# Table of contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>1-1</td>
</tr>
<tr>
<td>Exercise 1: Log in to the Console</td>
<td>1-1</td>
</tr>
<tr>
<td>Exercise 2: Reviewing the Patch Management Domain</td>
<td>1-2</td>
</tr>
<tr>
<td>Exercise 3: Applying a patch</td>
<td>1-4</td>
</tr>
<tr>
<td>Exercise 4: Configuring patch constraints</td>
<td>1-5</td>
</tr>
<tr>
<td>Exercise 5: Creating patch baselines</td>
<td>1-7</td>
</tr>
</tbody>
</table>
Overview

IBM® Endpoint Manager for Patch Management provides an automated, simplified patching process that is administered from a single console. Built on IBM Bigfix® technology, this software gives you unified, near real-time visibility and enforcement to deploy and manage patches to all distributed endpoints. This software can help you reduce business risk, control costs and enhance security.

IBM Endpoint Manager for Patch Management:

• Automatically manages patches to hundreds of thousands of endpoints for multiple operating systems and applications, regardless of location, connection type or status.

• Applies only the correct patches to the correct endpoint.

• Gives you greater visibility into patch compliance with flexible, near real-time monitoring and reporting.

• Provides near real-time visibility and control from a single management console.

• Can help reduce security risk by streamlining remediation cycles from weeks to hours.

This document will assist new users with the trial of the IBM Endpoint Manager for Patch Management. through the presentation of a few simple use case scenarios.

It should be noted that this document was created using a controlled lab environment and it is expected that your unique environment will have a few subtle differences such as host names, IP addresses, and patches relevant to your managed systems. Don’t worry though, the exercise steps presented here are to help clarify the process to you as you perform them in your environment.

• Our IP domain name: training.tivoli.edu

• Our server name: IEMServer

• Our Windows client name: IEMClient1

• Our Linux client name: IEMClient2

Exercise 1: Log in to the Console

___ 1. From the desktop of the system on which the trial was installed, start the Console:

Click Start > All Programs > IBM Endpoint Manager > IBM Endpoint Manager Console.
Alternatively, you can double-click the Console shortcut on the server desktop.

2. Log in with the following credentials:
   - Server: **IP of the server installed to**
   - User name: **EvaluationUser**
   - Password: `<password you created during installation>`

3. Click **Login** and wait while data loads into the Console cache.

4. This process can take several minutes to complete in this lab environment. When data loading is complete, the Console is displayed.

**Exercise 2: Reviewing the Patch Management Domain**

1. Click the **Patch Management Domain**. The **Patch Overview Dashboard** is displayed.

2. Review the various statistics in the **All Patch Sites at a Glance** pane.

3. Hover over the critical patches section of the bar graph for each site in the **Overview of Critical Patches vs Other Patches by Site** pane. Determine the number of critical patches outstanding for each site displayed.
Note: The information that is displayed in the **Patch Overview Dashboard** varies, depending on the latest released patches. Since the lab environment is isolated from the Internet, the **Patch Overview Dashboard** might not display any recent patch content.

4. Review the other panes of the **Patch Overview Dashboard**.

5. Expand the **OS Vendors** node in the navigation tree for the Patch Management domain.

6. Review the list of vendors and the relevant Fixlet counts.

7. Expand the **Application Vendors** node in the navigation tree for the Patch Management domain.

8. Review the list of vendors and the relevant Fixlet counts.

9. Expand the **All Patch Management > Dashboards** node and select the **Patches for Windows Overview** node.

10. Review the information in the dashboard. You can use this dashboard to assess the status of Windows patches in your environment.
Exercise 3: Applying a patch

There are several methods and paths for applying a patch. In this exercise, you locate and apply a Windows Hot Fix.

___ 1. Expand the **OS Vendors > Microsoft Windows > Microsoft OS and Application Patches** node in the navigation tree for the Patch Management Domain and select the **Hot Fixes** node.

___ 2. The **Hot Fixes** list is displayed. Enter **time zone** in the Hot Fix live search field in the upper right corner to show only hot fixes that contain the word **time zone** in the name.

**Tip:** Clear the **Show Non-Relevant Content** button at the top of the Console to restrict the Hot Fixes displayed to relevant to the clients in the lab environment.

___ 3. Select the **2779562: December 2012 cumulative time zone updated for Windows operating systems - Windows XP SP3** from the hot fix list.

___ 4. You need to obtain the Knowledge Base number for the patch. The number should start with **KB**.

___ a. Click the **Description** tab and note that the applicable **Knowledge Base number** for the patch is **KB2779562**.

___ 5. Click **Take Action** and select **Click here to initiate the deployment process**.

___ 6. Select a client in the **Target** computers list and click **OK**.
7. Monitor the status of the action. You can periodically click the Refresh Console button at the top of the IBM Endpoint Manager Console to see the status changes. Wait until the status is Fixed or Pending Restart before continuing.

8. Optionally, you may log into the managed system to which the patch was applied to verify the patch was installed. Log in to that system as Administrator.

9. Click the Windows Start menu and select Control Panel.

10. When the Control Panel opens, double-click Add or Remove Programs.

11. Click Change or Remove Programs and verify that the Show updates check box is selected.

12. Using the KB number previously recorded, verify that the update you recently installed is listed. It should be located near or at the bottom of the scroll list as all updates are sorted by the date on which they were installed.

13. Close the Add or Remove Programs window.


15. If the action had a status of Pending Restart, restart the IEMClient1 virtual machine. After the virtual machine restarts, log back in as Administrator with the password of P@ssw0rd. Otherwise, a status of Fixed indicates that the work is complete.

16. Switch to the IEMSERVER virtual machine.

Exercise 4: Configuring patch constraints

You can use Take Action parameters to control how and when a patch is installed. For example, you can use time constraints to patch Windows servers during a preset maintenance window. In this exercise, you define various constraints for the deployment of patches.

1. In the hierarchy, expand OS Vendors > Microsoft Windows > Microsoft OS and Application Patches node in the Patch Management domain and select Hot Fixes.
   The Hot Fixes list is displayed.

2. Enter Update in the live search field to show hot fixes with the string Update in the patch name or description.


4. Click Take Action. The TAKE Action pane is displayed.

5. Click the Execution tab.
6. Perform the following steps to set the **Execution** settings:
   a. Clear the **Ends on** option.
   b. Select **Run between 1:00:00 AM and 2:59:00 AM**.
   c. Select **Run only on** and **Sat** (clear any other day of the week that might be selected).
   d. Select **Start client downloads before constraints are satisfied**.

7. Click the **Users** tab.

8. Select **Run independently of user presence, and display the user interface to the selected user** and **All users** under the Selected Users section.

9. Click the **Messages** tab.

10. Perform the following steps to set the **Message** settings:
    a. Select **Display message before running action** and enter **Required patch must be installed** for the description.
    b. Set the deadline to **15 minutes** and select **Run action automatically** for the At deadline option.
    c. Select **Display message while running action** and enter **Required patch is being installed** for the Description. Do not change the Title text.

11. Click the **Post Action** tab.

12. Perform the following steps to define the **Post Action** settings:
    a. Select **Restart computer after action completes**.
    b. Select **Allow user to cancel restart**.
    c. Set the deadline to **1 day**.
    d. Select **Restart automatically** for the At deadline option.

13. Optionally, review the other tabs. Do not change any other settings.

14. Click **Save Preset**.

15. Enter **Windows Server Maintenance Window** for the name, and select **Make this preset available to all operators**.

16. Click **Save**.

**Note:** You can use this preset to set the Take Action parameters for other Fixlets and tasks.

17. Click the **Target** tab.
18. Select **Dynamically target by property** option.

19. Browse the tree view below the option for **All Computers > By Retrieved Properties > By OS > WinXP 5.1.2600**.

**Note:** Choosing this option targets all computers that match the applicability relevance of the selected patch for this action that first match the specified property. In this case, check the OS property to target all Windows XP clients. Selecting All Computers, including the server, as a target could cause minor inconvenience to your labs.

20. Click **OK** to run the task.

21. Monitor the status of the action. You can periodically click the **Refresh Console** button at the top of the IBM Endpoint Manager Console to see the status changes. Wait until the status is **Pending Downloads** or **Waiting** before continuing.

**Note:** The action remains in Waiting status and is not taken until all of the constraint conditions are met.

**Exercise 5: Creating patch baselines**

In this exercise, you create a baseline for applying Windows patches in the custom site that is previously created to keep your custom work more organized.

**Note:** Creating a baseline as a master operator can affect system performance. Therefore, in a production environment, it is suggested that you create baselines as a non-master operator. The impact to this lab environment is minimal. Therefore, for simplicity, you use the master operator account.

1. From the IBM Endpoint Manager Console menu, select **Tools > Create New Baseline**.

2. Enter **Latest Windows Patches** for the **Name** and in the text field that contains `<enter a description of the baseline here>` (located below the blue Description header), enter **Windows patches as of <date>** for the description, replacing `<date>` with the current date.

3. Select **My Custom Site** for the **Create in site** field.

4. Click the **Components** tab.

5. Click **edit name** next to Component Group 1.

6. Enter **Windows Patches** for the **Group Name** and click **Save Group Name**.

7. Click **add components to group** under Windows Patches.
8. Click the column header **Name** to sort the list.

9. Press **Ctrl** and select the two Microsoft Security Bulletins that start with **MS11-015: Vulnerabilities in Windows Media** and **MS11-017: Vulnerability in Remote Desktop Client**, then click **OK**.

10. Verify **Action1** is the default for all of the components that you added.

**Note:** You can use the up and down arrows next to the patches to change the installation order. If one of the patches shows a **CORRUPT PATCH** in the component list, remove it and add a different patch. Do not select corrupted patches in a production environment. You want to ensure all the patches in the baseline are successfully tested in your environment.

11. Click **OK** to create the baseline.

12. Review the baseline information.

13. Click the **Applicable Computers** tab. If **IEMCLIENT1** is not in the list, wait a few minutes for the relevance statements to evaluate. You can periodically click **Refresh Console** at the top of the IBM Endpoint Manager Console to update the Console.

14. Click the **Description** tab.

15. To deploy the baseline, click the hyper-link within the **Click here to deploy this action group** text.

16. Select **IEMCLIENT1** in the **Target** list.

17. Click the **Execution** tab. Verify that the Behavior setting **Run all member actions of action group regardless of errors** is selected. Click **OK** to run the baseline actions.

18. Monitor the status of the baseline action. You can periodically click **Refresh Console** at the top of the IBM Endpoint Manager Console to see the status changes. Wait until the status changes to **Completed** before continuing.