



System Center Configuration Manager Overview

This document provides some background information on the Microsoft Systems Center Configuration Manager (SCCM) system, which has been selected for use as an Asset Management tool on the MSU Denver campus.

The following guide is designed to help answer some of the more frequently asked questions about this system and illustrate some of the system's features. If you have any questions or concerns regarding the system, please contact the MSU Denver ITS Helpdesk using the contact information posted at the end of this document.

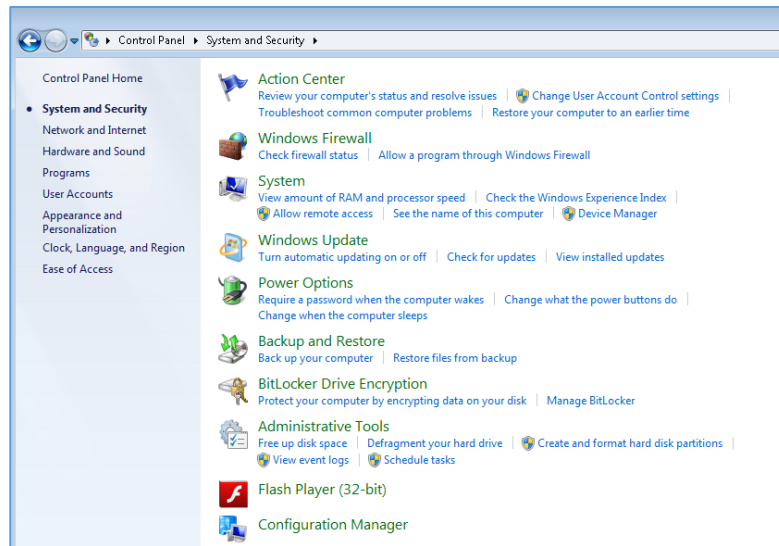
What is SCCM?

SCCM is a software product developed by Microsoft to simplify asset management for large groups of computers running a range of popular operating systems. SCCM includes hardware and software inventory management tools, software and patch management and guided remote support utilities.

How Can I Tell if SCCM is Installed on a Computer?

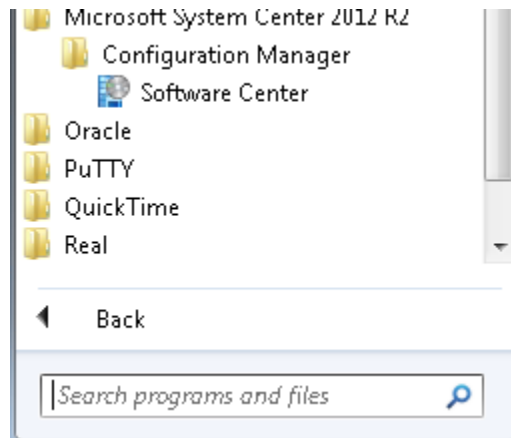
The SCCM system leverages a small application on each device, which will check in to the server on a regular basis. To determine whether SCCM has been installed on a specific workstation, try one of the two instruction sets below:

1. Open the Control Panel by clicking the Start Orb, then select Control Panel in the right-hand column.
2. Select the System and Security Category
3. The presence of the Configuration Manager icon in this list indicates that SCCM has been installed on the device.



Additionally, SCCM will add entries to the system Start menu.

1. Click on the Start Orb, then select All Programs
2. Click on Microsoft System Center 2012 R2. The Configuration Manager folder will include an entry for Software Center.

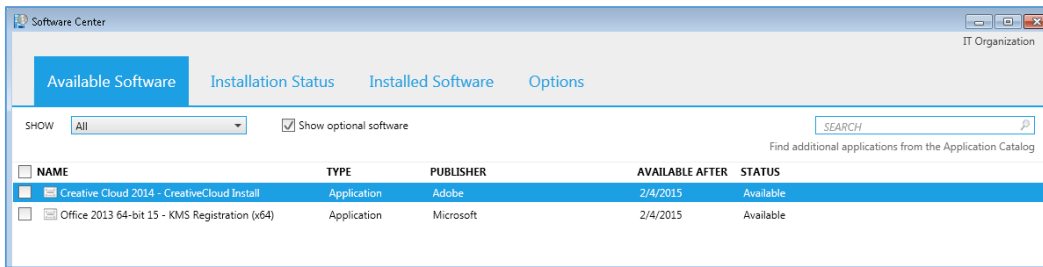


How Does SCCM Help Me?

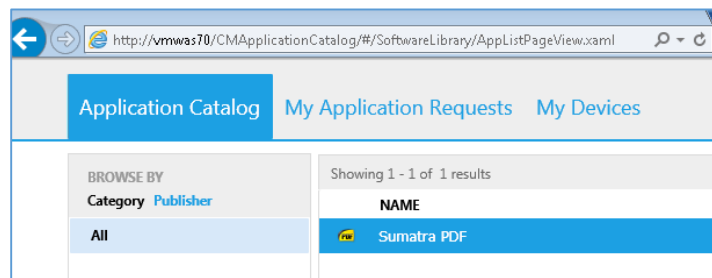
SCCM offers several self-service functions that can simplify routine tasks for campus computer users!

Install Approved Applications

SCCM allows for the publication of pre-approved applications to all qualified computers or user accounts. This allows users to install applications to their systems without requiring ITS support or intervention. Applications available to a given computer will be visible in the Software Center, accessible on the device (see above):



Applications available to an individual NetID will be visible in the Application Catalog, which is a website hosted on the SCCM server:



Minimize Interruptions due to updating and patching

Deployment of software updates and patches serves two very important purposes: maintenance of a robust information security posture and minimization of interruptions and distractions during a user’s workday. Proactive maintenance of software updates and patches is a critical function performed by ITS, and can be made easier by SCCM.

SCCM allows ITS to pre-define the periods during which patches are released, deploys the patches in the background and manages when or if system reboots are required, minimizing midday impact.

SCCM also permits an end user to “snooze” an update until a more convenient time if an installation is attempted while they are working.

How Does SCCM Help ITS Support Me?

SCCM offers a range of tools that allow ITS to better support (and anticipate) the technology needs of the campus.

Hardware Inventory Management

Maintaining an accurate inventory of computers deployed across campus allows ITS to better manage availability and performance of devices and to plan computer lifecycles more effectively. SCCM offers

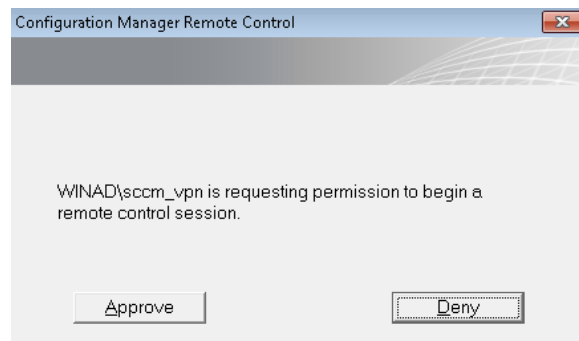
reporting of device hardware and serial numbers which ITS will use to schedule upgrades and replacements.

Software License Management

Accurate accounting of installed software licenses is a critical function, carrying financial and legal implications for inaccurate tracking. SCCM facilitates a more streamlined software inventory process, permitting ITS to actively manage available software licenses, upgrade outdated applications easily and provide valid reports of software used in case of audit.

Remote Assistance with User Permission

SCCM includes a remote assistance tool very similar in function to the Bomgar application presently in use by ITS. In some cases an ITS technician may recommend a remote support session to better diagnose and resolve a case opened by an end user. In this situation, the user must authorize remote access before any screen-sharing is initiated. A green bar will appear on-screen to ensure the viewer is aware of the remote session, and the session can be terminated at any time by the end user.



What Information Does SCCM Collect?

The SCCM system collects data about the computer and software installed on the device, but **DOES NOT** collect any personal information. Examples of the type of data that can be detected and reported against are as follows:

Hardware Information	Software Information
Computer Make & Model	Operating System & Version
Hard Disk Size	Installed Software
Available RAM	Software Versions
Computer Name	Software Metering
IP Address	Windows Updates
Connected Peripherals	User Login Timestamp

Personal files - including documents, email, passwords and browsing history - are not collected by SCCM.

Logging

SCCM retains a log of nearly all Configuration Manager activity, so any ITS use of the system can be audited. All Remote Control sessions and Administrative actions are logged, allowing for review if necessary. The logged data can be pulled as a report showing, for example, all remote control sessions initiated by a single user.

If you have any questions or concerns, please contact the ITS Helpdesk for assistance using the contact information below.

Thank you,

Information Technology Services

[Find a solution](#) | [IT Service Status](#) | [Reset your Password](#)

CALL ITS Helpdesk at 303-352-7548

CLICK

Submit a service ticket online at www.msudenver.edu/gethelp

VISIT

ITS Helpdesk | Walk-in Assistance | West ([WC 241](#))
Monday - Friday 8AM - 6PM

ITS Helpdesk | Walk-in Assistance | Admin ([AD 475](#))
Monday - Friday 8AM - 6PM