Secunia PSI for Application Patch Management

An installation and user guide to Secunia Personal Security Investigator (PSI)
# Table of Contents

**Introduction** ........................................................................................................... 1
Secunia PSI .................................................................................................................. 1
Secunia CSI .................................................................................................................. 1
Purpose of Deployment ............................................................................................... 1

**Quick Reference Guide to Secunia PSI** ................................................................. 2
Installation Steps for Secunia PSI ........................................................................ 2  
  - *Windows Domain Machines* ........................................................................ 2
  - *Windows Manual Installation or Non-Domain Machines* ....................... 2
  - *Macintosh* .......................................................................................................... 2
How to Use Secunia PSI ............................................................................................ 2  
  - *Windows* ............................................................................................................ 2
  - *Macintosh* .......................................................................................................... 2

**Secunia PSI for Windows** ..................................................................................... 3
After The Install .......................................................................................................... 3
Starting a Scan ............................................................................................................. 3
Blocking Updates to a Program .............................................................................. 4
Stages of the Update Process .................................................................................. 5  
  - *Downloading Update* .................................................................................... 5
  - *Examining Program* ....................................................................................... 5
  - *Click to Update* ............................................................................................... 5
Microsoft Update Requirement ............................................................................... 6

**Secunia CSI for Mac** ............................................................................................ 8

**Secunia CSI Console** ........................................................................................... 9
Introduction

Secunia PSI
Secunia Personal Software Inspector (PSI) is a computer security solution that identifies vulnerabilities in several third-party software packages that can leave your machine open to attacks. For home use, this product is FREE and is highly recommended for any Windows machine you own. The great thing about PSI is that it requires little to no user intervention. Once installed, PSI will scan the computer for any and all third-party applications. It does this by primarily looking for .exe, .dll, and .ocx files. It then checks, across a secured channel, the installed version against a centralized database, housed by Secunia. This database contains the current patch and version level for millions of programs and also the location of required updates. PSI then uses this information to update the third-party software for you, or prompt you for intervention when items such as language selection are required.

Secunia CSI
UT System has purchased a system-wide license to use not only Secunia PSI at our University, but also Secunia Corporate Software Inspector (CSI). The way we will be leveraging CSI is by allowing the various installations of PSI around campus to report their statistics to CSI. This will allow us to see what software is the greatest risk on our campus and also maintain a current security profile report for campus departments. This console can be used by departmental techs to understand the risks in their areas of responsibility. Since we are ONLY using the CSI component for reporting, this means that nothing is required for CSI to function other than the PSI installation. Also, since PSI handles its own patching and retrieves its information from Secunia, Information Security is not pushing updates or software onto University computers. CSI is available to provide system metrics, not software deployment.

Purpose of Deployment
Secunia PSI in conjunction with CSI will resolve the single largest threat to computer security UT Dallas, third-party software that is out of date. Across the thousands of machines on campus, there are tens of thousands of third-party software installations. These pose a security threat to not just the University but to anyone’s personal information being accessed by that computer and to any personal computer that attaches to the University network – student, staff or faculty.
Quick Reference Guide to Secunia PSI

Installation Steps for Secunia PSI

Windows Domain Machines

- Link to the GPO named “Secunia PSI Install” and allow machines checking in to the domain to install the PSI executable.

Windows Manual Installation or Non-Domain Machines

- Browse to \campus\utd\allshare\Installs\Misc\Secunia PSI\ and install the file named “PSISetup!UTDallas.exe”.
  - Please do not change the file name.
  - You can run this silently using a “/S” switch form on the command line.
  - During this installation, you can take all of the defaults, i.e. change nothing.
    - If on the Proxy Settings section, you see text in the fields, there is no regkey to find and is technically a PSI error reporting mechanism. Clear the fields and continue with the installation, leaving them blank.

Macintosh

- SMB mount smb://utdfs01.campus.ad.utdallas.edu/Allshare$/Installs/Misc/Secunia PSI/ and copy “csia_OSX” locally to your drive.
  - Open a terminal and change to the location where you have copied the file.
  - Run the following command: “./csia_OSX –i –L”.
    - Runs script with install (-i) and local system (-L) switches.
  - This will perform the install and do an initial scan.

How to Use Secunia PSI

Windows

- You will now have the PSI icon in your system tray.
- Double click the icon. You can choose to start a scan at any time or view the status of your computer.
- For the majority of application updates, you will be required to do nothing.
  - If you are required to do something, you will see a prompt.
  - You may be prompted to install Microsoft Updates to patch non-OS related Microsoft Products. Please do so.
- To uninstall, simply remove via add/remove programs or programs and features as you would any other software.

Macintosh

- This is used for reporting purposes only, so you do not have to interact with the product once it is installed. It will not update software packages like the Windows version.
- You will not see it in applications or in system preferences.
- To uninstall, open terminal and run the following command: “./csia_OSX –r”.
  - Runs script with the remove (-r) switch.
Secunia PSI for Windows

After The Install
Once you have installed Secunia PSI, you will be able to open the console and view what programs are listed for your machine as either patched, end of life, or needing to be patched. An object that is patched is fully up-to-date and no action is required. For those items needing patches, the vast majority of time, Secunia will download and install these patches for you with no intervention. For items listed as end-of-life, there is no update available by the manufacturer. It is highly recommended that you find a replacement product for the one at end-of-life to keep your machine safe and use software that has a certain level of support and patch development.

Below is an example of what you will see when you first open your console after an installation. There will most likely be items that need to be upgraded and they will show at the top of the console. As you can see below, in Figure 1, there are 13 items in various states that are listed as programs that need updating. Figure 2 shows the section listing already patched programs.

![Figure 1: First Time Opening PSI – Programs Needing Updates Section](image-url)
Starting a Scan
In the bottom left corner of the PSI console you will see the scan again button. Upon clicking this, PSI will begin scanning your machine for all the third party software applications you have installed and for their version and patch level. You will see a progress bar replace the view above indicating the scan’s status. Once completed, the information will be refreshed in your view and the list of programs and their status as well as the current Secunia System Score will be updated.

Blocking Updates to a Program
At times, there may be a certain program on your computer that cannot be updated for reasons such as compatibility or user preference. Normally, PSI would update these automatically, but you can prohibit this from happening. After opening PSI and getting to the list of installed programs, simply right-click the program name that you do not wish to update any more. From the menu that appears, select “Ignore updates to this program.” This is all you will need to do to prevent that program from being updated in the future.
Stages of the Update Process
You will find different status messages next to the programs listed in PSI from time to time. The most common ones you will see are that the program is being examined, an update is downloading, or that a manual update is required. Below are these stages listed out and what they will mean to you. Also, below are three samples showing how these different stages will be represented in the PSI console.

![Downloading update](image)
Downloaded update
Adobe Reader 9.x

![Examining program](image)
Examining program
Adobe Reader 9.x

![Click to update](image)
Click to update
DAEMON Tools Lite 4.x

**Figure 3: Downloading Update**  **Figure 4: Examining Program**  **Figure 5: Manual Update Required**

*Downloading Update*
This message indicates that a new version, or an update to the version you have, of an installed program has been detected. At this time, PSI has now checked against the Secunia database, found the change, and has begun downloading it to your system for installation. As this is happening, no intervention is required. Simply allow PSI to continue the download and it can install the software automatically.

*Examining Program*
When this message is present in the PSI console, the installed program noted is currently being inspected by PSI. The software version and patch level is being evaluated against the Secunia database containing the list of all known software packages and their current release level. If an update is found to the program, then the status will either change to downloading update, showing the update process has begun, or click to update, showing manual intervention is required.

*Click to Update*
A program showing click to update indicates that manual intervention is required. This is normally seen when the software update or installation contains options that must be set by the user at time of installation. The most common two are the language selection and optional software package installs bundled with the one required. When you click on the link, as seen in Figure 5, you will be directed to the download page for that program in your default web browser. From there, you will simply need to run the installation as you did when first installing the program on your computer. If the PSI console is minimized or closed, you may see the following message balloon indicating a program needs user input for updating.

![Secunia PSI](image)
Secunia PSI
You have programs that require manual updates

Figure 6: PSI Manual Update Notification
Microsoft Update Requirement

Chances are your computer has Microsoft Update (MU) already installed on it. This is different than just Windows Update (WU). While WU is used to patch the computer’s Windows Operating System, MU is used to patch Microsoft based products such as Office, .Net Framework, and XML Core. To allow for PSI to update the Microsoft specific packages, it will need the ability to check with Microsoft for those packages to be downloaded. To do this, MU must be installed.

You will be notified upon first launch of the PSI console if your machine does not have MU installed. What you will receive is a box identical to the one below:

![Microsoft Update notification]

*Figure 7: Microsoft Update Required Notification*

Once you click on Install Microsoft Update, you will be directed to a download page within Internet Explorer. The page should have the following at the top signifying you are about to install MU.

![Microsoft Update installation page]

*Figure 8: MU Installation Page*

From this page, click the start now button. Once you have done this you will be directed to a page with the license agreement. There will be a continue button listed on the page that you will
need to click. Once you do this, you will be prompted to install an Active X component prior to installing MU. Your browser will show a yellow bar at the top stating this:

![Active X Control](image)

Figure 9: Active X Control

Right click this yellow bar and select “Install This Add-on for All Users on This Computer...” Once you have done this, you will then be prompted for the installation of MU. A dialog box will appear which looks like the following:

![MU Installation Prompt](image)

Figure 10: MU Installation Prompt

Click the Install button to continue. Once MU has been installed, you should not see the warning within the PSI console again, as seen in Figure 7. The various Microsoft products should begin going through the different stages of update as described in the previous section.
Secunia CSI for Mac
The Secunia installation for Macs is intended for reporting purposes only. Once Secunia CSI has had an agent placed on a Mac, it will perform a scan, find installed products and then report this back to the CSI console. Periodically, it will repeat this scan and report to the CSI console again. These scans can also be triggered whenever you would like. The scans can be run behind the scenes as a service or directly in the command line to see the output. If you want, you can always pipe the information out to a file to read or search through. Below are some screenshots showing the commands to use and also what the expected output will be once the scan has started and then once it has completed.

Figure 11: Mac Installation Command
```
eins:/ cedwards$ ./csia_OSX -l -L
```

Figure 12: Mac Removal Command
```
eins:/ cedwards$ ./csia_OSX -r
```

Figure 13: Mac Manual Run Command
```
eins:/ cedwards$ ./csia_OSX -c -L
```

Figure 14: Mac Manual Run Command with Output to Text File
```
eins:/ root# ./csia_OSX -c -L > SecuniaScan.txt
```

Figure 15: CSI Scan Executing on Mac
```
[06/16 18:25:23.477] Status: Secure
[06/16 18:25:23.477] Product ID: 45711
[06/16 18:25:23.477] [06/16 18:25:23.477] Apple GarageBand 5.x
[06/16 18:25:23.477] Status: Secure
[06/16 18:25:23.477] Product ID: 26388
[06/16 18:25:23.477] [06/16 18:25:23.477] Mozilla Firefox 20.x
[06/16 18:25:23.477] Status: End of Life
[06/16 18:25:23.477] Product ID: 45133
[06/16 18:25:23.477] Path: /Applications/Firefox.app/Contents/Info.plist
```

Figure 16: CSI Scan Results for Mac
Secunia CSI Console

The Secunia CSI Console is used for reporting purposes and to gage the overall patch level of those machines with PSI installed on them. The console is integrated with Active Directory allowing for computer objects to be pulled in and domain groups to be used for access to the console itself. Within the console, the primary two screens used are the dashboards and the hosts result page. On these two pages, you will be able to view useful information such as:

- What computers have PSI installed and when did they last scan/update.
- Of the third-party software installed on a computer, what is listed as insecure, patched, or end-of-life.
- What are the most critical security advisories affecting your systems.
- What are the most prevalent insecure or end-of-life software installations.
- What is the most insecure software based on threat scores.

These items are some of the major points you can gain from viewing your assets within the CSI console. To request access for this, please email infosecurity@utdallas.edu with the AD OUs you wish to view and who should have this access. Below are screenshots depicting what you will typically see on the dashboard and then on your hosts report page.

![Figure 17: CSI Dashboard View](image-url)
Figure 18: Report of Computers running PSI

Figure 19: Overview of a Single Host

Figure 20: Scan Results Showing Installed Software and Patch State