**Table of Contents**

[ConfigMgr 2012 – Primary 3](#_Toc423339615)

[Pre-Flight Checks 3](#_Toc423339616)

[Blueprint Deployment 3](#_Toc423339617)

[Manual Tasks 7](#_Toc423339618)

[Environment Variables that are set on Blueprint 8](#_Toc423339619)

[ConfigMgr 2012 – Secondary 9](#_Toc423339620)

[Pre-Flight Checks 9](#_Toc423339621)

[Blueprint Deployment 9](#_Toc423339622)

[Environment Variables that are set on Blueprint 12](#_Toc423339623)

[Manual Tasks 12](#_Toc423339624)

[ConfigMgr 2012 – Site System Server 13](#_Toc423339625)

[Pre-Flight Checks 13](#_Toc423339626)

[Blueprint Deployment 13](#_Toc423339627)

[Environment Variables that are set on Blueprint 13](#_Toc423339628)

[Manual Tasks 13](#_Toc423339629)

[Avecto Defendpoint – Server 14](#_Toc423339630)

[Pre-Flight Checks 14](#_Toc423339631)

[Blueprint Deployment 14](#_Toc423339632)

[Environment Variables that are set on Blueprint 15](#_Toc423339633)

[Manual Tasks 16](#_Toc423339634)

[Active Directory (Resource Domain) 16](#_Toc423339635)

[CSC Service Accounts 16](#_Toc423339636)

[CSC Groups (PERMISSIONS) 16](#_Toc423339637)

[CSC Groups (ROLES) 18](#_Toc423339638)

[Customer Groups 18](#_Toc423339639)

## ConfigMgr 2012 – Primary

### Pre-Flight Checks

1. Edit the following file:

“<DeployShare\deployScript\PC Devices\System Center\Server Provisioning\Primary\ConfigMgr\Scripts\CM2012-Console Config (PRI).ps1"

… and confirm the following static variable(s) are correct:

$SSRS\_DBInstanceName =

1. Verify the following SQL Server requirements:
   1. SVC account has ‘LOCAL ADMIN’ rights (to connect to WMI remotely)
   2. SVC account has SQL ‘SYSADMIN’ rights on ‘MWSPCDEVICES01’ instance (to create CM2012 & WSUS DB)
   3. SVC account has SQL ‘SYSADMIN’ rights on ‘MWSSSRS05’ instance (to create Reporting DB)
   4. Ensure the "SQL Server (MWSPCDEVICES01)" service is started and configured to Log on using either a domain account, NETWORK SERVICE, or LOCAL SYSTEM account
   5. Ensure the “‘NO\_SMS\_ON\_DRIVE.sms” file is placed on all volumes except data and log volumes
   6. Ensure SSRS Instance is online and services are started
2. Ensure the SVC account has rights to create groups under the "Administration/Permissions/PC Devices" and "Administration/Roles/PC Devices" OUs. This is required for the CM2012 Groups that are created during the Blueprint deployment.
3. Ensure the SVC account is added to Global Repository
4. Ensure AD Schema has been extended for CM2012 and the SVC account has full rights to “System/System Management” Container

### Blueprint Deployment

1. Navigate to the “MWS2R2 - ConfigMgr2012\_Primary” Blueprint and click ‘Advanced Deploy’
2. On the ‘Location and Policy’ screen, expand the tree and choose folder you wish to place the provisioned server in. Click NEXT
3. On the ‘Plan’ screen, select the desired values and click NEXT
4. On the ‘Set Variables’ screen untick the “Required” checkbox and click on the ‘Name’ column to sort by Name
5. Confirm the following mandatory variables (other variables not listed because they have default values, and are not mandatory. You can still change them as required)

**Note**: You can ignore “CM\_SECONDARY\_xxxx” variables

| Variable Name | Description | Default Value if not modified |
| --- | --- | --- |
| CM\_SITECODE | Three character identifier for the CM2012 Sitecode (as per design documents) | P01 |
| CM\_SITEDESCRIPTION | Friendly name to describe this server. Will be shown in CM2012 console and appended to the sitecode text | - |
| CM\_SMSINSTALLDIR | Folder that CM2012 will be installed to | C:\SMS\_ConfigMgr |
| COMPONENTID | Three letter abbreviation of the server component being stood up. For SCCM = **SCC** | SCC |
| INSTANCEID | Three number identifier that will make up the server name. This will be the sequential number following the previous server that was deployed. The first Primary server to be stood up will = **001** | - |
| SQL\_COMPONENTID | Three letter abbreviation of the SQL server hosting the SQL Primary server DB | CNN |
| SQL\_DATAFILEPATH | Folder where SQL DB Data files will be created | J:\SQL1\DATA1 |
| SQL\_INSTANCEID | Three number identifier of the SQL server name. The first Primary server to be stood up will = 001 | - |
| SQL\_INSTANCENAME | SQL DB Instance name to use | MWSPCDEVICES01 |
| SQL\_LOGFILEPATH | Folder where SQL DB Log files will be created | J:\SQL1\LOGS1 |
| SQL\_SERVICEPORT | SQL DB port used | 49001 |

1. Click NEXT
2. On the ‘Deploy’ screen click the “Deploy this blueprint” icon
3. Navigate to the new Topology and start the VM Template. This will start the VM and blueprint scripts that will run the following scripts/tasks:

| Script | Task |
| --- | --- |
| MWS2R2 - CM2012 - Static Vars Primary   * 1,800 second timeout * REBOOTS after running | * Sets the following system Environment variables   $CM\_SITECODE  $CM\_SITEDESCRIPTION  $CM\_SMSINSTALLDIR  $SQL\_COMPONENTID  $SQL\_INSTANCEID  $SQL\_DATAFILEPATH  $SQL\_LOGFILEPATH  $SQL\_INSTANCENAME |
| MWS2R2 - CM2012 - Prereqs Common   * 1,800 second timeout * REBOOTS after running | * Copies required source content locally to “C:\Users\<AgilityUserID> * Sets the “$CM\_SERVICEACCOUNT” system Environment variable * Sets the OS Timezone based on the “$OS\_TIMEZONE” Agility variable * Copies CMTrace.exe to “%ProgramFiles%\CMTrace” folder * Defines OS Windows Firewall by running   “$ScriptPath\ConfigMgr\\_SERVER Builds\Windows Firewall\CM2012-Windows Firewall.cmd”   * Installs the following Windows Roles   .NET 3.5 - includes .NET 2.0 and 3.0 (plus KB2966828)  IIS  WDS   * Installs the following Windows Features   BITS, BranchCache, GPMC, RDC, AD Psh Modules, AD Tools, Share & Storage Mgt, File Resource Mgr   * Installs .NET 4.5.2 * Create AD Role and Permissions Groups, including membership and System Management Container rights, by modifying and running:   "$ScriptPath\ConfigMgr\Scripts\CM2012-AD Object-Creation.ps1"   * Add server to required AD group(s) by running:   "$ScriptPath\ConfigMgr\Scripts\CM2012-AD Group-Membership.ps1"   * Defines the following Local Admins   Create and add local account named “PCDevices\_Admin”  <domain>\svc\_sccm\_install  <domain>\ROLE-SCCM-Servers  <domain>\DEL-G-CSC Infrastructure Services   * Add “NO\_SMS\_ON\_DRIVE.sms” to C: * Create “IIS Logs-Cleanup” Scheduled Task, which will run once a month to remove logs older than 60 days * Create “Agility-DelProf” Scheduled Task, which will delete the local Agility user account after 5 days. This is the account used during provisioning |
| MWS2R2 - CM2012 - Prereqs Primary   * 3,600 second timeout * 300 second delayed start * REBOOTS after running | * Validates computer is a member of “ROLE-SCCM-Servers”. If not Blueprint will **QUIT** * Install the following:   Microsoft ADK for Windows 8.1  Microsoft Report Viewer 2012 (CLR Types & MSI)  Microsoft SQL Server 2012 Report Builder  Windows Server Update Services (WSUS) - **Configured to use remote SQL Cluster**  Microsoft System Center Updates Publisher (SCUP) 2011  Microsoft Deployment Toolkit (MDT) 2013 v6.2.5019.0  Microsoft SQL Server 2012 Express SP2 - Management Studio   * Configure SQL server OS and Database Delegation by modifying and running:   "$ScriptPath\ConfigMgr\Scripts\SQL-Server Config.ps1”  If this fails then Blueprint will **QUIT**   * Creates CM2012 Ops Source Repository (F:\ConfigMgr) to house content |
| MWS2R2 - CM2012 - Install Primary   * 5,400 second timeout * 300 second delayed start * REBOOTS after running | * Creates the following CM2012 unattended INI file and updates the following dynamic values %windir%\Debug\ConfigMgr2012\%Computername%\Unattend\_%Computername%.ini   SiteCode  SiteName  SMSInstallDir  SDKServer  PrerequisitePath  ManagementPoint  DistributionPoint  SQLServerName  DatabaseName  SQLDataFilePath  SQLLogFilePath   * Installs CM2012 using above INI file   Monitor “C:\ConfigMgrSetup.log” on the Primary server for installation status   * Installs CM2012 Cumulative Update |
| MWS2R2 - CM2012 - POST Config (PRI)   * 900 second timeout * 300 second delayed start | * Configures CM2012 Console items by updating and running   "$ScriptPath\ConfigMgr\Scripts\CM2012-Console Config (PRI).ps1"  which will perform the following:  Create Device Collection Folders  Create Security Roles  Create Security Admins  Create Security Accounts  Add New Roles  Import x86 and x64 Boot Images  Import OS Images   * Installs the following:   ConfigMgr 2012 Configuration Pack  ConfigMgr 2012 Servicing Extension  ConfigMgr 2012 Support Center |

1. Once completed, please check all steps ran successfully in all scripts within Agility.

### Manual Tasks

* Compliance Baselines
* SUM Sync
* Client Settings
* Site Maintenance Tasks
* Apps
* Boundaries
* Discovery
* NAA
* CliPush settings
* Collections
* Run MDT Integration
* Move console objects to “\_CM2012 Default” folder
* TSeq
* Dist content
* Change SSRS Site Settings to use Windows Creds instead of svc accnt to connect to DataSource

### Environment Variables that are set on Blueprint

The following environment variables are set during the provisioning process:

|  |  |
| --- | --- |
| CM\_ServiceAccount | svc\_SCCM\_Install |
| CM\_SiteCode | P01 |
| CM\_SiteDescription | Primary 01 |
| CM\_SMSInstallDir | F:\SMS\_ConfigMgr |
| SQL\_ActiveNode | DR2DBSCDC001W |
| SQL\_ComponentID | CNN |
| SQL\_DataFilePath | J:\SQL1\DATA1 |
| SQL\_InstanceID | 001 |

## ConfigMgr 2012 – Secondary

### Pre-Flight Checks

1. Ensure CM2012 Primary server is online and healthy.

### Blueprint Deployment

1. Navigate to the “MWS2R2 - ConfigMgr2012\_Secondary/SiteSystem” Blueprint and click ‘Advanced Deploy’
2. On ‘Location and Policy’ screen, expand tree and choose required folder. Click NEXT
3. On ‘Plan’ screen leave, select the desired values and click NEXT
4. On the ‘Set Variables’ screen untick the “Required” checkbox
5. Click on the ‘Name’ column to sort by Name
6. Confirm the following mandatory variables (other variables not listed but because they have default values, they are not mandatory. You can still change them as required)

| Variable Name | Description | Default Value if not modified |
| --- | --- | --- |
| COMPONENTID | Three letter abbreviation of the server component being stood up. For SCCM = **SCC** | SCC |
| INSTANCEID | Three number identifier that will make up the server name. This will be the sequential number following the previous server that was deployed. | - |

1. Click NEXT
2. On the ‘Deploy’ screen click the “Deploy this blueprint” icon
3. The Blueprint will run the following scripts/tasks

| Script | Task |
| --- | --- |
| MWS2R2 - CM2012 - Prereqs Common   * 1,800 second timeout * REBOOTS after running | * Copies required source content locally to “C:\Users\<AgilityUserID> * Sets the “$CM\_SERVICEACCOUNT” system Environment variable * Sets the OS Timezone based on the “$OS\_TIMEZONE” Agility variable * Copies CMTrace.exe to “%ProgramFiles%\CMTrace” folder * Defines OS Windows Firewall by running   “$ScriptPath\ConfigMgr\\_SERVER Builds\Windows Firewall\CM2012-Windows Firewall.cmd”   * Installs the following Windows Roles   .NET 3.5 - includes .NET 2.0 and 3.0 (plus KB2966828)  IIS  WDS   * Installs the following Windows Features   BITS, BranchCache, GPMC, RDC, AD Psh Modules, AD Tools, Share & Storage Mgt, File Resource Mgr   * Installs .NET 4.5.2 * Add server to required AD group(s) by running:   "$ScriptPath\ConfigMgr\Scripts\CM2012-AD Group-Membership.ps1"   * Defines the following Local Admins   Create and add local account named “PCDevices\_Admin”  <domain>\svc\_sccm\_install  <domain>\ROLE-SCCM-Servers  <domain>\DEL-G-CSC Infrastructure Services   * Add “NO\_SMS\_ON\_DRIVE.sms” to C: * Create “IIS Logs-Cleanup” Scheduled Task, which will run once a month to remove logs older than 60 days * Create “Agility-DelProf” Scheduled Task, which will delete the local Agility user account after 5 days. This is the account used during provisioning |
| MWS2R2 - CM2012 - Prereqs Secondary   * 3,600 second timeout * 300 second delayed start * REBOOTS after running | * Install Windows Server Update Services (WSUS) - **Configured to use local computer** |

1. Once the “MWS2R2 - CM2012 - Prereqs Secondary” is complete, this server is now ready to install CM2012
2. Navigate to the Primary VM within Agility and run the “MWS2R2 – AD Global Repository” Operational Script

**Note**: This will set up the scripting framework that subsequent scripts require.

1. Once complete (whilst still on the Primary VM), run the “MWS2R2 - CM2012 - Install Secondary” Operational Script, setting the following mandatory variables:

| Variable Name | Description | Default Value if not modified |
| --- | --- | --- |
| CM\_SECONDARY\_NETBIOSNAME | NetBIOS name of the Secondary Server  Eg DR2SCCAWS002w |  |
| CM\_SECONDARY\_SITECODE | Three character identifier for the CM2012 Sitecode (as per design documents) |  |
| CM\_SECONDARY\_DESCRIPTION | Friendly name to describe this server. Will be shown in CM2012 console and appended to the sitecode text |  |
| CM\_SECONDARY\_INSTALLDIR | Folder that CM2012 will be installed to |  |

1. The following scripts/tasks will run

| Script | Task |
| --- | --- |
| MWS2R2 - CM2012 - Install Secondary   * 900 second timeout * 300 second delayed start * REBOOTS after running | * Validates the following variables are defined. If not **QUIT**   CM\_SECONDARY\_NETBIOSNAME  CM\_SECONDARY\_SITECODE  CM\_SECONDARY\_DESCRIPTION  CM\_SECONDARY\_INSTALLDIR   * Copies additional source content locally to “C:\Users\<AgilityUserID> * Installs CM2012 by modifying and running   “%windir%\Debug\ConfigMgr2012\Unattend\_%computername%.ps1”   * Re-Creates “Agility-DelProf” Scheduled Task on Primary server (under scenarios where Secondary is stood up more than 5 days after Primary was), which will delete the local Agility user account after 5 days. This is the account used during provisioning |

1. Once completed, please check all steps ran successfully in all scripts within Agility.
2. Navigate to the Secondary VM within Agility and run the “MWS2R2 - CM2012 - POST Config (SEC)” Operational Script which will run the following scripts/tasks

| Script | Task |
| --- | --- |
| MWS2R2 - CM2012 - POST Config (SEC)   * 900 second timeout * 300 second delayed start * REBOOTS after running | * Installs CM2012 Cumulative Update |

### Environment Variables that are set on Blueprint

The following environment variables are set during the provisioning process:

### Manual Tasks

## ConfigMgr 2012 – Site System Server

### Pre-Flight Checks

1. Ensure CM2012 Primary server is online and healthy.

### Blueprint Deployment

1. Navigate to the “MWS2R2 - ConfigMgr2012\_Secondary/SiteSystem” Blueprint and click ‘Advanced Deploy’
2. On ‘Location and Policy’ screen, expand tree and choose required folder. Click NEXT
3. On ‘Plan’ screen leave, select the desired values and click NEXT
4. On the ‘Set Variables’ screen untick the “Required” checkbox
5. Click on the ‘Name’ column to sort by Name
6. Confirm the following mandatory variables (other variables not listed but because they have default values, they are not mandatory. You can still change them as required)

### Environment Variables that are set on Blueprint

The following environment variables are set during the provisioning process:

### Manual Tasks

## Avecto Defendpoint – Server

### Pre-Flight Checks

1. Ensure SSRS Instance in SQL Cluster is online and services are started.
2. Ensure the SCCM Primary Server has been stood up (as it creates required AD Groups as part of that Blueprint)

### Blueprint Deployment

1. Navigate to the “MWS2R2 – Avecto Defendpoint” Blueprint and click ‘Advanced Deploy’
2. On ‘Location and Policy’ screen, expand tree and choose required folder. Click NEXT
3. On ‘Plan’ screen leave, select the desired values and click NEXT
4. On the ‘Set Variables’ screen untick the “Required” checkbox
5. Confirm the following mandatory variables (other variables not listed but because they have default values, they are not mandatory. You can still change them as required)

| Variable Name | Description | Default Value if not modified |
| --- | --- | --- |
| COMPONENTID | Three letter abbreviation of the server component being stood up. For Avecto Defendpoint = **ADP** | ADP |
| INSTANCEID | Three number identifier that will make up the server name. This will be the sequential number following the previous server that was deployed. | - |

1. Click NEXT
2. On the ‘Deploy’ screen click the “Deploy this blueprint” icon
3. The Blueprint will run the following scripts/tasks

| Script | Task |
| --- | --- |
| MWS2R2 - Avecto – Prereqs   * 1,800 second timeout * REBOOTS after running | * Copies required source content locally to “C:\Users\<AgilityUserID> * Sets the “$CM\_SERVICEACCOUNT” system Environment variable * Sets the OS Timezone based on the “$OS\_TIMEZONE” Agility variable * Installs the following Windows Roles   .NET 3.5 - includes .NET 2.0 and 3.0 (plus KB2966828)   * Installs the following Windows Features   BITS, GPMC, AD Tools   * Defines the following Local Admins   Create and add local account named “PCDevices\_Admin”  <domain>\svc\_sccm\_install  <domain>\DEL-G-CSC Infrastructure Services   * Create “Agility-DelProf” Scheduled Task, which will delete the local Agility user account after 5 days. This is the account used during provisioning |
| MWS2R2 - Avecto - Defendpoint Install   * 5,400 second timeout * 300 second delayed start * REBOOTS after running | * Installs Defendpoint by running   “$ScriptPath\Defend Point\DefendpointManagementConsoles\_x64.exe” |

1. Once completed, please check all steps ran successfully in all scripts within Agility.
2. Manual Tasks include:

* Create Defendpoint policies to deploy to the PC Devices

### Environment Variables that are set on Blueprint

The following environment variables are set during the provisioning process:

### Manual Tasks

## Active Directory (Resource Domain)

### CSC Service Accounts

| Name | Description |
| --- | --- |
| svc\_1E\_Install | 1E provisioning account |
| svc\_Avecto\_DataAdmin |  |
| svc\_Avecto\_Install | Avecto provisioning account plus DatabaseCreator |
| svc\_Avecto\_Parser |  |
| svc\_Avecto\_ReportRdr |  |
| svc\_SCCM\_Install | ConfigMgr provisioning account |
| svc\_SCCM\_JoinDom | ConfigMgr OSD account used to join devices to the domain |
| svc\_SCCM\_NetAccess | ConfigMgr Network Access account |
| svc\_SCCM\_SQL | ConfigMgr SQL broker account for SSRS |
| svc\_SCCM\_SUP | ConfigMgr SUP account used as proxy user to sync updates with Microsoft |

### CSC Groups (PERMISSIONS)

| Name | Type | Description | Default Members |
| --- | --- | --- | --- |
| PERM-L-SCCM-Admins | Domain Local | Members are admins on CM2012 servers and console | ROLE-L-SCCM-Infrastructure Admins |
| PERM-L-SCCM-Package Admins | Domain Local | Members have READ rights to SQL Jobs | ROLE-L-AppSense-Policy Admins |
| PERM-L-SCCM-Servers | Domain Local | Contains all CM2012 Servers | <all CM2012 servers> |
| PERM-L-SQL-PCDEVICES Admins | Domain Local | Members have FULL rights to SQL MWSPCDEVICES Instance | ROLE-L-SCCM-Infrastructure Admins  svc\_SCCM\_SQL |
| PERM-L-SQL-PCDEVICES Job Monitoring | Domain Local | Members have READ rights to SQL Jobs |  |
| PERM-L-SQL-PCDEVICES Read | Domain Local | Members have READ rights to SQL MWSPCDEVICES Instance |  |

### CSC Groups (ROLES)

| Name | Type | Description | Default Members |
| --- | --- | --- | --- |
| ROLE-L-AppSense-Policy Admins | Domain Local | Members have rights to export policies from AppSense Console to CM2012 |  |
| ROLE-L-SCCM-Infrastructure Admins | Domain Local | Performs SCCM Infrastructure, SCCM escalation support |  |
| ROLE-L-SCCM-Images Admins | Domain Local | Full permissions to Image management in SCCM |  |
| ROLE-L-SCCM-Images Deploy | Domain Local | Members can prestage PCs in SCCM (ie comp assoc) and have rights to deploy SOE |  |
| ROLE-L-SCCM-Package Admins | Domain Local | Full permissions to Package management in SCCM |  |
| ROLE-L-SCCM-Patch Admins | Domain Local | Full permissions in Software Updates node of SCCM |  |
| ROLE-L-SCCM-Report Admins | Domain Local | Full permissions on Report management in SCCM |  |
| ROLE-L-SCCM-Report Users | Domain Local | Members can open Reporting Website |  |
| ROLE-L-SCCM-Viewers | Domain Local | Read only to all sections of SCCM |  |

### Customer Groups

| Name | Type | Description | Default Members |
| --- | --- | --- | --- |
| Avecto-ADP-Baseline | Domain Local | Users in this group receive Defendpoint BASELINE policy |  |
| Avecto-ADP-Guest-Guest | Domain Local | Users in this group receive Defendpoint GUEST policy |  |
| Avecto-ADP-Guest-Knowledge Worker | Domain Local | Designed to segment Guests from Production users to receive Defendpoint KNOWLEDGE WORKER policy |  |
| Avecto-ADP-Guest-Task Worker | Domain Local | Designed to segment Guests from Production users to receive Defendpoint TASK WORKER policy |  |
| Avecto-ADP-Knowledge Worker | Domain Local | Users in this group receive Defendpoint KNOWLEDGE WORKER policy |  |
| Avecto-ADP-Task Worker | Domain Local | Users in this group receive Defendpoint TASK WORKER policy |  |
| Avecto-GPO-Event Subscription Computers | Domain Local | Computers in this group will receive Avecto GPO. Used for Security Filtering |  |