

## **Table of Contents**

1. [Introduction](#)
2. [Inventory and Privacy](#)
3. [Self Service](#)
4. [Software Management](#)
5. [Purchased Software](#)
6. [Security](#)

# 1. Introduction

Welcome to the JAMF Pro Inventory and Software Management suite, (also known as the Casper Suite), brought to you by Duquesne University.

Utilizing the latest features in OS X/macOS provided by Apple, the JAMF Pro system allows CTS to provide your Apple computer with the highest level of support possible.

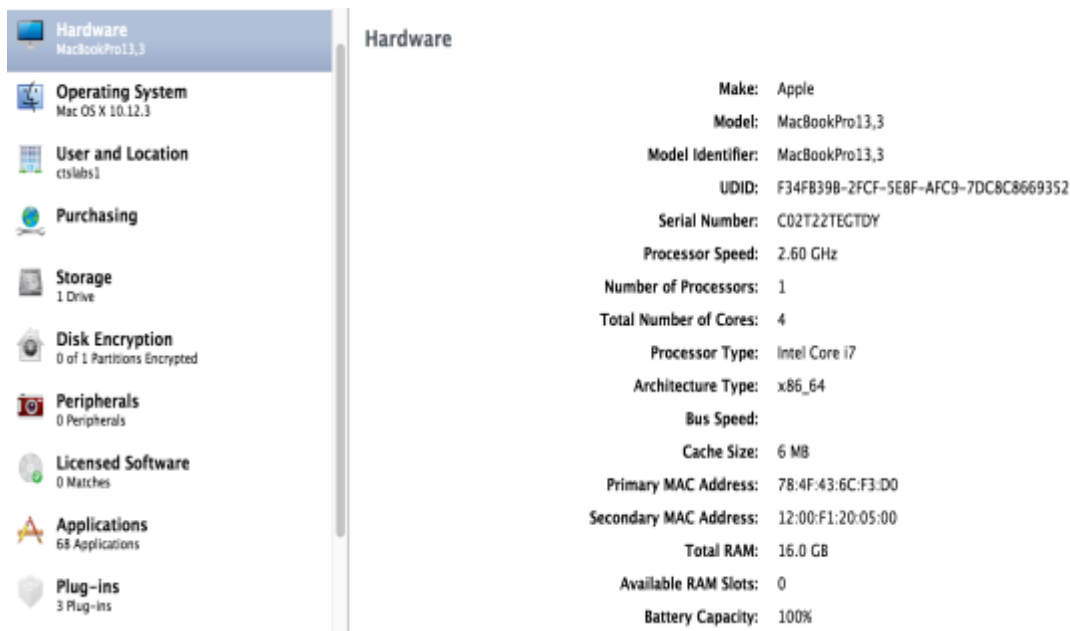
The JAMF Pro suite brings many of the services currently offered to our Windows systems over to the Apple environment for the first time. These include:

- Curated, tested, and up to date software available for install via the [Self Service](#) application.
- Information about your [hardware configuration](#) will allow the CTS Help Desk to assist your machine with the correct repairs for your unique laptop or desktop.
- A complete [inventory](#) will allow CTS to offer you the most up to date security fixes, and prevent exploits from spreading among University machines.
- A faster deployment of software purchased through the University Computer Store via [Self Service](#)

## 2. Inventory and Privacy

To enable the best possible support for your hardware, your machine will generate an initial, and weekly, inventory report of your hardware and software.

This inventory allows CTS to ensure that any security issues with your machine can be addressed appropriately, as well as ensure that you are offered the most up to date applications for your operating system.



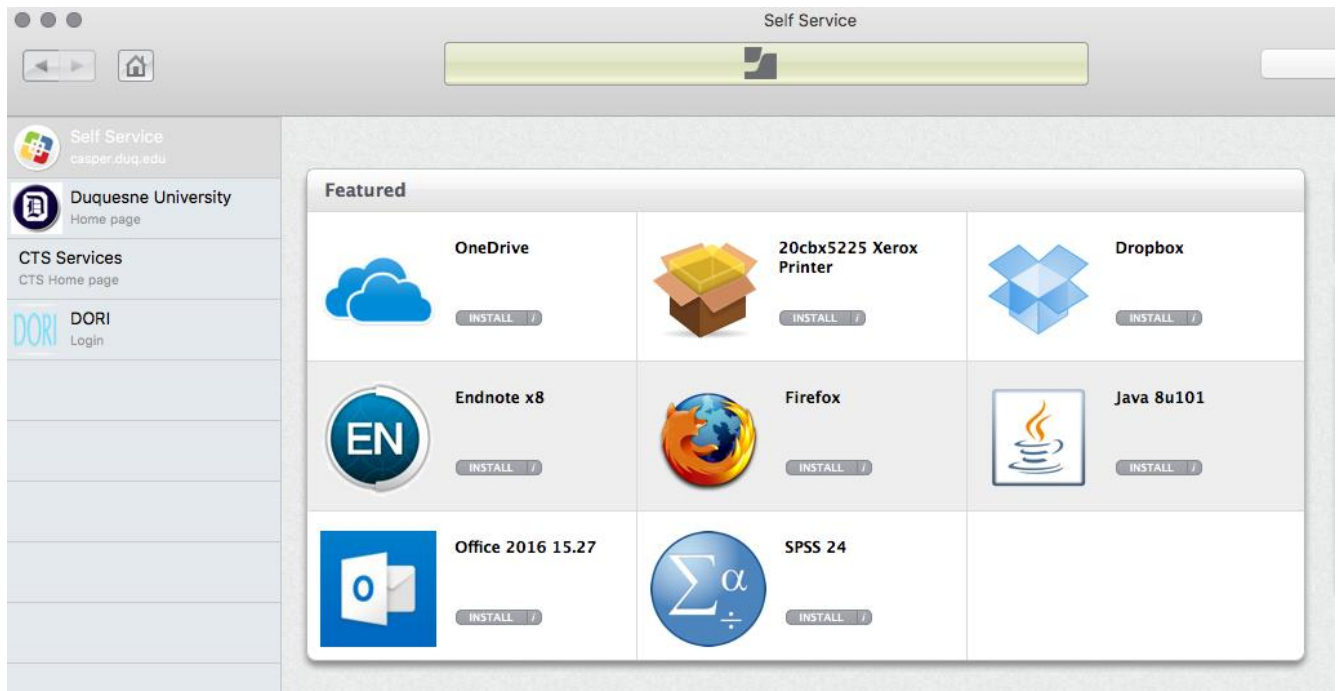
This inventory record is associated to you only by user name and email entered at the time of enrollment. **NO** personal data is inventoried in this process as only system Applications and Operating System are checked. These records are only accessible to CTS staff members trained to assist you in on going issues.

The contents of your user profile including: documents, pictures, movies, etc. are not inventoried by the JAMF Pro system.

### 3. Self Service

Self Service is the Software Catalogue of applications provided to you by CTS. These applications have been vetted for compatibility, security, and functionality.

The applications within Self Service will alleviate the stress of downloading common software from Websites while also providing you with an accurate catalogue of all the software made free to use by Duquesne University.



Self Service is already installed on your machine, and is available by opening Finder and navigating to your Applications folder.

Within Self Service, you will also find quick links to the most commonly used Duquesne University websites. Clicking on any of the links adorning the left side of Self Service will open these websites in your web browser of choice.

## 4. Software Management

Utilizing the Application records generated during the [Inventory](#) process, CTS will periodically offer you updates to your installed software. Below is an example of what that record looks like:



|                              |                |   |     |
|------------------------------|----------------|---|-----|
| iMovie.app                   | 10.1.4         | /Applications/iMovie.app                    | Yes |
| iTunes.app                   | 12.5.5         | /Applications/iTunes.app                    | No  |
| Keychain Access.app          | 9.0            | /Applications/Utilities/Keychain Access.app | No  |
| Keynote.app                  | 7.0.5          | /Applications/Keynote.app                   | Yes |
| Launchpad.app                | 1.0            | /Applications/Launchpad.app                 | No  |
| Mail.app                     | 10.2           | /Applications/Mail.app                      | No  |
| Maps.app                     | 2.0            | /Applications/Maps.app                      | No  |
| Messages.app                 | 10.0           | /Applications/Messages.app                  | No  |
| Microsoft Excel.app          | 15.29.16120900 | /Applications/Microsoft Excel.app           | No  |
| Microsoft OneNote.app        | 15.29.16120900 | /Applications/Microsoft OneNote.app         | No  |
| Microsoft Outlook.app        | 15.29.16120900 | /Applications/Microsoft Outlook.app         | No  |
| Microsoft PowerPoint.app     | 15.29.16120900 | /Applications/Microsoft PowerPoint.app      | No  |
| Microsoft Remote Desktop.app | 8.0.27246      | /Applications/Microsoft Remote Desktop.app  | Yes |

In the presence of a severe security breach, such as those that have recently struck the Adobe Flash Player, CTS may update an application silently to ensure that your machine is not left in compromised position. Below is an example of that prompt that will accompany such an update:



## 5. Purchased Software Deployment

Software purchased through the Duquesne University Computer Store can be deployed at an accelerated rate via Self Service.

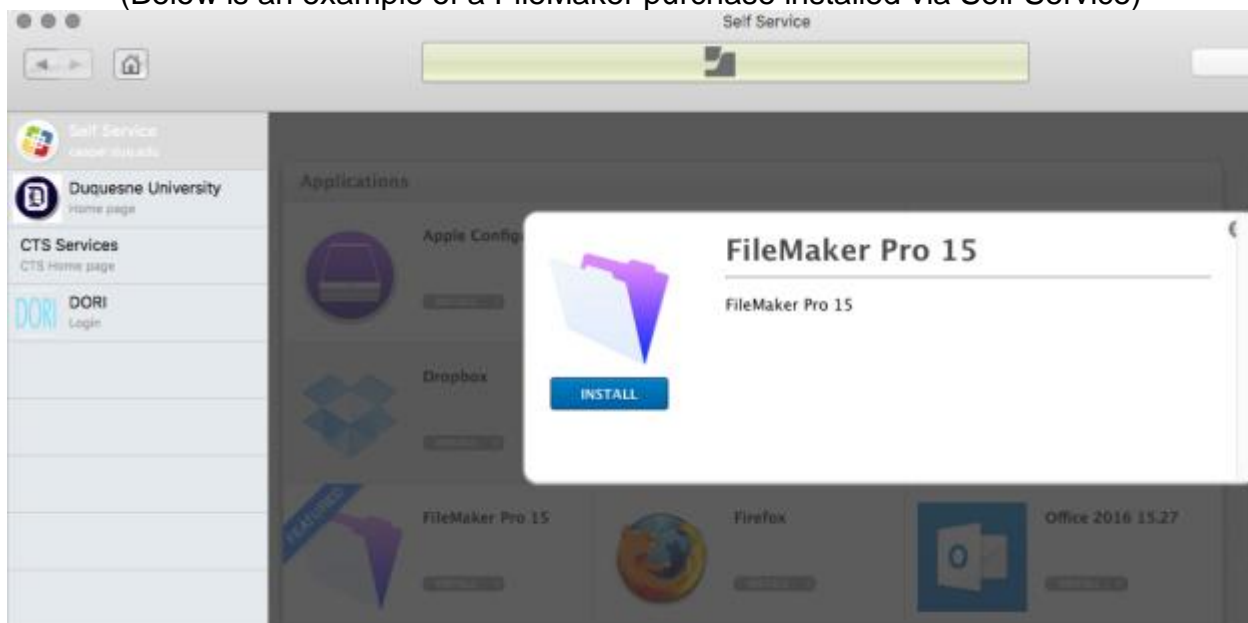
This ability extends to those products offered by Microsoft, Adobe, FileMaker and many more.

Though these pieces of software may still be installed by an on-sight Technician, they can also be deployed to your computer in a number of ways via Jamf Pro including:

- Silent Install
- Self install via Self Service
- CTS Assisted install via Self Service

This will decrease the wait time between order and installation, especially in orders for multiple department machines.

(Below is an example of a FileMaker purchase installed via Self Service)



## 6. Security

The continued security of the files and intellectual property on your computer remain the highest priority at CTS. To aid in this, we will not only monitor and offer the [latest security updates](#), but will scan your machine for known system exploits as they are reported to us by Apple.

When an exploit is made known, your machine may be scanned for any malicious files matching the exploit during your weekly inventory. This search is performed in addition to the ongoing Kaspersky Anti-viral scans already taking place.

|   | OS              |  | Fruitfly Exploit |
|---|-----------------|---|------------------|
|   | Mac OS X 10.9.5 |   | Not Infected     |
|   | Mac OS X 10.9.5 |   | Not Infected     |
| 1 | Mac OS X 10.9.5 |   | Not Infected     |
|   | Mac OS X 10.9.5 |   |                  |
|   | Mac OS X 10.9.5 |   | Not Infected     |
|   | Mac OS X 10.9.5 |   | Not Infected     |
|   | Mac OS X 10.9.5 |   | Not Infected     |
| 2 | Mac OS X 10.9.5 |   | Not Infected     |
|   | Mac OS X 10.9.5 |   |                  |
|   | Mac OS X 10.9.5 |   | Not Infected     |

(Above is an example of a report run against the presence of the most recent Fruitfly exploit affecting Apple computers.)