15.08.2013

David O'Brien

David LAB

15.08.2013

System Center 2012 Configuration Manager inventory report for Customer David LAB



Table of Contents

[Summary of all Sites in this Hierarchy 3](#_Toc364289888)

[Configuration Summary for Site PRI 3](#_Toc364289889)

[Site Maintenance Tasks for Site PRI 3](#_Toc364289890)

[Summary of Management Points for Site PRI 3](#_Toc364289891)

[Summary of Distribution Points for Site PRI 3](#_Toc364289892)

[Summary of Software Update Point Servers for Site PRI 4](#_Toc364289893)

[Summary of Hierarchy Wide Configuration 4](#_Toc364289894)

[Summary of Site Boundaries 4](#_Toc364289895)

[Summary of Site Boundary Groups 4](#_Toc364289896)

[Summary of Custom Client Device Settings 4](#_Toc364289897)

[Administrative Users 7](#_Toc364289898)

[Custom Security Roles 7](#_Toc364289899)

[Configured Accounts 7](#_Toc364289900)

[Assets and Compliance 7](#_Toc364289901)

[Summary of User Collections 7](#_Toc364289902)

[Summary of Device Collections 7](#_Toc364289903)

[Compliance Settings 7](#_Toc364289904)

[Configuration Items 7](#_Toc364289905)

[Configuration Baselines 7](#_Toc364289906)

[User Data and Profiles 7](#_Toc364289907)

[Endpoint Protection 8](#_Toc364289908)

[Antimalware Policies 8](#_Toc364289909)

[Windows Firewall Policies 11](#_Toc364289910)

[Software Library 11](#_Toc364289911)

[Applications 11](#_Toc364289912)

[Packages 11](#_Toc364289913)

[Driver Packages 11](#_Toc364289914)

[Operating System Images 12](#_Toc364289915)

[Operating System Installers 12](#_Toc364289916)

[Boot Images 12](#_Toc364289917)

[Task Sequences 13](#_Toc364289918)

# Summary of all Sites in this Hierarchy

The following Primary Sites are installed:

|  |  |  |
| --- | --- | --- |
| **Site Name** | **Site Code** | **Version** |
| Primary | PRI | 5.00.7884.1000 |

# Configuration Summary for Site PRI

## Site Maintenance Tasks for Site PRI

|  |  |
| --- | --- |
| **Task Name** | **State** |
| Backup SMS Site Server | True |
| Check Application Title with Inventory Information | True |
| Clear Undiscovered Clients | False |
| Delete Aged Application Request Data | True |
| Delete Aged Application Revisions | True |
| Delete Aged Client Operations | True |
| Delete Aged Collected Files | True |
| Delete Aged Computer Association Data | True |
| Delete Aged Delete Detection Data | True |
| Delete Aged Device Wipe Record | True |
| Delete Aged Discovery Data | True |
| Delete Aged Distribution Point Usage Stats | True |
| Delete Aged Enrolled Devices | True |
| Delete Aged EP Health Status History Data | True |
| Delete Aged Exchange Partnership | True |
| Delete Aged Inventory History | True |
| Delete Aged Log Data | True |
| Delete Aged Metering Data | True |
| Delete Aged Metering Summary Data | True |
| Delete Aged Notification Server History | True |
| Delete Aged Notification Task History | True |
| Delete Aged Replication Data | True |
| Delete Aged Replication Summary Data | True |
| Delete Aged Status Messages | True |
| Delete Aged Threat Data | True |
| Delete Aged Unknown Computers | True |
| Delete Aged User Device Affinity Data | True |
| Delete Inactive Client Discovery Data | False |
| Delete Obsolete Alerts | True |
| Delete Obsolete Client Discovery Data | False |
| Delete Obsolete Forest Discovery Sites And Subnets | True |
| Evaluate Provisioned AMT Computer Certificates | True |
| Monitor Keys | True |
| Rebuild Indexes | True |
| Summarize File Usage Metering Data | True |
| Summarize Installed Software Data | True |
| Summarize Monthly Usage Metering Data | True |

## Summary of Management Points for Site PRI

CM12.do.local

## Summary of Distribution Points for Site PRI

**CM12.do.local**

* Disk information:
* **Partition C:**
* 99.66 GB Size
* 37.46 GB Free Space
* **Hardware Info:**
* This server has a total of 3 GB RAM.
* PXE Enabled
* Supports unknown machines: false

This Distribution Point is a member of the following DP Groups:

* on-premises

## Summary of Software Update Point Servers for Site PRI

CM12.do.local

|  |  |  |  |
| --- | --- | --- | --- |
| **Property Name** | **Value** | **Value 1** | **Value 2** |
| AnonymousProxyAccess | 1 |  |  |
| DBServerName | 0 |  | CM12.do.local\MICROSOFT##WID |
| Enabled | 1 |  |  |
| IsINF | 0 |  |  |
| IsIntranet | 1 |  |  |
| NLBVIP | 0 |  |  |
| ProxyName | 0 |  |  |
| ProxyServerPort | 80 |  |  |
| PublicVIP | 0 |  |  |
| SSLWSUS | 0 |  |  |
| UseParentWSUS | 0 |  |  |
| UseProxy | 0 |  |  |
| UseProxyForADR | 0 |  |  |
| UserName | 0 |  |  |
| WSUSAccessAccount | 0 |  |  |
| WSUSIISPort | 8530 |  |  |
| WSUSIISSSLPort | 8531 |  |  |

# Summary of Hierarchy Wide Configuration

## Summary of Site Boundaries

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Boundary Name** | **Boundary Type** | **Associated Site Systems** | **Value** | **Assigned Site** |
| internal subnet | IP Subnet | CM12.do.local | 172.16.0.0 | PRI |
| AD Site | Active Directory Site | CM12.do.local | Default-First-Site-Name | PRI |

## Summary of Site Boundary Groups

**intern**

* Description:
* Member names: internal subnet
* Member names: AD Site

## Summary of Custom Client Device Settings

**Client Settings Name: Notebook**

* Client Settings Description:
* Client Settings ID: 16777217
* Client Settings Priority: 1
* This is a custom client Device Setting.

Configurations

* Software Inventory
* Enable software inventory on clients: True

Schedule software inventory and file collection: Occurs every 1 days effective 02/01/1970 00:00:00

Inventory reporting detail: Full details

* Inventory these file types:
* Do not exclude WinDir and Subfolders

---------------------

* Remote Tools
* Enable Remote Control on clients: Enabled: Domain.
* Users can change policy or notification settings in Software Center: False
* Allow Remote Control of an unattended computer: True
* Prompt user for Remote Control permission: True
* Grant Remote Control permission to local Administrators group: True

Access level allowed: Full Control

* Permitted viewers of Remote Control and Remote Assistance:
* DO\Domain Admins
* Show session notification icon on taskbar: True
* Show session connection bar: True

Play a sound on client: Beginning and end of session.

* Manage unsolicited Remote Assistance settings: False
* Manage solicited Remote Assistance settings: False

Level of access for Remote Assistance: None.

* Manage Remote Desktop settings: True
* Allow permitted viewers to connect by using Remote Desktop connection: False
* Require network level authentication on computers that run Windows Vista operating system and later versions: True

---------------------

* Computer Agent
* Deployment deadline greater than 24 hours, remind user every (hours): 48
* Deployment deadline less than 24 hours, remind user every (hours): 4
* Deployment deadline less than 1 hour, remind user every (minutes): 15
* Default application catalog website point:
* Add default Application Catalog website to Internet Explorer trusted sites zone: True
* Allow Silverlight applications to run in elevated trust mode: True
* Organization name displayed in Software Center: CM12 LAB
* Install Permissions: All Users
* Suspend Bitlocker PIN entry on restart: Never
* Additional software manages the deployment of applications and software updates: No
* Powershell execution policy: Bypass
* Show notifications for new deployments: Yes
* Software Metering
* Enable software metering on clients: True

Schedule data collection: Occurs every 1 days effective 02/01/1970 00:00:00

---------------------

* Software Updates
* Enable software updates on clients: True

Software Update scan schedule: Occurs every 1 days effective 02/01/1970 00:00:00

Schedule deployment re-evaluation: Occurs every 7 days effective 02/01/1970 00:00:00

When any software update deployment deadline is reached, install all other software update deployments with deadline coming within a specified period of time: No.

---------------------

* Client Policy
* Client policy polling interval (minutes): 60
* Enable user policy on clients: True
* Enable user policy requests from Internet clients: False

---------------------

* Hardware Inventory
* Enable hardware inventory on clients: True
* Hardware inventory schedule: Occurs every 7 days effective 02/01/1970 00:00:00

---------------------

* Software Deployment
* Schedule re-evaluation for deployments: Occurs every 2 hours effective 02/01/1970 00:00:00

---------------------

* Power Management
* Allow power management of clients: True
* Allow users to exclude their device from power management: False
* Enable wake-up proxy: False

---------------------

* Endpoint Protection
* Manage Endpoint Protection client on client computers: True
* Install Endpoint Protection client on client computers: True
* Automatically remove previously installed antimalware software before Endpoint Protection is installed: True
* Allow Endpoint Protection client installation and restarts outside maintenance windows. Maintenance windows must be at least 30 minutes long for client installation: False
* For Windows Embedded devices with write filters, commit Endpoint Protection client installation (requires restart): True
* Suppress any required computer restarts after the Endpoint Protection client is installed: True
* Allowed period of time users can postpone a required restart to complete the Endpoint Protection installation (hours): 24
* Disable alternate sources (such as Microsoft Windows Update, Microsoft Windows Server Update Services, or UNC shares) for the initial definition update on client computers: True

---------------------

## Administrative Users

Enumerating administrative users:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Account name** | **Account Type** | **Security Roles** | **Security Scopes** | **Collections** |
| DO\adobrien | User | Full Administrator | All | All Systems All Users and User Groups |
| DO\asobrien | User | Operating System Deployment Manager | Default | Davids\_Notebook Davids\_Surface |

## Custom Security Roles

There are no custom built security roles.

## Configured Accounts

Enumerating all accounts used for specific tasks.

|  |  |  |
| --- | --- | --- |
| **User Name** | **Account Usage** | **Site Code** |
| do\adobrien | SMS SRS Reporting Point SMS\_AD\_SYSTEM\_DISCOVERY\_AGENT SMS\_AD\_USER\_DISCOVERY\_AGENT SMS\_CLIENT\_CONFIG\_MANAGER Software Distribution | PRI |

# Assets and Compliance

## Summary of User Collections

There are 3 User Collections.

## Summary of Device Collections

There are 11 Device collections.

## Compliance Settings

### Configuration Items

Enumerating Configuration Items:

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Last modified** | **Last modified by** | **CI ID** |
| Integriert | 07/25/2013 13:44:03 |  | 16777398 |

### Configuration Baselines

There are no Configuration Baselines configured.

### User Data and Profiles

There are no User Data and Profile configurations configured.

## Endpoint Protection

### Antimalware Policies

**Default Client Antimalware Policy**

Description: Settings enforced across the entire network of clients unless otherwise specified by a custom settings deployment

* **Scheduled Scans**
* Run a scheduled scan on client computers: True
* Scan type: Quick Scan
* Scan day: Saturday
* Scan time: 2:00
* Run a daily quick scan on client computers: True
* Daily quick scan schedule time: 2:00
* Check for the latest definition updates before running a scan: True
* Start a scheduled scan only when the computer is idle: False
* Force a scan of the selected scan type if client computer is offline during two or more scheduled scans: True
* Limit CPU usage during scans to (%): 50
* **Scan settings**
* Scan email and email attachments: True
* Scan removable storage devices such as USB drives: False
* Scan network drives when running a full scan: False
* Scan archived files: True
* Allow users to configure CPU usage during scans: False

User control of scheduled scans: No control

* **Default Actions**

Severe threats: Quarantine

High threats: Quarantine

Medium threats: Quarantine

Low threats: Quarantine

* **Real-time protection**
* Enable real-time protection: True
* Monitor file and program activity on your computer: True

Scan system files: Scan incoming and outgoing files

* **Exclusion settings**
* Excluded files and folders:
* %windir%\SoftwareDistribution\Datastore\Datastore.edb
* %windir%\SoftwareDistribution\Datastore\Logs\Res\*.log
* %windir%\SoftwareDistribution\Datastore\Logs\Res\*.jrs
* %windir%\SoftwareDistribution\Datastore\Logs\Edb.chk
* %windir%\SoftwareDistribution\Datastore\Logs\Tmp.edb
* %windir%\Security\Database\\*.edb
* %windir%\Security\Database\\*.sdb
* %windir%\Security\Database\\*.log
* %windir%\Security\Database\\*.chk
* %windir%\Security\Database\\*.jrs
* %ALLUSERSPROFILE%\NTuser.pol
* %SystemRoot%\System32\GroupPolicy\Machine\registry.pol
* %SystemRoot%\System32\GroupPolicy\User\registry.pol
* Excluded file types:
* Excluded processes:
* **Advanced**
* Create a system restore point before computers are cleaned: False
* Disable the client user interface: False
* Show notifications messages on the client computer when the user needs to run a full scan, update definitions, or run Windows Defender Offline: False
* Delete quarantined files after (days): 30
* Allow users to configure the setting for quarantined file deletion: False
* Allow users to exclude file and folders, file types and processes: False
* Allow all users to view the full History results: False
* Enable reparse point scanning: False
* Randomize scheduled scan and definition update start time (within 30 minutes): False
* **Threat overrides**
* **Microsoft Active Protection Service**

Microsoft Active Protection Service membership type: Do not join MAPS

* Allow users to modify Microsoft Active Protection Service settings: False
* **Definition Updates**
* Check for Endpoint Protection definitions at a specific interval (hours): (0 disable check on interval) 8
* Check for Endpoint Protection definitions daily at: (Only configurable if interval-based check is disabled) 2:00
* Force a definition update if the client computer is offline for more than two consecutive scheduled updates: False
* Set sources and order for Endpoint Protection definition updates:
* AMDefinitionFallbackOrderFromCM
* InternalDefinitionUpdateServer
* MicrosoftUpdateServer
* MMPC
* If Configuration Manager is used as a source for definition updates, clients will only update from alternative sources if definition is older than (hours): 72
* If UNC file shares are selected as a definition update source, specify the UNC paths:

**SCEP2012 Standard Desktop**

Description: SCEP2012 Standard Desktop

* **Default Actions**

Severe threats: Recommended

High threats: Recommended

Medium threats: Recommended

Low threats: Recommended

* **Scheduled Scans**
* Run a scheduled scan on client computers: True
* Scan type: Quick Scan
* Scan day: Saturday
* Scan time: 3:00
* Run a daily quick scan on client computers: False
* Daily quick scan schedule time: 0:00
* Check for the latest definition updates before running a scan: True
* Start a scheduled scan only when the computer is idle: True
* Force a scan of the selected scan type if client computer is offline during two or more scheduled scans: False
* Limit CPU usage during scans to (%): 50
* **Exclusion settings**
* Excluded files and folders:
* %windir%\SoftwareDistribution\Datastore\Datastore.edb
* %windir%\SoftwareDistribution\Datastore\Logs\Res\*.log
* %windir%\SoftwareDistribution\Datastore\Logs\Res\*.jrs
* %windir%\SoftwareDistribution\Datastore\Logs\Edb.chk
* %windir%\SoftwareDistribution\Datastore\Logs\Tmp.edb
* %windir%\Security\Database\\*.edb
* %windir%\Security\Database\\*.sdb
* %windir%\Security\Database\\*.log
* %windir%\Security\Database\\*.chk
* %windir%\Security\Database\\*.jrs
* %ALLUSERSPROFILE%\NTuser.pol
* %SystemRoot%\System32\GroupPolicy\registry.pol
* Excluded file types:
* Excluded processes:
* **Microsoft Active Protection Service**

Microsoft Active Protection Service membership type: Do not join MAPS

* Allow users to modify Microsoft Active Protection Service settings: False
* **Real-time protection**
* Enable real-time protection: True
* Monitor file and program activity on your computer: True

Scan system files: Scan incoming and outgoing files

* **Advanced**
* Create a system restore point before computers are cleaned: False
* Disable the client user interface: False
* Show notifications messages on the client computer when the user needs to run a full scan, update definitions, or run Windows Defender Offline: False
* Delete quarantined files after (days): 0
* Allow users to configure the setting for quarantined file deletion: False
* Allow users to exclude file and folders, file types and processes: False
* Allow all users to view the full History results: False
* Enable reparse point scanning: False
* Randomize scheduled scan and definition update start time (within 30 minutes): True
* **Definition Updates**
* Check for Endpoint Protection definitions at a specific interval (hours): (0 disable check on interval) 0
* Check for Endpoint Protection definitions daily at: (Only configurable if interval-based check is disabled) 2:00
* Force a definition update if the client computer is offline for more than two consecutive scheduled updates: True
* Set sources and order for Endpoint Protection definition updates:
* AMDefinitionFallbackOrderFromCM
* InternalDefinitionUpdateServer
* MicrosoftUpdateServer
* MMPC
* If Configuration Manager is used as a source for definition updates, clients will only update from alternative sources if definition is older than (hours): 72
* If UNC file shares are selected as a definition update source, specify the UNC paths:
* **Scan settings**
* Scan email and email attachments: True
* Scan removable storage devices such as USB drives: False
* Scan network drives when running a full scan: False
* Scan archived files: True
* Allow users to configure CPU usage during scans: False

User control of scheduled scans: No control

### Windows Firewall Policies

There are no Windows Firewall policies configured.

# Software Library

## Applications

There are 3 applications configured.

## Packages

There are 41 packages configured.

## Driver Packages

There are 1 Driver Packages configured.

## Operating System Images

The following OS Images are imported into your site:

* **Name: Windows Server 2008 R2 SP1**
* Package ID: PRI0001B
* Source Path: \\srv1\sources\CM12\_datenbackup\logix\_capture\_files\Windows Server 2008 R2 SP1\install.wim
* **Name: WindowsServer2012-64**
* Package ID: PRI00036
* Source Path: \\srv1\sources\CM12\_datenbackup\deploy\_win2012\_files\WindowsServer2012-64\Server2012.wim
* **Name: XenApp6.5**
* Description: 30.07.2013
* Package ID: PRI00048
* Source Path: \\srv1\sources\osd\Images\W2k8R2SP1\_XenApp65\_20130731\_002757.wim
* **Name: Windows 8 Pro**
* Package ID: PRI0004C
* Source Path: \\srv1\sources\osd\Images\Win81.wim

## Operating System Installers

The following OS Installers are imported into this environment:

## Boot Images

The following Boot Images are imported into this environment:

* **Boot image (x86)**
* Source Path: \\CM12.do.local\SMS\_PRI\osd\boot\i386\boot.PRI00002.wim
* Package ID: PRI00002

Architecture: x86

* Command line support is not enabled
* The following drivers are imported into this WinPE
* There are no drivers imported into the Boot Image.
* The following Optional Components are added to this Boot Image:
* WinPE-Scripting
* WinPE-SecureStartup
* WinPE-WDS-Tools
* WinPE-WMI
* **Boot image (x64)**
* Source Path: \\CM12.do.local\SMS\_PRI\osd\boot\x64\boot.PRI00005.wim
* Package ID: PRI00005

Architecture: x64

* Custom Background: \\srv1\sources\Tools\pictures\ConcordeInFlightBA\_P2\_0.jpg
* Command line support is enabled
* The following drivers are imported into this WinPE
* The following Optional Components are added to this Boot Image:
* WinPE-DismCmdlets
* WinPE-Dot3Svc
* WinPE-StorageWMI
* WinPE-NetFx4
* WinPE-PowerShell3
* WinPE-Scripting
* WinPE-SecureStartup
* WinPE-WDS-Tools
* WinPE-WMI
* **MDTBootImage**
* Source Path: \\srv1\sources\bootimages\x64\MDTBootImage.wim\WinPE.PRI00047.wim
* Package ID: PRI00047

Architecture: x64

* Custom Background: \\srv1\sources\bootimages\x64\MDTBootImage.wim\Background.bmp
* Command line support is enabled
* The following drivers are imported into this WinPE
* There are no drivers imported into the Boot Image.
* The following Optional Components are added to this Boot Image:
* WinPE-Scripting
* WinPE-SecureStartup
* WinPE-WDS-Tools
* WinPE-WMI

## Task Sequences

The following Task Sequences are configured:

* sepagoLogix-XA65-Capture
* sepagoLogix-XA65-Deploy
* Deploy Windows Server 2012
* Script debugging
* mdt test
* sepagoLogix-XA65-Capture-VHD
* Deploy Win8\_1