

Release Notes

Title: Vanderbilt Security Management System 7.0.0 Release

Date: July 2021

Superseded Version: v6.5.0

PREREQUISITES

Read and follow the instructions in this document while installing or upgrading Vanderbilt SMS Version 7.0.0. Failure to do so may result in software malfunction after installing Version 7.0.0.

Vanderbilt strongly recommends backing up the SMS database(s) before performing this upgrade. The Database Maintenance Utility (DatabaseMaintenance.exe) is accessible from the Bin folder and can be used to back up the database(s). If an error occurs during the upgrade, and no backup is available, all the data in the database(s) may be lost.

The SMS v7.0.0 upgrade is fully compatible with SMS version 6.1.0 and higher. Installations upgrading from a version lower than 6.1.0 should contact Vanderbilt Technical Support for assistance before performing the upgrade.

SMS Web compatible with SMS v7.0.0 is expected to be released 4 – 6 weeks after SMS v7.0.0 release. Existing SMS Web installations will cease to function after upgrade to SMS v7.0.0.

Free disk space on the SMS PC / Server for an upgrade should be at least four times the total size of the SMS database(s). Please contact Vanderbilt Technical Support at techsupport@vanderbiltindustries.com for assistance determining the size of the SMS SQL database(s).

NOTICE

SMS v6.3.x and above require version specific licensing. A v7.0 license is required to upgrade to v7.0.x and the cost is included with the upgrade if licensed clients, licensed Guest Pass locations, licensable video cameras and licensable 3rd party devices have not changed.

This document outlines the major bug fixes, new modules, enhancements and features that are added to SMS Software v7.0.0. SMS v7.0.0 is designated to work with VRCNX-A / VSRC-A firmware v7.54A and VRCNX-M / VSRC-M firmware v7.11M. VSRC / VRCNX-R (legacy) controllers should be updated to v6.70V. SRCNX (legacy) controllers should be upgraded to firmware v6.58L. All SMS v7.0.0 features are not supported on legacy controllers. SMS v7.0 is designed to work with Authentic Mercury protocol controllers VMRC-1, VMRC-1L, VMRC-2, & VMRC-2L with firmware v1.29.x. While it is possible to utilize the SMS v7.0.0 software with lower firmware versions not all new features will be available. It is recommended that all controllers be updated to the latest firmware version available.

VANDERBILT SMS VERSION INSTALLATION REQUIREMENTS

OPERATING SYSTEM

Vanderbilt SMS v7.0.0 software is compatible with the following operating systems:

- Microsoft Windows 8 or 8.1 (*except Home edition*)
- Microsoft Windows 10 (*except Home edition*)
- Microsoft Windows Server 2012 or 2012 R2 Essentials, Standard or Datacenter Editions
- Microsoft Windows Server 2016 Essentials, Standard or Datacenter Editions
- Microsoft Windows Server 2019 Essentials, Standard or Datacenter Editions

*Windows 7 and Windows Server 2008 and 2008 R2 are not supported
32-bit Operating Systems are not supported*

SQL SERVER

Vanderbilt SMS v7.0.0 software supports the following versions of Microsoft SQL Server:

- SQL Server 2012: Express / Standard / Enterprise SP2 or above
- SQL Server 2014: Express / Standard / Enterprise SP1 or above
- SQL Server 2016: Express / Standard / Enterprise SP1 or above
- SQL Server 2017: Express / Standard / Enterprise
- SQL Server 2019: Express / Standard / Enterprise

The SMS Install Media Includes 64-bit SQL 2014 Express SP3

UPGRADE

You may install Vanderbilt SMS v7.0.0 upgrade on any of the following SMS Versions:

- v6.1.x
- v6.2.x
- v6.3.x
- v6.4.x
- v6.5.x

WHAT'S NEW?

LICENSING

All SMS v7.0.x installations require a v7.0 Electronic License Key.

ELECTRONIC LICENSE KEY

- SMS requires an Electronic License Key
- All v6.5.x and below Electronic License Keys must be replaced
- The Electronic License is tied to a specific computer and cannot be transferred
- Easily upgradable when expanding SMS features such as concurrent client workstations in use, V-VMS cameras integrated, Guest Pass Locations, etc.
- New or upgraded v7.0.x installations will include a one-time use, unlimited SMS functionality, 5-day “Installation License”

THIRD PARTY DEVICE LICENSING

Vanderbilt SMS v6.1.0 and newer requires individual licensing for all non-Vanderbilt devices:

- The Electronic License Key contains the maximum number of 3rd party online devices which may be activated within SMS
- The Electronic License Key contains the maximum number of offline (local decision) devices which may be activated within SMS
- Device licensing is easily upgradeable

ENHANCEMENTS

AUTHENTIC MERCURY PROTOCOL CONTROLLERS

- Implement IPB Lockdown for Schlage locks connected to Authentic Mercury protocol controllers.

Schlage ENGAGE NDE and LE Series locks supporting Bluetooth credentials are NOT supported on Authentic Mercury protocol controllers at this time.

ALL APPLICATIONS

- Utilize Trusted SQL connections for all SMS Operator connections to the SMS database for Active Directory linked Operators in place of Operator SQL login connections.
- Optionally use a trusted SQL connection via the logged in Active Directory account in place of the SMSAdmin SQL login.

SMSAdmin is used in the SMS context when no Operator is logged into SMS (i.e. start-up applications) or elevated permissions are required (SQL job creation/update and archive export, System Security user creation and Report Launcher restore archive history). Active Directory linked Operator's running these applications will require elevated SQL permissions (see software manual).

- The SMSAdmin SQL login is still required on workstations where the Database Maintenance application is executed due to the elevated privileges required to create and

update SQL jobs, regardless if an Active Directory linked or traditional SQL login Operator runs the application.

SMS will continue to use some SQL login connections and the SMSAdmin account until ALL Operators, ALL SMS services and all SMS Workstation Registry Settings are configured for optional Active Directory accounts and Trusted SQL connections.

The SMSAdmin account is always required for the Database Maintenance application.

ALL SMS SERVICES

- Allow services configured with an Active Directory service account (*via the Windows Service Manager service properties Log On tab*) to use Trusted SQL connections for connections to the SMS database in place of the SMSAdmin SQL login connection.

SYSTEM SECURITY

- Provide the option to link SMS Operators to an Active Directory account. Operator passwords are not stored in the SMS database for Active Directory linked Operators.
- Elevate Operator permissions if the Security Group assigned to the Operator contains access to System Security.
- The Active Directory accounts for SMS Operators running System Security must contain permissions to read all Active Directory objects/OUs containing Active Directory Users who will become AD-Linked SMS Operators.

SMS will continue to use some SQL login connections and the SMSAdmin account until ALL Operators, ALL SMS services and all SMS Workstation Registry Settings are configured for optional Active Directory accounts and Trusted SQL connections.

The SMSAdmin account is always required for the Database Maintenance application.

SYSTEM SETTINGS

- Add new “AD Integration” tab to provide settings to control System Security Active Directory querying.
- The Active Directory accounts for SMS Operators running System Settings to configure System Security Active Directory container search filtering must contain permissions to read all Active Directory objects/OUs containing Active Directory Users who will become AD-Linked SMS Operators.

REGISTRY EDITOR

- Provide the option to specify that an Active Directory service account should be used for Database Connections for all SMS services on the workstation. The account used must have full permissions to SMS Data Folder and SMS database.

- Provide the option to specify that the logged in Active Directory account is used to connect to the SMS SQL Server via a trusted connection in place of the SMSAdmin SQL login.

SMSAdmin is used in the SMS context when no Operator is logged into SMS (i.e. start-up applications) or elevated permissions are required (SQL job creation/update and archive export, System Security user creation and Report Launcher restore archive history). User's running these applications will require elevated SQL permissions (see software manual).

LAUNCHER

- Active Directory linked Operators are authenticated via Active Directory using the Operator's entered Active Directory password without Single Sign-on (SSO) enabled. If SSO is enabled for an Active Directory linked Operator, the currently logged in Active Directory user account is validated against Active Directory and the SMS Operator table.

CALENDAR MANAGED INTERVALS SERVICE

- Implement optional diagnostic logging.

FIXES

The following issues have been resolved in this version:

ALARM MONITOR

- Alarm comments attributed to an incorrect Operator under some circumstances.

BADGE CREATE

- Error selecting Cardholder field adding annotation in certain circumstances.

REPORT LAUNCHER SERVICE

- Errors incorrectly logged to Windows Event Logs.

VANDERBILT PRIVACY POLICY

SMS does not transmit any data back to Vanderbilt. Any personal data collected within SMS is managed and used exclusively by the end-user of SMS entirely on customer owned equipment. Vanderbilt does not collect, manage or sell personal data. Please visit the Vanderbilt website at <https://usa.vanderbiltindustries.com/legal> for more information on our privacy policy.