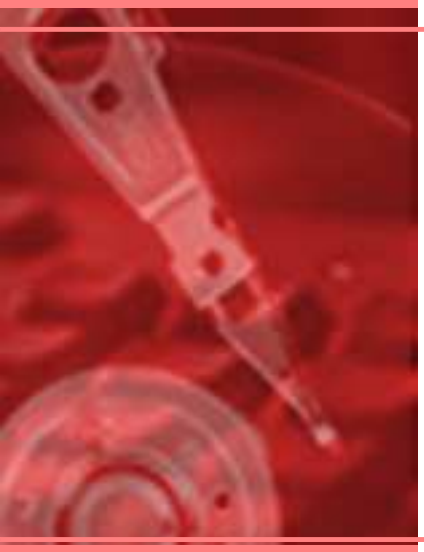


SNARE

System iNtrusion Analysis & Reporting Environment

Snare for Windows
Creating a custom MSI

INTERSECT ALLIANCE

Documentation History

Version No.	Date	Edits	By whom
1.0	26 June 2008	Initial release	David Mohr
1.1	14 July 2008	Windows XP update	David Mohr
1.2	22 Dec 2008	64 bit and Vista support	David Mohr
1.3	21/09/10	Vista, 2008 and Windows 7 Support	George Cora

About this guide

This guide provides you with step-by-step instructions on how to create a Windows MSI file for Snare, which will allow you to remotely deploy Snare for Windows, with a customized configuration, using the Microsoft Installer (MSI).

Other guides that may be useful to read include:

- Guide to Snare for Windows.
- Snare Server User's Guide.
- Snare Server Installation Guide.
- Snare Server Troubleshooting Guide.
- The Snare Toolset - A White Paper.

Table of contents:

1. Introduction

The Microsoft Installer utility (MSI) is an application that allows MSI compliant applications to be remotely deployed to workstations and servers that run the MSI service, without significant administrator intervention.

Snare does not come packaged as a MSI file by default, as the standard 'setup' executable offers significantly more flexibility at this stage. However, organizations that wish to remotely deploy pre-configured Snare agents to workstations and servers, without physically moving from system to system, appreciate the functionality provided by MSI.

This document provides administrators with step-by-step instructions on how to create a MSI file, based on the required organizational security settings, using the freely available Windows Installer XML (WiX) toolset

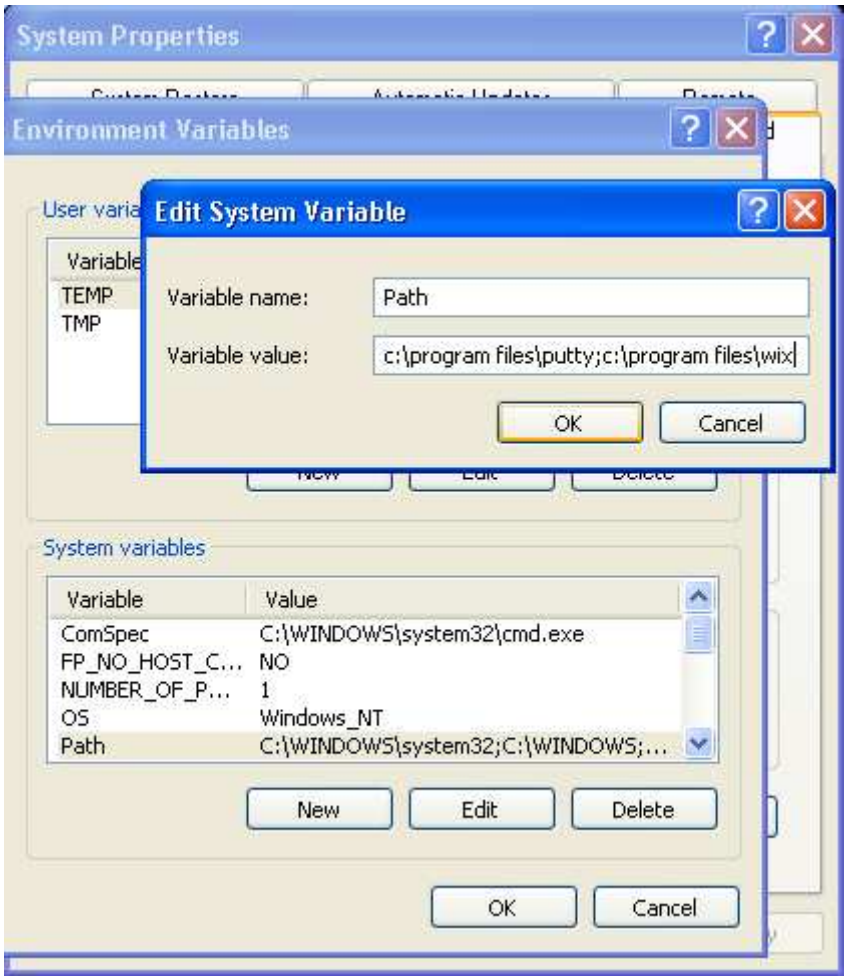
2. Initial Requirements

Please ensure you have the following available:

- The latest Snare for Windows setup package, available from http://www.intersectalliance.com/projects/SnareWindows/index.html
- The Snare for Windows MSI pack, available from http://www.intersectalliance.com/projects/SnareWindows/Download/SnareMSI-1.3.zip
- A Windows 2000 (or later) system.
- Administrator-level access to the system.
- At least 8 Megabytes of disk space on your system.
- The Windows Installer XML (WiX) version 2.0 core toolset (binaries), available from (ensure it is Version 2.0, and NOT any other version) http://http://wix.codeplex.com/releases/view/44405

How to... Installation instructions follow:

1. As Administrator, unzip the **wix2-binaries.zip** file to C:\Program Files\wix.
2. Open the Control Panel, then double click on 'System'.
3. Under the 'Advanced' tab, click the 'Environment Variables' button.
4. Under 'System variables', modify the 'Path' variable and add 'C:\Program Files\wix' (remember to use a semicolon as the separator).



5. Click 'OK' until you are back to the Control Panel. On some later versions of Windows, you may have to log out and log back in again for the PATH environment variables to take effect.
6. Check that the above procedures have worked by typing “candle” on the Command Prompt. If there are any errors, then either the software has not been installed or the environment variables have not been set. If an error dialog which states “...application failed to initialize properly...” appears, then this indicates that the .NET framework has not been installed. This will need to be installed for wix to work.

3. Creating the MSI package

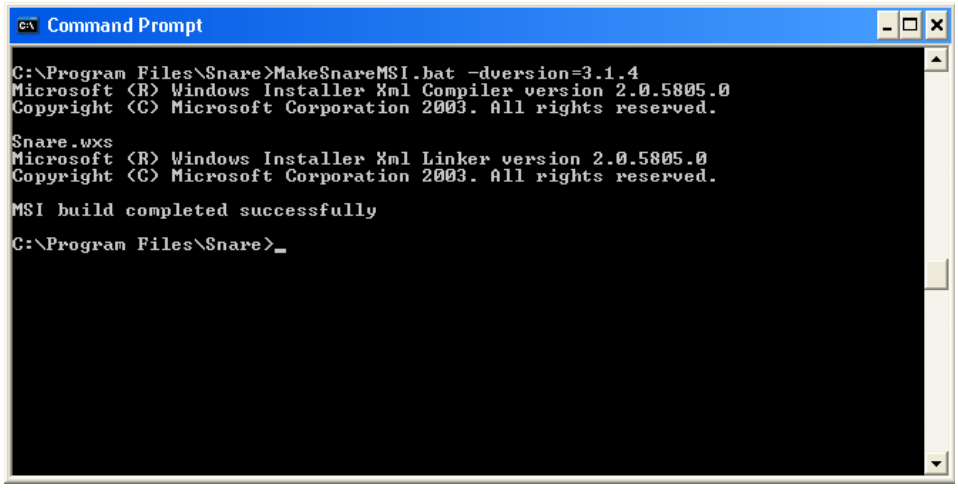
How to... Build instructions follow:

1. Download, install and configure the latest Snare for Windows agent according to the 'Guide to Snare for Windows'.
2. Unzip **SnareMSI-1.2.zip** into C:\Program Files\Snare\.
3. If you are building an MSI package that is destined for systems with the same version of Windows, and the same architecture as the system on which you are building the package, you can skip step 4, and proceed directly to step 5.
4. If you are building an MSI package for a version of Windows, or architecture, that is different than the system on which you are building the MSI (eg: If you are building a MSI package for 64 bit Vista machines, on a 32 bit Windows XP system), then you will need to copy the 'SnareCore.exe' executable that is appropriate for the target architecture/version, into the local C:\Program Files\Snare\ directory. The simplest way to do this, is install the appropriate Snare agent, on a system with the same version/architecture as your targets, then copy the SnareCore.exe binary from that system, to the C:\Program Files\Snare\ directory on the MSI build system.
5. Decide on the appropriate command line arguments.
   `MakeSnareMSI.bat -dversion=<version> [-dwin64] [-dvista]`

   If your target systems are 64 bit, include the `-dwin64` flag. If your target systems are Vista, Windows 2008 or Windows 7, include the `-dvista` flag. The `-dversion=<version>` flag (eg: `-dversion=3.1.3`) is compulsory and allows you to specify the version number that should be associated with the MSI build, and will be displayed in Add/Remove Programs.
6. Open a command prompt (ensure it is “Run As Administrator” on later versions of Windows) and run your selected command, eg:

   a. `cd "\Program Files\Snare"`

   b. `MakeSnareMSI.bat -dversion=<version>`



7. Check for any errors in the build process. Also carefully check the Snare.REG file for any errors.

   If you need to change the registry file:

   a. Manually update the Snare.REG file

   b. Edit MakeSnareMSI.bat and remove lines 2 and 3.

   c. Rerun the batch file.

8. The customized MSI is now available at C:\Program Files\Snare\Snare.msi. Please test the MSI before use in production networks. For systems running User Account Control (UAC), you will need to test the MSI from within a "Run as Administrator" Command Prompt. To install the MSI from the command line, use the following command:
   ```
   msiexec /i snare.msi
   ```

9. To ensure the agent is working correctly, check the "Latest Events" window in the Remote Control Interface. If no events appear in this window in a timely manner, double check the agent configuration or run the agent in Debug Mode ('net stop snare', '"c:\program files\snare\snarecore.exe" -d9') to check for any problem reports.

4. About Intersect Alliance

Intersect Alliance is a team of leading information technology security specialists in both the "technical" and "policy" areas. In particular, Intersect Alliance are noted leaders in key aspects of IT Security, including host intrusion detection. Our solutions have and continue to be used in the most sensitive areas of Government and business sectors. Intersect Alliance consult and contract to number of agencies in Australia and in Asia Pacific, for both the business and Government sectors.

The Intersect Alliance business strategy includes demonstrating our commitment and expertise in IT security by releasing Open Source products such as Snare. Intersect Alliance intend to continue releasing tools that enable users, administrators and clients worldwide to achieve a greater level of productivity and effectiveness in the area of IT Security, by simplifying, abstracting and/or solving complex security problems.

Visit the Intersect Alliance website for more information at www.intersectalliance.com.