Inventory Report for System Center Configuration Manager

**12/1/2014**

David Lassen

DXP Enterprises

12/1/2014



Table of Contents

[Summary of all Sites in this Hierarchy 4](#_Toc405184164)

[Configuration Summary for Site HOU 4](#_Toc405184165)

[Site Maintenance Tasks for Site HOU 4](#_Toc405184166)

[Summary of Management Points for Site HOU 5](#_Toc405184167)

[Summary of Distribution Points for Site HOU 5](#_Toc405184168)

[Summary of Software Update Point Servers for Site HOU 5](#_Toc405184169)

[Summary of Hierarchy Wide Configuration 6](#_Toc405184170)

[Summary of Site Boundaries 6](#_Toc405184171)

[Summary of Site Boundary Groups 7](#_Toc405184172)

[Summary of Custom Client Device Settings 7](#_Toc405184173)

[Administrative Users 18](#_Toc405184174)

[Custom Security Roles 19](#_Toc405184175)

[Configured Accounts 19](#_Toc405184176)

[Assets and Compliance 20](#_Toc405184177)

[Summary of User Collections 20](#_Toc405184178)

[Summary of Device Collections 20](#_Toc405184179)

[Compliance Settings 20](#_Toc405184180)

[Configuration Items 20](#_Toc405184181)

[Configuration Baselines 20](#_Toc405184182)

[User Data and Profiles 20](#_Toc405184183)

[Endpoint Protection 20](#_Toc405184184)

[Antimalware Policies 20](#_Toc405184185)

[Windows Firewall Policies 37](#_Toc405184186)

[Software Library 37](#_Toc405184187)

[Applications 37](#_Toc405184188)

[Packages 37](#_Toc405184189)

[Driver Packages 37](#_Toc405184190)

[Operating System Images 37](#_Toc405184191)

[Operating System Installers 37](#_Toc405184192)

[Boot Images 38](#_Toc405184193)

[Task Sequences 38](#_Toc405184194)

# Summary of all Sites in this Hierarchy

The following Primary Sites are installed:

|  |  |  |
| --- | --- | --- |
| **Site Name** | **Site Code** | **Version** |
| DXP Enterprises - SCCM 2012 R2 | HOU | 5.00.7958.1000 |

# Configuration Summary for Site HOU

## Site Maintenance Tasks for Site HOU

|  |  |  |
| --- | --- | --- |
| **Task Name** | **State** | **Location** |
| Backup SMS Site Server | True | \\hou-cf-02\departments\IT\SysOps\SCCM\Backup\Housccm03 |
| 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 | True |  |
| Delete Obsolete Alerts | True |  |
| Delete Obsolete Client Discovery Data | True |  |
| Delete Obsolete Forest Discovery Sites And Subnets | True |  |
| Evaluate Provisioned AMT Computer Certificates | True |  |
| Monitor Keys | True |  |
| Rebuild Indexes | False |  |
| Summarize File Usage Metering Data | True |  |
| Summarize Installed Software Data | True |  |
| Summarize Monthly Usage Metering Data | True |  |

## Summary of Management Points for Site HOU

HOUSCCM03.dxpe.com

## Summary of Distribution Points for Site HOU

**HOUSCCM03.dxpe.com**

* PXE disabled

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

* Houston

**housccm04.dxpe.com**

* PXE disabled

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

* Houston

## Summary of Software Update Point Servers for Site HOU

housccm04.dxpe.com

|  |  |  |  |
| --- | --- | --- | --- |
| **Property Name** | **Value** | **Value 1** | **Value 2** |
| AnonymousProxyAccess | 1 |  |  |
| DBServerName | 0 |  | HOUSCCM04 |
| 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** |
| dxpe.corp/Houston | Active Directory Site | n/a | Houston |  |
| dxpe.corp/Houston/10.0.0.0/8 | IP Range | housccm04.dxpe.com | 10.0.0.1-10.255.255.254 | HOU |
| dxpe.corp/Houston/192.168.0.0/16 | IP Range | housccm04.dxpe.com | 192.168.0.1-192.168.255.254 | HOU |
| dxpe.corp/Houston/38.155.0.0/16 | IP Range | housccm04.dxpe.com | 38.155.0.1-38.155.255.254 | HOU |
| dxpe.corp/Houston/38.185.0.0/16 | IP Range | housccm04.dxpe.com | 38.185.0.1-38.185.255.254 | HOU |
| dxpe.corp/Omaha | Active Directory Site | n/a | Omaha |  |
| dxpe.corp/Omaha/10.0.0.0/24 | IP Range | n/a | 10.0.0.1-10.0.0.254 |  |
| dxpe.corp/Omaha/10.129.0.0/16 | IP Range | n/a | 10.129.0.1-10.129.255.254 |  |
| dxpe.corp/Omaha/10.77.0.0/23 | IP Range | n/a | 10.77.0.1-10.77.1.254 |  |
| dxpe.corp/Omaha/10.77.13.0/24 | IP Range | n/a | 10.77.13.1-10.77.13.254 |  |
| dxpe.corp/Omaha/10.77.2.0/24 | IP Range | n/a | 10.77.2.1-10.77.2.254 |  |
| dxpe.corp/Omaha/10.77.3.0/24 | IP Range | n/a | 10.77.3.1-10.77.3.254 |  |
| dxpe.corp/Omaha/192.168.3.0/24 | IP Range | n/a | 192.168.3.1-192.168.3.254 |  |
| dxpe.com/HOU | Active Directory Site | n/a | HOU |  |
| dxpe.com/OMA | Active Directory Site | n/a | OMA |  |
| dxpe.com/OMA/10.77.0.0/16 | IP Range | n/a | 10.77.0.1-10.77.255.254 |  |
| dxpe.com/OMA/10.78.0.0/16 | IP Range | n/a | 10.78.0.1-10.78.255.254 |  |
| Helpdesk | IP Range | n/a | 10.88.6.1-10.88.6.254 |  |
| Natpro.com/Default-First-Site-Name | Active Directory Site | n/a | Default-First-Site-Name |  |
| Natpro.com/Default-First-Site-Name/10.10.1.0/24 | IP Range | n/a | 10.10.1.1-10.10.1.254 |  |

## Summary of Site Boundary Groups

**HOU - Site Assignment**

* Description: Site assignment for all of DXP
* There are no Site Systems associated to this Boundary Group.

**HOU - Content**

* Description: Content (DP) for Housccm04 - Main HOU DP
* Member names: dxpe.corp/Houston/10.0.0.0/8
* Member names: dxpe.corp/Houston/192.168.0.0/16
* Member names: dxpe.corp/Houston/38.155.0.0/16
* Member names: dxpe.corp/Houston/38.185.0.0/16

## Summary of Custom Client Device Settings

**Client Settings Name: Workstation**

* Client Settings Description:
* Client Settings ID: 16777235
* Client Settings Priority: 8
* This is a custom client Device Setting.

Configurations

* Remote Tools
* Enable Remote Control on clients: Enabled: Domain, Private, Public.
* 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:
* DXPE\Domain Admins
* DXPE\HelpDesk
* DXPECOM\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: Remote viewing.

* Manage Remote Desktop settings: 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: True
* 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: False

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

**Client Settings Name: DC Servers**

* Client Settings Description:
* Client Settings ID: 16777236
* Client Settings Priority: 6
* This is a custom client Device Setting.

Configurations

* 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.

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

* Background Intelligent Transfer
* Limit the maximum network bandwidth for BITS background transfers: False
* Throttling window start time: 9
* Throttling window end time: 17
* Maximum transfer rate during throttling window (kbps): 1000
* Allow BITS downloads outside the throttling window: False
* Maximum transfer rate outside the throttling window (Kbps): 9999

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

* 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: True
* 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: False

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

**Client Settings Name: Citrix 6.5 Servers**

* Client Settings Description:
* Client Settings ID: 16777238
* Client Settings Priority: 4
* This is a custom client Device Setting.

Configurations

* Software Inventory
* Enable software inventory on clients: False

Schedule software inventory and file collection: Occurs every 7 days effective 02/01/1970 00:00:00

Inventory reporting detail: Full details

* Inventory these file types:
* \*.exe
* \*
* Exclude WinDir and Subfolders

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

* 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: housccm04.dxpe.com(2)
* 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: DXP Enterprises
* Install Permissions: Only Administrators
* Suspend Bitlocker PIN entry on restart: Never
* Additional software manages the deployment of applications and software updates: No
* Powershell execution policy: All signed
* Show notifications for new deployments: No
* 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.

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

* User and Device Affinity
* User device affinity usage threshold (minutes): 2880
* User device affinity usage threshold (days): 30

Automatically configure user device affinity from usage data: No

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

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

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

* Endpoint Protection
* Manage Endpoint Protection client on client computers: True
* Install Endpoint Protection client on client computers: False
* 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

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

**Client Settings Name: Servers**

* Client Settings Description:
* Client Settings ID: 16777243
* Client Settings Priority: 7
* This is a custom client Device Setting.

Configurations

* Background Intelligent Transfer
* Limit the maximum network bandwidth for BITS background transfers: False
* Throttling window start time: 7
* Throttling window end time: 18
* Maximum transfer rate during throttling window (kbps): 256
* Allow BITS downloads outside the throttling window: True
* Maximum transfer rate outside the throttling window (Kbps): 2000

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

* 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: True
* 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: False

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

* Computer Restart
* Display a temporary notification to the user that indicates the interval before the user is logged of or the computer restarts (minutes): 10
* Display a dialog box that the user cannot close, which displays the countdown interval before the user is logged of or the computer restarts (minutes): 5

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

**Client Settings Name: Excluded from SCEP**

* Client Settings Description:
* Client Settings ID: 16777245
* Client Settings Priority: 1
* This is a custom client Device Setting.

Configurations

* Endpoint Protection
* Manage Endpoint Protection client on client computers: False
* Install Endpoint Protection client on client computers: False
* 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: True
* 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: False

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

**Client Settings Name: NatPro Workstations**

* Client Settings Description:
* Client Settings ID: 16777246
* Client Settings Priority: 5
* This is a custom client Device Setting.

Configurations

* 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:
* DXPE\Domain Admins
* DXPE\HelpDesk
* 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: False

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

* 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: housccm04.dxpe.com(2)
* 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: DXP Enterprises
* 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: All signed
* Show notifications for new deployments: Yes
* Software Updates
* Enable software updates on clients: False

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

Schedule deployment re-evaluation: Occurs every 1 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.

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

* Background Intelligent Transfer
* Limit the maximum network bandwidth for BITS background transfers: True
* Throttling window start time: 7
* Throttling window end time: 18
* Maximum transfer rate during throttling window (kbps): 512
* Allow BITS downloads outside the throttling window: True
* Maximum transfer rate outside the throttling window (Kbps): 2000

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

* Client Policy
* Client policy polling interval (minutes): 30
* Enable user policy on clients: True
* Enable user policy requests from Internet clients: False

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

* Software Deployment
* Schedule re-evaluation for deployments: Occurs every 1 days effective 02/01/1970 00:00:00

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

* Endpoint Protection
* Manage Endpoint Protection client on client computers: False
* Install Endpoint Protection client on client computers: False
* 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: True
* 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: False

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

**Client Settings Name: Citrix 4.5 Servers - Scep**

* Client Settings Description:
* Client Settings ID: 16777247
* Client Settings Priority: 2
* This is a custom client Device Setting.

Configurations

* Software Inventory
* Enable software inventory on clients: False

Schedule software inventory and file collection: Occurs every 7 days effective 02/01/1970 00:00:00

Inventory reporting detail: Full details

* Inventory these file types:
* \*.exe
* \*
* Exclude WinDir and Subfolders

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

* 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: housccm04.dxpe.com(2)
* 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: DXP Enterprises
* Install Permissions: Only Administrators
* Suspend Bitlocker PIN entry on restart: Never
* Additional software manages the deployment of applications and software updates: No
* Powershell execution policy: All signed
* Show notifications for new deployments: No
* 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.

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

* User and Device Affinity
* User device affinity usage threshold (minutes): 2880
* User device affinity usage threshold (days): 30

Automatically configure user device affinity from usage data: No

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

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

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

* Endpoint Protection
* Manage Endpoint Protection client on client computers: True
* Install Endpoint Protection client on client computers: False
* 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

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

**Client Settings Name: Citrix 4.5 Servers - Symantec**

* Client Settings Description:
* Client Settings ID: 16777248
* Client Settings Priority: 3
* This is a custom client Device Setting.

Configurations

* Software Inventory
* Enable software inventory on clients: False

Schedule software inventory and file collection: Occurs every 7 days effective 02/01/1970 00:00:00

Inventory reporting detail: Full details

* Inventory these file types:
* \*.exe
* \*
* Exclude WinDir and Subfolders

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

* 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: housccm04.dxpe.com(2)
* 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: DXP Enterprises
* Install Permissions: Only Administrators
* Suspend Bitlocker PIN entry on restart: Never
* Additional software manages the deployment of applications and software updates: No
* Powershell execution policy: All signed
* Show notifications for new deployments: No
* 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.

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

* User and Device Affinity
* User device affinity usage threshold (minutes): 2880
* User device affinity usage threshold (days): 30

Automatically configure user device affinity from usage data: No

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

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

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

* Endpoint Protection
* Manage Endpoint Protection client on client computers: False
* Install Endpoint Protection client on client computers: False
* 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** |
| DXPECOM\dlassen | User | Full Administrator | All | All Systems All Users and User Groups |
| DXPE\SCCM-Full Admins | Group | Full Administrator | All | All Systems All Users and User Groups |
| DXPECOM\SCCMADMIN | User | Full Administrator | All | All Systems All Users and User Groups |
| DXPECOM\SCCM-Full Admins | Group | Full Administrator | All | All Systems All Users and User Groups |
| DXPE\SCCM-HelpDesk | Group | Asset Manager Assistant Collection Manager Endpoint Protection Manager Assistant Read-only Analyst Remote Tools Operator Application Deployment Manager | Default | All Systems All Users and User Groups |
| DXPE\SCCM-Operators | Group | Endpoint Protection Manager Assistant Read-only Analyst Remote Tools Operator Asset Manager Application Deployment Manager Operating System Deployment Manager | Default | All Systems All Users and User Groups |
| DXPE\sccmadmin | User | Full Administrator | All | All Systems All Users and User Groups |
| DXPECOM\SCCM-HelpDesk | Group | Asset Manager Assistant Collection Manager Endpoint Protection Manager Assistant Read-only Analyst Remote Tools Operator Application Deployment Manager | Default | All Systems All Users and User Groups |
| DXPECOM\SCCM-Operators | Group | Endpoint Protection Manager Assistant Read-only Analyst Remote Tools Operator Asset Manager Application Deployment Manager Operating System Deployment Manager | Default | All Systems All Users and User Groups |
| DXPE\Sccm 2012 R2 - Report Users | Group | Report Users | Default | All Systems All Users and User Groups |
| DXPECOM\Sccm 2012 R2 - Report Users | Group | Report Users | Default | All Systems All Users and User Groups |

## Custom Security Roles

Enumerating all custom build security roles:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Description** | **Copied from** | **Members** | **Role ID** |
| Asset Manager Assistant | Junior Asset Manager Role Customized | Asset Manager | DXPE\SCCM-HelpDesk DXPECOM\SCCM-HelpDesk | HOU00001 |
| Collection Manager | Grants permission to create, delete, and manage membership of collections. | Software Update Manager | DXPE\SCCM-HelpDesk DXPECOM\SCCM-HelpDesk | HOU00002 |
| Endpoint Protection Manager Assistant | Junior SCEP Manager | Endpoint Protection Manager | DXPE\SCCM-HelpDesk DXPE\SCCM-Operators DXPECOM\SCCM-HelpDesk DXPECOM\SCCM-Operators | HOU00003 |
| Report Users | Users who need report rights | Read-only Analyst | DXPE\Sccm 2012 R2 - Report Users DXPECOM\Sccm 2012 R2 - Report Users | HOU00004 |

## Configured Accounts

Enumerating all accounts used for specific tasks.

|  |  |  |
| --- | --- | --- |
| **User Name** | **Account Usage** | **Site Code** |
| DXPECOM\svcSCCMNAA | Software Distribution | HOU |
| DXPE\svcSCCM | SMS\_AD\_SECURITY\_GROUP\_DISCOVERY\_AGENT SMS\_AD\_USER\_DISCOVERY\_AGENT SMS\_CLIENT\_CONFIG\_MANAGER | HOU |
| DXPECOM\svcSCCM | SMS\_AD\_SECURITY\_GROUP\_DISCOVERY\_AGENT SMS\_AD\_USER\_DISCOVERY\_AGENT SMS\_CLIENT\_CONFIG\_MANAGER | HOU |
| DXPECOM\SCCMADMIN | SMS\_MIGRATION\_MANAGER | HOU |
| DXPE\dlassen | SMS\_MIGRATION\_MANAGER | HOU |
| DXPECOM\svcSCCMRpt | SMS SRS Reporting Point SMS\_ALERT\_NOTIFICATION | HOU |
| DXPECOM\SVCSCCM | SMS\_AD\_FOREST\_DISCOVERY\_MANAGER | HOU |
| DXPE\SVCSCCM | SMS\_AD\_FOREST\_DISCOVERY\_MANAGER | HOU |
| DXPECOM\dlassen |  | HOU |

# Assets and Compliance

## Summary of User Collections

There are 11 User Collections.

## Summary of Device Collections

There are 390 Device collections.

## Compliance Settings

### Configuration Items

Enumerating Configuration Items:

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Last modified** | **Last modified by** | **CI ID** |
| WSUS Setting | 11/11/2014 10:32:25 | DXPE\dlassen | 16825363 |
| Built-In | 10/13/2014 19:46:17 |  | 16777407 |

### 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: False
* Daily quick scan schedule time: 2:00
* Check for the latest definition updates before running a scan: False
* 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: True
* Limit CPU usage during scans to (%): 50
* **Scan settings**
* Scan email and email attachments: False
* 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: False
* 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
* %ProgramData%\Microsoft\Search\Data\Applications\Windows
* %windir%\SoftwareDistribution\Datastore
* Excluded file types:
* .xml, .bin, .dsc, .grxml, .cfg, .dir, .ci, .lzx, .edb, .chk, .wsb, .dia, .config, .mdb
* 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: True
* 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
* **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) 0
* Check for Endpoint Protection definitions daily at: (Only configurable if interval-based check is disabled) 7:00
* 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): 4
* If UNC file shares are selected as a definition update source, specify the UNC paths:

**Domain Controller Policy**

Description: Endpoint Policy - Domain Controllers

* **Default Actions**

Severe threats: Quarantine

High threats: Quarantine

Medium threats: Quarantine

Low threats: Quarantine

* **Exclusion settings**
* Excluded files and folders:
* %allusersprofile%\NTUser.pol
* %systemroot%\system32\GroupPolicy\registry.pol
* %windir%\Security\database\\*.chk
* %windir%\Security\database\\*.edb
* %windir%\Security\database\\*.jrs
* %windir%\Security\database\\*.log
* %windir%\Security\database\\*.sdb
* %windir%\SoftwareDistribution\Datastore\Datastore.edb
* %windir%\SoftwareDistribution\Datastore\Logs\edb.chk
* %windir%\SoftwareDistribution\Datastore\Logs\edb\*.log
* %windir%\SoftwareDistribution\Datastore\Logs\Edbres00001.jrs
* %windir%\SoftwareDistribution\Datastore\Logs\Edbres00002.jrs
* %windir%\SoftwareDistribution\Datastore\Logs\Res1.log
* %windir%\SoftwareDistribution\Datastore\Logs\Res2.log
* %windir%\SoftwareDistribution\Datastore\Logs\tmp.edb
* 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: True
* **Scan settings**
* Scan email and email attachments: True
* Scan removable storage devices such as USB drives: True
* Scan network drives when running a full scan: True
* Scan archived files: False
* Allow users to configure CPU usage during scans: True

User control of scheduled scans: Full control

**EDI Server Policy**

Description: Endpoint Policy - EDI Servers

* **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
* c:\edi\_tradingpartners\application\edi855\edi855.exe
* c:\edi\_tradingpartners\application\edi850\edi850.exe
* c:\saveattachment\saveattachment.exe
* c:\edi\_tradingpartners\application\edi856\edi856.exe
* C:\EDI\_TradingPartners\Application
* Excluded file types:
* .xml, .bin, .dsc, .grxml, .cfg, .dir, .ci, .lzx, .edb, .chk, .wsb, .dia, .config, .mdb
* .EDI856.exe
* .edi850.exe
* Excluded processes:

**Exchange Server Policy**

Description: Endpoint Policy - Exchange Servers

* **Default Actions**

Severe threats: Quarantine

High threats: Quarantine

Medium threats: Quarantine

Low threats: Quarantine

* **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
* %systemroot%\IIS;%SystemRoot%\System32\Inetsrv;%Program Files%\Microsoft\Exchange Server\ClientAccess;%USERPROFILE%\AppData\Local\Temp;%Program Files%\Microsoft\Exchange Server\ExchangeOAB
* %systemroot%\IIS
* %SystemRoot%\System32\Inetsrv
* %Program Files%\Microsoft\Exchange Server\ClientAccess
* %USERPROFILE%\AppData\Local\Temp
* %Program Files%\Microsoft\Exchange Server\ExchangeOAB
* %Program Files%\Microsoft\Exchange Server\Mailbox\MDBTEMP
* %systemroot%\IIS Temporary Compressed Files
* %SystemRoot%\System32\Inetsrv folder
* %Program Files%\Microsoft\Exchange Server\Working\OleConvertor
* %Program Files%\Microsoft\Exchange Server\TransportRoles\Data\SenderReputation
* %Program Files%\Microsoft\Exchange Server\TransportRoles\Data\Adam
* %Program Files%\Microsoft\Exchange Server\UnifiedMessaging\grammars
* %Program Files%\Microsoft\Exchange Server\UnifiedMessaging\Prompts
* %Program Files%\Microsoft\Exchange Server\UnifiedMessaging\voicemail
* %Program Files%\Microsoft\Exchange Server\UnifiedMessaging\badvoicemail
* %Winnt%\Cluster
* g:\
* h:\
* I:\
* J:\
* K:\
* N:\
* Excluded file types:
* .xml, .bin, .dsc, .grxml, .cfg, .dir, .ci, .lzx, .edb, .chk, .wsb, .dia, .config, .mdb
* .chk; .log; .edb; .jrs; .que; .cfg; .grxml; .config; .dia; .wsb; .lzx; .ci; .dir; .wid; .000; .001; .002
* Excluded processes:
* Microsoft.Exchange.Cluster.Replayservice.exe
* Microsoft.Exchange.Edgesyncsvc.exe
* Microsoft.Exchange.Imap4.exe
* Microsoft.Exchange.Imap4service.exe
* Microsoft.Exchange.Infoworker.Assistants.exe
* Microsoft.Exchange.Monitoring.exe
* Microsoft.Exchange.Pop3.exe
* Microsoft.Exchange.Pop3service.exe
* Microsoft.Exchange.Search.Exsearch.exe
* Microsoft.Exchange.Servicehost.exe
* Msexchangeadtopologyservice.exe
* Msexchangefds.exe
* Msexchangemailboxassistants.exe
* Msexchangemailsubmission.exe
* Msexchangetransport.exe
* Msexchangetransportlogsearch.exe
* Msftefd.exe
* Oleconverter.exe
* Powershell.exe
* Sesworker.exe
* Speechservice.exe
* Store.exe
* Transcodingservice.exe
* Umservice.exe
* Umworkerprocess.exe
* W3wp.exe
* Cdb.exe
* Cidaemon.exe
* Cluster.exe
* Dsamain.exe
* Edgecredentialsvc.exe
* Edgetransport.exe
* Galgrammargenerator.exe
* Inetinfo.exe
* Mad.exe
* Microsoft.Exchange.Antispamupdatesvc.exe
* Microsoft.Exchange.Contentfilter.Wrapper.exe
* **Scan settings**
* Scan email and email attachments: True
* Scan removable storage devices such as USB drives: True
* Scan network drives when running a full scan: True
* Scan archived files: False
* Allow users to configure CPU usage during scans: False

User control of scheduled scans: No control

**NetApp Share Scan Servers**

Description: Endpoint Policy - NetApp Servers

* **Scheduled Scans**
* Run a scheduled scan on client computers: True
* Scan type: Full Scan
* Scan day: Friday
* Scan time: 18:30
* Run a daily quick scan on client computers: False
* 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: 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 (%): 70
* **Scan settings**
* Scan email and email attachments: True
* Scan removable storage devices such as USB drives: True
* Scan network drives when running a full scan: False
* Scan archived files: False
* Allow users to configure CPU usage during scans: False

User control of scheduled scans: Full control

**Server Policy**

Description: Endpoint Policy - Server Endpoints (Generic)

* **Default Actions**

Severe threats: Quarantine

High threats: Quarantine

Medium threats: Quarantine

Low threats: Quarantine

* **Scan settings**
* Scan email and email attachments: False
* 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: Full control

**SQL Server Policy**

Description: Endpoint Policy - SQL server

* **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
* C:\Program Files\Microsoft SQL Server\MSSQL.X\OLAP\Data
* c:\edi\_tradingpartners\application\edi856\edi856.exe
* c:\saveattachment\saveattachment.exe
* c:\edi\_tradingpartners\application\edi850\edi850.exe
* c:\edi\_tradingpartners\application\edi855\edi855.exe
* C:\EDI\_TradingPartners\Application
* %windir%\Cluster
* Q:\
* Excluded file types:
* .sqlaudit, .sql, .trc, .ndf, .ldf, .mdf
* .EDI856.exe
* .BAK
* .trn
* Excluded processes:
* sqlaudit
* sqlsrvr.exe
* sqlagent.exe

**Workstation Policy**

Description: Endpoint Policy - Desktop Endpoints (Generic)

* **Scheduled Scans**
* Run a scheduled scan on client computers: True
* Scan type: Full Scan
* Scan day: Saturday
* Scan time: 20:00
* Run a daily quick scan on client computers: False
* Daily quick scan schedule time: 4:00
* 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 (%): 70
* **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
* C:\infor
* c:\infor\pvx\pvxwin32.exe
* %ProgramFiles(x86)%\Solidworks Corp
* %ProgramFiles%\Solidworks Corp
* Excluded file types:
* .xml, .bin, .dsc, .grxml, .cfg, .dir, .ci, .lzx, .edb, .chk, .wsb, .dia, .config, .mdb
* Excluded processes:
* C:\infor\pvx\pvxwin32.exe
* **Microsoft Active Protection Service**

Microsoft Active Protection Service membership type: Basic membership

* 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): 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): True
* **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: True

User control of scheduled scans: No control

**Citrix Server Policy**

Description: Endpoint Policy - Citrix Servers

* **Scheduled Scans**
* Run a scheduled scan on client computers: False
* **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
* C:\JFSRVR\
* C:\PROGRAM FILES\CITRIX\SERVER RESOURCE MANAGEMENT\MEMORY OPTIMIZATION MANAGEMENT\PROGRAM\CTXSFOSVC.EXE
* X:\
* C:\Documents and Settings\All Users\Application Data\Citrix\
* C:\PROGRAM FILES\CITRIX\
* C:\PROGRAM FILES (x86)\CITRIX\
* C:\Program Files\Citrix\Server Resource Management\CPU Utilization Management\bin\ctxcpubal.exe
* C:\Program Files\Citrix\Server Resource Management\CPU Utilization Management\bin\ctxcpusched.exe
* c:\program files\UPHClean\uphclean.exe
* C:\Program Files\Citrix
* C:\Program Files\CommerceCenter
* C:\Program Files\Activant
* C:\Program Files\Citrix\System32
* C:\WINDOWS\system32\spool\PRINTERS
* c:\pagefile.sys
* %windir%\Program Files\Citrix\Personal vDisk\BIN\WIN7\
* %AppData%\ICAClient\Cache
* %AllUsersProfile%\Application Data\Citrix\System Monitoring\Data
* D:\Citrix
* %windir%\System32\drivers\CvhdBusP6.sys
* %windir%\System32\drivers\CfsDep2.sys
* C:\ProgramData\Citrix\Provisioning Services\Tftpboot\ARDBP32.BIN
* %windir%\System32\drivers\bnistack6.sys
* %windir%\system32\spoolsv.exe
* %windir%\system32\csrss.exe
* %windir%\system32\winlogon.exe
* %windir%\system32\userinit.exe
* %windir%\system32\smss.exe
* d:\pagefile.sys
* %programfiles(x86)%\Citrix
* d:\.vdiskcache
* c:\.vdiskcache
* %programfiles%\Microsoft Security Client\msmpeng.exe
* %programfiles%\Citrix
* Excluded file types:
* .jrs
* .chk
* .sdb
* .pf
* .pol
* .TMP
* .stm
* .edb
* .mdb
* .ldf
* .mdf, .dat, .log
* .vdiskcache
* .vhdx
* .evt
* Excluded processes:
* UserProfileManager.exe
* CTXPVD.exe
* CTXPVDSVC.exe
* bndevice.exe
* Streamprocess.exe
* Streamservice.exe
* Soapserver.exe
* Inventory.exe
* MgmtDaemon.exe
* Notifier.exe
* BNTFTP.exe
* PVSTSB.exe
* BNPXE.exe
* BNAbsService.exe
* CdfSvc.exe
* C:\PROGRAM FILES\CITRIX\SERVER RESOURCE MANAGEMENT\MEMORY OPTIMIZATION MANAGEMENT\PROGRAM\CTXSFOSVC.EXE
* C:\Program Files\Citrix\Server Resource Management\CPU Utilization Management\bin\ctxcpubal.exe
* C:\Program Files\Citrix\Server Resource Management\CPU Utilization Management\bin\ctxcpusched.exe
* c:\program files\UPHClean\uphclean.exe
* %windir%\system32\spoolsv.exe
* %windir%\system32\csrss.exe
* %windir%\system32\winlogon.exe
* %windir%\system32\userinit.exe
* %windir%\system32\smss.exe
* %programfiles%\Microsoft Security Client\msmpeng.exe
* Winlogon.exe
* LogonUI.exe
* ctxcpubal.exe
* ctxcpusched.exe
* ctxsfosvc64.exe
* ctxsfosvc.exe
* msmpeng.exe
* fbserver.exe
* IMAAdvancesrv.exe
* IMAsrv.exe
* SSONsvr.exe
* xte.exe
* CitrixCseEngine.exe
* cuagent.exe
* PMAgentAssist.exe
* PXXI.exe
* SplWOW64.exe
* vmtoolsd.exe
* WmiPrvSE.exe
* **Real-time protection**
* Enable real-time protection: True
* Monitor file and program activity on your computer: True

Scan system files: Scan incoming files only

* **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) 7:00
* 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): 4
* If UNC file shares are selected as a definition update source, specify the UNC paths:
* **Scan settings**
* Scan email and email attachments: False
* 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

**SCCM Site Servers Policy**

Description: Endpoint Policy - SCCM Site servers

* **Default Actions**

Severe threats: Quarantine

High threats: Quarantine

Medium threats: Quarantine

Low threats: Quarantine

* **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: False
* Daily quick scan schedule time: 2:00
* Check for the latest definition updates before running a scan: False
* 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: True
* 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
* Q:\
* Excluded file types:
* .sqlaudit, .sql, .trc, .ndf, .ldf, .mdf
* .EDI856.exe
* .BAK
* .trn
* Excluded processes:
* sqlaudit
* sqlsrvr.exe
* sqlagent.exe
* **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: False
* Monitor file and program activity on your computer: False

Scan system files: Scan incoming files only

* **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: True
* 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) 7:00
* 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
* FileShares
* InternalDefinitionUpdateServer
* 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:
* \\housccm03\Resources\Updates\SCEP Definitions and Updates
* **Scan settings**
* Scan email and email attachments: False
* 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: True

User control of scheduled scans: Full control

### Windows Firewall Policies

There are no Windows Firewall policies configured.

# Software Library

## Applications

There are 142 applications configured.

## Packages

There are 28 packages configured.

## Driver Packages

There are 2 Driver Packages configured.

## Operating System Images

The following OS Images are imported into your site:

* **Name: Windows 7 x64 - BaseOS - AllApps**
* Package ID: HOU00018
* Source Path: \\housccm03\Resources\OSD\OS Capture\Current Production\Win7x64BaseOS\_AllApps\_16Nov2014.wim
* **Name: Windows 7 x64 - BaseOS - Office**
* Package ID: HOU00019
* Source Path: \\housccm03\Resources\OSD\OS Capture\Current Production\Win7x64BaseOS\_Office\_16Nov2014.wim

## Operating System Installers

The following OS Installers are imported into this environment:

## Boot Images

The following Boot Images are imported into this environment:

* **MDT Boot Image x64**
* Source Path: \\housccm03\Resources\OSD\BootImage\Mdt\x64\WinPE.HOU00010.wim
* Package ID: HOU00010

Architecture: x64

* Custom Background: \\housccm03\Resources\OSD\BootImage\Mdt\x64\Background.bmp
* Command line support is enabled
* The following drivers are imported into this WinPE
* The following Optional Components are added to this Boot Image:
* WinPE-Scripting
* WinPE-SecureStartup
* WinPE-WDS-Tools
* WinPE-WMI
* **MDT Boot Image x86**
* Source Path: \\HOUSCCM03\Resources\OSD\BootImage\Mdt\x86\WinPE.HOU00011.wim
* Package ID: HOU00011

Architecture: x86

* Custom Background: \\HOUSCCM03\Resources\OSD\BootImage\Mdt\x86\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:

* New Computer - Windows 7 x64 Enterprise
* Replace Computer - Windows 7 x64 Enterprise