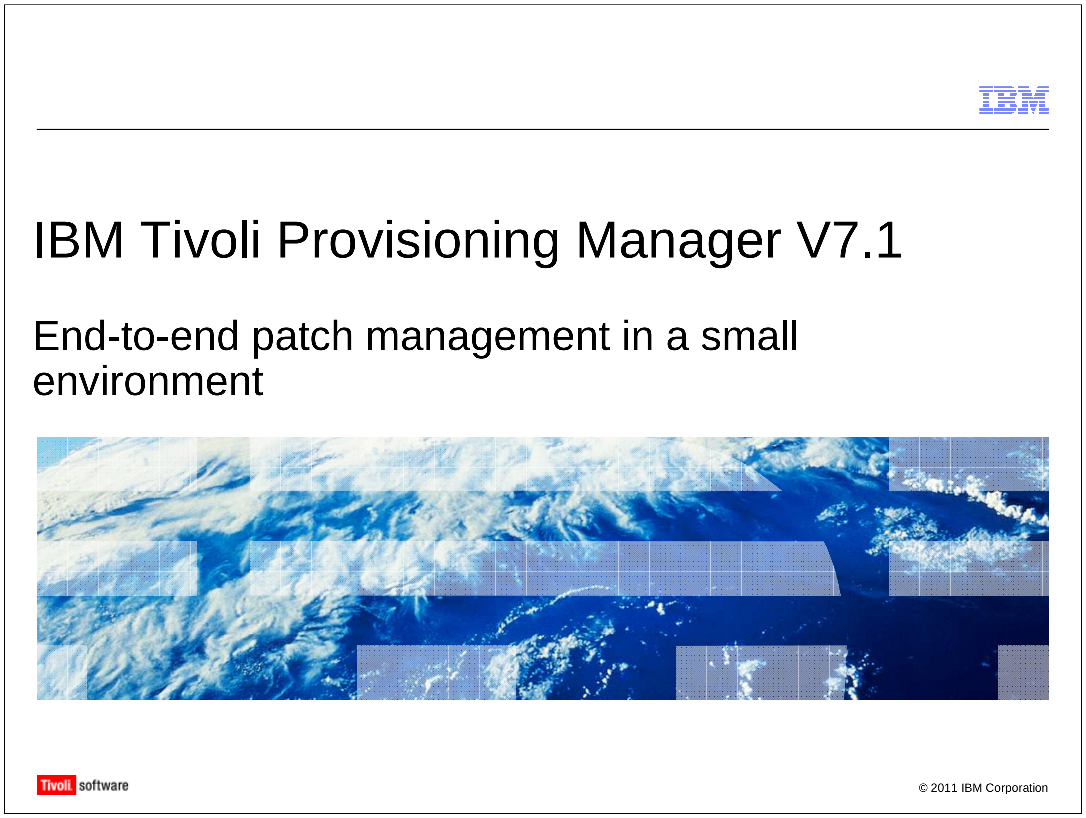
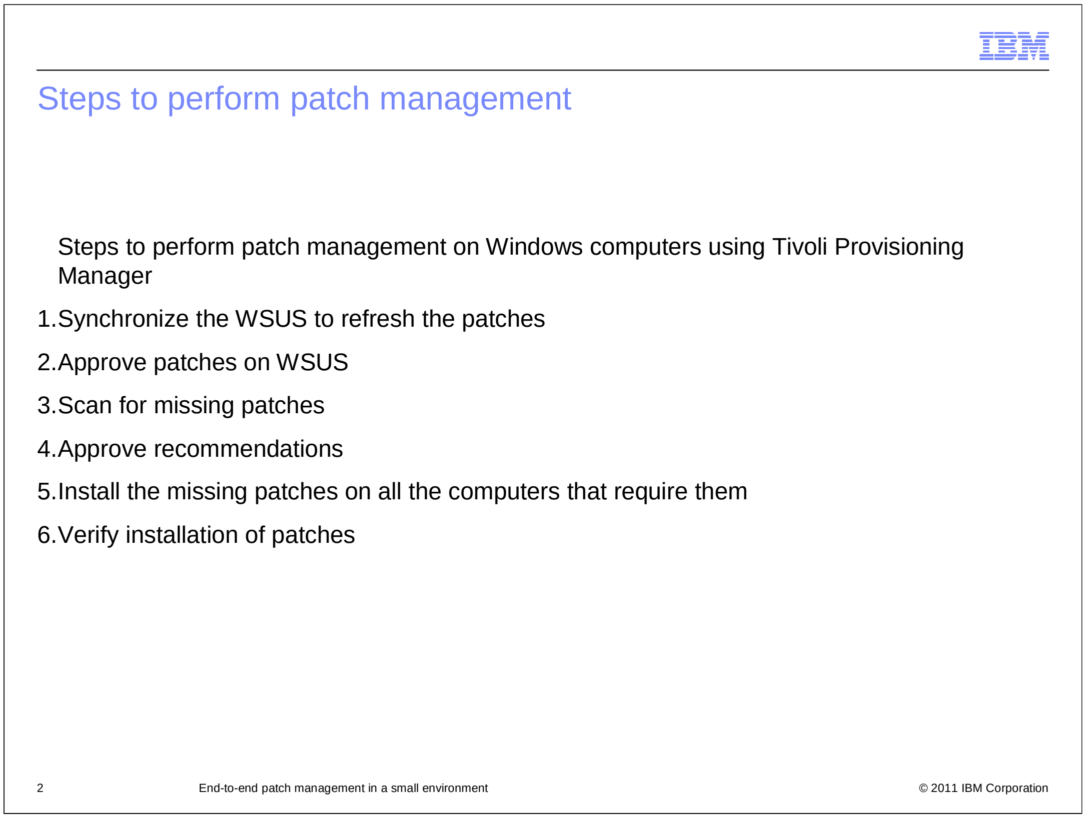


IBM Tivoli Provisioning Manager V7.1

End-to-end patch management in a small environment

Welcome to this training module on IBM Tivoli® Provisioning Manager version 7.1, end-to-end patch management in a small environment. In this presentation, you learn about managing Windows® Server Update Services in a small network environment.



Steps to perform patch management

Steps to perform patch management on Windows computers using Tivoli Provisioning Manager

1.Synchronize the WSUS to refresh the patches

2.Approve patches on WSUS

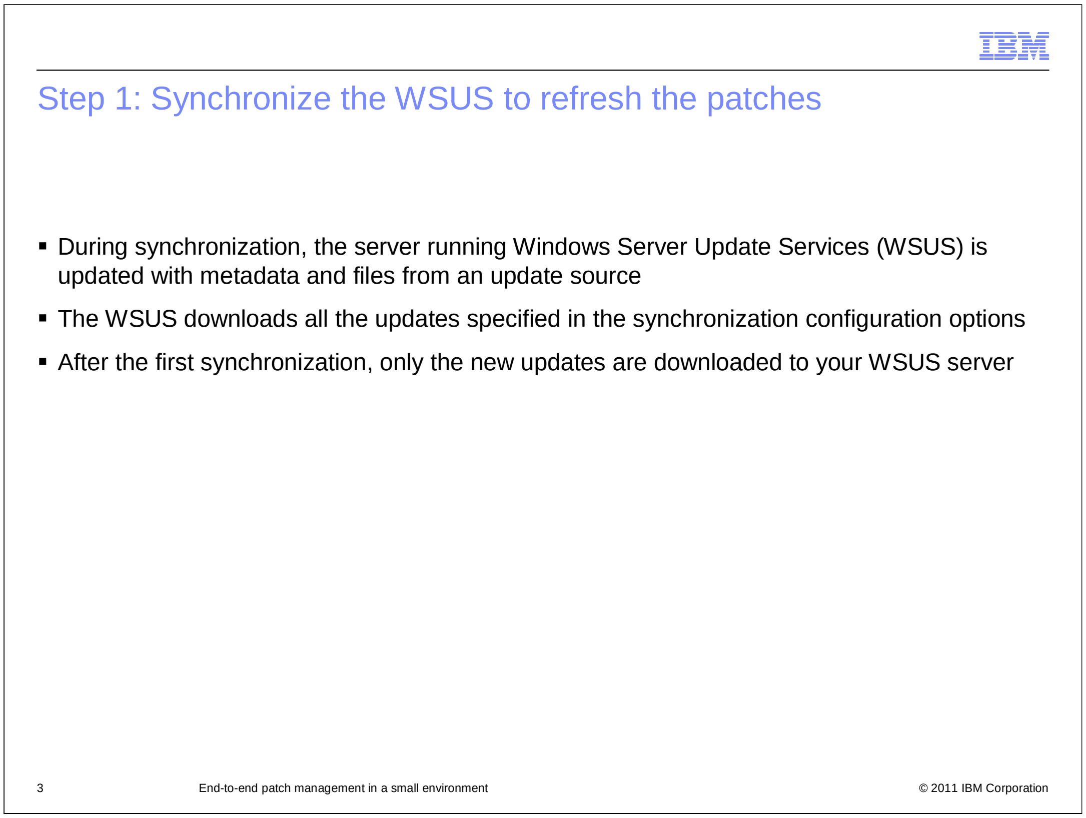
3.Scan for missing patches

4.Approve recommendations

5.Install the missing patches on all the computers that require them

6.Verify installation of patches

You use patch management to deploy missing software patches to target computers or groups of computers that require them. To perform patch management on Windows computers, you first synchronize the Windows Server Update Services (WSUS) server to refresh the patches.

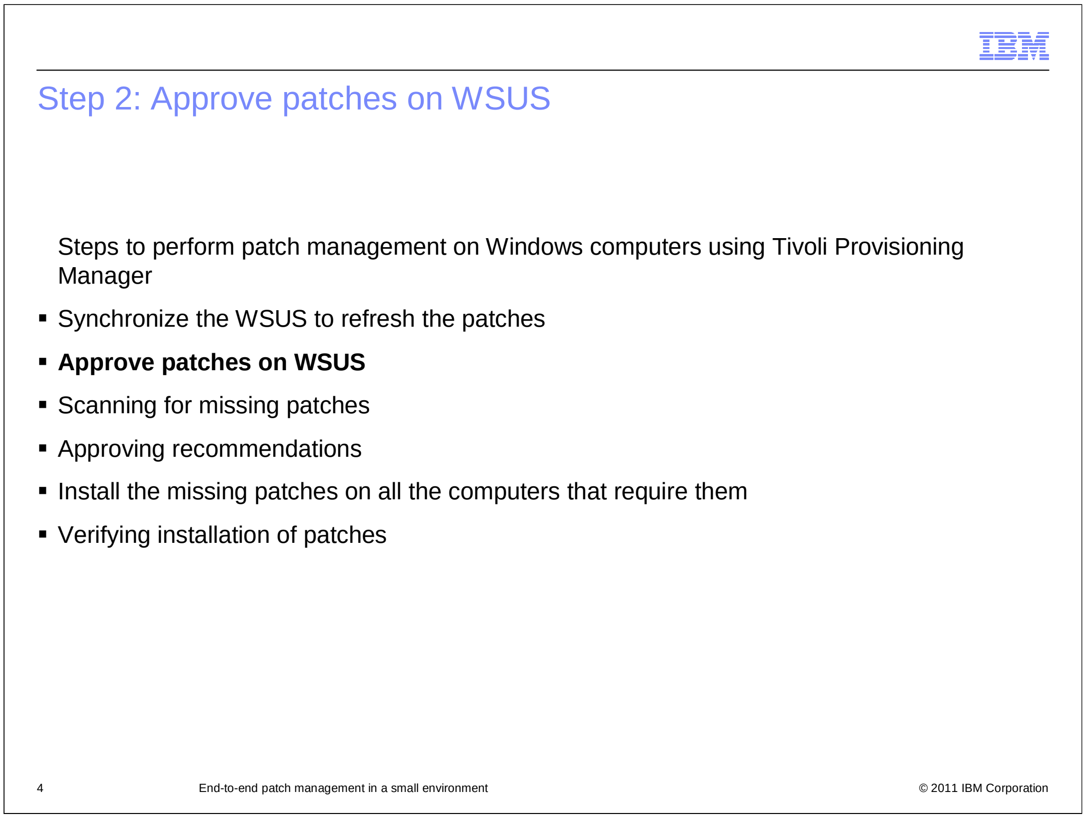


Step 1: Synchronize the WSUS to refresh the patches

- During synchronization, the server running Windows Server Update Services (WSUS) is updated with metadata and files from an update source
- The WSUS downloads all the updates specified in the synchronization configuration options
- After the first synchronization, only the new updates are downloaded to your WSUS server

3 End-to-end patch management in a small environment © 2011 IBM Corporation

During synchronization, the server running Windows Server Update Services is updated with metadata and files from the update source. After the first synchronization, your WSUS server downloads and updates only new patches.



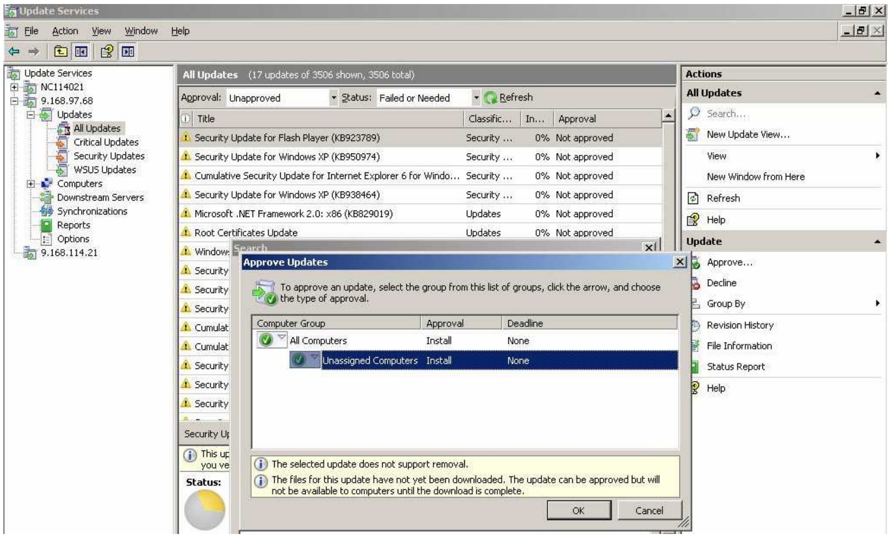
Step 2: Approve patches on WSUS

Steps to perform patch management on Windows computers using Tivoli Provisioning Manager

- Synchronize the WSUS to refresh the patches
- **Approve patches on WSUS**
- Scanning for missing patches
- Approving recommendations
- Install the missing patches on all the computers that require them
- Verifying installation of patches

The next step in patch management is to approve the patches downloaded by Windows Server Update Services.

Approving patches



All Updates (17 updates of 3506 shown, 3506 total)

Approval: Unapproved Status: Failed or Needed Refresh

Title	Classific...	In...	Approval
Security Update for Flash Player (KB923789)	Security ...	0%	Not approved
Security Update for Windows XP (KB950974)	Security ...	0%	Not approved
Cumulative Security Update for Internet Explorer 6 for Windo...	Security ...	0%	Not approved
Security Update for Windows XP (KB938464)	Security ...	0%	Not approved
Microsoft .NET Framework 2.0: x86 (KB829019)	Updates	0%	Not approved
Root Certificates Update	Updates	0%	Not approved
Window:			
Security			
Security			
Security			
Cumulat			
Cumulat			
Security			
Security			
Security			

Approve Updates

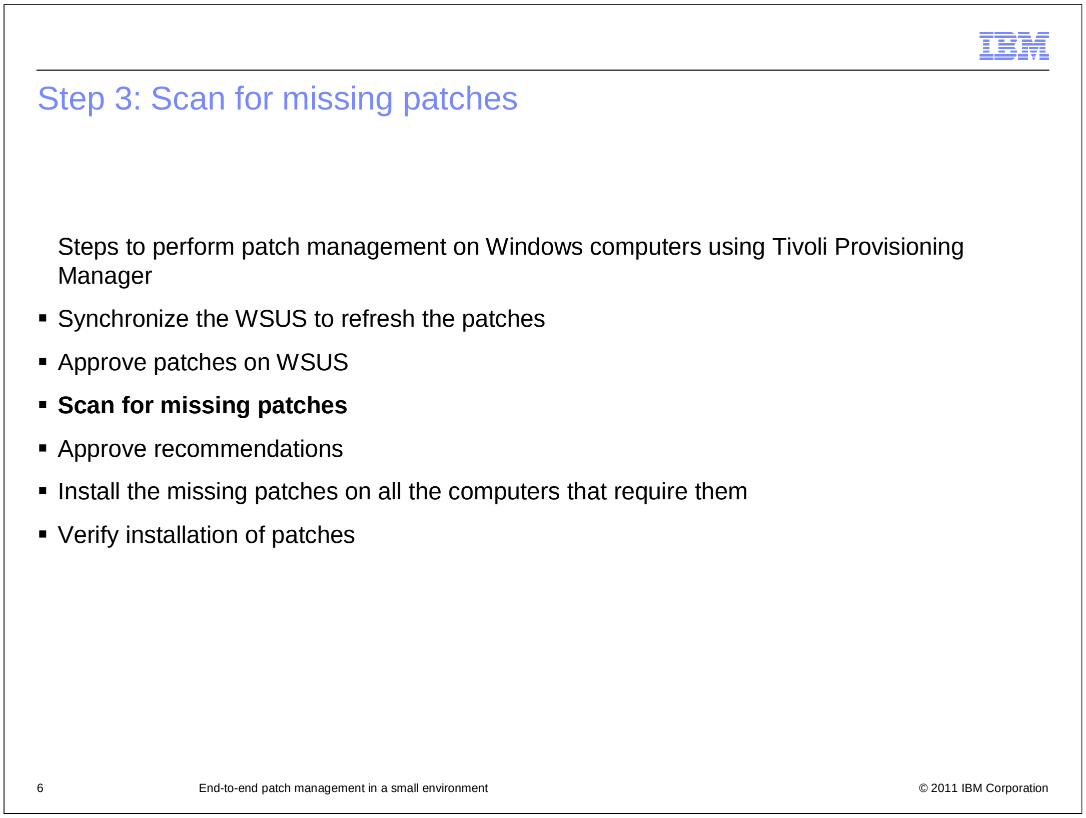
To approve an update, select the group from this list of groups, click the arrow, and choose the type of approval.

Computer Group	Approval	Deadline
All Computers	Install	None
Unassigned Computers	Install	None

The selected update does not support removal.

The files for this update have not yet been downloaded. The update can be approved but will not be available to computers until the download is complete.

Here, you see the Windows Server Update Services GUI with patches to approve. Right-click any of the patches that are listed in the Approve Updates window. Click the arrow to select the type of approval, and click OK.

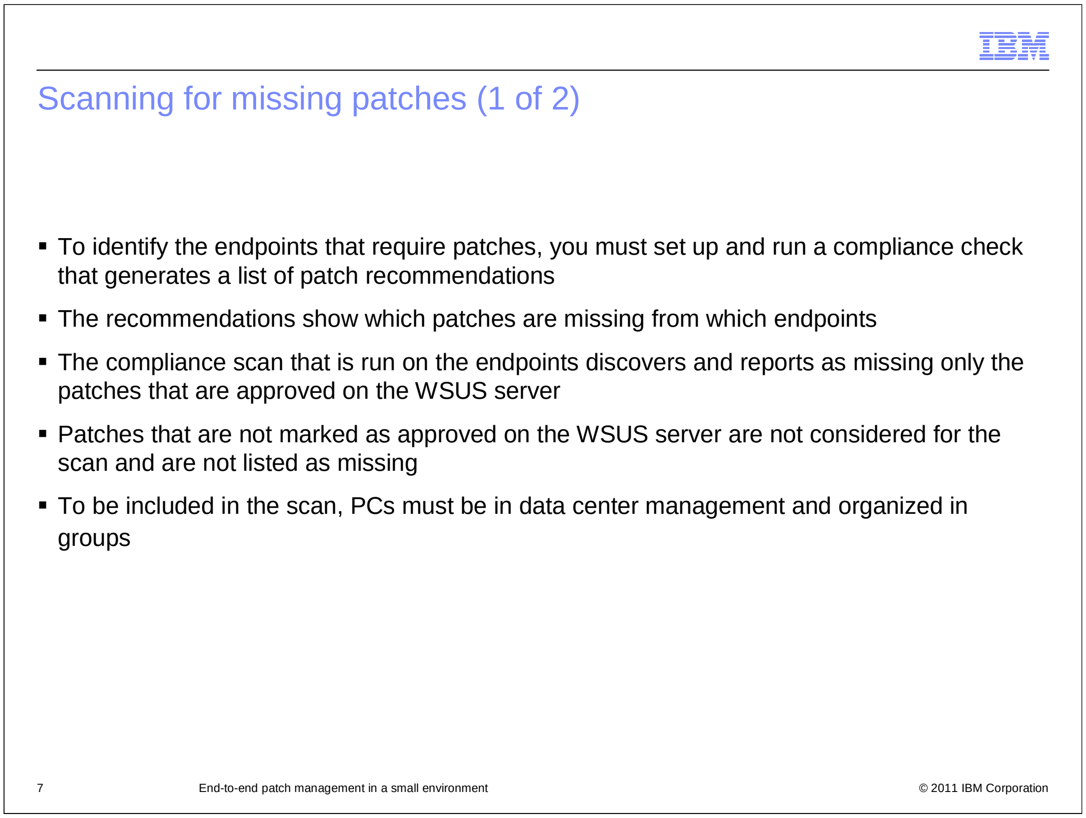


Step 3: Scan for missing patches

Steps to perform patch management on Windows computers using Tivoli Provisioning Manager

- Synchronize the WSUS to refresh the patches
- Approve patches on WSUS
- **Scan for missing patches**
- Approve recommendations
- Install the missing patches on all the computers that require them
- Verify installation of patches

The third step is to scan for missing patches.



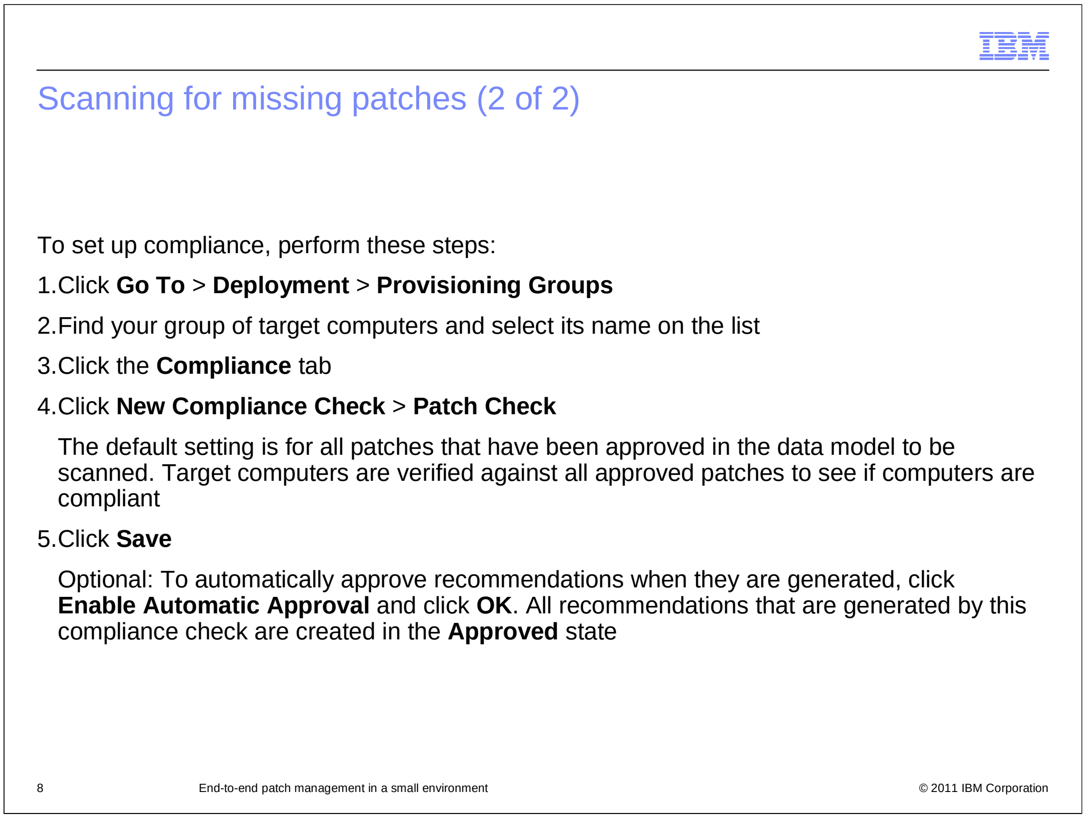
Scanning for missing patches (1 of 2)

- To identify the endpoints that require patches, you must set up and run a compliance check that generates a list of patch recommendations
- The recommendations show which patches are missing from which endpoints
- The compliance scan that is run on the endpoints discovers and reports as missing only the patches that are approved on the WSUS server
- Patches that are not marked as approved on the WSUS server are not considered for the scan and are not listed as missing
- To be included in the scan, PCs must be in data center management and organized in groups

To identify the endpoints that require patches, you set up and run a compliance check scan to generate a list of patch recommendations. The list shows which endpoints require patches.

This scan only reports missing patches that have already been approved for the Windows Server Update Services server. Unapproved patches are not considered in the scan.

PCs must be in data center management and organized by groups for this compliance check scan. Discovery creation and user group configuration must be completed before performing this scan.



Scanning for missing patches (2 of 2)

To set up compliance, perform these steps:

1.Click **Go To** > **Deployment** > **Provisioning Groups**

2.Find your group of target computers and select its name on the list

3.Click the **Compliance** tab

4.Click **New Compliance Check** > **Patch Check**

The default setting is for all patches that have been approved in the data model to be scanned. Target computers are verified against all approved patches to see if computers are compliant

5.Click **Save**

Optional: To automatically approve recommendations when they are generated, click **Enable Automatic Approval** and click **OK**. All recommendations that are generated by this compliance check are created in the **Approved** state

To set up the compliance scan, click Go To > Deployment > Provisioning Groups.

Select the name of your grouped target computers.

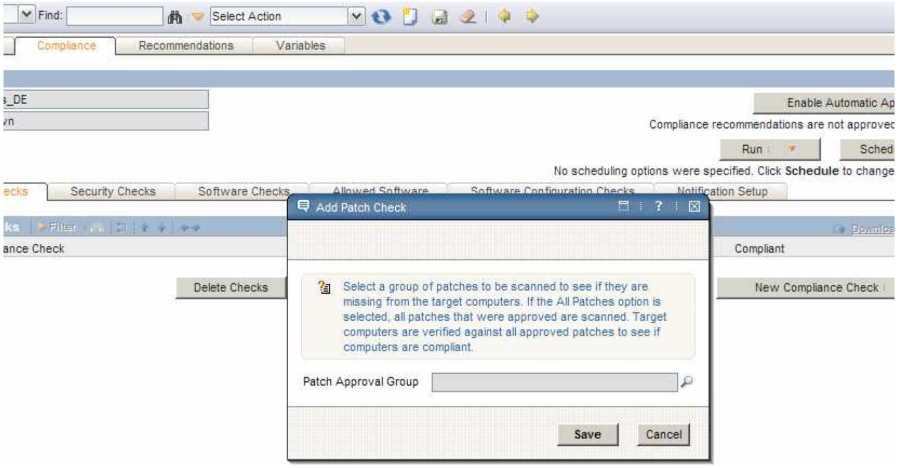
Click the Compliance tab.

Click New Compliance Check > Patch Check. If you click Select Value in this field, you can select a group of patches to be scanned for more rigorous control over the patches that are deployed to specific computers.

Click Save.

An optional step is to automatically approve recommendations when they are generated. Click Enable Automatic Approval and click OK in the message box.

Scanning for a group of missing patches



Compliance recommendations are not approvec

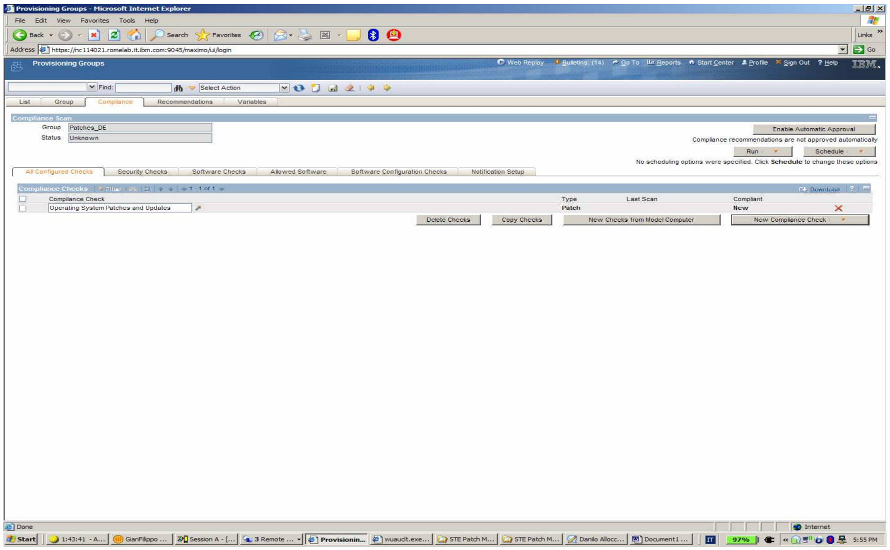
No scheduling options were specified. Click **Schedule** to change

Select a group of patches to be scanned to see if they are missing from the target computers. If the All Patches option is selected, all patches that were approved are scanned. Target computers are verified against all approved patches to see if computers are compliant.

Patch Approval Group

In this example, you use the Add Patch Check dialog box to select a group of patches to scan. Use the Select Value option to select the group.

Compliance check



Address: https://nc114021.romelab.it.ibm.com:9045/maximo/ui/login

Provisioning Groups

Select Action

Compliance Scan

Group: Patches_DE

Status: Unknown

Enable Automatic Approval

Compliance recommendations are not approved automatically

Run | Schedule

No scheduling options were specified. Click **Schedule** to change these options

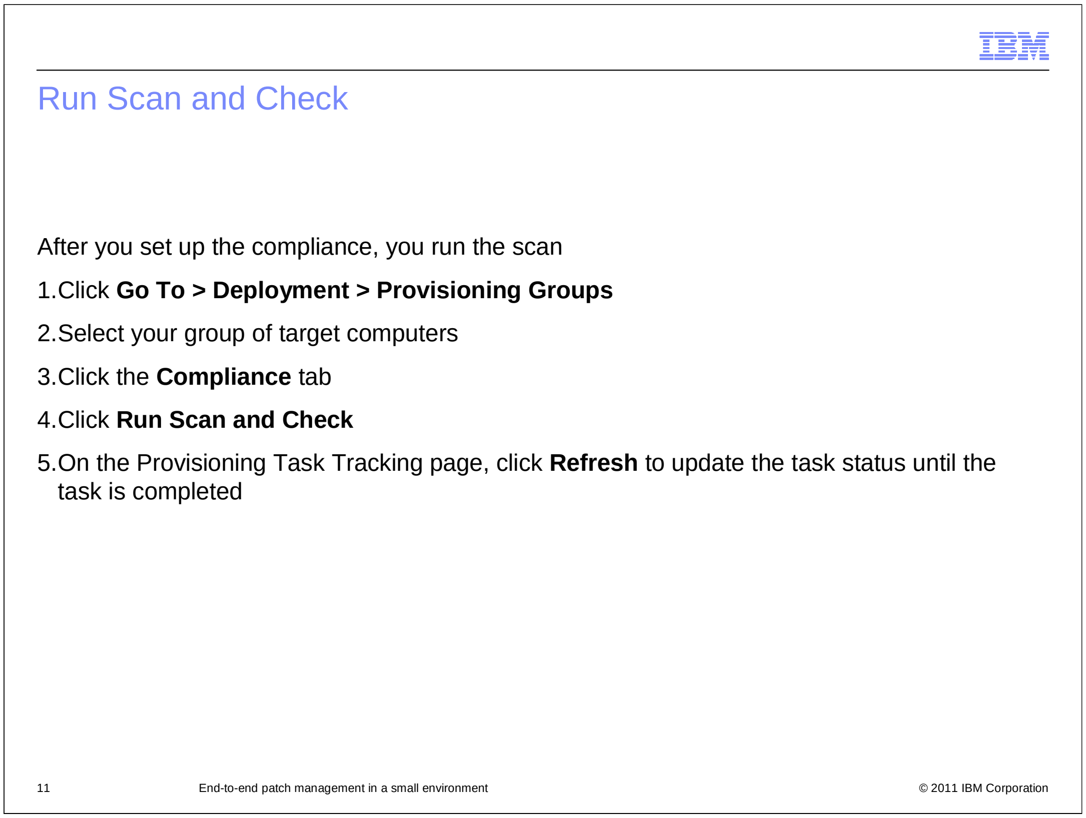
All Configured Checks | Security Checks | Software Checks | Allowed Software | Software Configuration Checks | Notification Setup

Compliance Checks | Filter | 1 - 1 of 1 | Download

□	Compliance Check	Type	Last Scan	Compliant
□	Operating System Patches and Updates	**Patch**		**New**

Delete Checks | Copy Checks | New Checks from Model Computer | New Compliance Check

This screen capture shows a compliance check of the operating system patches and updates.



Run Scan and Check

After you set up the compliance, you run the scan

1. Click **Go To > Deployment > Provisioning Groups**
2. Select your group of target computers
3. Click the **Compliance** tab
4. Click **Run Scan and Check**
5. On the Provisioning Task Tracking page, click **Refresh** to update the task status until the task is completed

After you set up compliance, you run a scan and check.

Click Go To > Deployment > Provisioning Groups.

Select your target computers.

Click the Compliance tab.

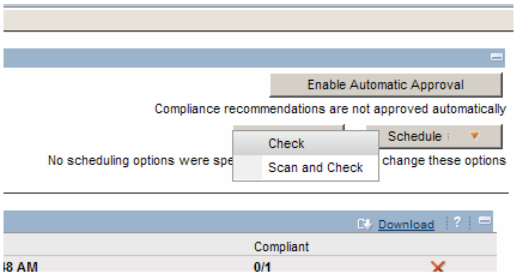
Click Run Scan and Check.

On the Provisioning Task Tracking page, click Refresh to update the task status until the task is completed.

Run Check

You can run Scan and Check or Check

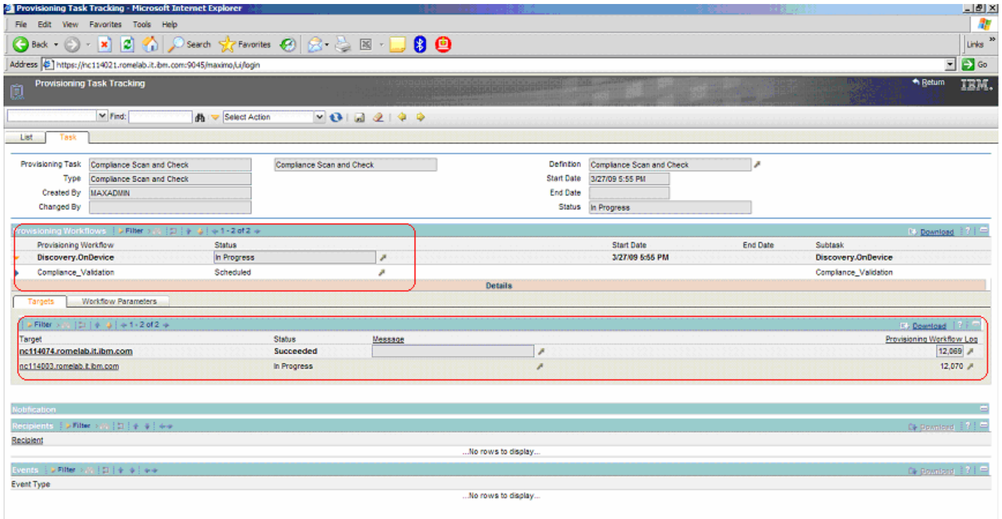
- Run Check without scan only if a compliance scan was previously performed
- Run Check without scan when an operator is present to evaluate the recommendations


Enable Automatic Approval
Compliance recommendations are not approved automatically
Check
Scan and Check
Schedule
No scheduling options were spe
change these options
Download
?
Compliant
8 AM
0/1

12 End-to-end patch management in a small environment

You can run a Check instead of a Scan and Check by selecting Check from the Run menu. You should only run a check without a scan if a compliance scan was performed previously. An operator is typically present when you run a check without a scan. The operator evaluates the recommendations.

Scanning for missing patches: Tasks



Provisioning Task Tracking

Provisioning Task	Compliance Scan and Check	Definition	Compliance Scan and Check
Type	Compliance Scan and Check	Start Date	3/27/09 5:55 PM
Created By	MAXADMIN	End Date	
Changed By		Status	In Progress

Provisioning Workflows

Provisioning Workflow	Status	Start Date	End Date	Subtask
Discovery.OnDevice	In Progress	3/27/09 5:55 PM		Discovery.OnDevice
Compliance_Validation	Scheduled			Compliance_Validation

Details

Targets

Target	Status	Message	Provisioning Workflow Log
nc114074.romelab.it.ibm.com	Succeeded		12,069
nc114003.romelab.it.ibm.com	In Progress		12,070

Notification

Recipients

Recipient

...No rows to display...

Events

Event Type

...No rows to display...

In the Provisioning Task Tracking window, you refresh your browser until the task status changes to Succeeded.

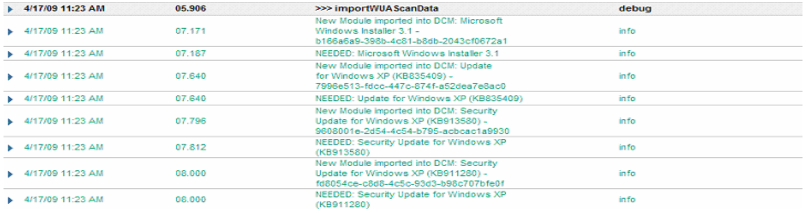
Scanning for missing patches

Run the Provisioning Task Compliance **Scan and Check** to start the workflow MS_WUA_Scan

- Download the vbs script, wua.vbs, to all machines in the group by using an RXA protocol
- The script is copied into the **%WINDIR%/tmp** directory and is run

```
cscript //Nologo wua.vbs 1 http://wsus_fully_qualified_name
wua_missing_updates_device_id
```

- The results are collected in the file **wua_missing_updates_device_id**, and data is uploaded to the data center management
- If a patch is approved on the WSUS, it is uploaded, and the status is set as **Approved**



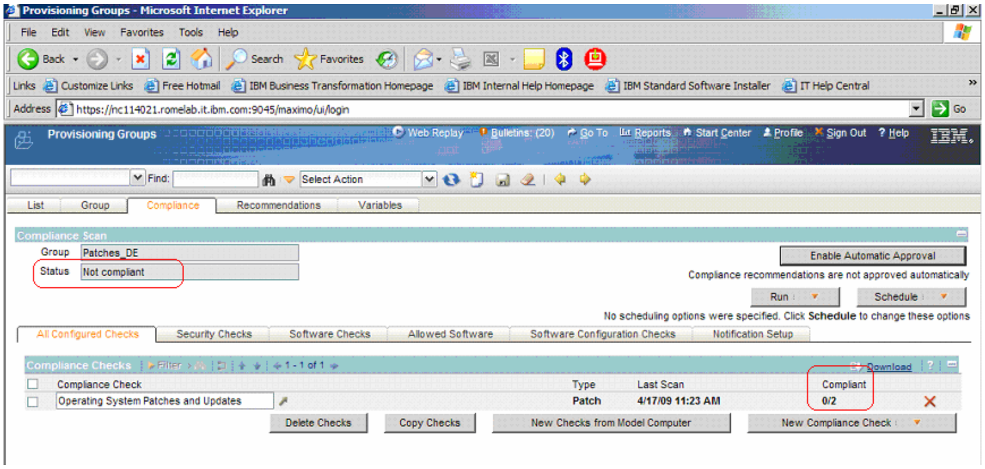
4/17/09 11:23 AM	05.906	>>> importWUAScanData	debug
4/17/09 11:23 AM	07.171	New Module imported into DCM: Microsoft Windows Installer 3.1 - b166a6a9-398b-4c81-b8db-2043cf0672a1	info
4/17/09 11:23 AM	07.187	NEEDED: Microsoft Windows Installer 3.1	info
4/17/09 11:23 AM	07.640	New Module imported into DCM: Update for Windows XP (KB835409) - 7996e513-fdcc-447c-874f-a52dea7e8ac0	info
4/17/09 11:23 AM	07.640	NEEDED: Update for Windows XP (KB835409)	info
4/17/09 11:23 AM	07.796	New Module imported into DCM: Security Update for Windows XP (KB913580) - 9608001e-2d54-4c54-b795-acbcac1a9930	info
4/17/09 11:23 AM	07.812	NEEDED: Security Update for Windows XP (KB913580)	info
4/17/09 11:23 AM	08.000	New Module imported into DCM: Security Update for Windows XP (KB911280) - fd8054ce-c8d8-4c5c-93d3-b98c707bfe0f	info
4/17/09 11:23 AM	08.000	NEEDED: Security Update for Windows XP (KB911280)	info

Use Scan and Check to start the MS_WUA_Scan workflow and download the vbs script, wua.vbs, to all target machines. Use an RXA protocol for this download.

The script is copied into the %WINDIR%/tmp directory and runs like the example on the slide.

The results of the script are collected in wua_missing_updates_device_id. If necessary, results are uploaded to the data center management.

Scanning for missing patches: Results



Compliance Scan

Group: Patches_DE

Status: Not compliant

Compliance recommendations are not approved automatically

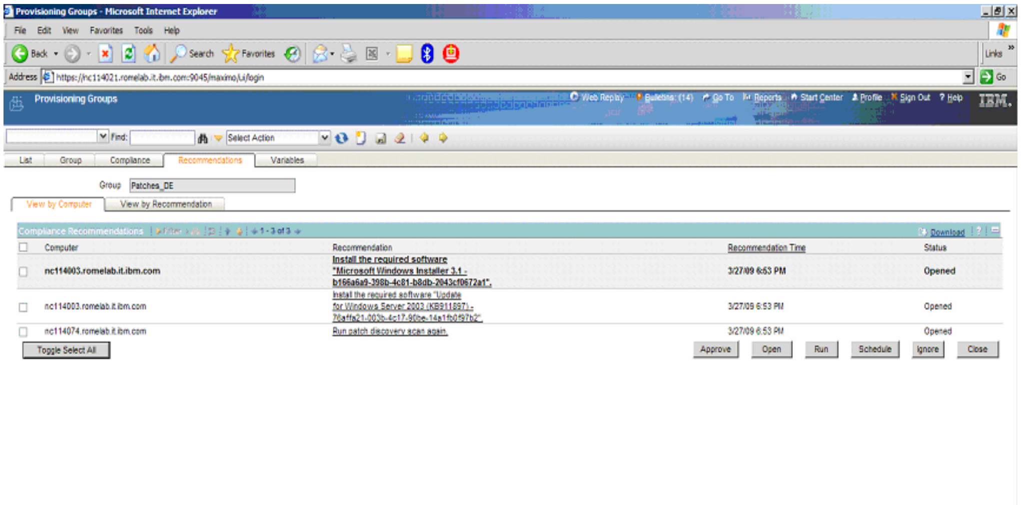
No scheduling options were specified. Click **Schedule** to change these options

Compliance Checks

□	Compliance Check	Type	Last Scan	Compliant
□	Operating System Patches and Updates	**Patch**	**4/17/09 11:23 AM**	**0/2**

When the scanning task is completed, the status is displayed on the Provision Task Tracking page. You can see if the patch group is in compliance by going to the Compliance tab. In this case, no devices are in compliance.

Scanning for missing patches: Recommendations



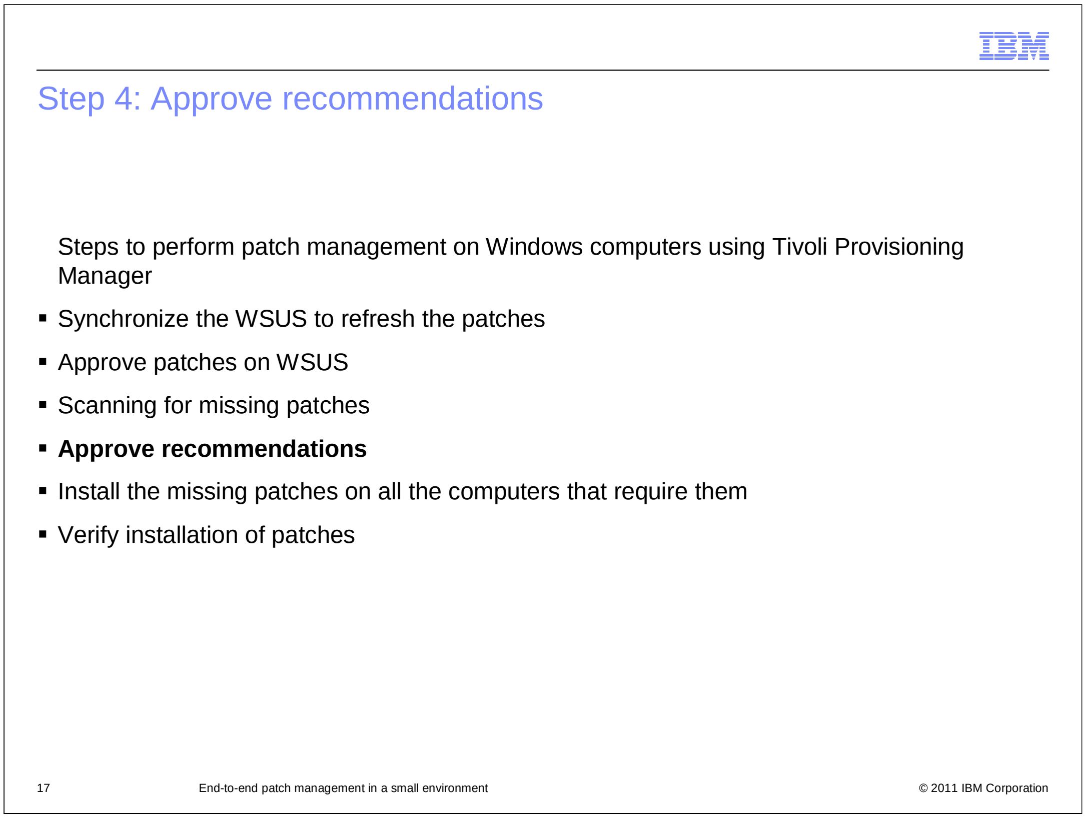
Provisioning Groups - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://nc114021.romelab.it.ibm.com:9045/maximo/ui/login
Provisioning Groups
Find:
Select Action
List
Group
Compliance
Recommendations
Variables

Group: Patches_DE

View by Computer
View by Recommendation
Compliance Recommendations
1 - 3 of 3
Download

□	Computer	Recommendation	Recommendation Time	Status
□	nc114003.romelab.it.ibm.com	Install the required software "Microsoft Windows Installer 3.1 - b166a6a9-398b-4c81-b8db-2043cf0672a1".	3/27/09 6:53 PM	Opened
□	nc114003.romelab.it.ibm.com	Install the required software "Update for Windows Server 2003 (KB911897) - 76affa21-003b-4c17-90be-14a1fb0f97b2".	3/27/09 6:53 PM	Opened
□	nc114074.romelab.it.ibm.com	Run patch discovery scan again.	3/27/09 6:53 PM	Opened

You can view a generated list of recommended patches by clicking the Recommendations tab. In this screen capture, you see a list of recommended patches.

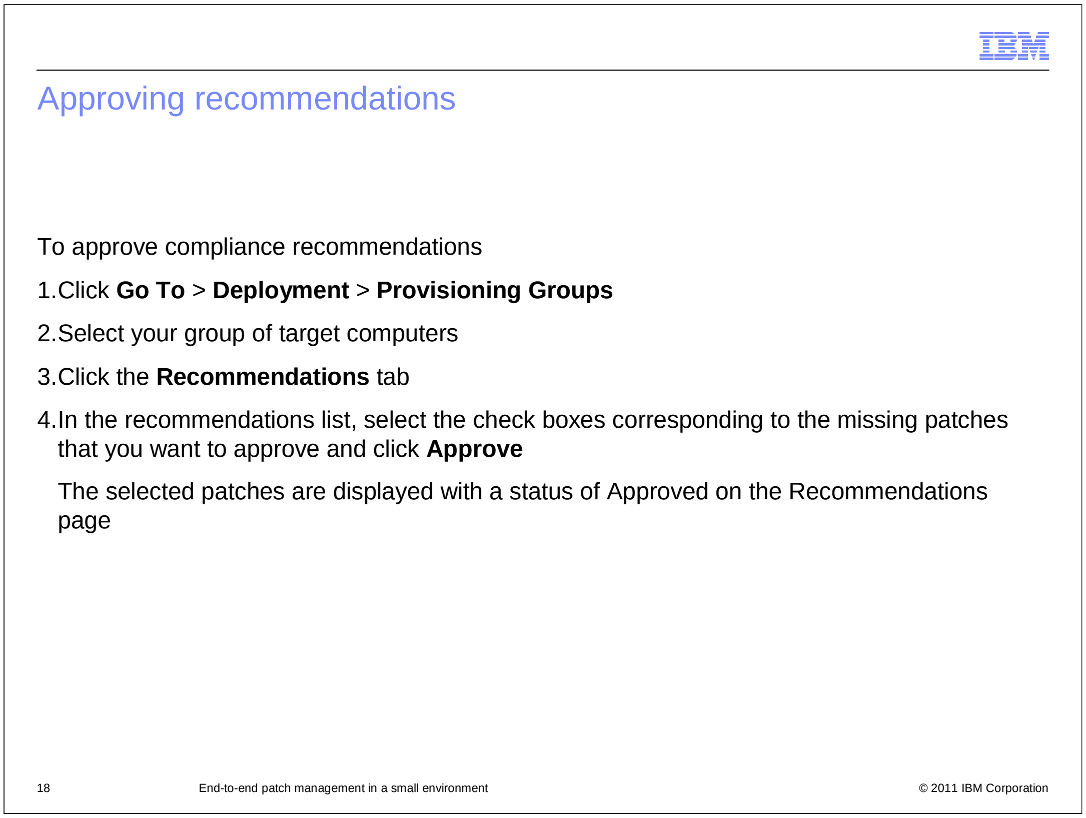


Step 4: Approve recommendations

Steps to perform patch management on Windows computers using Tivoli Provisioning Manager

- Synchronize the WSUS to refresh the patches
- Approve patches on WSUS
- Scanning for missing patches
- **Approve recommendations**
- Install the missing patches on all the computers that require them
- Verify installation of patches

The next step in patch management is to approve patch recommendations.



Approving recommendations

To approve compliance recommendations

1. Click **Go To** > **Deployment** > **Provisioning Groups**
2. Select your group of target computers
3. Click the **Recommendations** tab
4. In the recommendations list, select the check boxes corresponding to the missing patches that you want to approve and click **Approve**

   The selected patches are displayed with a status of Approved on the Recommendations page

Decide which patches you want to install after scanning and checking for compliance.

Click Go To > Deployment > Provisioning Groups.

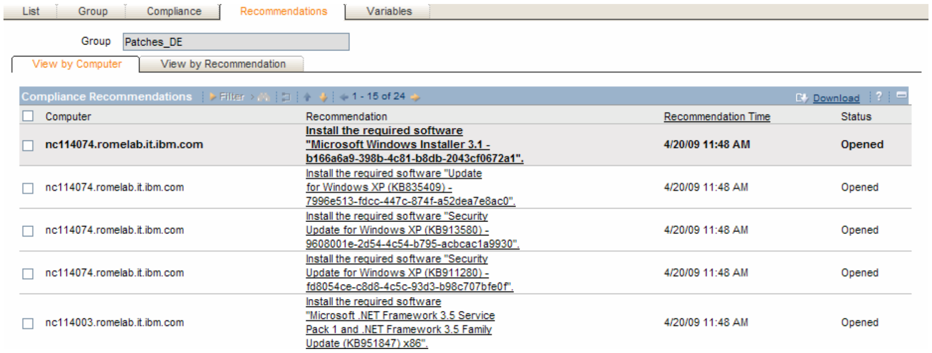
Select your group of target computers.

Click the Recommendations tab.

In the Recommendations list, select the check boxes corresponding to the missing patches that you want to approve and click Approve. The selected patches are displayed with the status of Approved on the Recommendations page.

Approving recommendations: Result

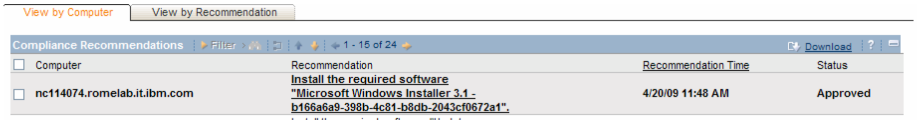
Before approval



Group: Patches_DE

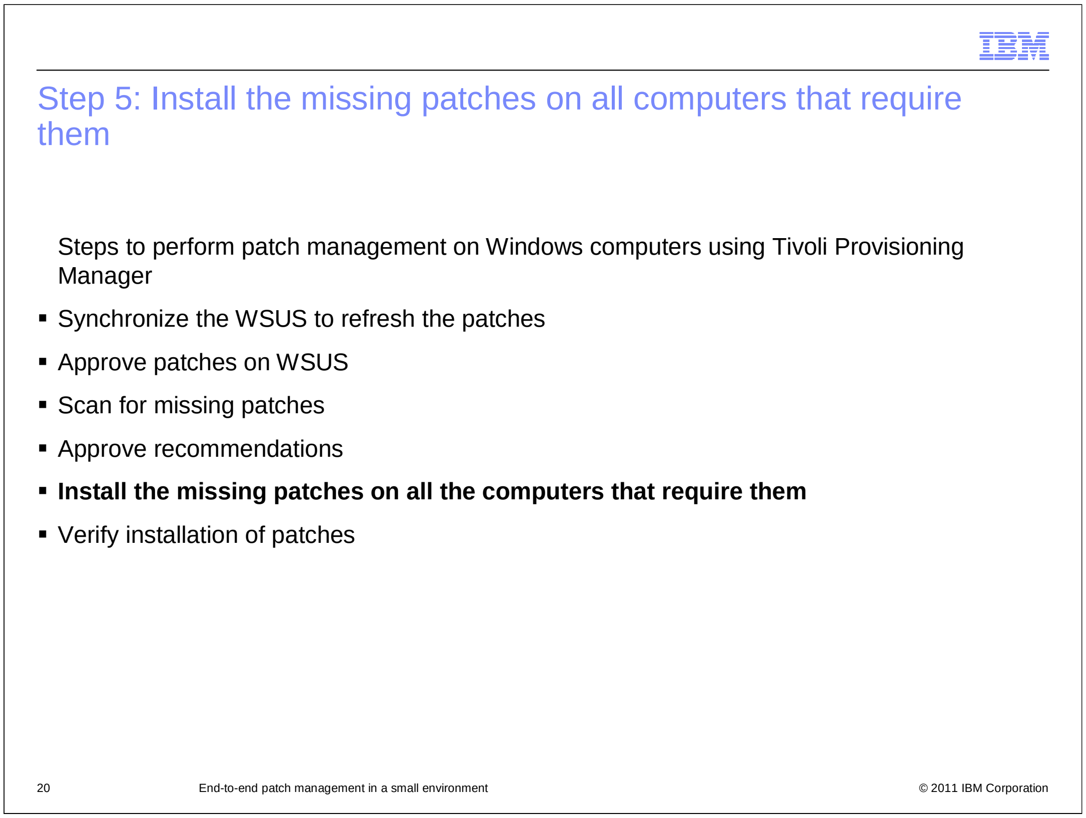
□	Computer	Recommendation	Recommendation Time	Status
□	**nc114074.romelab.it.ibm.com**	**Install the required software "Microsoft Windows Installer 3.1 - b166a6a9-398b-4c81-b8db-2043cf0672a1".**	**4/20/09 11:48 AM**	**Opened**
□	nc114074.romelab.it.ibm.com	Install the required software "Update for Windows XP (KB835409) - 7996e513-fdcc-447c-874f-a52dea7e8ac0".	4/20/09 11:48 AM	Opened
□	nc114074.romelab.it.ibm.com	Install the required software "Security Update for Windows XP (KB913580) - 9608001e-2d54-4c54-b795-acbcac1a9930".	4/20/09 11:48 AM	Opened
□	nc114074.romelab.it.ibm.com	Install the required software "Security Update for Windows XP (KB911280) - fd8054ce-c8d8-4c5c-93d3-b98c707bfe0f".	4/20/09 11:48 AM	Opened
□	nc114003.romelab.it.ibm.com	Install the required software "Microsoft .NET Framework 3.5 Service Pack 1 and .NET Framework 3.5 Family Update (KB951847) x86".	4/20/09 11:48 AM	Opened

After approval



□	Computer	Recommendation	Recommendation Time	Status
□	**nc114074.romelab.it.ibm.com**	**Install the required software "Microsoft Windows Installer 3.1 - b166a6a9-398b-4c81-b8db-2043cf0672a1".**	**4/20/09 11:48 AM**	**Approved**

In this example, the list of recommendations has a status of Opened. After approval, the status is Approved. After these patches have Approved status, you can install them.

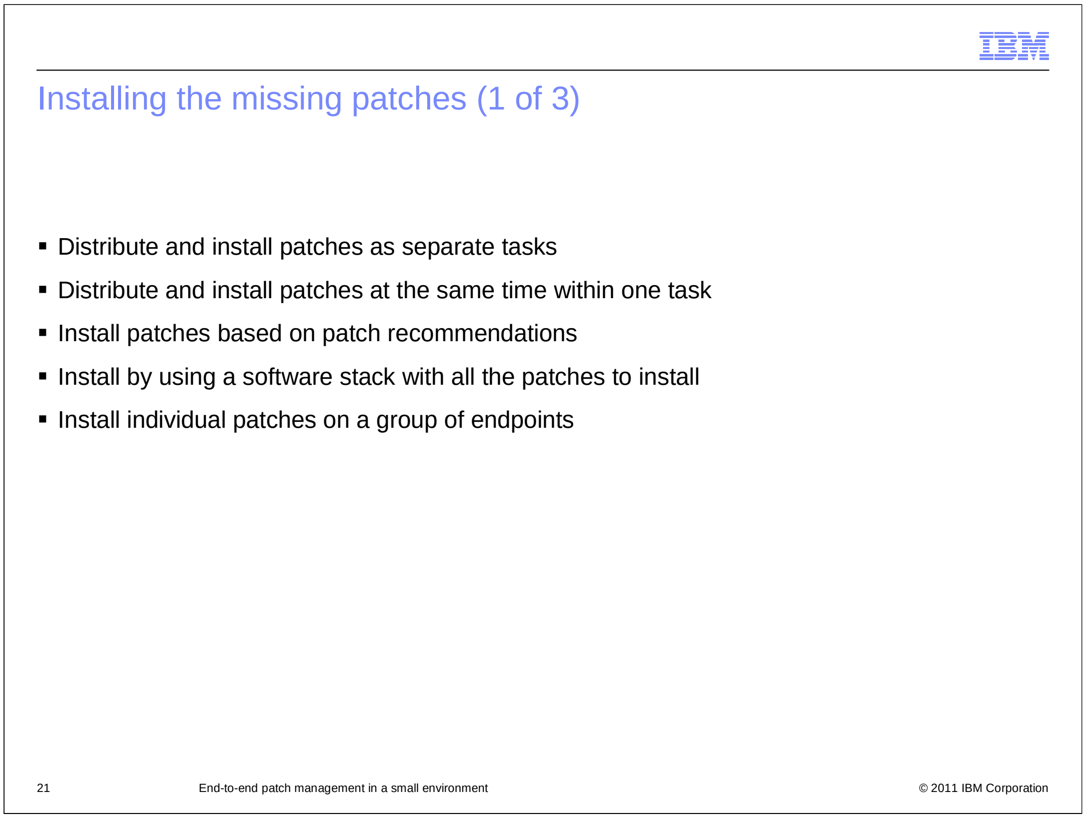


Step 5: Install the missing patches on all computers that require them

Steps to perform patch management on Windows computers using Tivoli Provisioning Manager

- Synchronize the WSUS to refresh the patches
- Approve patches on WSUS
- Scan for missing patches
- Approve recommendations
- **Install the missing patches on all the computers that require them**
- Verify installation of patches

After approving the recommended patches, you install the patches.



Installing the missing patches (1 of 3)

- Distribute and install patches as separate tasks
- Distribute and install patches at the same time within one task
- Install patches based on patch recommendations
- Install by using a software stack with all the patches to install
- Install individual patches on a group of endpoints

When installing patches, you have several options.

You can install the missing patches on all computers that require them as separate tasks.

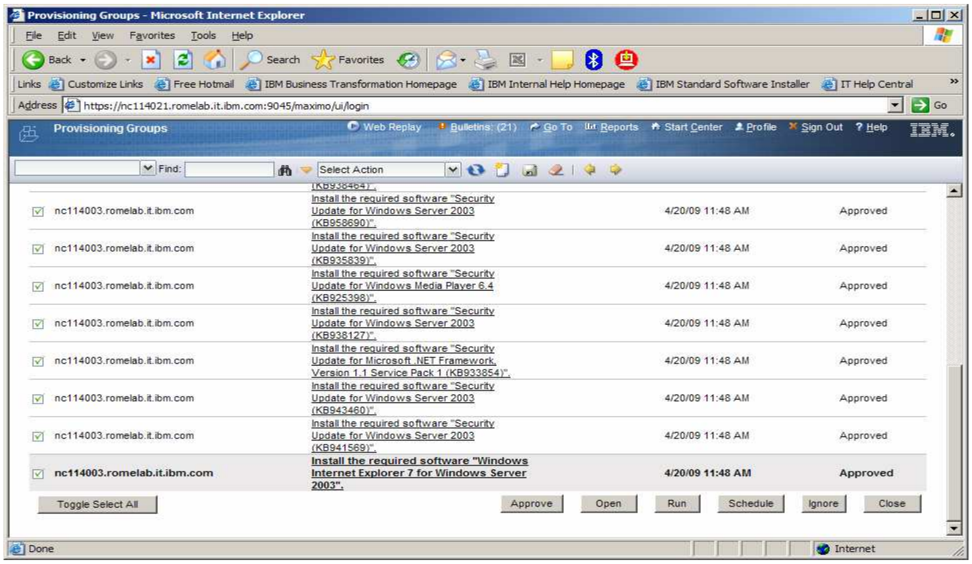
You can distribute the patches and install them as one task.

You can install patches based on patch recommendation.

You can install patches by using the software stack with all the patches to install.

You can install individual patches on groups of endpoints.

Installing the missing patches (2 of 3)



Provisioning Groups - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Links Customize Links Free Hotmail IBM Business Transformation Homepage IBM Internal Help Homepage IBM Standard Software Installer IT Help Central
Address https://nc114021.romelab.it.ibm.com:9045/maximo/ui/login
Go
Provisioning Groups
Web Replay Bulletins: (21) Go To Reports Start Center Profile Sign Out Help
Find:
Select Action

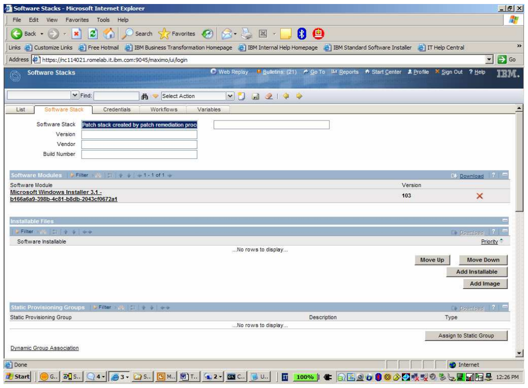
		(KB938464)".		
☑	nc114003.romelab.it.ibm.com	Install the required software "Security Update for Windows Server 2003 (KB958690)".	4/20/09 11:48 AM	Approved
☑	nc114003.romelab.it.ibm.com	Install the required software "Security Update for Windows Server 2003 (KB935839)".	4/20/09 11:48 AM	Approved
☑	nc114003.romelab.it.ibm.com	Install the required software "Security Update for Windows Media Player 6.4 (KB925398)".	4/20/09 11:48 AM	Approved
☑	nc114003.romelab.it.ibm.com	Install the required software "Security Update for Windows Server 2003 (KB938127)".	4/20/09 11:48 AM	Approved
☑	nc114003.romelab.it.ibm.com	Install the required software "Security Update for Microsoft .NET Framework, Version 1.1 Service Pack 1 (KB933854)".	4/20/09 11:48 AM	Approved
☑	nc114003.romelab.it.ibm.com	Install the required software "Security Update for Windows Server 2003 (KB943460)".	4/20/09 11:48 AM	Approved
☑	nc114003.romelab.it.ibm.com	Install the required software "Security Update for Windows Server 2003 (KB941569)".	4/20/09 11:48 AM	Approved
☑	**nc114003.romelab.it.ibm.com**	**Install the required software "Windows Internet Explorer 7 for Windows Server 2003".**	**4/20/09 11:48 AM**	**Approved**

In this example, you see a list of approved patches in the Provisioning Groups. Click Run to install the patches.

Installing the missing patches (3 of 3)

Running the LDO:
ComplianceRecommendationGroup.
Remediate

- Starts the workflow Default_Compliance_Recommendation_Group_Remediate
- Creates a software stack containing the patches approved
- Starts the workflow MS_WUA_Install_Updates


Software Stacks - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Links Customize Links Free Hotmail IBM Business Transformation Homepage IBM Internal Help Homepage IBM Standard Software Installer IT Help Central
Go
Web Replay Bulletins: (21) Go To Reports Start Center Profile Sign Out Help
IBM.
Find:
Select Action
List Software Stack Credentials Workflows Variables
Filter
1 - 1 of 1
Download
Move Up
Move Down
Add Installable
Add Image
Assign to Static Group
Dynamic Group Association
Done
Internet
Start
12:26 PM

Address: https://nc114021.romelab.it.ibm.com:9045/maximo/ui/login

Software Stacks

Software Stack: Patch stack created by patch remediation proc
Version:
Vendor:
Build Number:

Software Modules

Software Module	Version
Microsoft Windows Installer 3.1 - b166a6a9-398b-4c81-b8db-2043cf0672a1	103

Installable Files

Software Installable	Priority

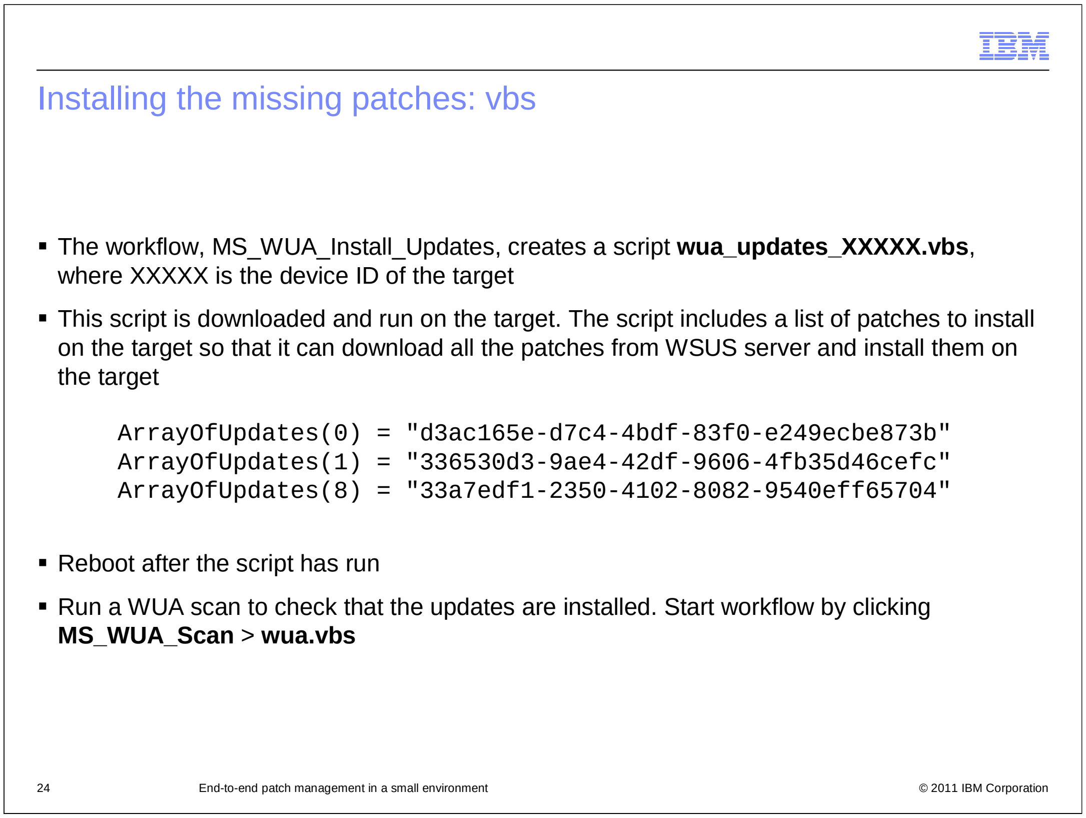
...No rows to display...

Static Provisioning Groups

Static Provisioning Group	Description	Type

...No rows to display...

Run the logical device operation named ComplianceRecommendationGroup.Remediate to begin the workflow, Default_Compliance_Recommentation_Group_Remediate. This workflow creates a software stack with the approved patches and begins the workflow, MS_WUA_Install_Updates.



Installing the missing patches: vbs

- The workflow, MS_WUA_Install_Updates, creates a script **wua_updates_XXXXX.vbs**, where XXXXX is the device ID of the target
- This script is downloaded and run on the target. The script includes a list of patches to install on the target so that it can download all the patches from WSUS server and install them on the target

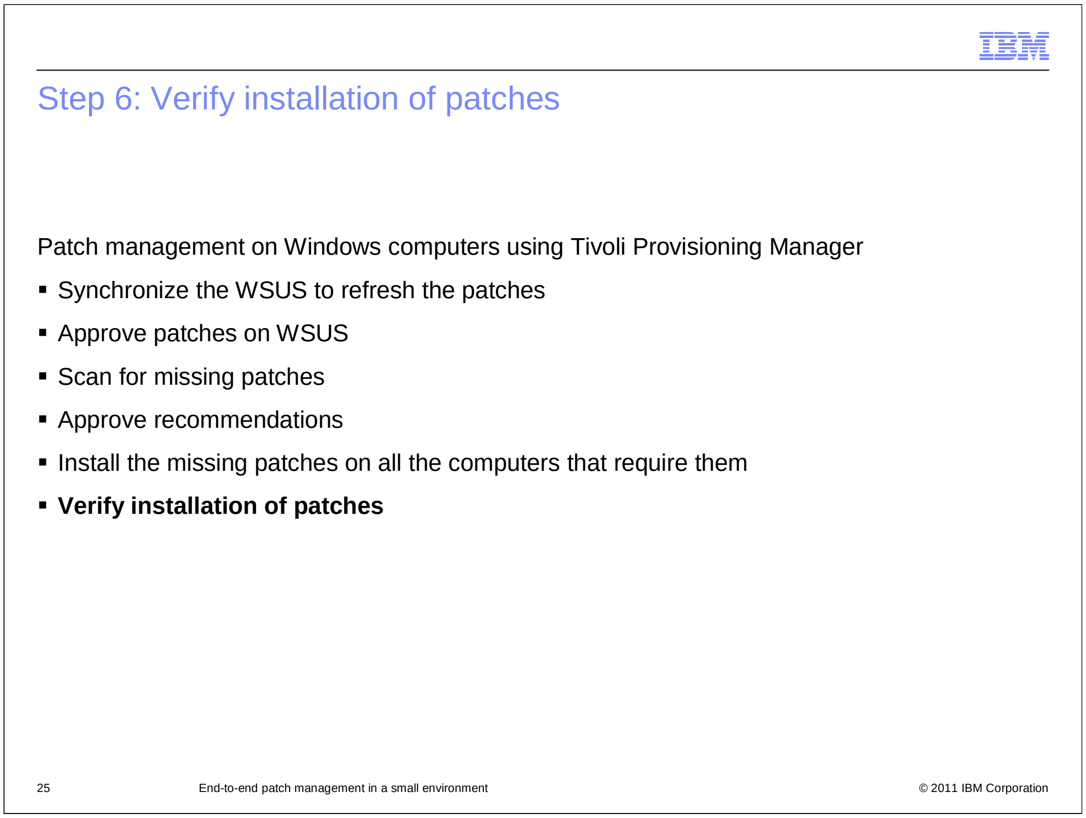
```
ArrayOfUpdates(0) = "d3ac165e-d7c4-4bdf-83f0-e249ecbe873b"
ArrayOfUpdates(1) = "336530d3-9ae4-42df-9606-4fb35d46cefc"
ArrayOfUpdates(8) = "33a7edf1-2350-4102-8082-9540eff65704"
```

- Reboot after the script has run
- Run a WUA scan to check that the updates are installed. Start workflow by clicking **MS_WUA_Scan** > **wua.vbs**

The workflow MS_WUA_Install_Updates creates a script named wua_update_XXXXX.vbs, where XXXXX is the device ID of the target. The script is downloaded from the Windows Server Update Services server and run on the target.

After the script is run, you might need to reboot. You can set an endpoint reboot notification through Tivoli Provisioning Manager End User Interaction Services, if reboot is required.

After you reboot, run a WUA scan to ensure the update is installed.



Step 6: Verify installation of patches

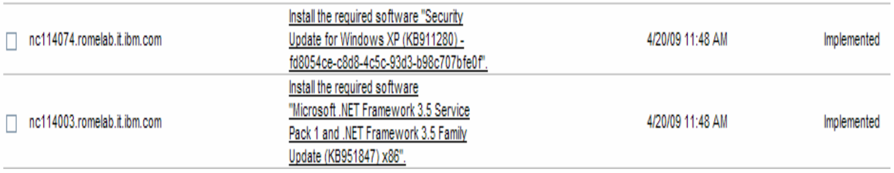
Patch management on Windows computers using Tivoli Provisioning Manager

- Synchronize the WSUS to refresh the patches
- Approve patches on WSUS
- Scan for missing patches
- Approve recommendations
- Install the missing patches on all the computers that require them
- **Verify installation of patches**

The final step in patch management is to verify the installation of your patches.

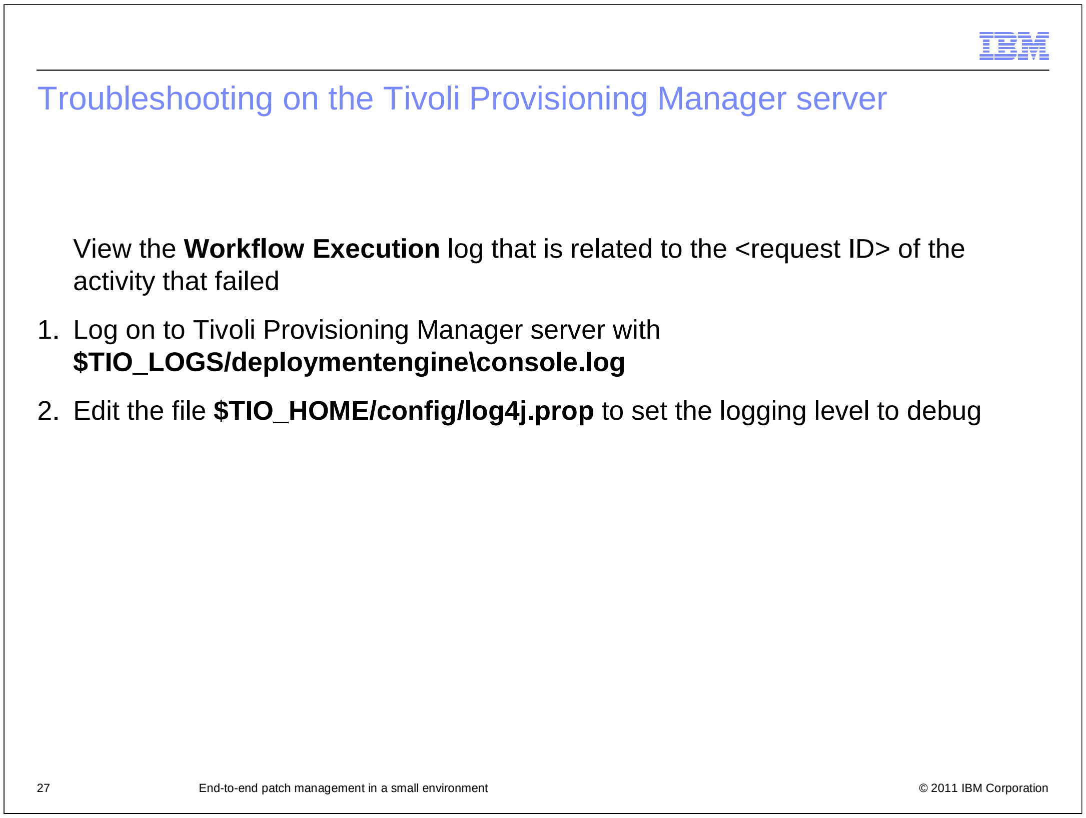
Verifying installation of patches

- After installing patches, you can verify patch compliance for your endpoints
- On the Group Recommendations tab, you can verify the Status column for your endpoints. For the patches that were installed successfully, you see a status of **Implemented**



□	nc114074.romelab.it.ibm.com	Install the required software "Security Update for Windows XP (KB911280) - fd8054ce-c8d8-4c5c-93d3-b98c707bfe0f".	4/20/09 11:48 AM	Implemented
□	nc114003.romelab.it.ibm.com	Install the required software "Microsoft .NET Framework 3.5 Service Pack 1 and .NET Framework 3.5 Family Update (KB951847) x86".	4/20/09 11:48 AM	Implemented

On the Group page of the Recommendations tab, verify patch compliance in the Status column for your endpoints. In the columns where patches were successfully deployed, you see a status of Implemented.



Troubleshooting on the Tivoli Provisioning Manager server

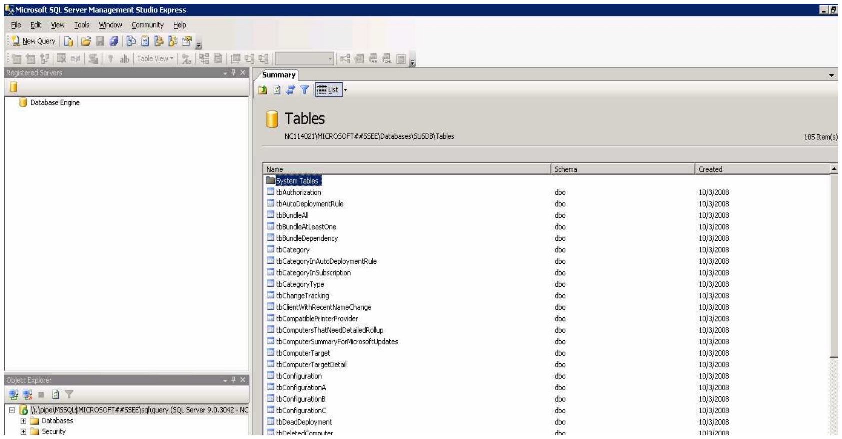
View the **Workflow Execution** log that is related to the <request ID> of the activity that failed

1. Log on to Tivoli Provisioning Manager server with **$TIO_LOGS/deploymentengine\console.log**
2. Edit the file **$TIO_HOME/config/log4j.prop** to set the logging level to debug

To troubleshoot on the Tivoli Provisioning Manager server, review the Workflow Execution Log for a failure of a <request ID> activity. Log on to the Tivoli Provisioning Manager server using the information on the slide and edit the file shown. Edit the file $TIO_HOME/config/log4j.prop to set the logging level to debug.

Troubleshooting on the WSUS server

- Access the database that stores the data, Microsoft® SQL Server 2005 Embedded Edition
- Use one of these tools:
  - – The graphical tool, Microsoft SQL Server Management Studio Express
  - – The command line tool, Microsoft SQL Server 2005 Command Line Query Utility



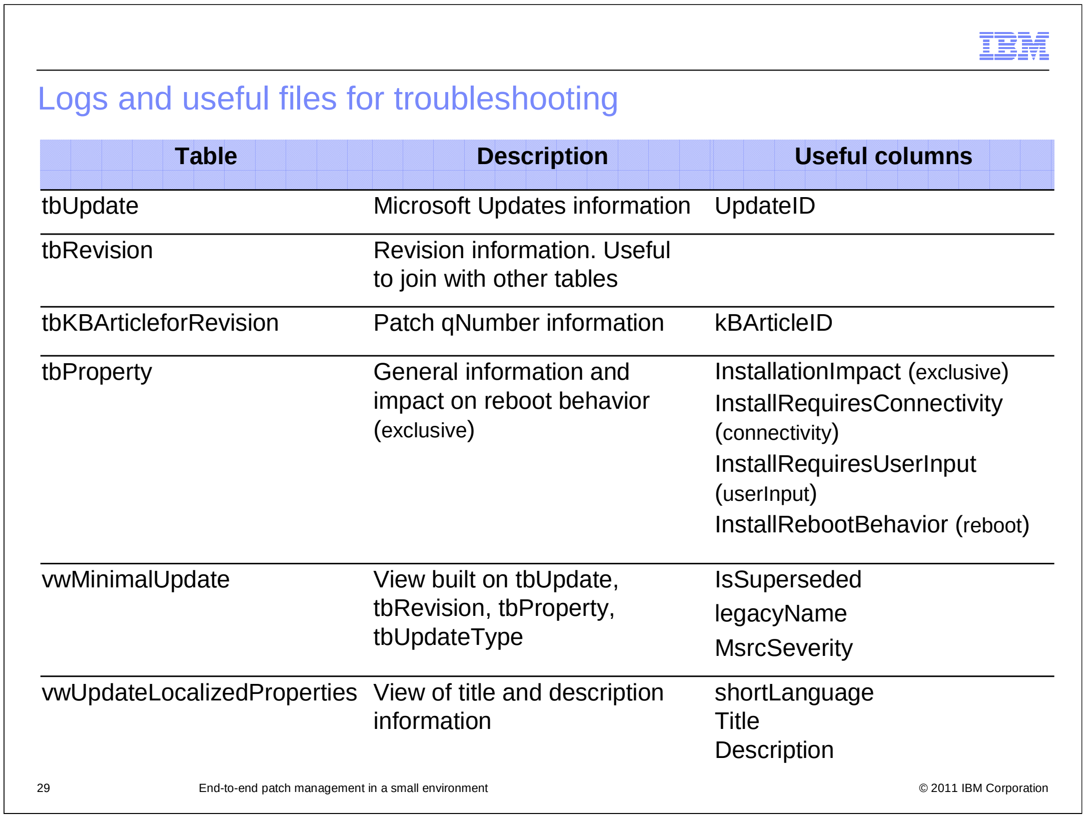
Tables

NC114021\MICROSOFT##SSEE\Databases\SUSDB\Tables

105 Item(s)

Name	Schema	Created
System Tables		
tbAuthorization	dbo	10/3/2008
tbAutoDeploymentRule	dbo	10/3/2008
tbBundleAll	dbo	10/3/2008
tbBundleAtLeastOne	dbo	10/3/2008
tbBundleDependency	dbo	10/3/2008
tbCategory	dbo	10/3/2008
tbCategoryInAutoDeploymentRule	dbo	10/3/2008
tbCategoryInSubscription	dbo	10/3/2008
tbCategoryType	dbo	10/3/2008
tbChangeTracking	dbo	10/3/2008
tbClientWithRecentNameChange	dbo	10/3/2008
tbCompatiblePrinterProvider	dbo	10/3/2008
tbComputersThatNeedDetailedRollup	dbo	10/3/2008
tbComputerSummaryForMicrosoftUpdates	dbo	10/3/2008
tbComputerTarget	dbo	10/3/2008
tbComputerTargetDetail	dbo	10/3/2008
tbConfiguration	dbo	10/3/2008
tbConfigurationA	dbo	10/3/2008
tbConfigurationB	dbo	10/3/2008
tbConfigurationC	dbo	10/3/2008
tbDeadDeployment	dbo	10/3/2008
tbDeletedComputer	dbo	10/3/2008

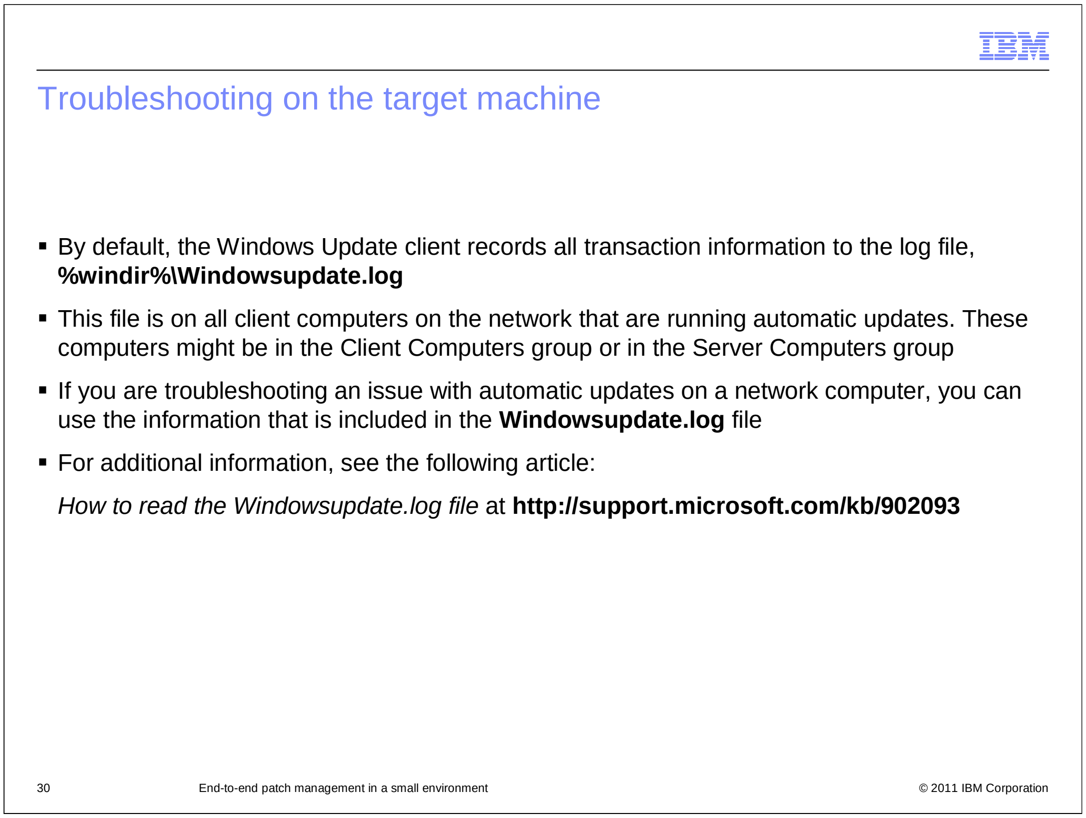
To troubleshoot on the WSUS server, access the database that stores the server data. Use the graphical tool, Microsoft SQL Server Management Studio Express, which is shown on this slide. You can also use a command line tool, Microsoft SQL Server 2005 Command Line Query Utility.



Logs and useful files for troubleshooting

Table	Description	Useful columns
tbUpdate	Microsoft Updates information	UpdateID
tbRevision	Revision information. Useful to join with other tables	
tbKBArticleforRevision	Patch qNumber information	kBArticleID
tbProperty	General information and impact on reboot behavior (exclusive)	InstallationImpact (exclusive) InstallRequiresConnectivity (connectivity) InstallRequiresUserInput (userInput) InstallRebootBehavior (reboot)
vwMinimalUpdate	View built on tbUpdate, tbRevision, tbProperty, tbUpdateType	IsSuperseded legacyName MsrcSeverity
vwUpdateLocalizedProperties	View of title and description information	shortLanguage Title Description

These tables are useful for troubleshooting various problems.

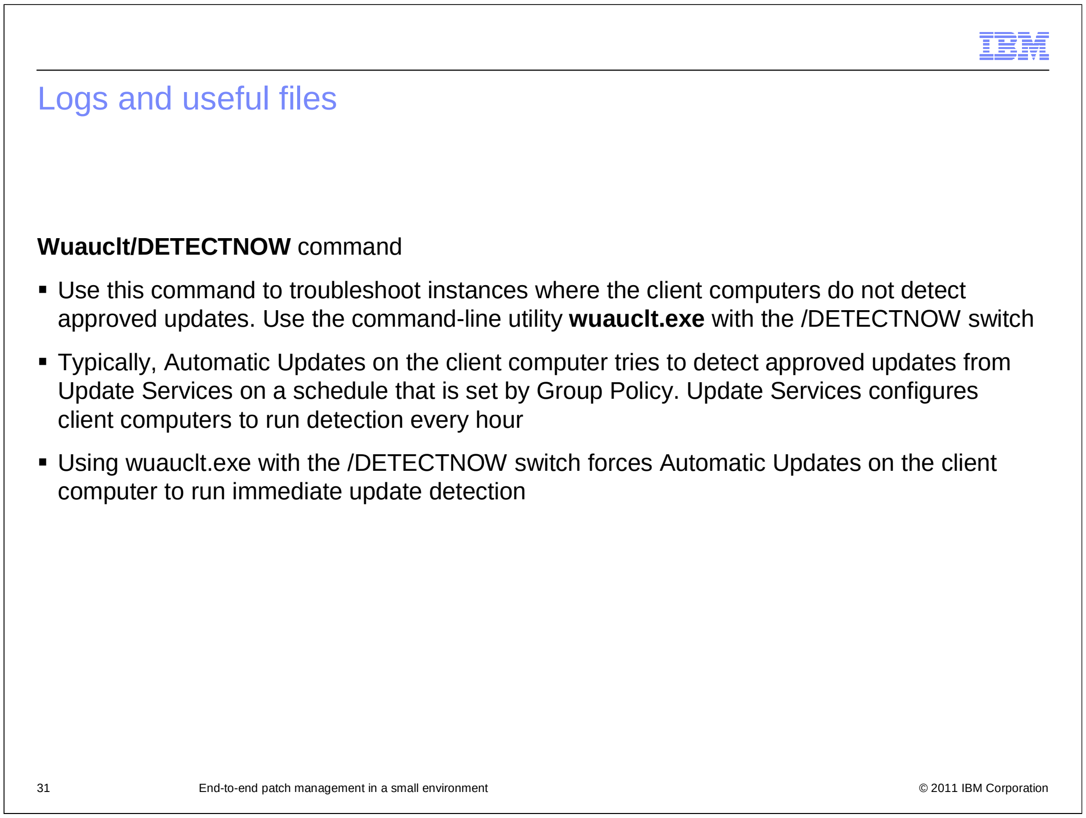


Troubleshooting on the target machine

- By default, the Windows Update client records all transaction information to the log file, **%windir%\Windowsupdate.log**
- This file is on all client computers on the network that are running automatic updates. These computers might be in the Client Computers group or in the Server Computers group
- If you are troubleshooting an issue with automatic updates on a network computer, you can use the information that is included in the **Windowsupdate.log** file
- For additional information, see the following article:

  How to read the Windowsupdate.log file at **http://support.microsoft.com/kb/902093**

On the target machine, check the Windowsupdate.log file located in %windir%. This file logs data from the Windows Update Agent and is present on any computer on the network running Automatic Updates.



Logs and useful files

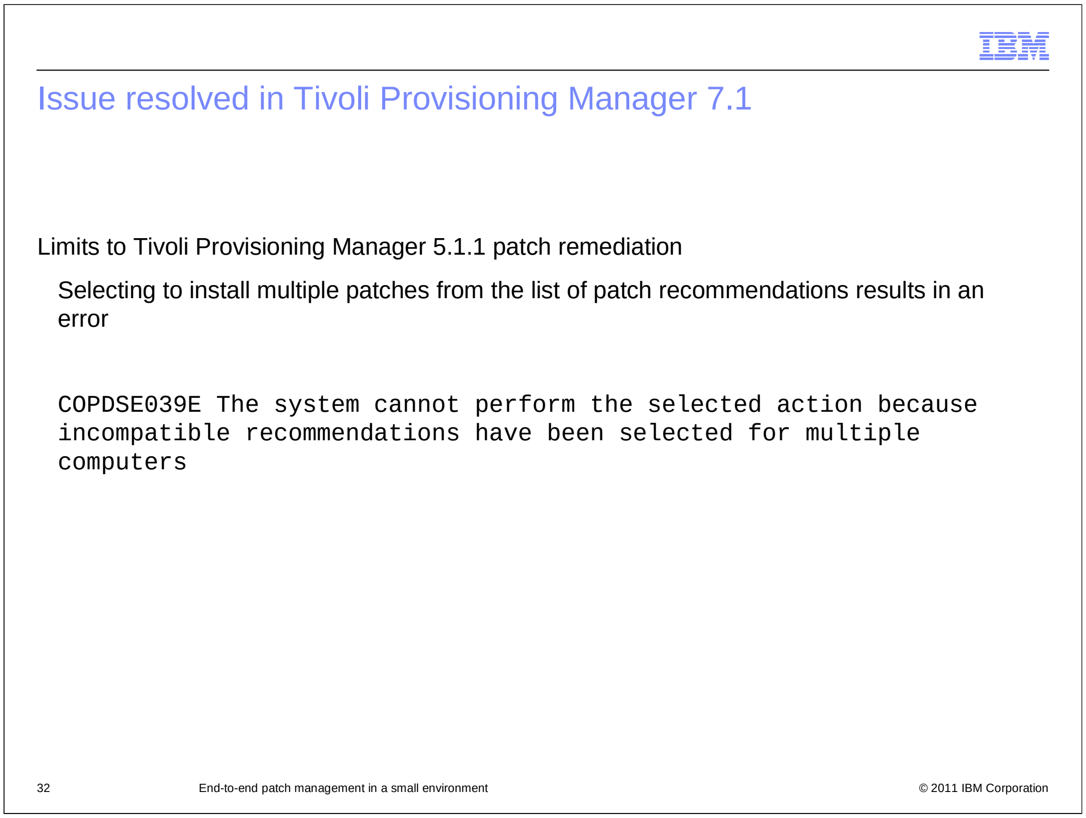
Wuauclt/DETECTNOW command

- Use this command to troubleshoot instances where the client computers do not detect approved updates. Use the command-line utility **wuauclt.exe** with the /DETECTNOW switch
- Typically, Automatic Updates on the client computer tries to detect approved updates from Update Services on a schedule that is set by Group Policy. Update Services configures client computers to run detection every hour
- Using wuauclt.exe with the /DETECTNOW switch forces Automatic Updates on the client computer to run immediate update detection

31 End-to-end patch management in a small environment © 2011 IBM Corporation

The command Wuauclt/DETECTNOW is useful for troubleshooting instances when the client computers do not detect approved updates.

Typically, Automatic Updates on the client computer attempts to detect approved updates every hour. By using wuauclt.exe with /DETECTNOW, you force Automatic Updates to run immediate update detection.



Issue resolved in Tivoli Provisioning Manager 7.1

Limits to Tivoli Provisioning Manager 5.1.1 patch remediation

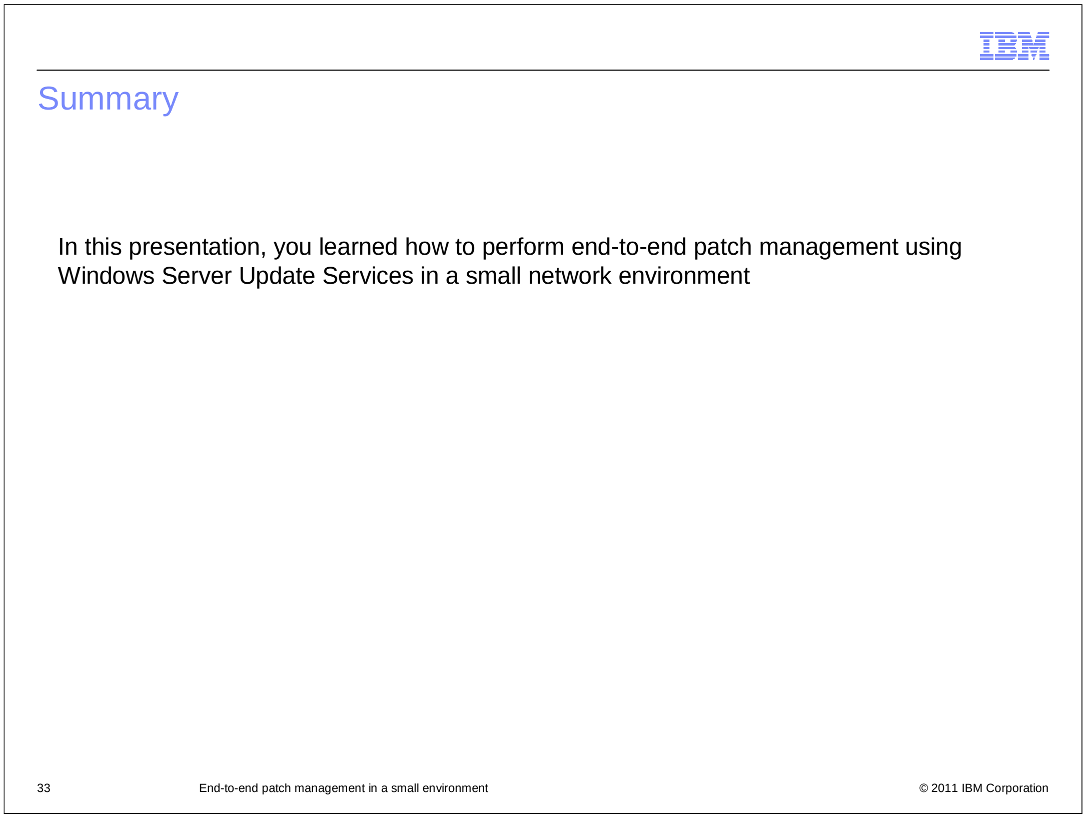
Selecting to install multiple patches from the list of patch recommendations results in an error

```
COPDSE039E The system cannot perform the selected action because
incompatible recommendations have been selected for multiple
computers
```

32 End-to-end patch management in a small environment © 2011 IBM Corporation

A limitation to the patch remediation mechanism is in Tivoli Provisioning Manager 5.1.1. An error occurs when you select to install multiple patches from a list of recommendations. Error code COPDSE039E is displayed. The error code indicates that the system cannot perform the selected action because incompatible recommendations were selected for multiple computers.

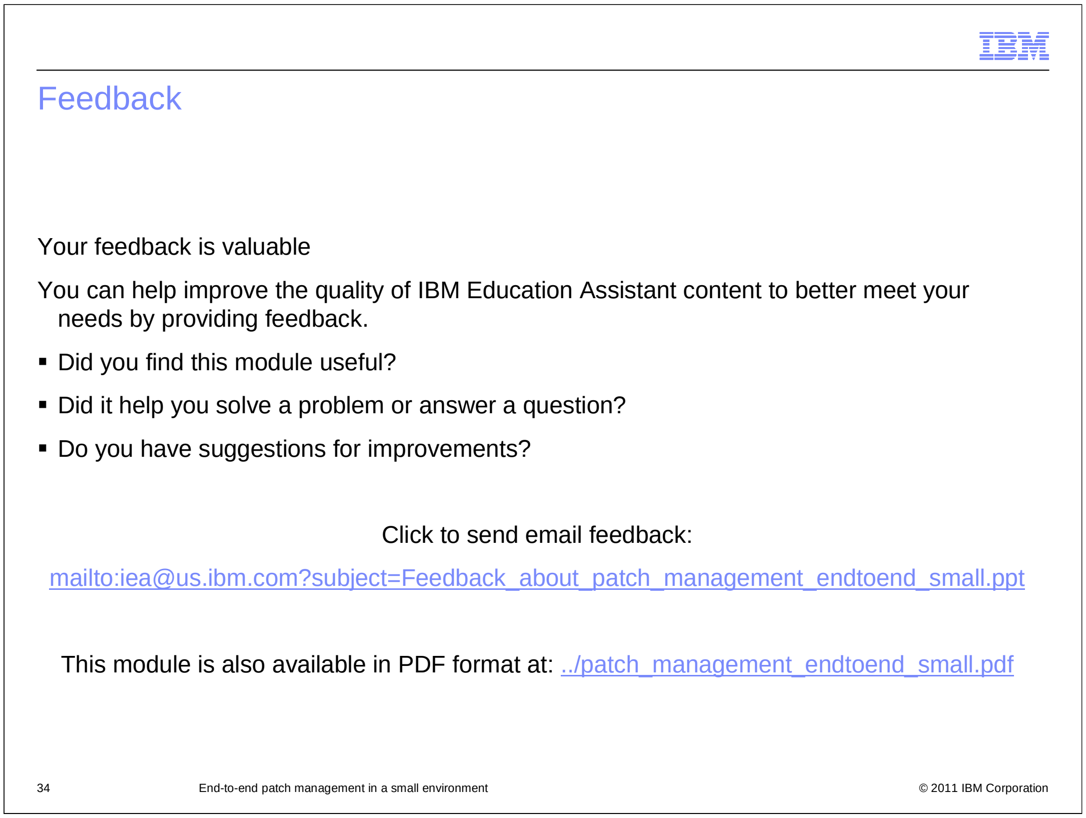
These limitations have been addressed in Tivoli Provisioning Manager 7.1, and the error no longer exists.



Summary

In this presentation, you learned how to perform end-to-end patch management using Windows Server Update Services in a small network environment

In this presentation, you learned how to perform end-to-end patch management using Windows Server Update Services in a small network environment.



Feedback

Your feedback is valuable

You can help improve the quality of IBM Education Assistant content to better meet your needs by providing feedback.

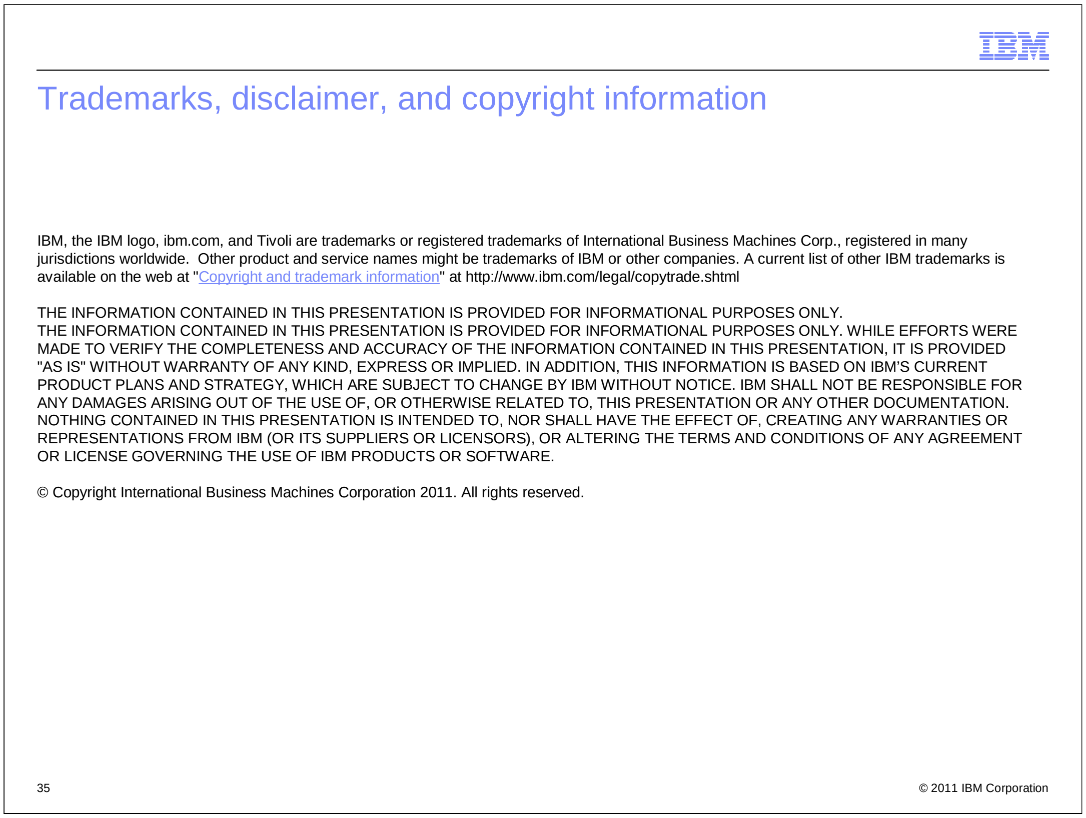
- Did you find this module useful?
- Did it help you solve a problem or answer a question?
- Do you have suggestions for improvements?

Click to send email feedback:

mailto:iea@us.ibm.com?subject=Feedback_about_patch_management_endtoend_small.ppt

This module is also available in PDF format at: ../patch_management_endtoend_small.pdf

You can help improve the quality of IBM Education Assistant content by providing feedback.



Trademarks, disclaimer, and copyright information

IBM, the IBM logo, ibm.com, and Tivoli are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of other IBM trademarks is available on the web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY.
THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS OR SOFTWARE.