



Microsoft®

System Center 2012 Endpoint Protection

System Center 2012 Configuration Manager Test Lab Extension System Center 2012 Endpoint Protection

Microsoft Corporation

Published: July 2012

Author: Kevin McKinnerney

Abstract

This document will assist architects, consultants, system engineers, and system administrators in deploying the System Center 2012 Endpoint Protection site system role for System Center 2012 Configuration Manager in a test lab.

Copyright

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred.

© 2012 Microsoft Corporation. All rights reserved.

Active Directory, Forefront, Microsoft, MS-DOS, Visual Studio, Windows, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

<i>System Center 2012 Configuration Manager Test Lab Extension System Center 2012 Endpoint Protection</i>	<i>1</i>
<i>Introduction</i>	<i>5</i>
In This Guide	5
Test Lab Overview	5
Hardware and Software Requirements	6
Steps for the Microsoft System Center 2012 Endpoint Protection Test Lab Extension	7
<i>Step 1: Complete the System Center 2012 Configuration Manager Test Lab Guide</i>	<i>8</i>
<i>Step 2: (Optional) Enable Internet Functionality using the TMG Core Configuration</i>	<i>9</i>
<i>Step 3: Install the System Center 2012 Endpoint Protection Site System Role</i>	<i>10</i>
Configure the Software Update Point Role	10
Endpoint Protection Site System Role Installation	10
Creating Antimalware Policy	11
Creating Client Settings	11
Deploying Endpoint Protection Clients	12
<i>Step 4: Setting up an Automatic Deployment Rule</i>	<i>13</i>
Creating the Automatic Deployment Rule	13

Introduction

In This Guide

This paper contains instructions for extending up a test lab based on the Microsoft System Center 2012 Configuration Manager Test Lab Guide and deploying Microsoft System Center 2012 Endpoint Protection using one server computer and one client computer. The resulting Microsoft System Center 2012 Endpoint Protection test lab demonstrates simple System Center 2012 Endpoint Protection functionality.

Test Lab Overview

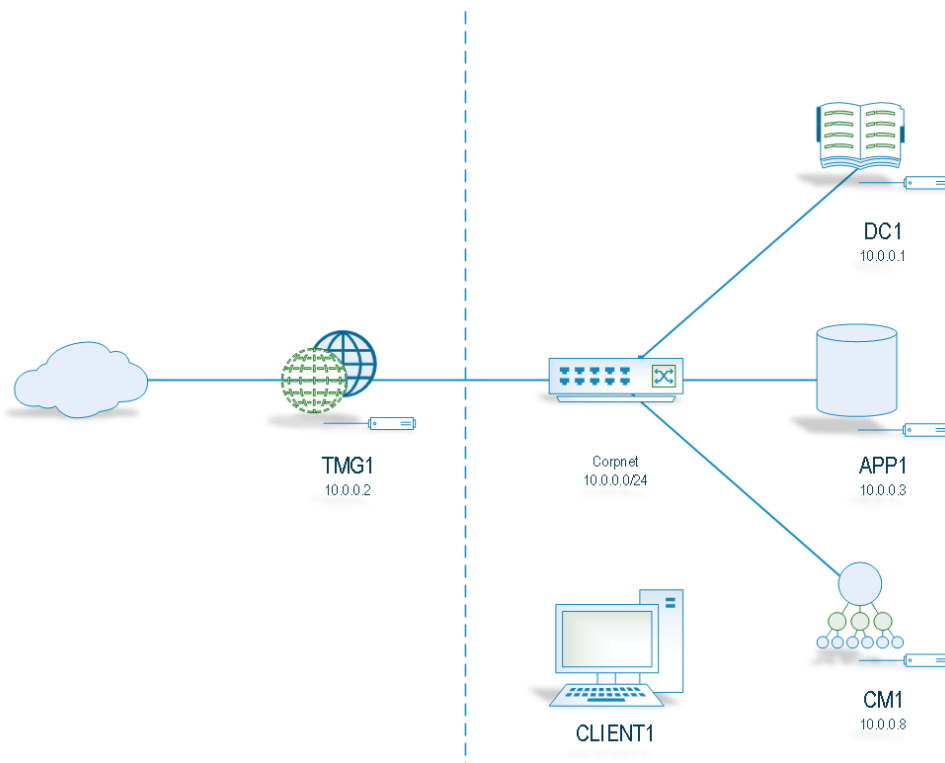
In this test lab, Microsoft System Center 2012 Endpoint Protection is deployed with:

- One pre-existing server running Microsoft System Center 2012 Configuration Manager named CM1. CM1 uses the Windows Server 2008 R2 SP1 Enterprise Edition operating system.
- One pre-existing server running SQL Server 2008 R2 Enterprise with Service Pack 2 named APP1. APP1 uses the Windows Server 2008 R2 SP1 Enterprise Edition operating system.
- One pre-existing client running on Windows 7 Ultimate Edition named CLIENT1.

The Microsoft System Center 2012 Endpoint Protection test lab uses the following subnet:

- The intranet established by the Base Configuration Test Lab Guide, referred to as the Corpnet subnet (10.0.0.0/24).

Computers on each subnet connect using a hub or switch. See the following figure.



This test lab will demonstrate Forefront Endpoint Protection 2010 Definition Update Automation Tool functionality. The purpose of this test lab is to allow for the creation of a basic test lab environment that consists of Forefront Endpoint Protection 2010 and the Definition Update Automation Tool.

The Definition Update Automation Tool (SUAT) is a small program that is used to update an assignment and package each time a synchronization occurs with WSUS. Because definition updates are published 3 times per day, we have set this synchronization to occur every 8 hours. SUAT is primarily needed for large, geographically-dispersed organizations that have only a few Software Update Points but many distribution points. If a company is not geographically-dispersed, it may be better for them to use WSUS to distribute the definition updates.

Hardware and Software Requirements

There are no additional Hardware and Software Requirements for the Microsoft System Center 2012 Endpoint Protection Test Lab Extension.

Steps for the Microsoft System Center 2012 Endpoint Protection Test Lab Extension

There are 4 steps to follow when setting up a System Center 2012 Endpoint Protection test lab based on the System Center 2012 Endpoint Protection Test Lab Extension.

1. **Complete the System Center 2012 Configuration Manager Test Lab Guide.** System Center 2012 Configuration Manager must be fully installed and functional prior to System Center 2012 Endpoint Protection installation.
2. **(optional) Enable Internet Functionality using the TMG Core Configuration.** Internet access is required for proper functionality of the Automatic Deployment Rule. The TMG Core Configuration can be used to provide internet access to the Test Lab.
3. **Install the System Center 2012 Endpoint Protection Site System Role.** Install the System Center 2012 Endpoint Protection Site System Role on CM1.
4. **Setting up an Automatic Deployment Rule.** Set up an Automatic Deployment Rule for the distribution of System Center 2012 Endpoint Protection definition updates.

This guide provides steps for configuring the computers of the System Center 2012 Configuration Manager test lab for System Center 2012 Endpoint Protection. The following sections provide details about how to perform these tasks.

Step 1: Complete the System Center 2012 Configuration Manager Test Lab Guide

Set up the Base Configuration with System Center 2012 Configuration Manager test lab using the Test Lab Guide: System Center 2012 Configuration Manager (<http://go.microsoft.com/?linkid=9815112>).

Step 2: (Optional) Enable Internet Functionality using the TMG Core Configuration

Internet access is required for the Automatic Deployment Rule to download updates from Microsoft Update. The TMG Core Configuration may be used enable full internet functionality using the Test Lab Guide: TMG Core Test Lab (<http://www.isaserver.org/tutorials/TMG-Core-Test-Lab.html>).

Step 3: Install the System Center 2012 Endpoint Protection Site System Role

The install the System Center 2012 Endpoint Protection Site System Role section of the System Center 2012 Endpoint Protection test lab extension consists of the following:

- Configuring the Software Update Point Role
- Endpoint Protection Site System Role Installation
- Creating Antimalware Policy
- Creating Client Settings
- Deploying Endpoint Protection Clients

Configure the Software Update Point Role

Configure the Software Update Point Role on CM1.

To configure the Software Update Point Role

1. Log on to the CM1.corp.contoso.com server as **Corp\Administrator**.
2. Click **Start**, click **All Programs**, expand **Microsoft System Center 2012**, expand **Configuration Manager**, and click **Configuration Manager Console**.
3. In the **Configuration Manager Console**, in the **Administration** workspace, expand **Site Configuration** and click on **Sites**.
4. Right-click on **CHQ – Contoso Headquarters Site** and expand **Configure Site Components**, and click **Software Update Point**.
5. In the **Software Update Point Component Properties**, on the **Classifications** tab, check the box next to **Definition Updates**.
6. In the **Software Update Point Component Properties**, on the **Products** tab, check the box next to **Forefront Endpoint Protection 2010** and press **OK**.
7. In the **Configuration Manager Console**, in the **Software Library** workspace, expand **Software Updates**.
8. Right-click on **All Software Updates** and select **Synchronize Software Updates**.
9. In the **Configuration Manager** dialog, click **Yes**.

Endpoint Protection Site System Role Installation

Install the Endpoint Protection Site System Role on CM1.

To install the Endpoint Protection Site System Role

1. In the **Configuration Manager Console**, in the **Administration** workspace, expand **Site Configuration** and click on **Servers and Site System Roles**.
2. Under **Servers and Site System Roles**, right-click on **\\CM1.corp.contoso.com** and click **Add Site System Roles**.
3. In the **Add Site System Roles Wizard**, on the **General** page, click **Next**.
4. On the **System Role Selection** page, under **Available Roles**, check the box next to **Endpoint Protection Point**.
5. In the **Configuration Manager** dialog, click **OK**.
6. On the **System Role Selection** page, click **Next**.
7. On the **Endpoint Protection** page, read the license terms and check the box next to **I accept the Endpoint Protection license terms**, and click **Next**.
8. On the **Microsoft Active Protection Service** page, click **Next**.
9. On the **Summary** page, click **Next**.
10. On the **Completion** page, click **Close**.

Creating Antimalware Policy

Create an Antimalware Policy on CM1.

To create an Antimalware Policy

1. In the **Assets and Compliance** workspace, expand **Endpoint Protection** and click on **Antimalware Policies**.
2. Right-click in the **Antimalware Policies** pane and click **Create Antimalware Policy**.
3. On the **General** page, enter **Contoso Antimalware Policy** in the **Name** field and press **OK**.

Creating Client Settings

Create Client Settings on CM1.

To create Client Settings

1. In the **Administration** workspace, click **Client Settings**.
2. Right-click in the **Client Settings** pane and click **Create Custom Client Device Settings**.
3. In the **Create Custom Client Device Settings** dialog, enter **Contoso Client Device Settings** in the **Name** field.
4. In the **Select the custom settings to be enforced on client devices** section, check the box next to **Endpoint Protection**.
5. Select the **Endpoint Protection** page in the **General** pane.
6. On the **Endpoint Protection** page, under **Device Settings**, set **Manage Endpoint Protection client on client computers** to **True** and click **OK**.

Deploying Endpoint Protection Clients

Deploy Endpoint Protection clients.

To deploy Endpoint Protection clients

1. In the **Assets and Compliance** workspace, expand **Endpoint Protection** and click on **Antimalware Policies**.
2. Right-click on **Contoso Antimalware Policy** and click **Deploy**.
3. In the **Select Collection** dialog, select the **All Systems** collection and click **OK**.
4. In the **Administration** workspace, click **Client Settings**.
5. Right-click on **Contoso Client Device Settings** and click **Deploy**.
6. In the **Select Collection** dialog, select the **All Systems** collection and click **OK**.

Step 4: Setting up an Automatic Deployment Rule

The setting up an Automatic Deployment Rule section of the System Center 2012 Endpoint Protection test lab extension consists of the following:

- Creating the Automatic Deployment Rule

Creating the Automatic Deployment Rule

Create the Automatic Deployment Rule for definition updates on CM1.

To create the Automatic Deployment Rule

1. Log on to the CM1.corp.contoso.com server as **Corp\Administrator**.
2. Click **Start** and click **Computer**.
3. Double-click on **Local Disk (C:)**.
4. Click on the **New Folder** button and type **EPDefs**.
5. Select the **EPDefs** folder and click **Share with** and select **Specific people**.
6. In the **File Sharing** dialog, drop down the list and select **Everyone** and click **Add**.
7. In the **File Sharing** dialog, click **Share**.
8. In the **File Sharing** dialog, click **Done**.
9. Click **Start**, click **All Programs**, expand **Microsoft System Center 2012**, expand **Configuration Manager**, and click **Configuration Manager Console**.
10. In the **Configuration Manager Console**, in the **Software Library** workspace, expand **Software Updates** and click **Automatic Deployment Rules**.
11. Right-click in the **Automatic Deployment Rules** pane and click **Create Automatic Deployment Rule**.
12. In the **Create Automatic Deployment Rule Wizard**, on the **General** page, enter **Endpoint Protection Definition Updates** in the **Name** field.
13. On the **General** page, next to **Collection**, click **Browse**.
14. On the **General** page, select the option button to **Add to an existing Software Update Group** and click **Next**.
15. On the **Deployment Settings** page, click **Next**.
16. On the **Software Updates** page, in the **Property filters** section, check the boxes next to **Product** and **Update Classification**.
17. On the **Software Updates** page, in the **Search Criteria** section, next to **Product** click **<items to find>**.
18. In the **Search Criteria** dialog, check the box next to **Forefront Endpoint Protection 2010** and click **OK**.
19. On the **Software Updates** page, in the **Search Criteria** section, next to **Update Classification** click **<items to find>**.

20. In the **Search Criteria** dialog, check the box next to **Definition Updates** and click **OK**.
21. On the **Evaluation Schedule** page, click **Customize**.
22. In the **Custom Schedule** dialog, **Configure the recurrence schedule** to **Recur every: 8 hours**.
23. On the **Evaluation Schedule** page, click **Next**.
24. On the **Deployment Schedule** page, in the **Installation Deadline** section, select the option button next to **As soon as possible** and click **Next**.
25. On the **User Experience** page, in the **Deadline Behavior** section, check the box next to **Software Installation** and click **Next**.
26. On the **Alerts** page, click **Next**.
27. On the **Download Settings** page, in the **Deployment options** section, select the option button next to **Download software updates from distribution point and install** and click **Next**.
28. On the **Deployment Package** page, enter **Endpoint Protection Definition Updates** in the **Name** field.
29. On the **Deployment Package** page, enter **\\CM1\EPDefs** in the **Package Source** field and click **Next**.
30. On the **Distribution Points** page, click **Add** and select **Distribution Point**.
31. In the **Add Distribution Point** dialog, check the box next to **\\CM1.corp.contoso.com** and click **OK**.
32. On the **Distribution Points** page, click **Next**.
33. On the **Download Location** page, click **Next**.
34. On the **Language Selection** page, click **Next**.
35. On the **Summary** page, click **Next**.
36. On the **Completion** page, click **Close**.
37. In the **Software Library** workspace, under **Automatic Deployment Rules**, right-click on **Endpoint Protection Definition Updates** and click **Run now**.
38. In the **Configuration Manager** dialog, and press **OK**.