



Release Notes

SystemX v1.9.1 Release Notes

CRN-0065

July 24th, 2024

TABLE OF CONTENTS

Overview	2
New Features	2
Improvements	3
Bug Fixes	4
Upgrade File Info	5
Table 1: Upgrade File Information	5
Upgrade Process	6
Upgrading from CCX Technologies Upgrade Server	6
Fig. 1: Upgrade System From Server	6
Upgrading with an Upgrade File	7
Fig. 2: Upgrade System Using Encrypted Upgrade File	7
Fig. 3: System Upgrade Reboot Notice	8
Fig. 4: System Upgrade - Rebooting	8
Fig. 5: System Software Version	8

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 Copies not obtained through the PLM system may be out of date.

© 2024 CCX Technologies Inc.

Overview

This document outlines the updates made to the SystemX software platform for release v1.9.1 and provides upgrade instructions.

New Features

NF1: Added support for the receipt and decoding of CAN Bus data.

NF2: Added support for ARINC-615 data decoding.

NF3: Added WPA3 support for WiFi access points and clients.

NF4: Added a new Configuration Manager that can be used to track the version of installed software, firmware, and configuration files to flag out of date software. Supports SystemX software and third-party software.

NF5: Added support for the AP-561 micro WAP with Secure Voice and an application manager for securely running third-party software.

NF6: Added a Certificate Manager tool that can generate, import, validate, and proxy PKI Certificates.

Improvements

IMP1: Updated the ARINC-429 label definition schema providing additional decoding options.

IMP2: Added a number of partitions control to table searches which can be used to decrease search times on large tables with many partitions

IMP3: Added a Connection Monitor Table to the Network Monitor.

IMP4: Avionics decoded message table now includes a column for the numeric value in decimal

IMP5: Added an option to clear test alerts and test data from within an Avionics IDS rule definition page

IMP6: PCAP files can now be exported directly from the UDP and AFDX recorders

IMP7: Added a dashboard button that can be used to load individual device configuration pages for the Device Manager.

IMP8: Added configurable delay to the Luxstream radio monitor to help prevent lock-up during terminal boot.

IMP9: Multiple improvements to system memory management, reducing overall memory usage.

IMP10: Upgraded all platforms to use a common 6.1 LTS version of the Linux Kernel.

IMP11: Improved table views in dark mode, to make the axis more visible.

Bug Fixes

BUG1: Fixed issue that would prevent an interrupted download over the Remote API from timing out correctly.

BUG2: Fixed issue where a failure to send an automated email would prevent sending to other configured addresses

BUG3: Fixed issue where the Overlay differences file would have incorrect scope based on the system configuration.

BUG4: Fixed issue where Ground-to-Air calls could still reach handset group extensions when Global DND was active

BUG5: Increased the time for the “Extension Unavailable” handset message to prevent premature cut-off of the audio playback

BUG6: Fixed an issue where the signal strength of an SBB or PPPoE based WAN would be incorrectly set to 0.

BUG7: Fixed system error that could occur when adding a large number of PBX handsets based on max number of proxies.

BUG8: Fixed issue where One Time Passcode (OTP) entry during login would not reset after a failed attempt.

BUG9: Fixed issue where the “Deg/180” decoder units type would not decode a value into the correct range.

BUG10: Fixed issue where configuring a VLAN on a disabled interface would result in an error

BUG11: Fixed issue that could cause MIL-1553 receivers to stop recording data unexpectedly on the AP-553 platform

BUG12: Fixed issue where the Routing Firewall diagram would not be displayed in the GUI

BUG13: Fixed an intermittent issue that could cause an upgrade to fail (and revert to the existing version) on a VM Support Server built prior to SystemX version 1.9.0.

BUG14: Updated OpenSSH to resolve CVE-2024-6387

BUG15: Resolved issue where a DataPHY upgrade process could fail (and revert to the existing version) due to memory allocation issues.

Upgrade File Info

Table 1: Upgrade File Information

Name	SHA256 Checksum
systemx-vm_server-1.9.1-JUL18-10.20.25-2024.upgrade	e80b3cd25288dc859aadd6e7e62080f8390b6d44b2fd9e579dbc1dbb6e4d28c6
systemx-vm_support-1.9.1-JUL18-13.06.00-2024.upgrade	5a5497350793d01d7597823a75b42f5091a303c9bb8911ad5cff69c02ac55698
systemx-vm_appliance-1.9.1-JUL18-17.22.03-2024.upgrade	73dc38bcf5da66dc381cf9568e44c12cc1cb375b74ed2631c5efd7e11408a72c
systemx-router_rootfs-1.9.1-JUL17-10.33.01-2024.upgrade	b980e351f167fab070f7058542d8fb579942fb5fffc5a551883ccb e955c93e928
systemx-erouter_rootfs-1.9.1-JUL17-14.25.17-2024.upgrade	b6184f922dc975a0ac30bca617dc718f9465d87eaa47a3035d4d9 0985fbdfa6c
systemx-dataphy_ng_rootfs-1.9.1-JUL23-06.33.12-2024.upgrade	6d316c1e6b97c34c02478a093ee20e778169f8ff217eba57f4c03 3046107ae36

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”

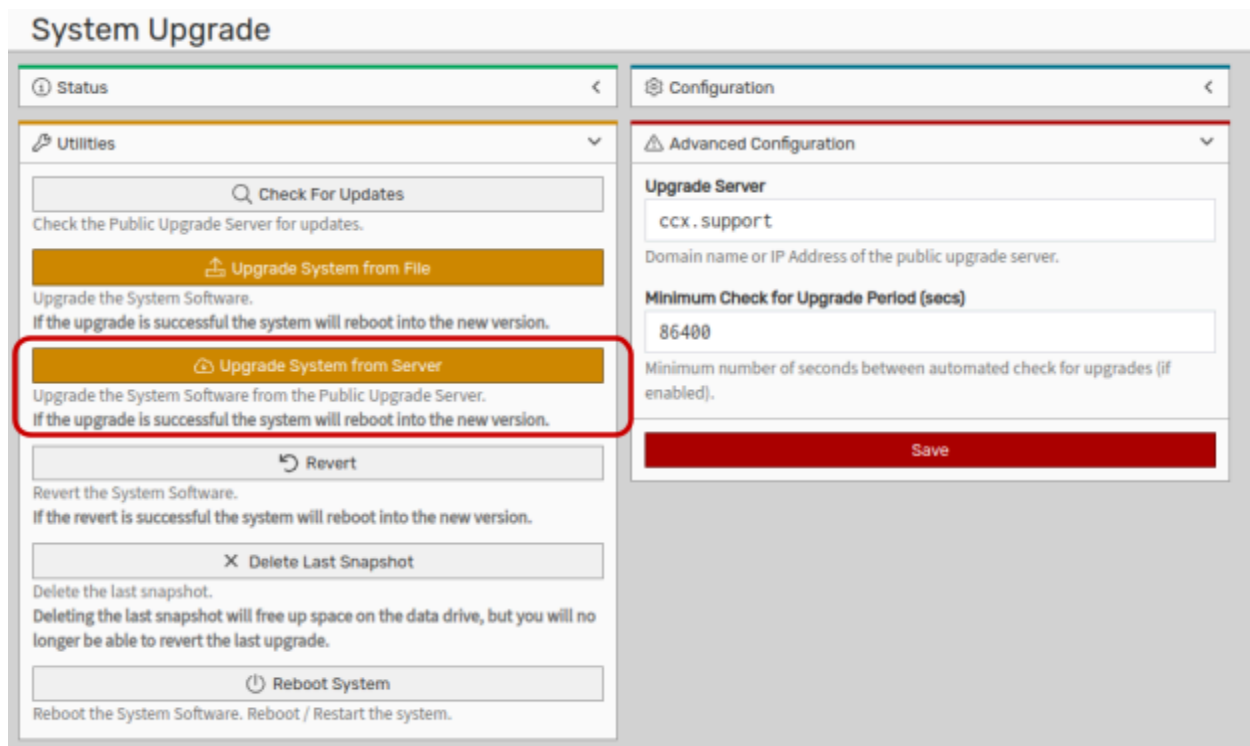


Fig. 1: Upgrade System From Server

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 from File"

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.

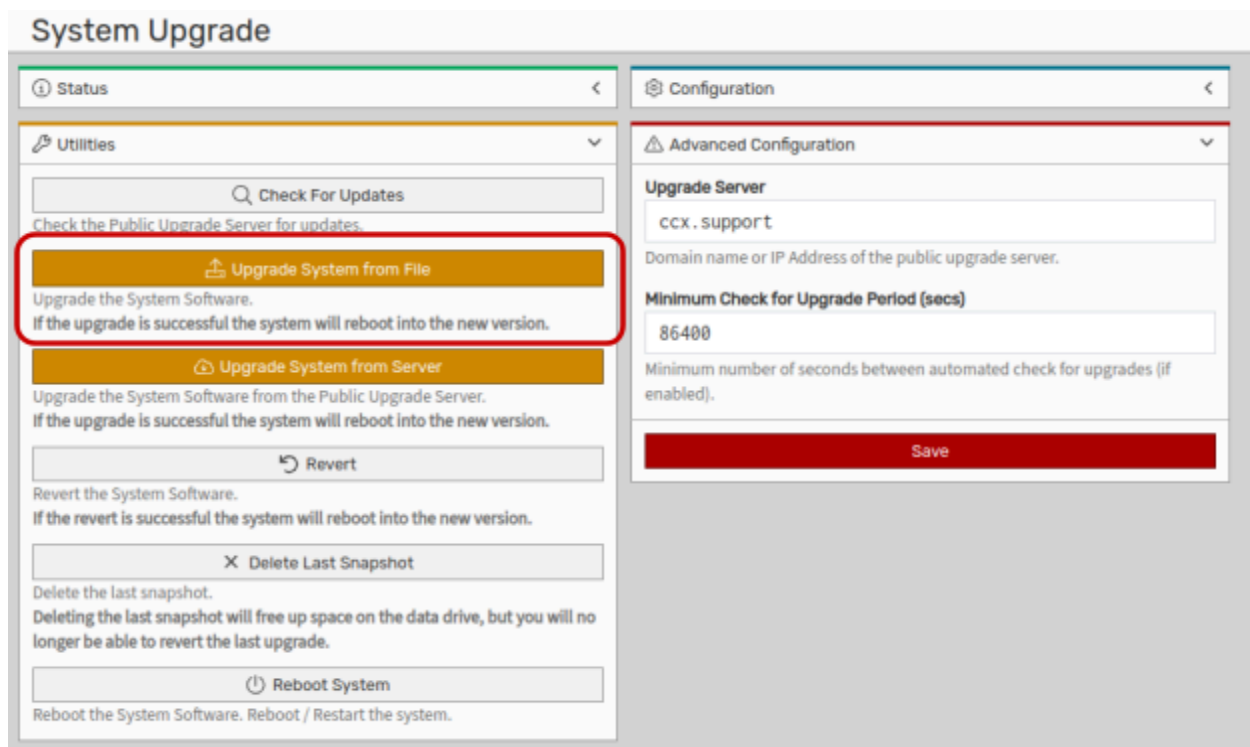


Fig. 2: Upgrade System Using Encrypted Upgrade File

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

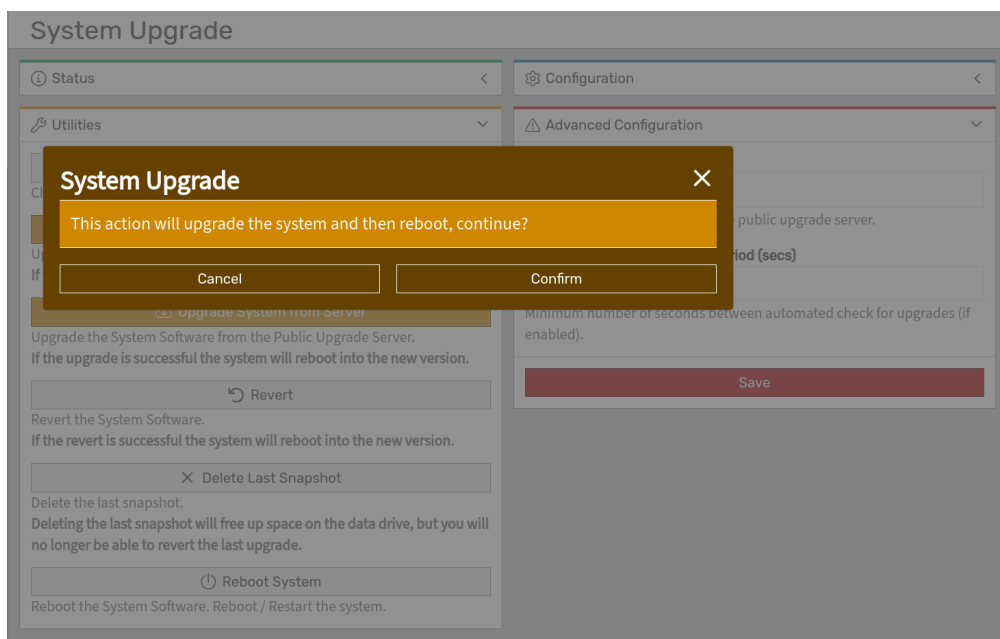


Fig. 3: System Upgrade Reboot Notice

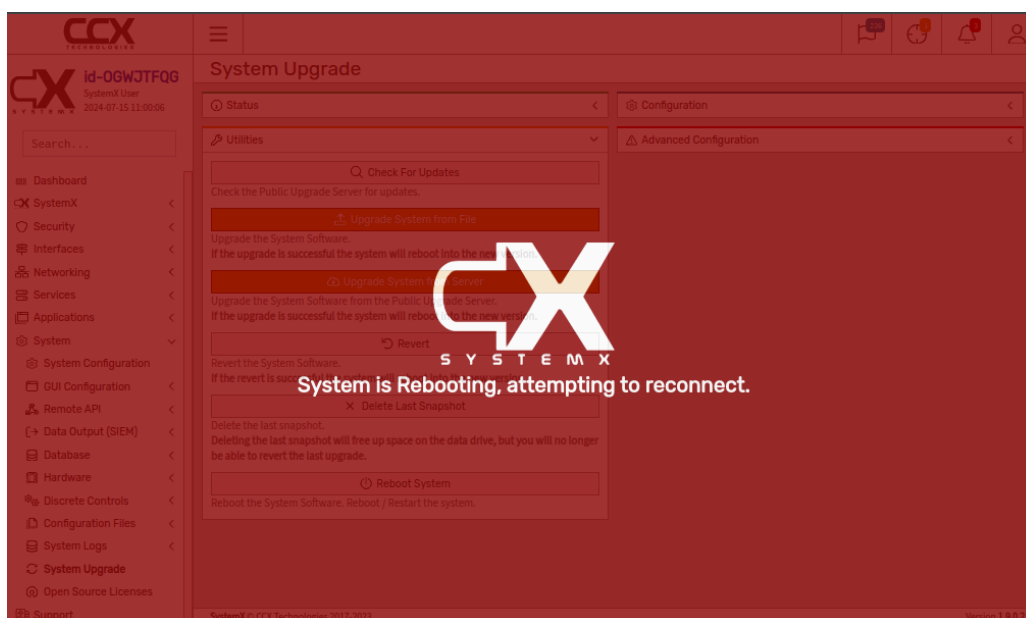


Fig. 4: System Upgrade - Rebooting

After the system has rebooted, the system will once again display the login page. Once logged-in the running software version is available in the bottom right-hand corner of the page (in the footer).

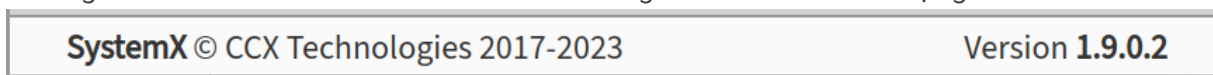


Fig. 5: System Software Version