

Secure Media Exchange (SMX)
R103.1
Software Change Notice

Revision Date: March 12, 2019
Document ID: SMX-SCN-1031A

Notices and Trademarks

© Honeywell International Inc. 2019. All Rights Reserved.

While this information is presented in good faith and believed to be accurate, Honeywell disclaims the implied warranties of merchantability and fitness for a particular purpose and makes no express warranties except as may be stated in its written agreement with and for its customer.









In no event is Honeywell liable to anyone for any indirect, special or consequential damages. The information and specifications in this document are subject to change without notice.

Other brand or product names are trademarks of their respective owners.

Honeywell International
Process Solutions
1860 West Rose Garden Lane
Phoenix, AZ, 85027, USA
+1 800-822-7673
www.honeywell.com/ps

Symbol Definitions

The following table lists those symbols used in this document to denote certain conditions.

Symbol	Definition
	ATTENTION: Identifies information that requires special consideration.
	TIP: Identifies advice or hints for the user, often in terms of performing a task.
	REFERENCE -EXTERNAL: Identifies an additional source of information outside of the bookset.
	REFERENCE - INTERNAL: Identifies an additional source of information within the bookset.
CAUTION	Indicates a situation which, if not avoided, may result in equipment or work (data) on the system being damaged or lost, or may result in the inability to properly operate the process.
	<p>CAUTION: Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury. It may also be used to alert against unsafe practices.</p> <p>CAUTION symbol on the equipment refers the user to the product manual for additional information. The symbol appears next to required information in the manual.</p>
	<p>WARNING: Indicates a potentially hazardous situation, which, if not avoided, could result in serious injury or death.</p> <p>WARNING symbol on the equipment refers the user to the product manual for additional information. The symbol appears next to required information in the manual.</p>
	WARNING, Risk of electrical shock: Potential shock hazard where HAZARDOUS LIVE voltages greater than 30 Vrms, 42.4 Vpeak, or 60 VDC may be accessible.
	ESD HAZARD: Danger of an electro-static discharge to which equipment may be sensitive. Observe precautions for handling electrostatic sensitive devices.

Contents

1	Introduction.....	5
1.1	About Secure Media Exchange (SMX).....	5
1.2	About this Document	5
1.3	Limitations	5
1.4	Technical Assistance	5
2	Contents of Release	6
3	Getting Started.....	6
4	Release Overview	6
4.1	New Features	6
5	Software/Hardware/Firmware Compatibility	7
6	Documentation Updates/Additional Information	7
7	Problems Resolved	8
8	Installation and Migration	9
9	Un-Install Instructions	9
10	Known Issues	9
11	Security-Related Issues	10

1 Introduction

1.1 About Secure Media Exchange (SMX)

Secure Media Exchange (SMX) is a system designed to enable the use of portable, removable storage media (e.g., USB thumb drives, flash drives, et. al.) while at the same time protecting critical environments against the threat of malware.

1.2 About this Document

This document provides information regarding the SMX functionality for a given release. It is provided to document specifics on functional issues, problems, warnings, etc. It should be fully read and understood prior to using any SMX software.

1.3 Document Revision History

Revision	Release	Date	Description
A	103.1	March 12, 2019	Initial document revision

1.4 Limitations

The SMX Gateway requires internet connectivity. Please see the Compatibility section below for details.

1.5 Technical Assistance

For support, contact your local Honeywell Process Solutions Customer Contact Center (CCC). To find your local CCC visit the website, <https://www.honeywellprocess.com/en-US/contact-us/customer-support-contacts/Pages/default.aspx>.

2 Contents of Release

2.1 SMX Gateway Components

Component	Version	Description
Secure Media Exchange (Core)	103.1.3.0	Optional component which will prevent the SMX Gateway from recognizing any keyboards connected to its USB ports.
<i>AtixBrokerClientInstaller</i>	<i>Removed</i>	<i>This component has been combined into Secure Media Exchange (Core).</i>

Other SMX Gateway components remain unchanged for this release.

2.2 SMX Client Driver Components

There are no changes to the SMX Client Driver for this release.

3 Getting Started

It is strongly recommended for the customer to read through the pre-requisites, requirements, etc. before they proceed with using SMX to make sure that all steps are understood and requirements are met. The documents to read are:

- SMX Read Me First
- SMX Quick Start Guide
- SMX Administrator's Guide

4 Release Overview

4.1 New Features

- Significant performance improvement using new central processing core and concurrent scanning.
- The SMX Gateway can now scan system hidden and other protected files (e.g. \$RECYCLE.BIN, System Volume Information) and folders that would previously be excluded.
- Suspected malware will now be quarantined in a folder named "SMX Quarantine" at the root of the drive rather than where it was found on the drive.

- AV signature updates can now be downloaded and applied without any disruption to the end-user while a scan is in progress.

5 Software/Hardware/Firmware Compatibility

The SMX Gateway supports the following:

- USB 2.0/3.0 Mass Storage Devices
- File systems: FAT16, FAT32, NTFS, and ExFAT
- BitLocker To Go encrypted drives secured with a password

The following client workstation operating are supported:

- Workstation systems: Windows 7, Windows 8.1, Windows 10 (32-bit and 64-bit)
- Server systems: Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2016 (64-bit)

The SMX Gateway requires unrestricted outbound internet connectivity in order to communicate with the Honeywell Advanced Threat Intelligence Exchange (ATIX) and other cloud-based services used to manage the device.

The SMX Gateway can be connected via Ethernet or Wifi. A cellular radio option for connectivity is available on some models. Customers may provide a SIM card from their own carrier, or, Honeywell can provide a SIM card for the following countries: Australia, Czech Rep, Egypt, Germany, Ghana, Greece, Hungary, India, Ireland, Italy, Malta, Netherlands, New Zealand, Portugal, Qatar, Romania, South Africa, Spain, Turkey, United Kingdom, USA/Canada/Mexico.

6 Documentation Updates/Additional Information

- N/A

7 Problems Resolved

Key	Summary
RSMX-797	"Review Logs" reports SMX system files as deleted.
RSMX-808	Logoff/Restart buttons are sometimes not responsive
RSMX-834	During Admin First Time setup: import certificate the password field does not clear in case of error
RSMX-908	Quarantining the infected file is creating the folders again in the path where the infected files are located.
RSMX-999	In some cases DAT fails to update
RSMX-1106	Checked-in drive connected to a workstation with a different certificate will un-obfuscate the drive, but some files will remain hidden.
RSMX-1140	"Unable to quarantine malware" on drives that do not allow write access to "Authenticated Users"
RSMX-1200	In some cases, the checkout times in the log appear blank
RSMX-1226	CheckInDateTime in logs is blank if no files are selected for scanning
RSMX-1352	Kiosk cannot hide or quarantine files on drives that have restrictive permissions
RSMX-1354	Checkout on replicate kiosk does not show deleted file details in log
RSMX-1686	SMX Gateway may be unable to quarantine very large files
RSMX-1753	Restart check-in does not always create a new session
RSMX-1840	CheckInDateTime is not properly synchronized if check-in gateway is offline
RMSX-1566	Double-tapping OK button during drive cataloguing could application not responding message
RSMX-1754	Review log after recheck in shows duplicate records
RSMX-888	Zero byte file with an Alternate Data Stream is always returned as clean (Note: ADS is always blocked by SMX driver)
RSMX-1582	Quarantined .zip file cannot be extracted on Windows systems with built-in extraction
RSMX-1574	As a user I want to scan System Hidden folders like \$RECYCLE.BIN
RSMX-1685	As a user I want zero-downtime AV updates so USB scanning is not impacted
RSMX-2063	.SMXInfo directory is not being set as system hidden.
RSMX-2067	Check in from 102.3 kiosk without ATIX connectivity and check out from 103.1 kiosk results in a permanently checked in device

8 Installation and Migration

Updates will typically be distributed by Honeywell via ATIX (Advanced Threat Intelligence Exchange). As a result, there is no need for migrations from one release to the next. If the user chooses to do a manual update, this release can be installed on systems currently running any previous releases of SMX. Please note that .Net Framework 4.7.1 is required on the SMX Gateway as of release 102.3.

To install the SMX Client Software, refer to the SMX Administrator's Guide. This release is compatible with all previous Client Software versions. Client software update is not necessary unless a fix has been provided that specifically addresses a client/end-node issue. See Section 7 for a list of problems resolved in this release.

9 Un-Install Instructions

The software version on the SMX Gateway is managed by Honeywell via ATIX. Do not attempt to manually uninstall any software from the SMX Gateway. For instructions on uninstalling the SMX Client Driver package, please refer to the Admin Guide.

10 Known Issues

Key	Summary	Workaround
RSMX-730	A white textbox (blank entry field) appears sometimes when USB is plugged in.	None - This is cosmetic only.
RSMX-835	"Admin Settings" passcode popup screen - passcode field does not clear consistently	None - This is cosmetic only
RSMX-923	Client logs files use local time without time zone info	Time in logs need to be manually converted to the appropriate time zone.
RSMX-926	After every reboot a new SMX event log is getting created even though it has not reached the size that the user specified.	None – there is no loss of events, just more files than expected.
RSMX-928	"Digitally signed driver is required" warning message is received after driver installation on Win7 64 bit	Ignore warning and reboot

RSMX-935	SMX Agent/Driver installed on client nodes will override McAfee Device Protection. McAfee Device Protection policies will not be in effect.	This works as intended
RSMX-1091	Issue in copying some files from the checked in drive to the end machine where there is Application Whitelisting present.	Launch a command prompt as Administrator and issue the following command: sadmin skiplist add -v E:\ (where E:\ is the drive letter assigned to the USB port)
RSMX-2527	During checkout the SMX may report the SMXReadMe.txt as a new file	Continue with check-out.
RSMX-2389	Cancelling the UAC prompt when launching SMX Driver Settings app gives the error "The operation was canceled by the user."	None – This is expected Windows behavior.
RSMX-2528	SMX Client Notification messages only appear for the user who installed the driver version 102.4.	Use driver version 102.3. Alternatively if 102.4 has already been installed contact Honeywell TAC for assistance on how to make SMX notification app available to all users.
RSMX-2241	After uninstalling SMX drivers, when connecting a drive Windows will still label the drive as "SMX Disk"	Ignore the message.
RSMX-1689	In some cases SMX driver notification app crashes on Windows 8.1	Contact Honeywell Technical Assistance Center.

11 Security-Related Issues

Key	Summary	Workaround
RSMX-706	Several compressed archive file formats are not supported for unpacking by the AV scan engine.	We cannot list all file formats that are not supported, but .7z, .wim, .xz are examples of file formats that the AV cannot unpack and extract individual files for scanning.