# Extended System Discovery – Fix Company Attributes

## Summary

We will implement PowerShell script on a scheduled task to identify and correct missing information in SCCM Discovery data. It will be executed automatically every hour on a daily basis starting at 4 AM for a duration of 12 hours.

There are custom AD attributes named companyAttributeMachineCategory and companyAttributeMachineType which identify critical production systems and is used for identifying systems that are non-standard. Not all systems use these properties but if a system in an AD domain has values for these attributes but SCCM does not then the script will create an SCCM discovery record to fix the information in SCCM..

**Examples of the two companyAttributes**

|  |  |
| --- | --- |
|  |  |
| MachineType | MachineCategory |
| GXP-LABPC | NON-STANDARD |
| IA-HOL | NON-STANDARD |
| LABPC | NON-STANDARD |

**Solution Process**

To resolve this issue we have created PowerShell script that will synchronize SCCM data with Active Directory for SCCM records whose company attribute values do not match Active Directory. It will be executed automatically on a daily basis

* For each domain we manage, identify computer accounts which have values for either of the two company attributes
* For each computer identified lookup the SCCM data for the two company attributes
* If the data does not match then use AD data to write an SCCM discovery record
* Write a log file in the C:\Temp\TempDDRs folder that records the script processing and logic when it is run
* Copy the DDR files to the SCCM CAS site server for processing

## Business Case

Ensure that critical data used for administration of clients within SCCM is correct

## Systems Impacted

SCCM 2012 Production

## Service Impact Assessment

* What is the business impact?
  + No business impact is expected
* Where is the business/end users located?
  + The SCCM data will be corrected for all systems in all domains that have incorrect data in SCCM.
* Where is the location of activity (where the CI's are located)?
  + This will be executed from a schedule task executing a PowerShell script
* What is the scheduling and length of the actual outage/performance degradation?
  + There will be no outage and the script will be scheduled to run daily
* Is the appropriate communications planned before a change will be implemented (Business/Accenture/etc.)?
  + This will be communicated to the SCCM Global Administrators prior to implementation
* Is the appropriate communications planned after a change is completed (Business/Accenture/etc.)?
  + The change will be announced at the SCCM Community Meeting
* Does this change have a GxP impact and if yes is Quality aware of the change?
  + There is no expected GxP impact with this change but SCCM clients that were previously unmanaged due to the missing data will become available for deployments and reporting after the data is corrected. These clients may receive previously deployed software or software updates that they should have received in the past
* What are the dependencies for this change?
  + Access to read Active Directory, MS Orchestrator, Access to the SCCM\_P00 and SCCM\_EXT databases. Access to the custom tables in the SCCM\_EXT database used for domain identification and change logging
* Can the change lead to possible collisions?
  + We do not know of any other changes that this will interfere with
* Does the change have transversal impact?
  + Unknown
* Has the change been successfully tested in a DEV/Test environment
  + The change has been developed and tested in the SCCM 2012 PRE2PROD. A peer reviewed execution of this change was conducted in the SCCM 2012 PREPROD environment

## Test Plan

See Test Case document located here

[http://wssamer.sanofi.com/ws/AutomationCenterProvTools/Documents/Change%20Requests/Extended%20AD%20Discovery%20-%20Fix%20Company%20Attributes/Test%20Case%20-%20Extended%20System%20Discovery%20Fix%20Company%20Attributes.docx](http://wssamer.sanofi.com/ws/AutomationCenterProvTools/Documents/Change%20Requests/_ARCHIVE/Extended%20AD%20Discovery%20-%20Fix%20Company%20Attributes/Test%20Case%20-%20Extended%20System%20Discovery%20Fix%20Company%20Attributes.docx)

## Communication Plan

Notify the SCCM Global Administrators of the intended change and its execution. Notify the general SCCM community at the next SCCM Community Meeting.

## Detailed Implementation (Installation) Plan

### Verify the Active Directory Module is Accessible

1. From PowerShell, run the following command

Get-Module –ListAvailable

It may take a while to run

1. If the module named ActiveDirectory is not listed in the output then copy folder   
   PTSSORCH01 C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\ActiveDirectory to the same location on the destination Orchestrator server

### Copy the SMS SDK Runtime DLL

1. From XSNW10X065B C:\TEMP\TempDDRs, copy the two folders OldDLLs and NewDLLs to the same location on the PROD Orchestrator

### Copy the PowerShell script to the Orchestrator server

1. From XSNW10X065B E:\PowerShell\_Tasks\ExtendedSystemDiscovery, copy the file Fix-CompanyAttributes.ps1 and the Invoke-FixCompanyAttributes.bat to the Orchestrator Production Server XSPW10X060S E:\PowerShell\_Tasks\ExtendedSystemDiscovery

### Modify the constants in the script to reflect the environment it is being used in

1. Edit the file Fix-CompanyAttributes.ps1 in PowerShell ISE

In the beginning of the \*\*\*\* MAIN \*\*\*\* section, edit the variables below for the environment it is being used for  
# Variables to modify per environment

$CASSiteServer = "XSPW10W200P"

$CASSiteCode = "P00"

$CASSQLServer = "XSPW10W207S"

$DefaultDDRSiteCode = "P00" # used for clients with no assigned site code

$DDRTargetFolder = "\D$\SCCMServer\inboxes\auth\ddm.box\" #must include trailing \

### Setup the Scheduled Task to Invoke the PowerShell script every morning at 7AM GMT-5

1. Create a new Scheduled task on XSPW10X060S
   1. Name = Invoke - Fix Company Attributes
   2. Trigger = Daily, 4AM
   3. Repeat Every Hour for 12 hours
   4. Action Command Line   
      E:\PowerShell\_Tasks\ExtendedSystemDiscovery\Invoke-FixCompanyAttributes.bat
   5. Run As = PHARMA\svc\_SCRB\_PROD
   6. Run = Whether or not a user is logged in
   7. Run with highest privileges = enabled
   8. Configure For : Win 7 & Server 2008 R2
   9. Save and supply the password for PHARMA\svc\_SCRB\_PROD

### Run the scheduled task and collect evidence

1. Run the scheduled task and wait for it to complete
2. Collect data for the post execution test results

### Back Out Plan

1. Stop the Scheduled Task from automatic execution by disabling it.