Leaving Windows Management Systems

Marc Doughty - 2019-04-13 - 0 Comments - in Windows and PC Computers

By default, Windows machines at Brown are connected to a variety of internal management systems. This document will cover why and how to disconnect from these systems and what the ramifications are.

Active Directory (AD)

Active Directory is the enterprise directory system, allowing user accounts and groups to access computer systems using their own credentials. It also defines group membership and can apply policies (settings) to computers. Deploying with OSD implies SCCM membership, but computer object location within AD defines the baseline level of management AD provides.

Ramifications of disconnecting

If you disconnect from Active Directory, your computer will lose the ability to let users log in unless local user accounts are created. Settings governing updates, appearance, and security will no longer come from CIS. ‘Single sign on’ access to services (print and file services) will be lost. The computer will not participate in any inventory.

How to disconnect

You must have both local administrative permissions and the permission to delete/modify the computer’s machine object in AD.

Create a local account with administrative permissions and a strong password.

Open an elevated PowerShell prompt (right-click PowerShell from Start Menu and ‘run as administrator’) and enter the following command:

PS> Remove-Computer -Restart -UnjoinDomainCredential (Get-Credential)

Enter domain credentials with permissions to remove the computer’s machine object in the AD\username format. The machine should automatically restart afterwards

Verify that Windows Update is properly configured for automatic updates.
System Center Configuration Manager (SCCM)

SCCM is the primary Windows endpoint deployment, managment, inventory, and antimalware system. All machines in AD except for ‘unmanaged’ machines should participate in SCCM in one way or another. Deploying with OSD implies SCCM membership, but computer object location within AD defines the baseline level of management SCCM provides.

Ramifications of disconnecting

If you disconnect from SCCM, your computer will no longer participate in advanced inventory, automatic CIS-approved updates to the operating system and core software, nor will it participate in managed antimalware configuration, updates, or reporting. You will not be able to deploy software using Software Center or via SCCM pushes.

How to disconnect

You must have local administrative permissions.

Open an elevated command prompt (right-click Command Prompt from Start Menu, ‘run as administrator’) and enter the following command:

C:\Windows\ccmsetup\ccmsetup.exe /Uninstall

Wait five minutes, then restart the machine.

Verify that the ‘Configuration Manager’ Control Panel is no longer present and that the ‘ccmexec.exe’ task is not running.

Key Management Service (KMS)

In lieu of manually entering permanent serial numbers to each machine, Microsoft enterprise products like Windows, Server, and Office regularly communicate with a server that tracks license usage. KMS provides much more accurate counts of in-use activations than distributing volume license keys, and allows full use of licensed products for up to 180 days without contact with the KMS server. KMS keeps products activated for machines that are on premises or via VPN.

Ramifications of disconnecting

If you disconnect from KMS, your computer will no longer participate in Microsoft product activation and you will need to manually enter volume license keys for Windows, Office, and any other KMS products. Responsibility for license compliance and volume key confidentiality falls on IT professionals who are manually authorizing the products.

Checking KMS activation status

Windows 7 & 10

cscript /H:CScript C:\Windows\System32\slmgr.vbs /dlv
Office 2016 (Substitute 'Office15' for Office 2013)

cscript //H:CScript 'C:\Program Files (x86)\Microsoft Office\Office16\OSPP.VBS'
/dstatusall

How to disconnect

You must have local administrative permissions.

Open an elevated command prompt (right-click Command Prompt from Start Menu, 'run as administrator') and enter the following commands, where XXX... is the MAK key for your product (available by request to software_services@brown.edu):

Windows

cscript //H:CScript C:\Windows\System32\slmgr.vbs /ipk XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

cscript //H:CScript C:\Windows\System32\slmgr.vbs /ato

Office 2016

cscript //H:CScript 'C:\Program Files (x86)\Microsoft Office\Office16\OSPP.VBS'
/inpkey:XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

cscript //H:CScript 'C:\Program Files (x86)\Microsoft Office\Office16\OSPP.VBS'
/act

Sassafras K2 (aka KeyClient, KeyAccess)

Sassafras K2 is a software asset and license management system for Brown-owned and personally owned computers, allowing CIS to grant some access to installed software titles to student and personally-owned machines. It is also used to generate operating system and software usage metrics. Sassafras K2 is included with Core Software task sequences.

Ramifications of disconnecting

If you disconnect from Sassafras K2, your computer will lose the ability to run keyed software, and software that is 'controlled unkeyed' will run outside of compliance with our license agreements; in addition, software and session metrics will not be reported to CIS.

How to disconnect

You must have local administrative permissions.

Open the Programs and Features Control Panel.

Right-click and uninstall Sassafras K2 Client.