What Is SCCM (System Center Configuration Manager)?

Microsoft System Center Configuration Manager (SCCM) is a Windows product that enables the management, deployment and security of devices and applications across an enterprise. Amongst other potential uses, administrators will commonly use SCCM for endpoint protection, patch management and software distribution. SCCM is part of the Microsoft System Center systems management suite.

The SCCM integrated console enables management of Microsoft applications such as Application Virtualization (App-V), Microsoft Enterprise Desktop Virtualization (Med-V), Citrix XenApp, Microsoft Forefront and Windows Phone applications. All these applications can then be managed by a single location.

Features of Microsoft SCCM

Some core features in Microsoft System Center Configuration Manager include:

- Windows management -- to keep pace with updates to Windows 10.
- Endpoint protection -- to provide identification and malware protection.
- Reporting -- to present information on users, hardware, software, applications and software updates.
- Operating system (OS) deployment -- to distribute operating systems to devices in an enterprise.
- Software update management --which allows users administrators to deliver and manage updates to devices across an enterprise.
- Application delivery --which allows administrators to deliver an application to all devices across an enterprise.
- Health monitoring -- which shows client activities and health in the console, and can alert users if health statistics decrease past a specified level.

Several key features of System Center Configuration Manager help administrators address the bring-your-own-device (BYOD) trend in enterprise organizations, including user-centric management. End users can search for applications with a self-service software center and specify times when installations and upgrades take place. IT administrators can install applications on different devices. For example, SCCM can be used to install a native application on a primary device, as a Remote Desktop Services app, or as an App-V program on a tablet. SCCM also includes role-based access control (RBAC), which enhances system security by only showing end users the interface elements that apply to their specific roles as defined by Active Directory.

SCCM Vs. SCOM

Microsoft System Center Configuration Manager is similar to Microsoft System Center Operations Manager (SCOM). The two can be easily confused upon first appearances. SCOM allows system and application administrators to deploy, configure, manage and monitor operations, services and applications of many devices. SCOM does this within an enterprise through a management console.

SCCM and SCOM are both Microsoft enterprise applications. SCOM, however, focuses on enterprise monitoring on the server-side. SCCM, instead, is not considered a monitoring application and focuses on the client-side.

How does SCCM work?

At the highest level, SCCM is installed on a Windows Server to help organizations manage endpoints. Generally, it requires an agent on the managed endpoints to work.

And typically devices outside the corporate network need to connect back via VPN to receive patches, configuration updates, software, and more (unless the organization has also set up cloud management gateway (CMG) servers to help reduce VPN dependence with SCCM).

VPN requirement for remote workforce management

Finally, SCCM uses an old methodology of software deployment that assumes devices will talk to your domain often. But the truth is, with remote workforces on the rise, devices don't check in as often as they should. Fewer check-ins with your legacy patching appliance results in more devices on outdated and potentially vulnerable software versions.

Relying on VPNs, as SCCM does, is a risky endeavor in and of itself. Connecting requires human effort. VPNs slow down work and are tedious to use, which means employees often avoid using them. Even if teams have moved past on-prem servers and are using a cloud instance for SCCM, there's still management overhead that requires human intervention. Because humans are fallible, errors are likely.

The more legacy software you use, the higher the chances of security threats to your system. Using old software not only affects your business but can also tank your market reputation. Breaches and potential incidents represent real risks to your business' reputation and could damage customer trust in your brand. It's bad news.

Further Disadvantages to Using SCCM

Unfortunately, SCCM background software installations come with a slew of other drawbacks and hidden risks:

- It can be impossible to know whether or not you've installed certain software. Until you stumble on it, you may not even detect installed SCCM software.
- During a software installation failure, you won't receive pop-up warnings. Moreover, you won't get immediate notices of failure.
- New applications silently pushed into your system signal malware or viruses.
- If the SCCM server isn't responding effectively, no user can install anything. This could damage your operations and affect your business's bottom line.
- When one user's computer is corrupted, they'll fail to receive updates or installations.
- Unless you patch everything in an automated fashion, there's simply no way to keep up with threat actors.
- Even if you manually patch vulnerabilities fast, humans are prone to error. Only automation ensures the highest level of security.
- You can't patch mobile devices like iOS, Android, etc. Another solution would absolutely be required to effectively provision and manage such devices.
- There's no touchless deployment option (e.g. Windows Autopilot). However, touchless deployment is a critical component of a modern, holistic device management approach.
- SCCM requires a steep learning curve for the administrator. You'll need to invest large amounts of time and effort to take full advantage of SCCM's capabilities.
- Other dependencies will require substantial additional time and expertise. For instance, you must have team members that can effectively run Active Directory, WSUS, and an SQL Database – at a minimum.

What are SCCM's requirements?

- **Infrastructure and other software requirements**
  - Active Directory (AD) or Azure AD domain
  - SQL database
  - WSUS
  - If you want no VPN requirement, need to create a manage a cloud management gateway (CMG)
- **Licensing**
  - Included in Microsoft 365 E3, E5, F5 or Enterprise Mobility and Security (EMS) E3 and E5, or with an Intune user subscription license (USL)

Is SCCM right for you?

Large organizations heavily invested in Windows may already use SCCM to manage their Windows devices and workstations. However, if you aren't already using SCCM, you may want to look elsewhere.

Microsoft is modernizing their toolset for device management, and tools like Intune may make more sense for most use cases (look for our next tooling blog to learn more about Intune). That said, managing servers with Intune isn't possible yet. So, you may need to use a tool like SCCM to manage them.

If you're not using 100% Windows in your organization, you'll need several other tools outside of the Microsoft ecosystem to manage your devices and workstations effectively. A better bet for your org would be an all-in-one endpoint management platform that provides visibility through a single pane of glass.