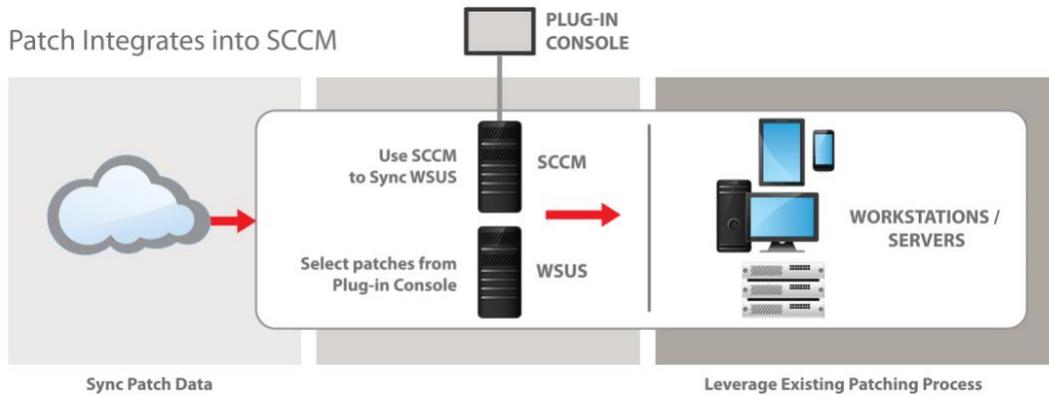


Simplified Patch Management for SCCM



Third-party software accounts for most software vulnerabilities today. But while the third-party updates feature released in Microsoft System Center Configuration Manager (SCCM) 1806 lets you deploy third-party updates using the existing SCCM software update management process, there are limitations to what it can do.

While employing the same infrastructure and workflows built into SCCM, the native plug-in Ivanti® Patch for SCCM provides an easier way to patch third-party apps from the SCCM console. It also adds features that further enhance your experience, like configurable alerts, integration with the SCCM Software Update Groups feature to help you organize and deploy your software updates, and CVE to patch list creation, which lets you easily convert a list of Common Vulnerabilities and Exposures (CVEs) to a list of patches to deploy.

Keep your software up-to-date and get time back in your day to focus on core business goals—without added infrastructure or cost.

Simplify Third-party Patching

As more applications are added to the environment, you devote more time to just keeping the systems up-to-date. Ivanti Patch for SCCM eliminates many of the manual

steps normally taken to define third-party application patches in SCCM for workstations and servers, removing much of the burden from your team and letting them concentrate on major business initiatives.

Patch for SCCM patches hundreds of popular applications: Adobe Reader, Apple iTunes, Google Chrome, Mozilla Firefox, and many more, including difficult updates like Java. And, with Ivanti’s years of experience patching applications in the enterprise, you gain the most accurate pre-tested patch data, giving you the confidence you need to patch critical resources quickly. Patch for SCCM provides you only the enterprise version of the software update and skips the toolbar installation. And, with the reporting capabilities already built into SCCM, you gain significant visibility into the patching process to remain compliant.

Reduce Complexity Without Added Infrastructure and Cost

Natively integrated, Patch for SCCM employs the same workflows used to patch the OS in SCCM to push out third-party application updates. The solution’s simplified approach to patching third-party applications within SCCM requires no expensive added infrastructure, consultants, or services.

Patch data is loaded from the Ivanti Cloud and users can view patch information instantly from within SCCM. You can manually click to deploy patches through SCCM software update packages or combine Patch for SCCM automation with SCCM automatic deployment rules for full third-party update automation.

Features That Sweeten the Pot

Let's take a quick look now at the CVE-to-patch feature. Patch for SCCM can take a vulnerability assessment from whatever vendor you're using—Rapid 7, Tenable, Qualys, BeyondTrust, and so on—find all of the third party patches that relate to those CVEs, and build a list of updates that you can quickly approve for remediation in your environment. It's a huge time-saver replacing today's manual process.

With Patch for SCCM you can take advantage of SCCM Software Update Groups through the plug-in, assigning vendors, products, or product version from any catalog and publishing the group and updates through SCCM. In addition, the scheduler will support dynamic updates to the Software Update Group and its contents.

Become more proactive with the recommended updates feature that uses inventory scans performed by SCCM to provide a list of updates based on software detected in your environment. Through smart filters, these updates can be published manually or automatically depending on your preference.

Save time when deploying scripts and custom files before or after updates. Custom patch templates let you create templates that deploy and apply a script each time an update is released.

Features at a Glance

- Go from vulnerability assessment to published update in minutes rather than hours
- Patch hundreds of the most popular applications, including those difficult to install
- Integrated plug-in for the SCCM console
 - Searchable view of available patches
 - Select patches to publish and expire
 - Smart filtering of patches based on multiple criteria—vendor, product, Information Assurance Vulnerability Alert (IAVA) number, etc.
- Customize patches to comply with company policies

- Check for and download new patch data automatically
- Add updates to a new or existing software update group automatically
- Publish new patches automatically, filtered based on business requirements
- Publish patch metadata separately for compliance, audit, or pre-deployment screening
- Expires a superseded patch with the new version
- Delete or republish updates
- Auto-detect Windows Software Update Server (WSUS)
- View and manage all products published to WSUS
- Digital certificate management—re-authorize expired certificates
- Localized in 10 languages for international support
- Supports authenticating proxies
- Supports disconnected networks
- Installation is easy, fast, and verifies SCCM configuration

Requirements

For system requirements, visit:

https://help.ivanti.com/sh/help/en_US/PAT/24/Topics/System_requirements.htm

For a current list of covered application updates, visit:

<https://forums.ivanti.com/s/article/Shavlik-Patch-for-SCCM-Supported-Products-list>

Learn More

-  **ivanti.com**
-  **1 800 982 2130**
-  **sales@ivanti.com**

Copyright © 2019, Ivanti. All rights reserved. IVI-1623 10/19 MK/DL