micros

# Simphony v2 Antivirus Recommendations

Document Date: April 8, 2014

# DECLARATIONS

## WARRANTIES

Although the best efforts are made to ensure that the information in this document is complete and correct, MICROS Systems, Inc. makes no warranty of any kind with regard to this material, including but not limited to the implied warranties of marketability and fitness for a particular purpose.

*Information in this document is subject to change without notice.*

MICROS Systems, Inc. shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this document.

## COPYRIGHT



## DOCUMENT INFORMATION

### GENERAL INFORMATION

Document Name: Simphony Antivirus Recommendations.doc
Last Edited: 03/06/2014
Document Revision: 1.1
Simphony Product Version: 2x
Prepared By: Gabe Shulman

### AUDIENCE

This document is intended to be read by members of the following groups:

- Product Development
- Product Management
- Account Management
- Sales
- Marketing

## USAGE

The information contained in this document is provided to give guidance on how to deploy and configure antivirus software for use with MICROS Simphony.

## SOFTWARE VERSION NOTICE

The information contained within this document is based on the Simphony v2 product version.

# CONTENTS

# VERSION CONTROL

| Version | Date | Editor | Changes |
|---|---|---|---|
| 1.0 | 3/10/2014 | G Shulman | Original |
| 1.1 | 4/3/2014 | N Low | Content edits and formatting changes |

# ABBREVIATIONS

| Abbreviation | Explanation |
|---|---|
| AV | Antivirus |
| PCI DSS | Payment Card Industry Data Security Standard |
| POS | Point-of-Sale |
| R&D | Research & Development |

# OVERVIEW

MICROS Systems, Inc. strongly recommends that Antivirus (AV) software be installed and maintained on all devices which are deployed in the payment network used by MICROS Simphony v2 (referred to as the Cardholder Data Environment or CDE) and have commercially available AV solutions. The following Point-of-Sale (POS) devices are commonly found on the CDE on which AV software should be installed and maintained:

- Application and Database servers
- Point-of-Sale Clients
- Shared Services Clients

In addition to the devices which are managed and controlled by the POS application, any other device that is deployed within the CDE or connects to the CDE should also have AV software installed on it, such as:

- Back Office PCs
- Manager's Laptops
- Third Party Integration Servers

The following list contains operating systems that are known to have commercially available AV solutions:

- Microsoft Windows XP
- Microsoft Windows 7
- Microsoft Windows POS Ready 7
- Microsoft Windows POS Ready 2009
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012

MICROS does not endorse or recommend any particular AV solutions or software packages. The MICROS Simphony Engineering and Quality Assurance teams develop and test the Simphony software on computers that have antivirus software installed on them. The machines are typically configured to use either the Symantec End Point Security or Microsoft Security Essentials packages.

From the Simphony application perspective, MICROS clients may use any AV solution that is compatible with the hardware and operating system on which it is installed. In the unlikely event a compatibility issue is discovered between Simphony and the AV software, MICROS will endeavor to assist the client with resolving the problem through the normal support channels.

## PCIDSS

The Payment Card Industry – Data Security Standard (PCIDSS) establishes requirements and regulations for the use of antivirus software within the CDE. MICROS clients are strongly encouraged to work with a Payment Card Industry Security Standards Council (PCISSC) certified Qualified Security Assessor (QSA) to ensure that their AV implementation and infrastructure as a whole complies with the applicable terms of the PCIDSS. Information regarding the PCIDSS can be found on the PCISSC Web site at this link:

https://www.pcisecuritystandards.org/security_standards/

## COMPENSATING CONTROLS

Compensating Controls are solutions design to meet the criteria established by the PCIDSS specification when that specification is not able to be implemented for a legitimate technical reason. According to PCI DSS (Appendix B, pg. 109) Compensating Controls must satisfy the following criteria:

- "Meet the intent and rigor of the original PCI DSS requirement.
- Provide a similar level of defense as the original PCI DSS requirement, such that the compensating control sufficiently offsets the risk that the original PCI DSS requirement was designed to defend against.
- Be "above and beyond" other PCI DSS requirements. (Simply being in compliance with other PCI DSS requirements is not a compensating control.) "

When discussing a Compensation Control for antivirus software, MICROS clients must consult with their QSA to identify a viable option that safeguards their system as well as an antivirus software would. If that is the case, the above recommendations need not be adhered to.

## SIMPHONY DEVICE USAGE

To mitigate virus or malware infections, MICROS strongly recommends that its users not use any of the Simphony POS devices or any other devices deployed on the CDE for any purpose other than its primary purpose. By avoiding Web surfing, social networks, downloading non-essential files or programs, personal email, streaming files and other recreational activities, the probability of a virus or malware infection can be greatly reduced.

## ANTIMALWARE

In addition to antivirus software solutions, there are antimalware solutions that are commercially available that could be used to provide additional protection for the CDE.

Malware, by definition, is intrusive and malicious software that attempts to gain access to computers via email, viruses, Trojan horses and other means of conveyance. Most antivirus software has one form of antimalware or another and it is something that customers must be cognizant of when selecting an antivirus tool.

In most cases where the devices are dedicated for use only as part of the POS system and do not allow activities such as Web surfing or checking email, the additional protection provided by antimalware solutions is not necessary.

# RECOMMENDATIONS

## GENERAL ANTIVIRUS CONFIGURATION RECOMMENDATIONS

AV software should be configured to regularly perform the following activities:

- Check for definition updates
  - These are generally provided either by a corporate definition management server or from the AV software vendor itself
- Check for software updates
  - Vendors will update their antivirus software and will typically deploy these updates through the same mechanism that distributes definition updates
- Exclude specific files, file types, or directories from real time scanning
  - This feature is used to ensure that the AV software does not cause system performance degradation
- Perform scheduled full system scans
  - This feature ensures that infrequently checked or files excluded from the real time scan do not get infected

## SERVER RECOMMENDATIONS

This section discusses specific configuration requirements for any AV solution that is used with Simphony. These recommendations are provided to mitigate the possibility of the AV software adversely affecting system performance.

MICROS clients should review these recommendations with their QSA to ensure that the deployment still meets the PCIDSS requirements.

There are two server deployments which are commonly used that are discussed in this document:

- Single Server
  - Contains both the database and application components
- Split Servers
  - Typically consists of the database components on a dedicated server and the application server components on one or more servers.

For single server deployments, the recommendation for both the database and application apply to the server. When using split servers, use the recommendation for the specific role that the server will be used for.

### ENTERPRISE DATABASE RECOMMENDATIONS

MICROS Simphony is supported on both Microsoft SQL Server® and Oracle® database platforms. Each vendor maintains recommendations for configuring AV software in a manner that is least likely to cause performance

issues with the database. MICROS recommends that users review the guidance provided by these vendors and follow it as best as possible.

In both cases, the vendors recommend disabling the real time scanner component of the database data and log files to ensure that scanning activities do not slow data access time. The real time scanning feature should continue to be used for the application and operating system files and directories.

Daily scans of the hard drives should be configured to occur when the system is at its lowest volume of activity.

### MICROSOFT SQL SERVER

The page located at the following URL is Microsoft's support article where this topic is covered in depth. The recommendations contained in this article should be followed when configuring AV software on a server that is running SQL Server.

http://support.microsoft.com/kb/309422

### ORACLE

Oracle's documentation for the configuration of antivirus on a Windows Server Running an Oracle Database is contained in support document (782354.1). This document may be accessed through Oracle support. The following information was taken from the article, which is dated 01-MAR-2013.

> When an AV performs a scan on a file it holds a lock on it. This lock interrupts the normal functioning of the database. To prevent any disaster situation such as database crash/hang, we recommend the following files to be excluded from online anti-virus scanning.
>
> - Oracle datafiles
> - Control files
> - Redo-log files
> - Archived redo-log files if database is in archive log mode
> - Files with extension '.ora'
> - Password file
> - Files with extension ' .log' under ORACLE_HOME
>
> You can also contact your anti-virus vendor to know more on the details of the scanning mechanism of the particular anti-virus software and for any additional Oracle files that has to be excluded from the scanner

There are numerous Oracle partner, antivirus software, and database (DB) support sites that reference this article and present the same guidance.

## ENTERPRISE APPLICATION RECOMMENDATIONS

Neither the Simphony POS nor Simphony Reporting application components have any recommended file exclusions which should be configured.

## CLIENT RECOMMENDATIONS

The Simphony client software is supported on a wide range of operating systems, many of which should have antivirus software installed on them. The following operating systems are supported by the Simphony client and are known to have AV software packages commercially available:

- Microsoft Windows XP
- Microsoft Windows 7
- Microsoft Windows POS Ready 7
- Microsoft Windows POS Ready 2009
- Microsoft Windows Server 2008 R2

**NOTE:** The list above is not necessarily an all-inclusive list of every operating system that could require antivirus software. Remember to check with a PCISSC QSA if there are any questions about whether or not a specific operating system or variant requires antivirus software. To obtain a list of PCISSC certified QSAs, please visit the PCISSC Web site at the link below:
https://www.pcisecuritystandards.org/approved_companies_providers/qsa_companies.php

There are no special recommendations for file exclusions on the Simphony clients.