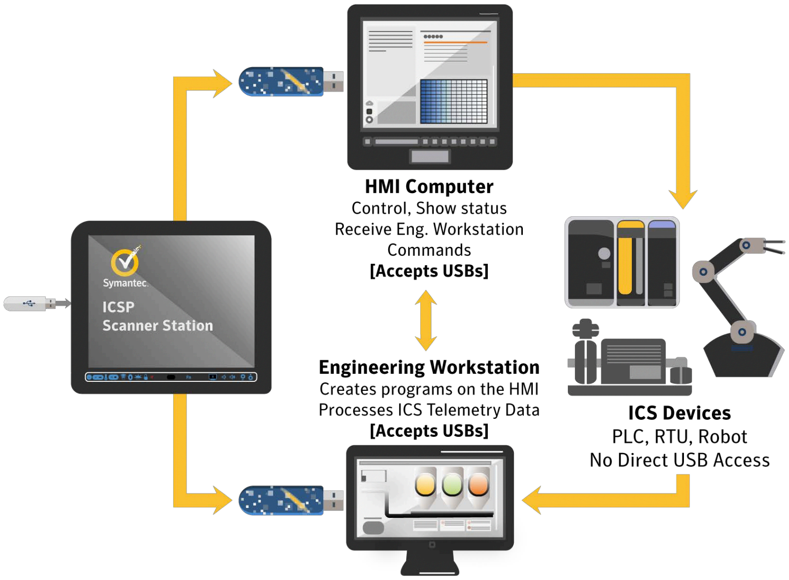
ICSP Enforcement Driver Guide

For use by partners and customers to evaluate and qualify interoperability with a target system

Overview

Symantec ICSP, or Industrial Control System Protection, is a versatile scanning station appliance that utilizes the most powerful Symantec technologies to scan and clean inserted USB storage devices. The implementation includes protections such as machine learning, emulation, file reputation, and signatures.



To validate that a USB was indeed scanned, a small file is placed onto the USB. This is a cryptographically signed watermark designed to assist the enforcement driver in deciding whether or not to mount a USB.

Driver Specification

The ICSP driver can be installed on a variety of operating systems to prevent unscanned USBs from being used.

It is an **MSI** installer package for 32/64-bit OS platforms in the size range of 2Mb, which should be installed on all Windows-based critical systems. It can also be installed on stand-alone systems, and deployed in enterprises through standard deployment (group policy) processes as well.

The following registry entries are added:

a) HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\ndevsec
b) HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\nspsvc
c) HKEY_LOCAL_MACHINE\Software\Symantec\ICS Protection (*)
d) HKEY_LOCAL_MACHINE\Software\Symantec\ICS Protection\nsptray (*)

Supported Operating Systems:

- Windows XP SP2 (x86 only)
- Windows Vista
- Windows 7
- Windows 8 and 8.1
- Windows Server 2003 SP1 (x86 only)
- Windows 10

- ○ Windows Server 2008
- ○ Windows Server 2008R2
- ○ Windows Server 2012R2
- ○ Windows Server 2016 (Will be included with ICSP 5.4)

Qualification Process

All use-cases below assume that user has both station and driver in possession and basic knowledge of scanner functionality.

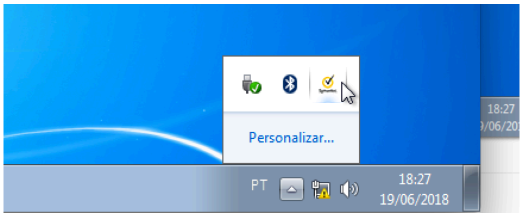
1. Installation of Driver
Purpose: Verify that a normal installation of the driver functions
Requirements: Driver MSI created from scanner station

1. Start installer
2. Run through steps with default installation path
3. Finish

Expected: Installed ICSP driver

2. Verify Driver is Running
Purpose: Verify that ICSP driver is running
Requirements: Driver MSI installed

1. Open taskbar and see ICSP driver icon
2. Run services.msc



Expected: ICSP driver icon is shown. “Symantec ICS Protection service” should be running.

3. Block non-validated USB device
Purpose: Verify that USBs that have not been scanned are blocked by driver
Requirements: Driver MSI installed

1. Insert non-scanned USB

Expected: USB device blocked

4. Allow validated USB device
Purpose: Verify that USBs that have been scanned are allowed by driver
Requirements: Driver MSI installed

1. Insert scanned and validated USB

Expected: USB device allowed and mounted

5. Block infected USB device

Purpose: Verify that infected USBs are blocked by driver
Requirements: Driver MSI installed

1. Insert USB with infection into ICSP
2. Insert scanned USB with infection into target system with driver running

Expected: USB device blocked

6. Block unscanned files and folders

Purpose: Verify that USBs with unscanned files or folders are blocked by driver
Requirements: Driver MSI installed

1. Insert scanned USB
2. Add file and/or folder
3. Remove USB
4. Insert USB

Expected: Files added in step (2) will be inaccessible

7. Uninstallation of Driver

Purpose: Verify that a normal uninstallation of the driver functions
Requirements: Driver MSI installed

1. Start installer
2. Run through steps to uninstall
3. Finish

Expected: Driver will no longer be installed