5/23/2013

Welcome to System Center Endpoint Protection – Microsoft's Antivirus/Antimalware Solution

Information Technology Services is migrating from McAfee Virusscan Enterprise (VSE) to System Center Endpoint Protection (SCEP) due to its inclusion in FSU's Microsoft Campus Agreement. Departments who are using the McAfee ePolicy Orchestrator (EPO) server to manage McAfee VSE on their computers should contact the FSU IT Security Team (its-security@fsu.edu or 645-8053) to begin the process of migration.

How does SCEP get installed?
Computers on the fsu.edu AD using McAfee VSE can be automatically migrated through the use of a login script in a Group Policy Object. The script will be provided when a department is ready to do the migration. The login script installs the System Center Configuration Manager (SCCM) client which then communicates with SCCM. This is analogous to the McAfee agent communicating with EPO. When a computer is recognized by SCCM, the SCEP installer removes McAfee, installs SCEP and updates it to the latest version. A restart may be required after the installation.

Workgroup and untrusted AD computers will require a manual installation of a certificate and the SCCM client.

How does SCEP protect the computers?
SCEP has many of the same features as McAfee VSE. The following list shows the default policy settings for SCEP.

- Definition updates: computers check in every 2 hours and receive updates as Microsoft releases them. If the SCCM client cannot reach SCCM for more than 36 hours, definition updates will be received directly from Microsoft.
- Full scan: Thursdays @ 12:20 a.m. with randomization, CPU Usage 30%
- Quick scan: daily @ 12:00 p.m. with randomization, CPU Usage 30%
- Scanned items: hard drive, email and attachments, removable storage devices, archived files
- User can set CPU usage %
- Default actions: All events are quarantined and deleted after 30 days
- Real-time protection: on
- Exclusions: To be determined as necessary

Why are Windows updates being installed?
The installation of the SCCM client also sets the registry key for Windows System Update Services (WSUS) to the SCCM environment. Computers will receive Microsoft updates in the same manner that updates are done by the IT Security Team on the campus WSUS server. Updates are released

SCCM provides critical and security updates and service packs for the following software on the Friday after Microsoft's Patch Tuesday (the second Tuesday of each month):

- Windows 8, 7, Vista, XP
- Microsoft Office 2003, 2010, 2013
- Internet Explorer 6, 7, 8, 9, 10
- Silverlight

- Visio

SCCM provides only critical and security updates for Windows Server 2003, 2008, and 2012 one month behind Microsoft's release. This allows sysadmins to install updates on their own schedules and provide backup security.

If there is a critical out-of-band update, it will be released as soon as it is tested.

How does SCEP compare to McAfee in terms of computer resource utilization?
SCEP is reported to be less resource intensive than McAfee. Scans have been run in the background during normal use of a computer and did not seem noticeable.

How can a department manage their own computers?
At some point in the future, permissions will be delegated to department sysadmins who want to manage their own computers. Access will be provided to a console and they will have the ability to create their own policies and collections (analogous to policies and groups in EPO).

What can users do with SCEP?
Users can access SCEP by clicking on the SCEP icon in the taskbar (green square with a white shield). They can run manual updates and/or scans but cannot change any settings defined by the default policy.

What is the difference between the three types of scans?
Quick Scan – focuses on areas where malware typically hides
Full Scan – scans all files on the hard drive and removable devices (e.g., USB devices)
Custom Scan – allows user to select what will be scanned

Is SCEP available for use on home computers of FSU faculty and staff?
Microsoft Security Essentials is the home version of SCEP. It is available for free on home computers running Windows workstation operating systems. It can be downloaded at http://windows.microsoft.com/en-us/windows/security-essentials-download.

What is Configuration Manager in Control Panel?
Configuration Manager is an item added by the SCCM client to the Control Panel which provides information about the SCCM client. Under the Actions tab there are actions that can be run to force the SCCM client to communicate in different ways with SCCM. This is similar to "Collect and Send Props" in the McAfee agent.

What is Software Center?
SCCM is a complex system that provides a number of options for enterprise management of computers. SCEP and Microsoft updates are tightly integrated in SCCM and Software Center is a program that is installed as part of the deployment process of Microsoft updates.

When the updates are released, the Software Center notifies the user that updates are available and need to be installed and that a restart is required. The user can set options in Software Center to prevent the installation from interfering with their workflow.