1. Introduction

The primary sections of the System Center Configuration Manager 2012 console are split up into four categories, as shown below.

The categories are split as follows:

- **Assets and Compliance**
- **Software Library**
- **Monitoring**
- **Administration**

This introduction will define each category and function within each category. Specific operations are covered later in this guide.

**Example Category**

**Example function/function folder**

**Example Sub-function**

**TIP**

This will contain useful information that will assist in using the SCCM console.

**NOTE**

This will contain information that pertains directly to an action within SCCM. Actions that could cause problems will be noted here.
**Assets and Compliance**

**Overview Section**
This section of the SCCM console is where all user and computer objects are managed. Under the “Overview” section on the left side of the screen, you will see many different options for managing the users and computers in your department.

**User Objects** – User objects will be listed by user ID. The user list can be viewed by clicking the “Users” object in the Overview list.

**Machine Objects** – Machine objects will be listed by user ID. The list of all computers can be viewed by clicking the “Devices” object in the Overview list.

The **Device Collections** and **User Collections** objects are also listed in the overview category. These collections can be thought of as folders for individual groups of users or machines. The collections can be created based off of rules, the rules that can be created for collection criteria are nearly limitless. The rules for collections can be based off of active directory groups, OUs, machine names, OS versions, and any other property that can be obtained by a WMI query. The collections can be made with no rules as well, and all machine or user objects can be added manually.

The collections are the basis for software deployment, reporting, software metering and several other SCCM functions. Building an organized collection structure will help greatly with managing the system. If an existing OU structure exists in Active Directory, it is convenient to replicate the structure within SCCM.

The **User State Migration** tool can be used to move an individual user profile from one desktop to another. The use of this tool is not recommended, and not guaranteed to work in all situations. Some data can be lost in the process. It is best to move user profiles manually.

**Asset Intelligence Folder**
Under the Asset Intelligence Folder, one will find Catalog, Inventoried Software, and Hardware Requirements options.

**Catalog** – The catalog is prepopulated with software categories that can be utilized for keeping available software in order. There are nearly a hundred pre-configured categories that can be used.

**Inventoried Software** – If software inventory is enabled, this option will list all software that is currently installed on machines in your department.

**Hardware Requirements** – The hardware requirements library is prepopulated with popular software. This can be used as a reference for any software that is being deployed. Reports can be ran against these objects to validate that hardware in collections meets requirements before software is deployed. New requirements can be created. The prepopulated objects cannot be removed or modified.

---

**TIP**
Avoid distributing software to root collections. This will allow tighter control of software distribution and can prevent potential problems.
**Software Metering**
Software metering can be used to track usage of software. This feature can be used for licensing, and can be used to trim away unwanted/unused software from departments. It allows for a good look at software usage throughout the department. The prepopulated metering options cannot be modified or removed. New metering rules can be created for specific software.

**Compliance Settings Folder**
The *Configuration Items* and *Configuration Baselines* can be used to be sure all computers in a specific location are at a certain level of compliance. The Configuration Items can be made for nearly any object on a machine, and use registry keys for testing. Reports can be ran that show computers that pass and/or fail particular Configuration Items. The Configuration Items can be bundled together in Configuration Baselines for reporting. Configuration baselines can also test for particular software updates.

**Endpoint Protection Folder**
The only available item in the Endpoint Protection folder is *Windows Firewall Policies*. This can be used to deploy specific firewall policies to machines in your department. This could be used instead of Active Directory GPO firewall rules. Please only utilize one or the other. Avoid using simultaneously to avoid potential connectivity problems. Also listed are the *Antimalware Policies*. However, the antimalware policies are to be handled by central administration.

---

**Software Library**

**Overview Section**
In the Overview Section one will find two primary folders; the Application Management folder and the Operating Systems folder. The Software Library section will be used to deploy software to all users and machine objects. It can also be utilized for operating system deployment over the network.

**Application Management Folder**
All software distribution activities will take place here. These applications can only be utilized by the owner of the application. The creator is automatically the owner of the application. The creator will be a member of a group in Active Directory that will tie this to other administrative users within the department. All administrators within a particular department will be able to deploy software. Across departments, applications cannot be modified or seen. If an application is created in Department A, they will be completely separated from the applications created in Department B. Some software will be provided through central administration. Common usage software packages that are used campus-wide will be made available centrally. The deployment and reporting of these applications will also be handled by system administrators in Information Technology.

*Applications* – This category is used to create, control, and modify software deployments. Only .msi files can be created and deployed with the Applications option. Most popular software has an .msi installer available. This is the recommended method for software deployment, and is the most compatible and reliable method of software deployment through SCCM. Utilize .msi installation whenever possible. Applications must be stored and located with network shares. Be sure to take note of where applications are stored for deployment.
Packages – Packages are used when an .msi installer is not available. Packages are usually folders that contain all installation files. The package (folder) is copied down to client computers as a whole. After the package is copied to the target client computer, SCCM runs a “program”. This program is executed via command line string that is set up by the package creator. Often a folder will be copied down that contains a script (.bat, .vbs) that executes automatically via command line. Usually larger programs with multiple parts will be distributed in this manner.

Approval Requests – Some packages can be created that require approval from the SCCM administrator before they can be installed. This can be useful for licensing restrictions. When a user tries to download and install a package with an Approval Request, the request will be sent to the SCCM administrator that configured the requirement. The Approval Requests will be listed in this section. Selecting yes or no for the approval will determine whether or not the user is able to install the software successfully. Users can monitor the status of this request.

Global Conditions – Global Conditions are used as rules that represent business or technical conditions to control how an application is deployed to client devices. For example “All Windows 7 Machines” or “All Machines With < 4 GB of RAM”. These are often configured with WMI queries or registry queries. It is more convenient to use SCCM collections with rules to determine conditions for deployment.

Operating Systems Folder
The objects listed in the Operating Systems Folder are objects that control the deployment of operating system images through SCCM.

Drivers – The Drivers category is used to import device drivers for computer hardware that an operating system will be deployed to through SCCM. The drivers must be .inf or txtsetup.oem format before they are imported. Drivers can be imported individually or in bulk.

Driver Packages – Driver Packages act as folders for individual drivers. The Drive Packages will be attached to OS images when the images are created. Usually the Driver Packages are based on machine type or OS type that is targeted for deployment.

Operating System Images – OS images are created and imported to the SCCM console and can be deployed to systems within SCCM.

Boot Images – Generic boot images used as a basis for creating bootable OS images to be deployed via SCCM.

Task Sequences – Task sequences are used during OS deployment to carry out automated operations before, during, and after OS installation. These tasks can be anything from software installation, profile creation, or even adding the machine to a domain.
Monitoring

Overview Section
The monitoring section is where all reporting and other client status functions will take place. The reporting section also has a summary of antimalware protection in your department. The monitoring section can be one of the most helpful for troubleshooting problems or tracking status of operations within SCCM.

Alerts
SCCM can provide a variety of alerts. Alerts are used primarily for antimalware and antivirus operations.

*Subscriptions* – In this section email subscriptions can be configured for alerts. Any time an alert is triggered, SCCM will automatically send out alerts to any email addresses that have subscriptions configured.

Queries
Queries can be created for any item that is inventoried by SCCM. Any information that is gathered via SCCM inventory actions or WMI can have queries created. This is an advanced function that can allow collections and reports to be generated more quickly based off of queries that are created here.

Reporting
SCCM contains a few hundred reports that can be ran to discover more information about your users and computers. Reports are a good way to measure software deployments, virus activity, machine inventory, and several other categories.

*Reports* – This is the section where all available reports are listed. SCCM contains 423 canned reports for use. Custom reports can also be created. Reports are required to be entered via SQL reporting language.

*Subscriptions* – Reports can be sent to a windows file share in an automated fashion based upon a schedule and format that is selected when configuring the subscription.

Site Hierarchy
This is a graphical representation of the SCCM site servers. Alerts and messages can be viewed here for the SCCM system. This object will only be used by central administration.

System Status
The *Conflicting Records* and *Status Message Queries* objects are only utilized by central administration.

Deployments
This object will give a detailed account of all software that is currently deployed. Selecting a deployment will give a quick summary of deployment status. The information will include success and failure information for software that succeeds or fails to install. The information also contains links to detailed reports which will allow for troubleshooting when applications fail to install.

TIP
Reviewing reports is a great place to start when troubleshooting a problem.
Client Status

Client Activity – This will give a quick summary of clients that are active.

Client Check – This gives a quick look to be sure that all SCCM clients are responding properly to the site server. Another place to check when troubleshooting problems.

Distribution Status

The three list items under distribution status are all different views of the health status of the distribution points and distribution point groups. It allows for a quick view of the distribution points themselves as well as all packages that have been distributed to them.

Endpoint Protection Status

System Center 2012 Endpoint Protection Status

This option provides a health report for the SCEP (formerly FEP) clients. It also shows a summary of any malware or virus activity among computers in the department. Alerts can be configured if a machine needs attention from a technician. This console helps to keep an eye on all antivirus and antimalware clients simultaneously and will overall ensure a safe and clean working environment for machines in the department.

Malware Detected

This option provides a list of all malware detected in viewable collections. It provides an easy way to view what sort of infections are occurring. To learn more about a particular infection/exploit, highlight one in the list and click “Malware Detail” in the ribbon. This will open the Microsoft Virus Encyclopedia and will give detailed information about the infection.

TIP

Check the Endpoint Protection Console daily or set up alerts to quickly be able to mitigate any potential security risks.

Administration

Overview

The administration section is used to monitor the health of the SCCM site servers, as well as make changes to the site systems. This feature will not be used for anything other than central administration tasks.

The Management Console

The management console will be distributed through the SCCM software distribution interface. It can be found under the start menu under “Microsoft System Center 2012.”
2. Collections

Collections are the basis of management within System Center Configuration Manager. Like in active directory, management objects are split between users and computer objects. Software can be deployed to both objects.

When to deploy to users
Deploying software to user objects will be most helpful with software that does not need to go to the entire department. Instead of identifying what computers belong to what users, it is often best to create a user collection that contains the target users. This software will only be available in the “Application Catalog” described later in this guide. Software deployed to users will be available to them anywhere they log in to a machine with the SCCM client installed in the “Application Catalog”.

When to deploy to machines
Deploying software to computer objects will be most helpful with software that has to go to every computer in the department. Software updates and department-specific software will be best distributed with a computer collection. This software will only be available in the “Software Center” described later in this guide.

How to create a collection
All users and computer can be viewed in the Assets and Compliance section of SCCM. The Users and Devices objects contain all users and computer that are available for administration.

To create a new collection, 1. Click the User Collections or Device Collections object within the SCCM console. It is helpful to think of collections as folders for objects. 2. Right click in the pane to the right and select “Create Device (or user) Collection”.

Note
Software deployment reports and anti-virus reports cannot be ran for user objects.
The **Create Device Collection Wizard** will appear that requires a name for the collection, and a limiting collection. The limiting collection is the resource that the collection will pull objects from.

Most operations in SCCM are completed using some type of “Wizard.” These setup wizards all follow the same basic format. The column on the left hand side displays the different sections of the wizard.

After naming the collection, and selecting a **Limiting Collection**, click next. The limiting collection is the collection that the rule will apply to, and pull resources from, when creating this new collection. The “Membership Rules” section allows for the creation of rules for the collection. SCCM 2012 offers a few options for creating membership rules. Click the “Add Rule” dropdown box for the available rules that can be set. This step can be skipped if the collection will have members added/removed automatically. There are four options for creating rules for collection membership.
Membership Rules

Direct Rule – This allows a membership rule to be set for a computer system attribute such as the name or OS version. This rule will not automatically add new machines to collections when the rule is set. It is a direct rule that is applied only when it is set. This will require the collection to have manual modification to the membership any time a change is made.

To create a direct rule, click the “Direct Rule” option from the “Add Rule” drop down menu. The Direct Rule Wizard will appear. Most rules are defined by resource class and attribute name. The “System Resource” allows attributes to be chosen for machine properties. The “User Resource” allows attributes to be chosen for user properties.

To create a direct rule that applies to machines of a certain name, select the “System Resource” resource class and the “Name” attribute. In the string box, enter the name that you are creating a rule for. The % sign can be used as a wildcard. For example to create a direct rule for all computers that start with “it-“, the string value would be “it-%”. Clicking the next button in the wizard will show all available resources that match the criteria. Check the boxes of the objects that need to be added to the collection via this membership rule. See the screen capture below for the example. Finish the wizard to apply the rule.
**Query Rule** – This is the most advanced and customizable way to create a membership rule. A collection with a query rule will automatically update the collection by adding or removing objects based on the rule without manual intervention.

To create a query rule, select “Query Rule” from the “Add Rule” drop down box. Query rules do not have a wizard for creation. They must be crafted by hand or selected from pre-existing rules.

In the Query Rule Properties box, the SQL query can be edited manually. (Creating raw SQL queries is beyond the scope of this documentation.) Or the query can be created by selecting individual properties of objects to query for.

The query setup works a lot like the direct rule membership above. However, the query rule is much more flexible. The first step is to name the Query. This name can be anything, make sure it is applicable to the actual query in case it has to be referenced in the future. Make sure that the Resource class is set to the object that you want to query upon. This will be a user or system resource. Click the “Edit Query Statement” button to open the Query Statement Properties window. The Query Statement Properties window can be seen below.
Click the “Criteria” tab and then click the yellow star button to create a new rule. In the “Criterion Properties” window that opens, click the “Select...” button. There are two drop down boxes that are important for query criteria. The “Attribute Class” and the “Attribute”. Choose an attribute class first, and then choose an attribute. The items in these drop down boxes are WMI queries to the hardware. Any of the information in these lists can be utilized to create a membership rule. Once the attribute class and attribute have been created, click ok to exit back to the “Criterion Properties” window. Now configure the Operator and Value fields. Clicking the Value... button will give the fields that are available. For example, if the collection was based upon all computers with name starting with “it-”, the Operator would be set to “is like” and the Value would be “it-%”. The % sign can be used as a wildcard. The underscore (_) wildcard can be used as well to replace a single character in queries.

Include/Exclude Collections
The other two rules for collection membership are include and exclude collections. Collections can be explicitly included or excluded as a membership rule. This can help for building collections with AND/OR statements without having to build a query. (Ex. “Adobe Flash Collection would include a Java Collection to show computers that have Flash AND Java installed.)

Manually Add Users/Computers to Collections
To add a computer or user to a collection manually, right click on the collection object. In the menu that appears click “Add Selected Items” and add the items to an existing collection. You can also create a collection from this menu.

TIP
The “System Resource” attribute class will give access to the attributes of machine objects. This is one of the most helpful attribute classes for building collections.

NOTE
Collections can be built based off of an existing AD structure with query rules. When creating the query, select the system resource attribute class, and the system OU name attribute.

NOTE
When creating Collections and Software Packages, always place the AD prefix of the department before the name. Example “IT-<collectionname>” for administrative purposes. Collections that do not follow this rule will be deleted periodically by SCCM administrators without warning.
3. Software Deployment

One primary benefit of SCCM is the ability to distribute software from one central location. Active Directory can also be used to deploy software, but it can be a little unfriendly to the application administrator, and there are no reporting functions available. As described in the introduction, there are Applications and Packages. Packages are used to deploy large, multi-file pieces of software, (or anything unavailable as an .msi file) and applications are used exclusively to deploy native Microsoft installer files (.msi).

To deploy software, it first has to be uploaded to a file share. Once uploaded to the share, the program deployment process will be set up through the SCCM console. Once the package/application is set up it will be sent to “Distribution Points”, these are servers that have the sole purpose of copying software down to client computers and reporting information back to the primary SCCM site.

Software Flow: Your hard disk → file share → sccm console → distribution point → deployment

Copy The File to a Drive Share
The file share that will be used to store applications will be given out after the SCCM console has been installed. This file share is only accessible by SCCM admins in your SCCM admin AD group.

Building and Distributing An Application
Click the Software Library category and select the Application Management > Applications object. In the window pane to the right, right click in the white space, and select “Create Application”. Keep the “Automatically detect information…” radio button selected. The “Type” is always going to be Windows Installer (native) the other three options are not supported.

In the “Location:” field, type the file share where the application is stored in the format \Server\share\filename.msi. Be sure all required pieces for the application installation are in the folder with the .msi file. The field should autopopulate as you type so that the path does not have to be entered completely from memory. After the filename has been entered, click next until prompted to “Specify Information About This Application”. Fill out the appropriate fields. “Administrative Catagories:” can be left blank. In the bottom two fields, as seen below, the install string is automatically populated. The /q is for quiet install, meaning that the user has no interaction with the program. This can be removed if the software required manual interaction. For the install behaviour, select install for user. If the software installs for system, it may not be usable by the end user. Install strings unique to the installation can be set here as well.

TIP
Keep a clean and organized file system for your application storage. As time goes on, it will be much easier to manage.
Click next through the remainder of the “Create Application Wizard.” On the last window, click close.

**Distribute Applications or Packages (Distribution Point, DP)**
The application now has to be copied to the distribution points. Right click on the application that was just created, and click “Distribute Content”. Click next until the prompt for the content destination. Add the distribution point by clicking add, distribution point, and check the box next to the appropriate DP, in this case SCCMDPTP01. Click ok to exit back to the content destination screen. Click next until the wizard is complete, and click close. Depending on the size of the file, it may take a little while to copy over to the distribution point server. Check the status by clicking “Content Status” after selecting the application. A pie chart will be shown with status. Click the refresh button or hit f5 every few minutes to get a refreshed view of the status. If the software has been deployed to a user or computer collection, the deployments can be viewed in the “Deployments” tab. These deployments can be deleted from this location as well. Doing so will make the software no longer available for installation.

**Configure Additional Properties for Applications**
.MSI application deployments have some additional properties that can be configured when compared to package deployments. Documentation and additional descriptions can be added for use in the Application Catalog, which will be covered later in this guide.

To attach user documentation, or add additional description properties, go to the Software Library category and select the Application Management > Application and find the application in the right
Right click on the application and click “Properties. This will open the properties of the Application. Many of the options displayed in the properties windows will not need to be modified. Select the “Application Catalog” tab to add additional information.

The “Application Catalog” tab has several properties that may be useful for Application Distributions. This information will be displayed with software listing in the Application Catalog. The (1) **Localized application name** is what the application will be titled in the catalog. (2) **User categories** can be created to sort and file the applications. Some examples of User Categories could be “Web Browsers” or “Utilities”. **User Documentation** can be any documentation such as Word documents, PDF files, or text files. These files should be uploaded to the same file share as the application itself. Users will be able to view the documentation from the application catalog by clicking the (3) “More Details” link in the application catalog. (4) **Link text** is what the documentation link will read instead of the file name of the document. Web URLs can be entered if the documentation is too lengthy or complex for a single piece of documentation. (5) **Localized description** can be used to further detail any information about the application. **Keywords** can be used to link to the application for searches. Unless the selection of applications is large, Keywords may not be needed. (6) **Icon** can be used to display a custom icon for the application that is being distributed in the application catalog. See the image below for details.
Application Catalog With Options Configured

More Details (3) of Application Catalog

Google Chrome Web Browser

**DESCRIPTION**

Google Chrome Web Browser. One alternative to Internet Explorer. The application catalog function of the Software Center may not function with this browser.

**ADDITIONAL INFORMATION**

- **Publisher:** Google
- **Category:** Web Browsers
- **Version:** 32
- **Requires approval:** No
- **Keywords:** Web Browser
- **Replaces:** None
- **Documentation:** [https://support.google.com/chrome/bin/answer.py?hl=en&amp;answer=155518](https://support.google.com/chrome/bin/answer.py?hl=en&amp;answer=155518)

TIP

Information in the “More Details” section of the application catalog. All of the “Additional Information” can be added via the “Application Catalog” tab in the properties of the application. Documentation can be active Web URL links as shown in the example.
Deploying Application or Package To A Machine

To deploy an application, right click on the application that needs to be deployed. Click the “Deploy” menu option. This will open the “Deploy Software Wizard”.

On the “General” page, select a collection to deploy the software to by clicking “Browse…” next to the collection field. The “Select Collection” window will open. The device collections drop down has options for User Collections and Device Collections. Choose the collection the software needs to be deployed to and click OK.

Enter any comments that pertain to the software deployment. Leave the “Automatically distribute content for dependencies” box checked. Click Next. The content destination should already be set, since the distribution points were set when the application was created. If the distribution points are not set, add the distribution point group at this stage.

On the Deployment Settings page, there are options for Action and Purpose of the deployment. The action can either be “Install” or “Uninstall”. The purpose can be “Available” or “Required”. If the software is just made available, it will not automatically install, it will only be made available in the software center on the client machines. If it is required, it can be scheduled to be installed automatically at any time. If the deployment is targeting a collection with user objects, “Require administrative approval request if users request this application” can be checked. This will send a notification to the

NOTE

To make the software available in the Software Center, deploy to Computer Collections. To make the software available in the Application Catalog, deploy to user collections.
Approval Requests section of the SCCM console under Software Library > Application Management > Approval Requests. This option will be grayed out if the application is only targeting machine objects.

The scheduling page can be used to schedule a required install date and time. The availability of the application can be scheduled as well. This way the application can be created one day, or time, and become available at another set date and time.

Set the amount of User Notifications that will be displayed in the “User Experience” page. The options are to display all notifications, or only display notifications when the computer is restarted. The default is to only show notifications upon reboot. These notifications are referring to the “New Software Available” notifications that appear in the system tray on client machines when new software is created in SCCM. There are also two operations that can be selected for operations outside of maintenance windows. No default windows are set, so these options can be left unchecked.

The “Alerts” page can be configured to send out alerts based upon the success rate of the deployed software. The threshold of success or failure can be set in this window as well. In most cases there will be a 5-10% failure rate among deployment unless all systems in the department have identical configurations. Do not enable operations manager alerts or enable maintenance mode on this page. Operations manager is not utilized in this environment.

The summary is a summary of all selected options.

The software will now roll out to the machines in the targeted collections.

Building and Deploying a Package
Copy the file(s) to the assigned drive share. This share will be the same drive share used for storage of applications. Be sure that the package is contained within a subfolder of the drive share. This entire folder is what is going to be defined as the “package.”

Click the Software Library category and select the Application Management > Packages object. In the window pane to the right, right click in the white space, and select “Create Package”.

The “Create Package and Program” wizard will appear. Fill out the Name, Description, Manufacturer, Language, and Version fields with the appropriate information. Check the “This package contains source files” and click the “Browse” button. Example below:

**NOTE**
All software that is deployed that requires multiple files will have to be created as packages. Software that is deployed with an .msi file will automatically detect dependencies within the home folder of the .msi.
After clicking browse, the “Set Source Folder” window will appear. Select the Network Path (UNC Name) radio button, and enter the fileshare path to the folder that will become the install package. This folder can contain as little as a single file, but the entire folder is considered the install package. After the source has been entered, click ok, and click Next.

Program Type – Screen below
In the “Program Type” section, always choose the “Standard Program” option. The Program for Device, and Do not Create Program options are not supported. Click Next.

The next window is a series of fields that are required to create the program. When SCCM copies the folder down, it will run a command line that is executed within the context of the folder. Even though the context is set during the installation, it is always a good idea to point any install scripts to the “Current Directory” of the script itself before executing any further commands.

Set the Name of the program, this is what will display to the end user when they select and execute the program.

Set the Command Line. This is the command that will be ran in the context of the current folder. Clicking “Browse” will open the package folder and allow for the selection of an executable from within the package. Therefore, click the Browse button and select the program this is going to execute. Modify the Command Line if needed with any install switches or additional commands.

Leave “Startup Folder” blank.

The “Run” option is where to set how the program will run. Normal will run the program as if the user simply execute the program from their machine. Minimized and Maximized run the program as either minimized or maximized. The Hidden option will run the program completely invisible to the user.

Select the appropriate option from the “Program can run:” drop down box. The options are “Only when a user is logged on”, “Whether or not the user is logged on”, or “Only when the user is not logged on”.

\[NOTE\]
If the program requires any input from the user at execution, do not select the Hidden option.
Select the appropriate option from the “Run mode:” drop down box. The options are run with administrator rights, or run with user’s rights. Determine what is necessary through testing or software documentation.

Leave the “Drive Mode:” set to “Runs with UNC name”.

Click next to proceed to Requirements.

**Requirements – Screen Below**

In the requirements section, there is an option to “Run another program first”. This option does exactly what is says. It will run another program first if it is required for the installation. This could be used for required software like .NET runtimes or C+ runtimes.

The “Platform Requirements” allow control over what operating systems this is available for. If the software can only be installed on a particular OS, it will only be available for install that OS(s). Take the time to select appropriate platform requirements to prevent accidental installation on server Operating Systems or vice-versa.

Set the amount of disk space that will be needed, and the maximum amount of time the installer can run before the software declares a time-out failure.

**Program Type Screen**

![Specify information about this standard program](image)
Requirements Screen

Summary
Summary list of all options that were set through the Package Wizard. Verify that these settings are correct. Click Next to build the package. Click close to exit the wizard.

The package is now available in the “Packages” section of the Application Management folder.

Distribute Package
See “Building and Deploying a Package” section above. The instructions are the same for applications and packages.

Deployment
See “Deploying an Application or Package to Machine” section above. The instructions are the same for applications and packages.

4. Software Center and Application Catalog

Software Center
The SCCM client has been greatly consolidated and improved in this new version. No longer does the end user have to navigate to the control panel (a frightening place), all software is accessible in the more user-friendly “Software Center.” The software center can be found in the start menu under All Programs.
Microsoft System Center 2012 > Configuration Manager > Software Center. The “Run Advertised Programs” option has been completely eliminated. The only program still in the control panel is the “Configuration Manager” program. It will only need to be accessed for troubleshooting purposes.

**Application Catalog**
The application catalog is accessed through the software center. It is a web-based program distribution center that works much more quickly than the software center, and makes software distribution a snap.

The **Software Center** is split up by four tabs.

**Available Software** – Displayed here are all of the optional or required programs that have not yet been installed. That software will be installed from this location. After the program is installed, it will move to the “Installation Status” section.

**Installation Status** – Displayed here are all of the packages that have been installed, with a status of “Failed”, “

**Installed Software** – Displayed here are all of the applications that have been installed. If the software was distributed as an application (versus as a package), the option to remove the software will be available in this section.

**Options** – Here the end user can set several options for the SCCM client. The SCCM client automatically calculates available maintenance hours based upon machine usage. The user can manually set their active hours in the “Work Information” section. The “Power Management” section allows the user to disable power management features of SCCM if they are utilized. The “Computer Maintenance” section allows the user to only allow the client to install required software outside of set business hours, and can suspend all SCCM activity while the machine is in presentation mode. (No more “New Software Available” notifications during an important presentation.) The “Remote Control” section lists the remote control options that are currently set for the client.

The **Application Catalog** is split up by three tabs as well.

**Application Catalog** – Displayed here are all available packages that are being distributed to user objects. Software can be installed from this location, and this is where users will send application requests for software that requires administrative approval.

**My Application Requests** – When a user requests software. The request is tracked in this section of the application catalog. The denial or approval will be viewed in this section.

**My Devices** – The user can set their machine as their primary usage device. Mobile devices can be set here as well. Due to the lack of mobile device support, mobile device management will not be utilized with SCCM 2012. The primary device can be set if a user uses multiple devices. When configuring a software deployment, the software can be configured to deploy only to “primary devices.” This way if a software deployment has tight licensing requirements, it can be set to only install on “primary devices.” The user can only set one primary device, therefore the licensed software will only be available on one device that the user sets as a primary device at a time.
Software Center – Note the “Find additional applications from the Application Catalog” in upper right.

Application Catalog
5. Endpoint Protection

System Center 2012 Endpoint Protection is tightly combined with the new System Center Configuration Manager. This functionality allows for a near real-time view of malware activity in departments. Use the Endpoint Protection objects found in the “Monitoring” console section.

6. Troubleshooting Information

All logs for the SCCM client are stored in C:\Windows\CCM\Logs. These logs keep track of all SCCM client activity. The execmgr log displays all software install information, and will log any errors that the installer package returns. This is an excellent starting point if software installations fail.

The client stores all software downloaded from the SCCM servers to C:\Windows\ccmcache. If a software installation is failing to install, it sometimes helps to manually go to this location and install the software to try and diagnose the problem.

The client works by pinging the SCCM servers every hour for policy updates. This can be initiated manually by going to Control Panel > Configuration Manager > Actions Tab. Initiate the user and machine policy update and retrieval process to fetch new software. This may be done to accelerate the time between deployment and availability. Useful to speed up testing process.

Error in ccmsetup log 80041002. We must first stop the WMI service. You may see a warning about stopping the WMI. Go ahead and say “yes” to stop the services. Once stopped you will need to rename the %WinDir%\System32\Wbem\Repository folder to “repository.old”. Reboot.

Installation errors from the Application Catalog. Be sure that the browser in use is Internet Explorer. Other web browsers could have “serious” looking errors if software is installed with them. After the update to SP1 in April 2013, this has been less of an issue. However, if there are problems installing software from the web-based application catalog, the first step will be to try the installer with Internet Explorer.

<END OF GUIDE>