persystent SUITE

Persystent Suite 6.0

PERSYSTENT DRIVE SANITIZATION

Background

Valuable data is often stored on the hard drives of servers, desktops, and laptop computers. The potential consequences of loss of control of that data can be significant; from embarrassment to enabling identity theft to, in rare cases, even loss of life. For this reason, it is often desirable to take precautions when repurposing or disposing of computers. This document describes a feature in Persystent that aids in efforts to ensure data is not accidentally disclosed.

Drive Sanitization Overview

The process of eradicating data on a disk drive is referred to as "sanitization." Over the years, various government agencies have taken an interest in the appropriate measures to help ensure sanitization of hard drives according to the potential threat presented by the unintended disclosure of data. For commercial purposes, the generally accepted authority is the National Institute of Standards and Technology (NIST) and the current reference document is 800-88 Revision 1 (hereafter, simply referred to as 800-88).

There is much misunderstanding about disk drive sanitization. Among the commonly held but mistaken beliefs is that 800-88 is a Standard - it is not. 800-88 is a "Special Publication" entitled "Guidelines for Media Sanitization" that contains recommendations. The sanitization of disk drives requires making numerous situationally dependent tradeoffs and therefore there is simply no universal process. There are many other commonly misheld beliefs like data can be recovered from drives that have been overwritten or that for overwriting data to be an effective countermeasure it must be performed multiple times or with alternating patterns. The best and most recent research has demonstrated that these formerly held beliefs are simply untrue and this is why, in part, 800-88 was recently revised.

As to the specifics of sanitization, 800-88 identifies three types of sanitization: 1) Clear, 2) Purge, and 3) Destroy. Although there are exceptions (one of the reasons again that 800-88 is a Guideline), generally, Purge affords a lower probability of disclosure than Clear and Destroy a lower probability than Purge.

It is vitally important however to understand that the details of the method chosen are even more important than the method itself. For example, Destroying a drive by firing a small arms projectile through it (shooting it), while rendering the drive itself inoperable actually leaves most of the media still readable because the only portions of the magnetic media rendered unreadable are those directly destroyed by the projectile. For this reason, literally shredding the drive is recommended with the shredded shards of such a small dimension that substantial distortion occurs over 100% of the platter surface.

The effectiveness of Purge also depends on such subtleties. For example, recent tests on a wide variety of hard drives show that most manufacturers do not correctly implement the native Purge command on the drive; leaving data easily obtainable from the drive. Even what is considered the most reliable Purge method - De-Gaussing - requires that the De-Gaussing hardware used be "matched" to the hysteresis characteristics of the magnetic material on the platters while in the drive. Because of the level of knowledge and/or expense to ensure proper Purging or Destruction, and the effectiveness of Clearing, it is generally accepted that for commercial purposes Clearing is not only adequate, but desirable.

Clearing Overview

800-88 provides the following description of Clearing in Appendix A:

"Overwrite media by using organizationally approved and validated overwriting technologies/methods/tools. The Clear pattern should be at least a single pass with a fixed data value, such as all zeros. Multiple passes or more complex values may alternatively be used. "The bit about "organizationally approved and validated" refers to the fact that no matter what method (Clear, Purge, or Destroy) is selected and no matter the details of the selected method, the organization has the responsibility of verifying that the method is accomplishing the goal.

Note especially that 800-88 recognizes that a single overwrite pass with a fixed data value (all zeroes, for example) is sufficient.

Planning Process

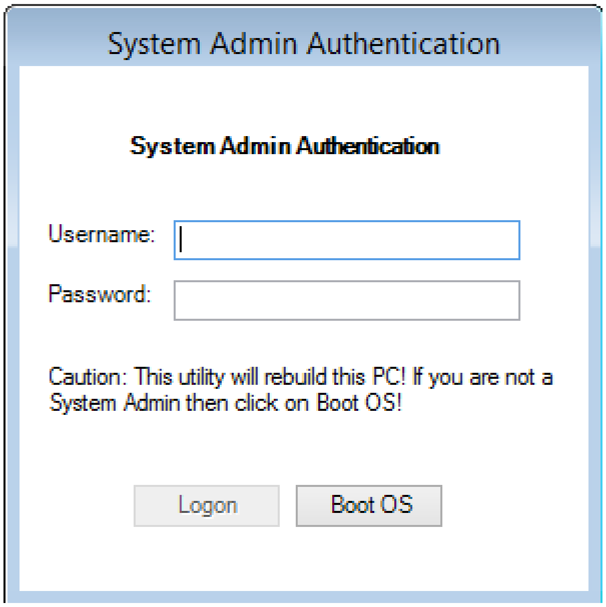
Computer should not be registered in Persystent. If computer is already registered in Persystent then make sure to delete it before continuing with Decommission process. Computer must be able to PXE boot in order to decommission it.

Persystent Clear Overview

Persystent implements a Clear method as described by 800-88. Specifically, Persystent utilizes a utility included in Microsoft Windows operating systems - DISKPART. More specifically, Persystent issues the DISPART CLEAR ALL command. This command overwrites all existing data on the target disk drive with zeroes. While the best research indicates it is unnecessary to make multiple passes on modern hard drives, Persystent includes the ability to make multiple passes if desired.

The automated steps of the Persystent Clear solution are as follows;

1. PXE Boot Computer
2. Administrator logs into the Persystent (Authorized users only)



System Admin Authentication

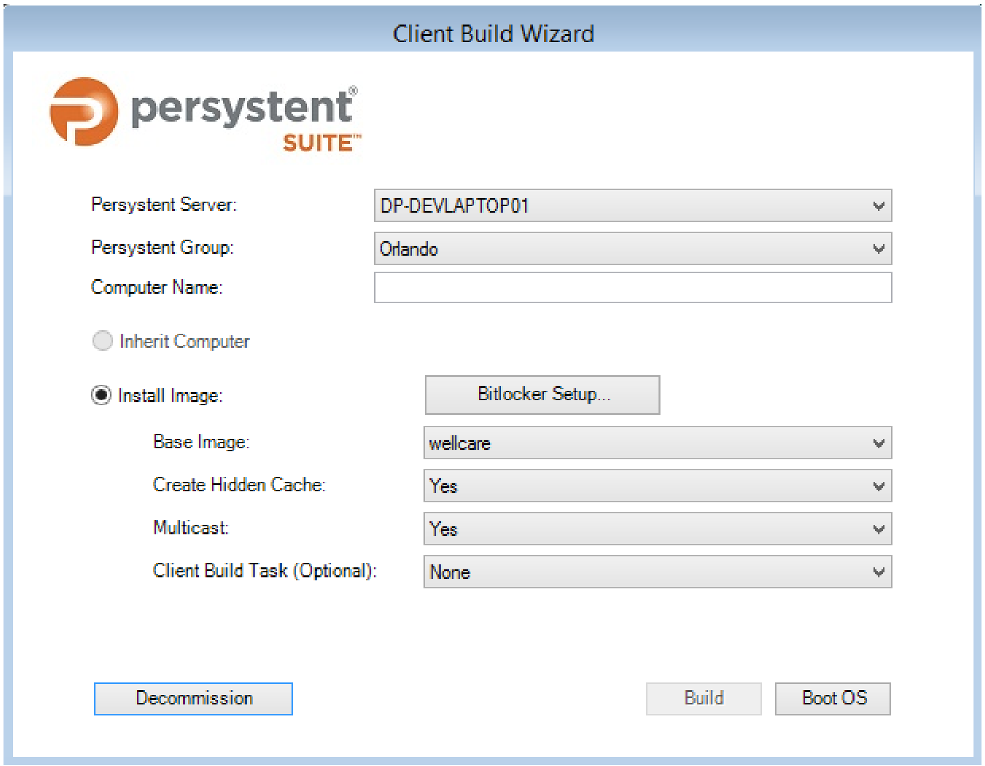
System Admin Authentication

Username:

Password:

Caution: This utility will rebuild this PC! If you are not a System Admin then click on Boot OS!

3. Click on "Decommission" button



Client Build Wizard

Persystent Server: DP-DEVLAPTOP01

Persystent Group: Orlando

Computer Name:

○ Inherit Computer

● Install Image:

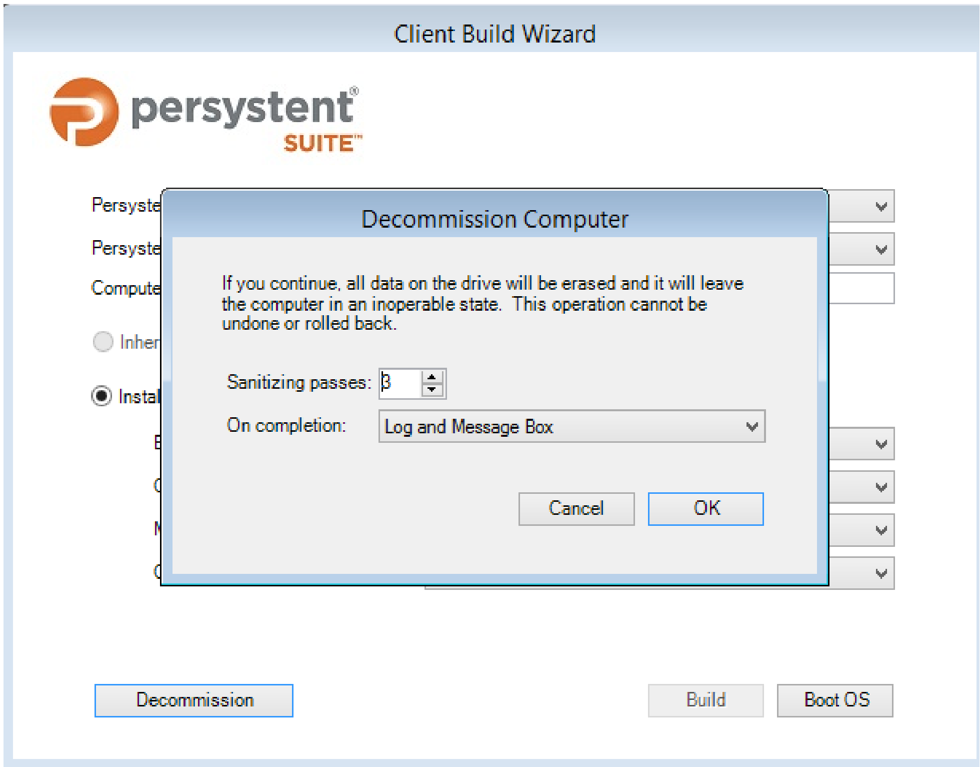
Base Image: wellcare

Create Hidden Cache: Yes

Multicast: Yes

Client Build Task (Optional): None

4. Select number of “Sanitizing Passes”

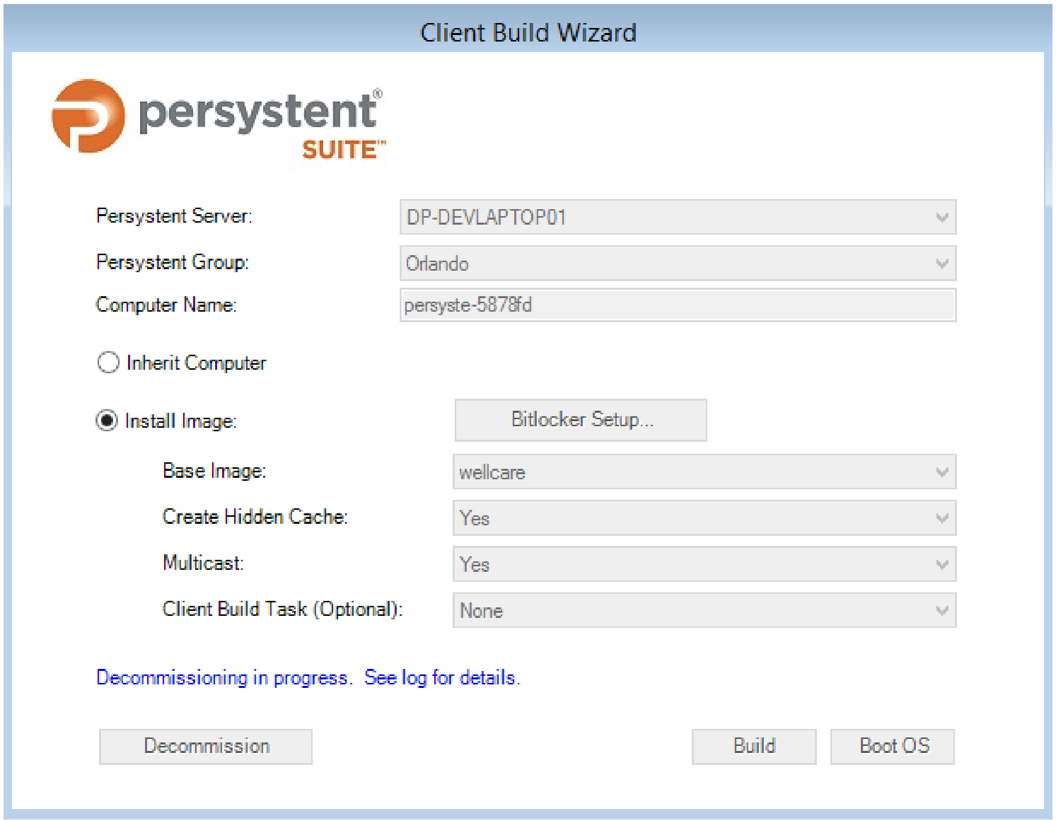


If you continue, all data on the drive will be erased and it will leave the computer in an inoperable state. This operation cannot be undone or rolled back.

Sanitizing passes: 3

On completion: Log and Message Box

5. Click “OK” to start



Client Build Wizard

Persystent Server: DP-DEVLAPTOP01

Persystent Group: Orlando

Computer Name: persyste-5878fd

○ Inherit Computer

● Install Image:

Base Image: wellcare

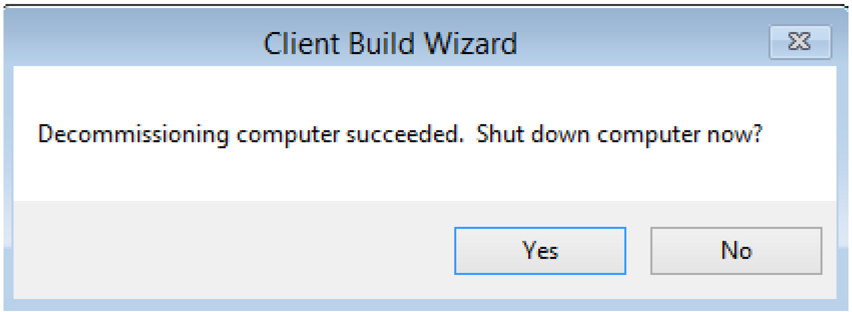
Create Hidden Cache: Yes

Multicast: Yes

Client Build Task (Optional): None

Decommissioning in progress. See log for details.

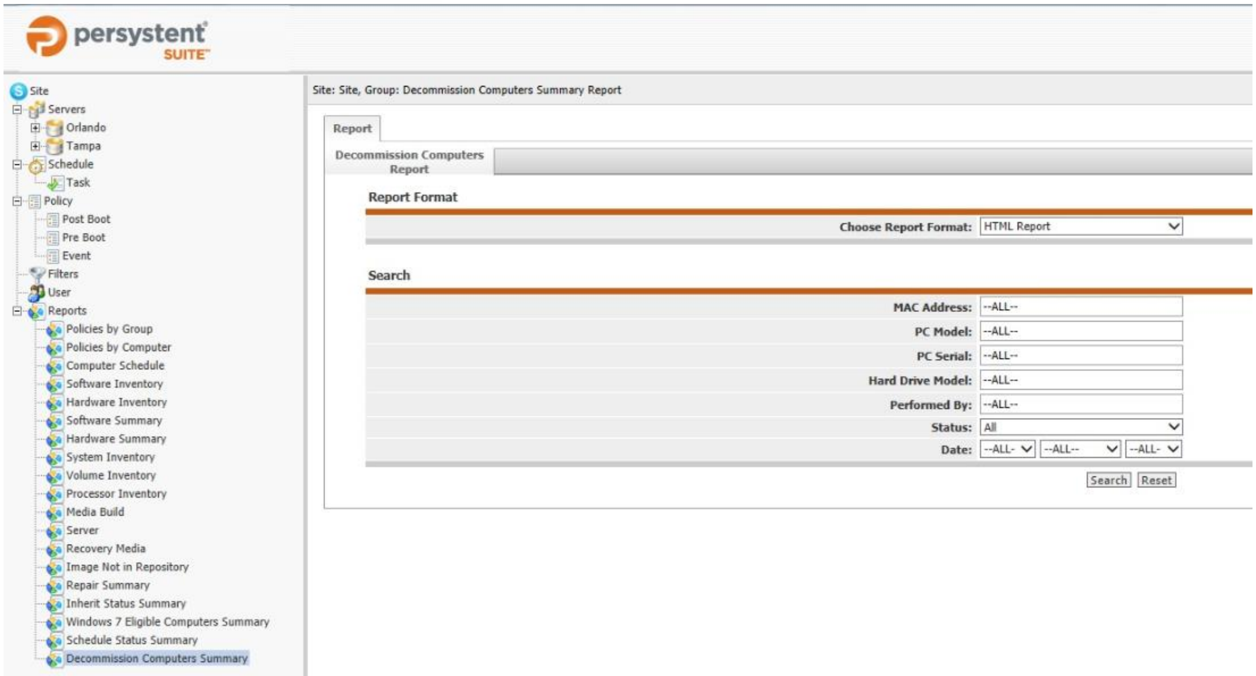
6. A message box will be shown upon completion of the decommission process.



Client Build Wizard

Decommissioning computer succeeded. Shut down computer now?

7. Click “Yes” to shut down the computer.
8. Results are uploaded to the Management Server
9. Administrator can run “Decommission Computer Report” on the WebUI



Site: Site, Group: Decommission Computers Summary Report

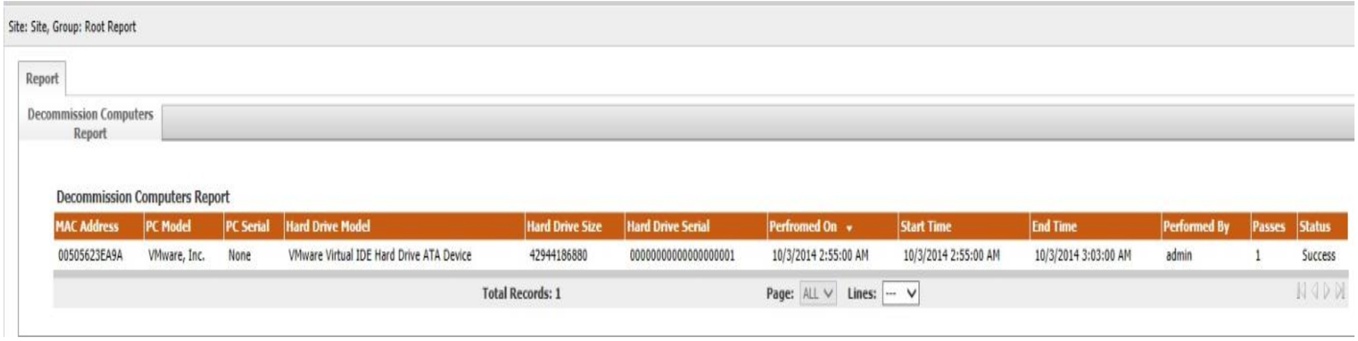
Report Format

Choose Report Format: HTML Report

Search

MAC Address: --ALL--
PC Model: --ALL--
PC Serial: --ALL--
Hard Drive Model: --ALL--
Performed By: --ALL--
Status: All
Date: --ALL- --ALL-- --ALL-

10. Administrator can search information by
    a. Mac Address
    b. Computer Name
    c. PC Model
    d. PC Serial #
    e. Hard Drive Model
    f. Performed By
    g. Performed Date and Time
    h. Status



Site: Site, Group: Root Report

Decommission Computers Report

MAC Address	PC Model	PC Serial	Hard Drive Model	Hard Drive Size	Hard Drive Serial	Perfromed On	Start Time	End Time	Performed By	Passes	Status
00505623EA9A	VMware, Inc.	None	VMware Virtual IDE Hard Drive ATA Device	42944186880	00000000000000000001	10/3/2014 2:55:00 AM	10/3/2014 2:55:00 AM	10/3/2014 3:03:00 AM	admin	1	Success

Total Records: 1 Page: ALL Lines: ---

Summary

Clearing a disk drive by overwriting the entire drive with zeroes is currently the most cost-effective and robust method compliant with 800-88 without engaging in time-consuming and costly research and verification procedures. For this reason, Utopic has chosen to implement Clear in Persystent.

UTOPIC

Utopic Software
1215 E 6th Avenue
Tampa, FL 33605

813.444.2231

support@utopicsoftware.com