# Introduction

The Microsoft Solution Accelerators team has released a set of *Extended DCM Checks* for the Security Compliance Manager (SCM) tool to help you quickly monitor security update status, identify changes to the local Administrators group, and report on the use of application whitelists using desired configuration management (DCM) capabilities of Microsoft® System Center Configuration Manager. Using these checks in conjunction with the traditional baselines from Microsoft provides a robust solution to monitor these key security controls. The controls are designed to help you measure whether the computers in your organization are staying in compliance with these guidelines.

The Extended DCM Checks, which are all Windows PowerShell®-based, require you to set the Windows PowerShell execution policy to RemoteSigned in order to make them function. The checks are designed to be exported from SCM in DCM management packs. These checks differ from most others available in SCM in that they do not include prescriptive values. This is because the best way to implement the countermeasures that correspond to each Extended DCM Check will vary from one organization to another. For example, the *Windows 7 SP1 Security Guide* includes detailed guidance on how to utilize Microsoft AppLocker® policies to limit the risk of malware infecting computers. However, the guide cannot provide a complete list of AppLocker policies that would be suitable for all organizations that use Windows 7, because every organization has a unique collection of business applications.

The rest of this article provides more details about each of the Extended DCM Checks.

# Check Whether AppLocker Is Enabled

This Extended DCM Check uses Windows PowerShell to check whether AppLocker policies are enabled on the system either locally or through Group Policy. The check is designed to be exported in DCM management packs. AppLocker advances the features and functionality of Software Restriction Policies. AppLocker allows you to create rules to allow or deny applications from running based on unique file identities, and to specify which users or groups can run those applications.

Whenever a user installs an unauthorized application on an organization's computer, there are risks associated with that process. At a minimum, the installation process modifies the attack surface of the computer, and creates the risk of starting additional services or opening firewall ports. It is also possible that the application is malicious in intent, and was installed either by mistake or intentionally by the user, which can then position it to launch an attack on other systems after the computer connects to the organization's network. Properly designed and tested AppLocker policies can significantly increase the security of a system, but poorly designed AppLocker policies can make a system difficult or even impossible to use.

You can find information about designing, testing, and deploying AppLocker policies in the *Windows 7 SP1 Security Guide* available in SCM. For more information about AppLocker, see [AppLocker Technical Documentation for Windows 7 and Windows Server 2008 R2](http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=13431).

# Check Administrator Group Membership

This Extended DCM Check uses Windows PowerShell to compare the membership of the local Administrators group on the system with a list of approved accounts. Users with administrative privileges could allow administrative tasks to occur accidentally or maliciously without the knowledge of the individual, as in the following examples:

* A user unknowingly downloads and installs malware from a malicious or infected website.
* A user is tricked into opening an email attachment that contains malware, which runs and possibly installs itself on the computer.
* A removable drive is inserted into the computer and the AutoPlay feature then attempts to run the malicious software automatically.
* A user installs unsupported applications that can affect the computer's performance or reliability.

To effectively use this Extended DCM Check, you must edit the second line of the script to define the list of accounts that are approved for membership in the local Administrator's group using the following steps:

1. Customize the baseline value in SCM with a comma-separated list of approved accounts.
2. Export the baseline with the configuration item as a DCM management pack.
3. Import the DCM management pack into System Center Configuration Manager.
4. Edit the script for this configuration item within System Center Configuration Manager by specifying a comma-separated list of approved accounts between the quotation marks in the following line of the script: $DesiredAdminList = ""

For example, $DesiredAdminList = "CONTOSO/Domain Admins,Administrators"

# Check for Missing Windows Updates

This Extended DCM Check is a Windows PowerShell-based script that checks to determine whether all required updates are installed on the system. You can control what is checked by configuring the appropriate Windows Update settings. In other words, if the Windows Update settings are at their default values, the list of available updates from the Microsoft online Windows Update service will be checked. You can also force this check to run against your internal Microsoft Software Update Services server instead, and control the list of available updates on that server.

The results of the check list any missing updates in the DCM report. The list includes the title and related Microsoft Knowledge Base article of any missing update. Although each version of Windows® is thoroughly tested before release, it is possible that problems will be discovered after a product is released. Configuring the Automatic Updates feature to install updates in a timely manner can help you ensure that the computers in your organization always have the latest critical operating system updates and service packs installed on them.