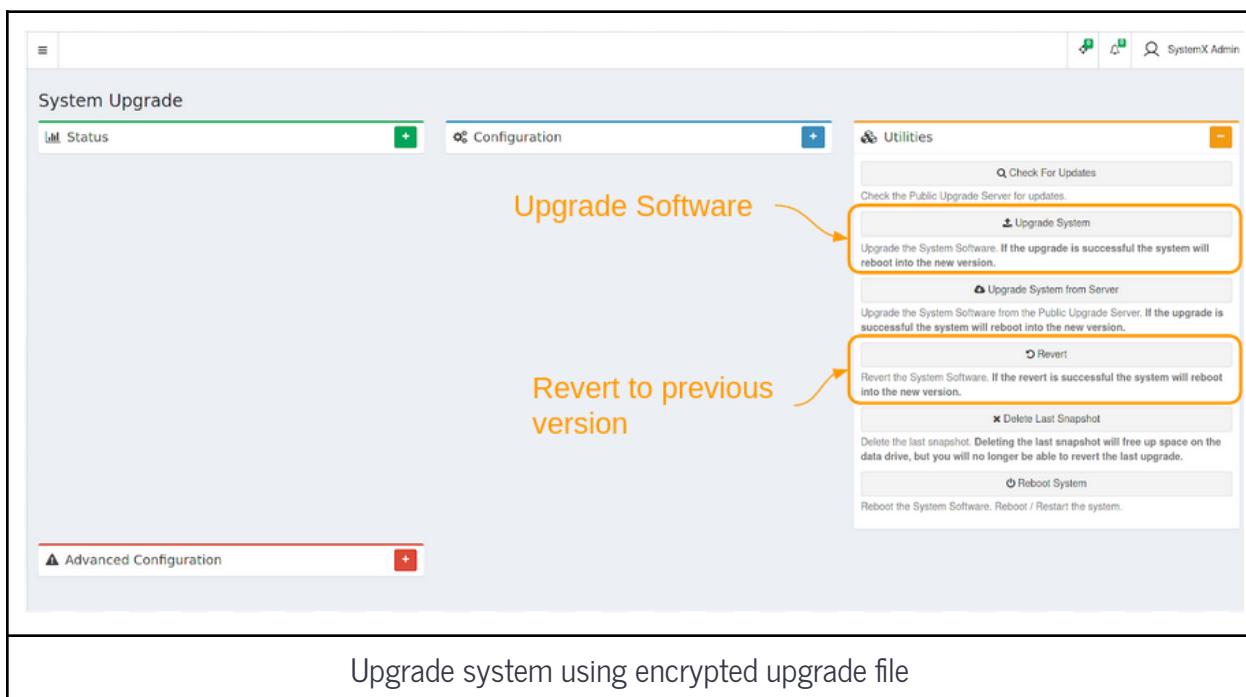
Upgrading with an Upgrade File

The system software can be upgraded from the System Upgrade page using an encrypted upgrade file provided by CCX Technologies, the latest upgrade file is available at ccx.support. System Administration information can be found in the Administrator's Guide (contact support@ccxtechnologies.com for a copy).

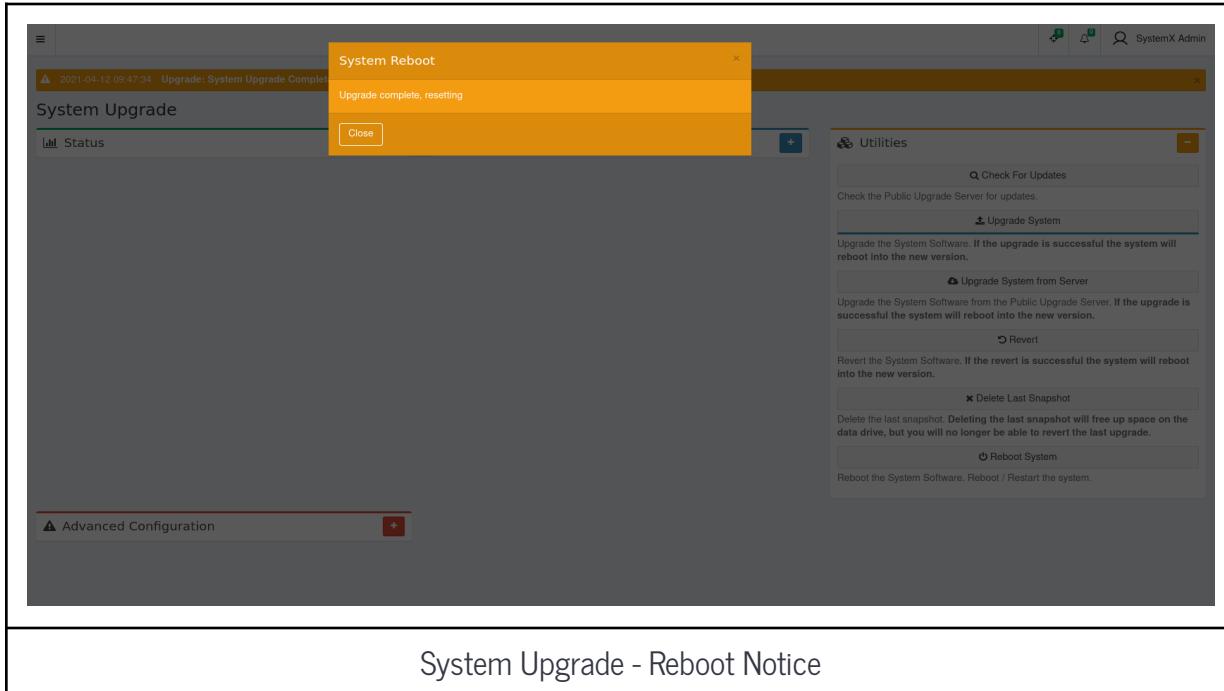
Steps to upgrade the system software from the GUI are outlined below.

1. Navigate to System -> System Upgrade
2. Under utilities click "*Upgrade System*"

The system software and configuration can be reverted to a state immediately prior to the last upgrade by using the Revert button on the System Upgrade page.



After the file is uploaded the upgrade process will start, and the system will automatically reboot.



System Reboot

Upgrade complete, resetting

Close

System Upgrade

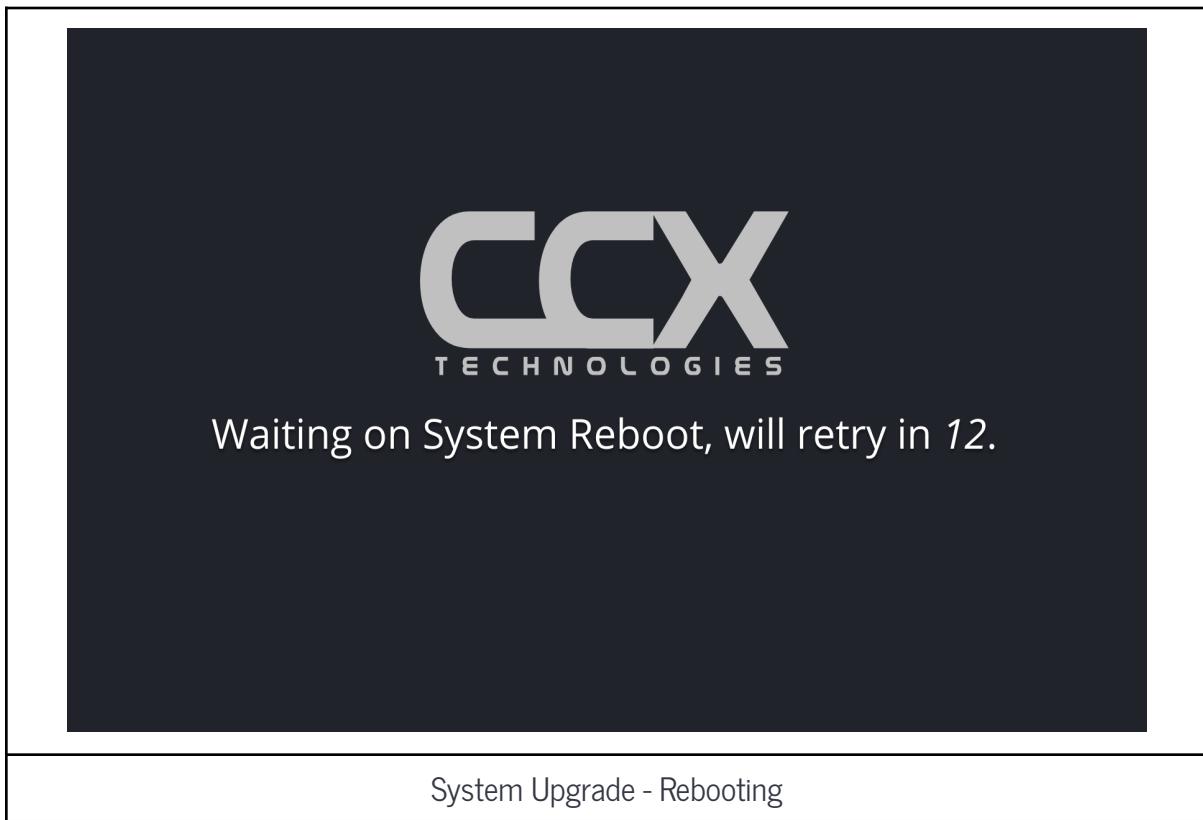
Status

Utilities

- Check For Updates
- Upgrade System
- Upgrade System from Server
- Revert
- Delete Last Snapshot
- Reboot System

Advanced Configuration

System Upgrade - Reboot Notice



CCX
TECHNOLOGIES

Waiting on System Reboot, will retry in 12.

System Upgrade - Rebooting

After rebooting the system will come up with the login page, after logging the running software version is available in the bottom right-hand corner of the page (in the footer).

