

# Ecora Patch Manager 5.0 Evaluation Guide

## **Table of Contents**

Introduction	3
Ecora <sup>®</sup> Patch Manager 5.0 Overview	. 3
Install the Software	. 4
Discover, Group, & Scan	. 5
Optional Exercises – for Added Value!	11
Approvals & Notes	11
Jsing Policy Manager	12
Set an Alert	14
Schedule a Scan	16
Schedule Agent Scans	17
Jse the Online Reporting Center	18
Congratulations!	19
Customer Support	19

### Introduction

Patch Manager is an IT management and security tool that automatically discovers and analyzes missing or installed patches for mission-critical platforms and applications. The software displays the status of patch configurations, provides information about the latest versions of security patches and hotfixes, and allows administrators to deploy patches in groups, individually, or during off hours. Software security and consistency can be easily maintained across the enterprise with Ecora's Patch Manager.

### Ecora<sup>®</sup> Patch Manager 5.0 Overview

**Sure-Scan / Rapid Scan Flexibility**– Your choice of Sure-Scan analysis, including file integrity verification for greatest accuracy and security, or Rapid-Scan for fastest results.

**Customization / Extensibility** – Customize or "extend" Patch Manager to support any applications and patches you define.

**Wake-on-LAN** – Ensure the broadest and most accurate security analysis by having Patch Manager start offline systems prior to starting a scan.

**Cross-platform support** – Support for Sun Solaris, Windows NT/2000/XP Pro/2003, MS-SQL Server, MSDE, Exchange 5.5 & 2000, Office 2000/XP, Windows Media Player, IE, IIS, MDAC, WINZip, MS-XML, Adobe Acrobat.

**Optional Agent** – Reduce network utilization (scans performed locally); improve support for laptops, other sporadically connected devices, and hardened hosts – with no remote registry or file sharing requirements.

**Reporting Center** – Review comprehensive, ready-made reports that provide details from a managerial to technical level, accessible centrally or web-based.'

**Sure-Scan™** – Ensures accurate analysis of missing patches in your environment by dynamically updating its database to include the most current patch information. Patch Manager uses both registry and file integrity checks to analyze your systems.

**3-D Patch Views™** –Quickly see what critical patches are missing and/or installed in your environment by host, application, or patch in sortable displays.

**Patch Rollback** –Automate removing a selected patch if conflicts develop due to a patch installation.

**Alerting** –Alert on multiple events, including new patch databases, new patches for a specific OS or application, patches missing, or failed patch installation.

**Repository Manager** – Automatically schedule patch downloads to repositories in your enterprise so patches are always readily available for immediate deployment.

**International Language Support** – Supports international versions of Microsoft and Sun operating systems, including: Danish, Dutch, French, Finnish, German, Italian, Japanese, Norwegian, Portuguese, Spanish, Swedish, and United Kingdom.

## Install the Software

This Evaluation Guide assumes that you have successfully downloaded, installed, and configured Ecora Patch Manager.

If you have not, please refer to the Start-up Guide, located on Ecora's Support webpage (<u>http://www.ecora.com/ecora/um/patchmanager/5.0/startup\_guide-</u> <u>patchmanager5.0.pdf</u>).

#### You should be here...



The main user interface of Patch Manager.

### Discover, Group, & Scan



Select a network discovery option. For this evaluation, choose NetBIOS (or Active Directory).

Domain selection          Domain name       Selected         ZADCICHILD       No         AUGHEY       No         BIRCH       No         BURCH       No         DOEVING       No         CHLID       No         DEVENG       No         CORADA       No         ECORADA       No         ECORADA       No         ECORADA       No         ECORADANO       No         ECORADANEZOUD <no< td="">       No         KENNEEEC       No         MARE       N</no<>	🐴 Hosts discove	:r				<u>? ×</u>
Domain name         Selected           ZKDCTCHILD         No           AUGHEY         No           BIRCH         No           BIRCH         No           BSP         No           OVENNET         No           ECORADOTOR         No           ECORADON         No           ECORADON No         No           ECORADADINO         No           MANE         No           MANE         No           MAPLE         No           MAPLE         No           MARINE         No           MARINE         No           MARINE         No           MARINE         No           MARINE         No           MARINE         No           Computer selection         Available	Domain selection					
ZXDCTCHILD         No           AUGHEY         No           BIRCH         No           BSP         No           CHLD         No           DEVENKS         No           DEVENKS         No           ECORADA         Yes           ECORADA         No           Maine         No           Marke         No	Domain name	Selected				
AUGHEY No BIFCH No BSP No CHILD No DEVENG No ECHILD No DEVENG No ECORADA No ECORADA No ECORADA No ECORADA No ECORADA No EXCHANGE2000 No KENNEBEC No MAINE No MARLE NO	2KDC1CHILD	No				
BIRCH No BSP No CHILD No DEVENG No DEVENG No ECORADDTOR No ECORADD No NATE No MAINE NO MA	AUGHEY	No				
BSP No CHLD No DEVENG No DOVERNET No ECT No ECT No ECT No ECTA NO ECT	BIRCH	No				
CHILD No DEVENG No DOVERNET No ECI No ECORAJDITOR No ECORAJA No OAK No PMERN No No ELENT MAREE No MAREE	BSP	No				
DEVENG No DOVENNET No ECI No ECORADA Yes ECORADATY Yes ECORADATY Yes ECORADATY Yes ECORADATY Yes ECORADATY No ECORADATY No ECORADATY No ECORADATY No ECORADATY No MAINE No MAZLE NO MAZ	CHILD	No				
DOVENNET No ECI No ECORADA No ECORADA No ECORADA No ECORADA No ECORADA No ECORADA No EXCHANGEZOU No EXCHANGEZOU No EXCHANGEZOU No MAINE No MARLE NO	DEVENG	No				
ECI No ECORAJA Yes ECORAJUDITOR No ECORAJUDITOR No ECORAJUDITOR No ECORAJUDITOR No ECORAJUDITOR No ECORAJON No ECORAJON No MANE No MANE No MANE No MARLE NO	DOVERNET	No				
ECORA No ECORAU Yee ECORAUDITOR No ECSP No ECSP No EDDMIND No EXCHANGE200 No KKNNEBEC No MAINE No MARLE NO	EC1	No				
ECORADITION No ECORADITION No ECORADITION No ECONNINO No ECONNINO No ECONNINO No ECONNINO No ECONNINO No ECONNINO NAPLE No MAPLE CORADA ECORADA EC	ECORA	No				
ECORADA No EXCHANGESCON No KXCHNAGECON No KXCHNAGECON No MARLE No MYSROUP No OAK No MARLE No MYSROUP No NITECORADA No OAK No Highlight All Select Inselect Available Highlight All Select Inselect Computer selec Domain Name ECORADA	ECORAQA	Yes				
ECSP No EDDIMINO No EXCHANGE2000 No KENNEBEC No MARLE NO	ECORAUDITOR	No				
EDOMINO No ECCHANE 2000 No KENNEBEC No MAINE No MAPLE No MYCROUP No OAK No PMERI No Highlight All Select Inselect Computer selection Help Computer selection Help Computer selection Help Computer selection Help Computer selection Help Computer selection ECCRAQA	ECSP	No				
EXCHANGE2000 No KENNEBEC No MAINE No MARLE No MYSROUP No NT4ECORADA No OAK No Pummn No Highlight All Select Unselect Selected Available Computer selec Help Kest Nest	EDOMINO	No				
KENNEBEC No MAINE No MARE No MAGRUP No OAK No PMERI No Available Econputer select Highlight All Select Inselect Computer select Heb Case New Computer select Econputer select	EXCHANGE 2000	No				
MAINE No MARLE No MYSROUP No DAK No PMPRD No Highlight All Select Unselect Available Computer select Highlight All Select Unselect Available Computer select Damin Name ECDRADA	KENNEBEC	No				
MARLE No MYGROUP No NT4ECORAQA No QAK No Pummn No Highlight All Select Linselect Selected Available Help Kest Select Nest Computer select	MAINE	No				
MYSROUP No NIECORADA No QAK No PMPRIN No Highlight All Select Unselect Selected Available Computer select Heb CORADA No Computer select Domain Name	MAPLE	No				
NT4ECORADA No OAK No PMPRO No Highlight All <u>Select</u> <u>Unselect</u> <u>Selected</u> Available <u>Help</u> <u>Kest&gt;</u> <u>Computer selec</u> <u>Domin Name</u> <u>ECORADA</u>	MYGROUP	No				
DAK     No     Image: Computer select       Highlight All     Select     Image: Computer select       Heb     < gack	NT4ECORAQA	No				
Implight All         Select         Implight All         Select         Available         Computer select           Help                 Domain Name ECOPRAQA              Domain Name ECOPRAQA	OAK	No				St Hosts diese
Highlight All         Select         Linselect         Computer select         Domini Name           Help         < 8ack	IPMPRO	No				-anoses disc
Help Constant Name CORADA	Highlight All	<u>S</u> elect	Unselect	Selected	Available	Computer selec
Help ECORAGA						Domain Name
ECORAQA	Help			< Back	Next>	ECORAQA
						ECORAQA

integrity check for greater speed and faster results display.
3. Click on the **Discover Systems** button.

 Isover Option:

 Isover Option:

 Specify Hosts

 Specify hosts

? ×

<u>N</u>ext> <u>C</u>ar

<u>?</u>×

2. Choose the Scan Type: Sure Scan or

for greatest accuracy and security.

Rapid Scan - analysis skips file

integrity (MD5 checksum) verification

**Rapid Scan** and click **Next >**. **Sure Scan** - analysis includes file

1. Click on the Scan button.

7. Double-click to select a few (3-5) systems and click **Finish**.

discover and click **Next** >.

6. Double-click to select the domain(s) to

5. Click on the **Next** > button.

- Tip: If possible, select devices in a test lab or non-production capacity. The following sections include the deployment of a patch, which should always be "tested" in a minimum-risk situation.
- Tip: If you wish to use agents, the Start-up Guide includes a section on deploying agents from this dialog box.

ble	Le comparer concern		(	1	
	Domain Name	Computer Name Ip Add	ress Computer Role	Selected	
	ECORAQA	ALBANY	Server	No	
	ECORAQA	AMY-VM	Server	No	
	ECORAQA	BACH	Server	No	
	ECORAQA	BOSTON	Server	No	
	ECORAQA	BUNNYEARS	Server	No	
	ECORAQA	DAYTON	Server	No	
	ECORAQA	DENVER	Workstation	Yes	
	ECORAQA	NEWYORK	Server	Yes	
	ECORAQA	NOVELL	Workstation	No	
	ECORAQA	OMAHA	Server	No	
	ECORAQA	PACIFIC1	Server	No	
	ECORAQA	PORTLAND	Server	Yes	
	ECORAQA	SEATTLE	Server	Yes	
	ECORAQA	STORAGE	Server	No	
	ECORAQA	TELLURIDE	Server	Yes	
	ECORAQA	TEMPE	Server	No	
	ECORAQA	VM2KPR0-SP3	Workstation	No	
	ECORAQA	VM-GERMAN2K	Server	No	
	ECORAQA	VM-0FF2KSP2	Workstation	No	
	ECORAQA	VM-SPANISHOFFIC	Server	No	
	FLUBAUA	VMXPP01	Workstation	No	<u> </u>
	Highlight All	<u>S</u> elect <u>U</u> nse	elect		Selected S Available
	Help				< Back Einish Cancel

- 8. Click on the **Systems Management** button.
- 9. Click on the New button.
- Enter a name (such as "test\_group") and description for the new group and click **OK**.
- 11. Select the **All Systems** group in the upper pane so you can see all the discovered systems.
- 12. In the lower pane, use CTRL + click or SHIFT + click to select some or all of the systems and click **Add to Group**.
- 13. Select the new group from the drop-down list and click **OK**.
- 14. Select the new test group in the upper pane and click on the **Properties** button.
- 15. Click on the **Windows Systems** tab.
- 16. Enter a Username (in domain \ user format) and Password and click **OK**.
- 17. Click **OK** to close systems management.

e	nt	Pro	perties						?
		Group	Window	s Systems					
		-Prope	rties						
		Itest	aroun						
ır	(״ר	Group	description						
יי ר	,,	for th	e Patch Man	ager evaluation					
5									
	St. Proper	l ties							?[X]
	Group	Window	is Systems						
	System Se	ettings	Non-Agent	Remediation Settings	MSI Path 9	ettings	Agent Settings		
	-Svstem	Settinas							
	Sustem	n Name	_		System Role			_	
	Gysten	mane	1		OS			_	Cancel
	NT Do	main	ALB	ION	OS Version			_	
	IP Add	ress							
	Usern	×	АБи	A drainistrator	Tip: Userna Domain\U:	me field sk ser name	iould be entered as (domain account) or	User	
	User n	ame	JAIDIO	onvedministrator	<b>name</b> (local Manager co	account). nverts the	In the second case, User name to	Patch	
	Passwi	ord	*****		System\Us	er name	format.		
	Drive (I	Remote)	Share* Adm	nin\$					
		le la							
	<u> </u>								
				<u>?</u>   x				Carros	

<b>**</b> *	ystems Managemen	nt				<u>? ×</u>
Mar	nage Systems					
Gr	oups					
	Group Name	Description				• <u>N</u> ew
1	All Systems					
2	test_group	for the Patch Man	a⊆			<u>D</u> elete
						E Proportion
						<u>-</u> ropentes
						✓ Deploy <u>Agents</u>
(	]				)	
	stems-					
l r	Windows (2) Univ (	01				Count
	System N	NT Domain	IP address	User Name	OS R(	Djscover
	DULFIN AI	LBIUN	192.168.55.12	Albion\Administrator	Windows XP Wo	
	SHENIFF A	LEIUN	132.166.33.1	Albion vadmimistrator	windows 2003 Sel	D <u>e</u> lete
						Properties
					~	- Tobewee
	<					Deploy <u>Ag</u> ent
	Add to Group Rem	nove <u>f</u> rom Group				
Ľ						
	Help					Close

18. Select the test group.

- 19. Click on the Select Products and Patches tab.
- 20. Click in the checkbox to enable **Use Selective Scan** to limit analysis to specific products or patches.
- 21. Use the tree in the left pane to locate and select **only Internet Explorer** (all versions) under **Applications** to analyze.

National Scan Wizard		<u>? ×</u>
System Selection		
Select Systems Select Products and Patches		
Use selective scan		Save
Products		Patches
🖶 🕀 All Operating Systems	1	▼ Q828750.E×E
🖕 🗹 Applications	2	☑ 0.269368 exe
INET Framework 1.0	3	✓ g818529 exe
INET Framework 1.1	4	✓ 1F5.01 sp2.KB867801.\W/indows2000sp2.vi
	5	✓ 1E5.01 sp4.KB910620.W/indows2000sp4.v
	6	✓ 123.01394 (8310020 WilliadW32000394 W
- DirectX 7.0		✓ Q313102.exe ✓ USE 01 - A KD0000223 \/ (n down20000- A v/
Construction of the server		15.01 sp4-KB830323-windows2000sp4-xi
Exchange Server 2003	8	IE5.01sp4-KB834707-Windows2000sp4-x
Exchange Server 5.5	9	✓ q265258.exe
FrontPage 2000	10	☑ Q832894.eXE
FrontPage 2002	11	▼ q306121.exe
- FrontPage 2003	12	▼ q824145.exe
··· 🗹 Internet Explorer 5.01	13	▼ Q828750.EXe
Internet Explorer 5.5	14	☑ 0259166 W/2K_SP1 x86 eve
Internet Explorer 5     Internet Explorer 5	15	
Internet Explorer 8.0 for windows server 2003	10	
Internet Information Services 5.0	16	▼ q832834.exe
- Internet Information Services 5.1	17	✓ ie5.01sp3-KB883939-Windows2000sp3-x8
- Internet Information Services 6.0	18	Vindows2000sp4.E
- 🗖 MDAC 2.5	19	🔽 IE5.01sp3-KB834707-Windows2000sp3-x
	<	<u>B</u> ack <u>F</u> inish <u>C</u> ancel

- 22. In the right pane, locate and select the patch(es) to analyze. For this evaluation, leave all selected.
- 23. Click **Finish** to begin scanning systems for patches.
- 24. Enter a Scan Description and click **OK**.

## **Review Scan Results**

- 1. Once scanning is complete, notice that the left window pane contains three tabs that allow you to choose how to organize the results. Click on the **Hosts** tab.
- Click on the plus sign(s) in the left pane to expand the tree for one of the hosts and select a host to see the results for that system in the right panes.
- Click on the Missing button (to see information about patches and service packs that need to be installed to bring the system up to the latest security fixes).
- 4. As you select items in the upper right pane, notice that the lower pane contains details such as test notes, vendor articles, and informational links. Click on a plus sign to expand.
- 5. Click on the **Products** tab in the left pane to see summary information about the configurations in your environment, such as IE versions and service packs. This view helps you enforce version consistency (and therefore performance, security, and compliance) across the entire enterprise.
- We are looking for a specific patch, so click on the Patches tab.
- Click on the All button (for all information; installed and missing patches and service packs).
- Click on the plus sign(s) in the left pane to expand the tree for Windows Patches. For the sake of this evaluation, we'll look for patch 828750 (MS03-040), a



cumulative patch for Internet Explorer that affects a wide range of systems and includes fixes for vulnerabilities with existing exploits in circulation.

- 9. Scroll down until you locate 828750.
  - For more information on this specific patch: <u>http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/</u><u>MS03-040.asp</u> <u>http://www.ciac.org/ciac/bulletins/o-002.shtml</u>
- 10. Click on patch **828750**. The right pane should display a list of machines scanned as well as their status regarding **828750**. Look for the icons to indicate the status:

Patch was detected as installed.



- 11. Click on the **Missing** button to filter out machines with the patch installed. The result is a list of machines that need to have 828750 installed.
  - **Tip**: Should you have no machines needing this patch CONGRATULATIONS! Pick another patch (use the lower right pane for information about each) and follow the remaining instructions.

# Install a Patch

#### 

It is strongly recommended (for this trial and as a general practice) that all patches be tested before deployment in the production environment. Particularly in environments with custom software or mission-critical applications, it is not worth risking potential conflicts or adverse reactions with an untested patch.

- 1. Identify a system on which to install patch 828750.
- 2. Locate the checkbox in the **Push** column.
- 3. Click in the Push checkbox to enable patch installation of 828750 for the host.
- 4. Click on the **Push** button in the toolbar.

📲 Ecora Patch Manager						
<u>File Edit View T</u> ools License <u>H</u> elp						
Scan Reports Test Center	Systems Schedule	Alerts	Repository Pus	2 Vpdate	What's This?	ecora
All Installed Missing	Policy					ecore
Hosts Products Patches	Results					
023003	Patch: 828750					
🥜 823718	Push ∇	Rollback	Status	Patch Name	Application	Domain Name
🥜 823803			🔀 Missing Patch	Q828750.exe	IE	ECORAQA
🥖 823980			🔀 Missing Patch	Q828750.exe	IE	ECORAQA
🥜 824105			🦁 Warning	Q828750.Exe	IE	ECORAQA
824146						
825119						
020113	<u> </u>					<u> </u>
🥖 828035	+ Euplanation of a	nalueie				
🥖 828750		nuiyərə				
🥖 N/A	Click here to retrieve Click here to downloa	<u>the Microsoft K</u> ad this natch no	nowledgeBase Article			
🖶 🔛 Windows Service Packs	. Mar Matan					
📄 🚍 Wed Nov 5 15:17:32 2003 🛛 🖳	+ my notes					
	+ Article MS03-04	D				
3.0 828750						///



#### Verify Successful Patch Deployment

- 1. Scan the test group again.
- 2. Once complete, click on the Hosts tab.
- 3. Locate the host you selected to update with 828750.
- 4. Click on the All button to show all patches (installed, missing, warnings).
- 5. Click on the IE tab in the upper right pane to show IE patches.
- Recora Patch Manager 6. Verify that the File Edit View Tools License Help host you Ø, ý Q Schedule Update ğe Push updated shows Test Cente Reports Repository Scar Suste patch 828750 B B P as installed. Installed Missin All DS IIS IE SQL 2000 MSDE 2000 / ECORA Hus.s Products Patches MDAC 2.8 Media Player Office 2000 < Internet Explorer 6 - Internet Explorer 6 SP1 Mon Nov 10 09:20:18 2003 Ļ. 関 🚊 📆 All Systems Follback Installed Push Fisk Patch Name Hotfix V Patch Fcun U328/50.exe 828750 1 ECORADA/ZOOLANDE 🔽 Warning HIGH Q310847.exe 810847 Thu Nov 6 11:12 40 2003  $\nabla$ ±... A MEDIUM 🔽 Warning U328970.exe 328970 🗄 - 🧱 Wed Nov 5 15:17:32 2003 ∀ 🔀 Missing. Superseded Q322925.EXE 822925 🔺 MEDIUM b 🛓 MEDIUM Q324929 eve

<u>H</u>elp

Push

# **Optional Exercises – for Added Value!**

### **Approvals & Notes**

Patch Manager provides the ability to add notes and conditions to each patch. This allows you to record your test findings or comments, approve patches for approval or rollback, and set certain patches to be ignored in analysis.

We have verified successful installation of patch 828750 and will now approve it for distribution and enable required approvals. Combined with policies (next section), required approvals further tighten security controls.

- 1. To enable approvals, choose File... Settings...
- Click in the Require approval for installation / rollback checkbox and click OK.
- 3. Choose **Tools... Patch Attributes Management...**from the main menu.
- 4. Click on the **Patch Name** column head to sort by the patch name.
- 5. Scroll to locate patch Q828750.exe and select it.
- Tip: You may see multiple listings for the patch. This is because Microsoft releases one for each version of IE being patched.
- 6. Click the **Properties...** button.
- 7. Click on the Approve Push tab.
- 8. Click in the radio button for **Approved for installation**.
- In the lower left pane, double-click on All Systems to approve the patch for the All

Systems group.

- 10. Verify the selection in the lower-right results pane and click the **Apply** button.
- 11. On the Manage Notes tab, click New .....
- 12. Name the Note (or accept the numbered default) and click **OK**.
- 13. Place the cursor in the text field and enter text for the note (perhaps "Pushed without incident").
- 14. In the lower left pane, select the All Systems group, then click the **Apply** button.
- 15. Click OK, then Close, to return to the GUI.

🏪 Setting	Js				? ×
Preference	es Maintenanc	e Database	Alerting Rep	ository Rep	orting Center
– Gener	al Settings				
Numb	ar of threads to use		E4 🔛		
Numb	er or uneaus to use.				
Notify	me if I have not che	ecked for updates i	n   5 📑 days	t.	
🗖 s	kip the checksum:				
I 🔽 9	tore system creden	tials			
	) on't ask for scan d	escription			
	equire approval for	installation/tollbaci	k		
	require approvarior	Installation / folibac			
				_	
Patch A	ttributes Manager	nent			? ×
(Patches					
	OS/Software	PatchName 🛆	Notes	Ignored 🔄	Eroperties
1	.NET Framework 1.0	.NET Framework 1.0	0	No	· · · · · · · · · · · · · · · · · · ·
2	.NET Framework 1.0	.NET Framework 1.0	0	No	
3	.NET Framework 1.0	.NET Framework 1.0	0	No	
4	.NET Framework 1.1	.NET Framework 1.1	0	No	
5	.NET Framework 1.1	.NET Framework 1.1	0	No	
6	SUNWeeetg	104018-03	0	No	
/	SUNWCCSNd	104018-03	0	No	
9	SUNWshinay	104018-03	0	No	
10	SUNWsnmpd	104018-03	0	No	
11	SUNWcccfa	104018-09	0	No	
12	SUNWeerev	104018-09	0	No	
13	SUNWccsnd	104018-09	0	No	-
				2	9
Help					Close
Part Ecora	PatchManager				<u>? ×</u>
Manag	ge Notes Appro	ve Push Appro	ove Rollback I	gnore Patch	
C API	provePush				
	Approved for inst	allation			
	Not approved for	installation			
	Not approved for	iristaliation			
- Sys	stems and Groups -				
- CA	Vailable		- C Selected		
	Ė-All Systems		📩 All Syste	ems	
	-BOSTON/	CORAQA	BOS	STON/ECORA	QA
	- DENVER/	CORAQA	- DEI	VVER/ECORAL	QA
			- NE	ATURN/ECOP	RAQA
	- SEATTLE/	ECORAQA	SEA	TTLE/ECORA	QA III
	E TELLURID	E/ECORAQA	TEL	LURIDE/ECO	RAQA
	⊕-test				
			JĽ		
	Help		Apply	OK	Cancel

## **Using Policy Manager**

### **Create a Policy**

Policies allow you to create generalized rules about how you want systems in your environment configured (presumably secured to the latest critical patches). You may choose to prioritize certain groups for stricter policies for applications you consider higher risk. Policies allow you to define these rules, apply them to groups you create, then schedule scans to ensure that you're always aware of systems that do not comply with your policies.

Since we've tested patch 828750 and approved it for distribution, let's create a policy that all systems in the test group must have 828750 installed to be in compliance.

- 1. Choose **Tools... Policy Management...** from the menu.
- 2. Click the New... button to access a dialog for creating a policy.
- 3. Enter a name (such as "test policy") and description (such as

"Ecora PM5 evaluation") for the new policy and click **OK**.

- In the Create Policy dialog box, on the Selection Criteria tab, click on the Platforms tab.
- 5. Click in the checkbox for each Windows OS version.
- 6. Click on the **Applications** tab.
- 7. Click in the **Display All** checkbox.
- 8. Click in the checkbox for the relevant version(s) of Internet Explorer (such as version 6.0).
- 9. Click on the Patches tab.
- **Tip**: If desired, click and drag the column heading dividers to resize the columns.
- 10. Click on plus signs to expand the tree by application to see patches. In this case, leave all patches set to **Ignore** so the policy applies regardless of installed status. You could choose to have a policy apply ONLY if a given patch was installed or not installed. Systems are displayed in Policy view only if they meet the selected criteria.



Policy

Name

Test Policy

? ×

- 11. Click on the Rules tab.
- 12. Click on plus signs to expand each version of Internet Explorer to see patches, locate patch 828750 wherever it occurs, and click in a radio button - **Must be Installed**. Your policy is thus that ANY Windows system running the specified version of Internet Explorer, MUST have this patch installed, and click **OK**.
- 13. Click OK to close.

### Apply the Policy

- Click Yes when asked if you'd like to attach the policy to systems (or choose Tools... Policies Selection...).
- 2. Select the policy in the upper pane.
- 3. Select the test group you created in the lower pane.
- 4. Click on the **Attach Policy** button to apply the policy to the test group.
- 5. Click **OK**.

#### View by Policy Compliance

- 1. Click the **Policy** button.
- Click on the **Policy** tab in the left pane.
- 3. Click on the plus sign to expand the tree until you locate your policy.
- 4. Select the policy in the left pane to see which systems comply in the right pane.
- Tip: Notice that any systems that do NOT comply have a checkbox for remediation (which includes both installation and rollback, if necessary, to bring the system into compliance with the policy). If you want to remediate by

? × 🐴 Create Policy Selection Criteria Rules Patches Hotfix Bulletin Must be installed Must not be installed Ignore Patches internet Explorer 6 - Internet Explorer 6 Gold internet Explorer 6 - Internet Explorer 6 SP1 🥜 Q324929.ехе 324929 MS02-068 🔿  $\odot$ 328970 MS02-066 🔿  $\circ$  $\odot$ 810847 MS03-004 🔿 0  $\odot$ Q813489.exe 813489 MS03-015 🔿 0 0 🥜 Q818529.exe 818529 MS03-020 🔿 0  $\odot$ 🥔 0822925.EXE 822925 MS03-032 🔿 0  $\odot$ 🥜 Q828750.exe 828750 MS03-040 🙆  $\cap$ 0 Internet Explorer 6.0 for Windows Server 2003 - Windo Internet Information Server 4.0 - Windows NT4 Service. - Internet Information Server 4.0 - Windows NT4 Service. - Internet Information Server 4.0 - Windows NT4 Service. Internet Information Services 5.0 - Windows 2000 Gold ■Internet Information Services 5.0 - Windows 2000 Gold (Internet Information Services 5.0 - Windows 2000 Servi., (Internet Information Services 5.0 - Windows 2000 Servi., (Internet Information Services 5.0 - Windows 2000 Servi.) Internet Information Services 5.1 - Windows XP Gold <u>O</u>K <u>C</u>ai



😤 Ecora Patch Manager				<u>_</u> _×
<u>File Edit ⊻iew Tools License H</u> elp				
Scan Reports Test Center	Systems Schedule	Alerts Repository	Push Update	What's This?
All Installed Missing	Policy			CCOICI
Hosts Products Policies	Results			
🖶 🛅 Thu Oct 23 11:09:20 2003	Policy: Test Polic	y		
🖕 🧱 Thu Oct 23 12:24:51 2003	Remediation	Compliance 🛆	System	Domain
🚊 📑 Policies		🐓 Does Not Comply	BUNNYEARS	ECORAQA
		Complies	WIN2KDCBU	ECORAQA
👜 🛗 Wed Oct 22 18:06:14 2003		Complies	WIN2K	ECORAQA
🖽 🛗 Wed Oct 22 18:17:38 2003		Complies	VS-SMS20	ECORAQA
		Complies	VMXPP01	ECORAQA
		Complies	VM-XPGERMAN	ECORAQA
		Complies	VMWXPPM	ECORAQA
		Complies	VM-SVE2KSERV	ECORAQA
		Complies	VM-OFF2KSP2	ECORAQA
		Up Complies	VM-GERMAN2K	ECORAQA
		Complies	VM2KADVSVR-SP1	ECORAQA
		5 Complies	TEMPE	ECORAQA
		Complies	TELLURIDE	ECORAQA
		Complies	STORAGE	ECORAQA
				C 2
3.0 Test Policy	J.			

policy, select the checkbox, click **Push**, and follow the Patch Installation instructions.

### Set an Alert

This section is strictly optional, but introduces you to the tip of the iceberg in automating scheduled scans and using Ecora's proactive alerting capabilities. Alerts are a method of notification based on a trigger you define.

🐴 Alert

Basics Email

Evaluati

Notify m

Basic

Name

Description:

Help

### **Enable Alerts & Triggers**

- Choose File... Settings... and click on the Alerting tab.
- 2. In the Alerting area, click in the **Enable** checkbox.
- 3. Accept the 10-minute interval for how often the software checks for the conditions you define.
- 4. In the Email (SMTP) Alerts area, click in the **Enable** checkbox to enable alerts via email.
- 5. Enter the SMTP Server name, Port number, and the Maximum Attachment Size (reports can get large). The SMTP Server is generally your mail server, such as mail.companyname.com.
- 6. Click OK.

	· · · ·	Y	( 11 e	r	
Preferences	Maintenance	Database	Alerting	Repository	Reporting Center
-Alerting					
🗹 Enable					
Interval: 1	J 🖥	minutes			
	s				
🔲 Enable					
SNMP Mar	ager:				
Port:	162				
-Email (SMT	P) Alerte				
	) Micita				
SMTP Serv	er mail.comp	anyname com			
Port	25			<u>.</u>	
May attach	ment size: 10240		KR	-	
Email from		· •	KD		
Emailmon.	Iname@ec	ora.com			

🐴 Alert Type

 ? ×

#### Set an Alert

We'll create an alert for too many missing patches.

- 1. Choose Edit... Alerts & Triggers... from the menu.
- 2. Click on the Alerting tab.
- 3. Click **New...**.
- 4. Select Email Alert and click OK.
- On the Basics tab, enter a Name (such as "Evaluation Test Alert") and Description for the alert.
- 6. On the Email tab, enter your email address in the To: field and enter a reminder note in the Subject: field.
- 7. Click OK.
- 8. Click on the Triggers tab.
- 9. Click **New...**.

10. On the Basics tab, enter a Name and Description.

	Shimi Aleit
n Test Alert	O Windows Event Log Alert
e by email	
	Alert ? X
he To: field.	Basics       Email         -Email (SMTP) Settings         To:       tester@yourcompany.com         Cc:
n.	Help QK Cancel

- 11. On the Condition tab, select Scan from the Type drop-down list and Patch Missing as the Condition.
- 12. Select the test group and verify the patch threshold is 10.
- 13. Accept the default on the Message tab.
- 14. On the Alerts tab, click in the checkbox next to the Alert you created and click OK.
- 15. Click Close.

🀴 Trigger

Name



## Schedule a Scan

Let's schedule a scan for overnight for you to review in the morning.

- 1. Click on the Schedule button.
- 2. Click on the New... button.
- Enter a name (such as "Evaluation Scan") and a description for the task.
- 4. Click OK.
- 5. Highlight your group and click the **Select** button.
- 6. Click **OK**.
- On the Task tab, use the **Run as** field and use the **Set Password...** button to enter credentials with administrative access.
- 8. Click on the **Schedule** tab.
- 9. Click **New** to create a schedule.
- 10. Set the task to run daily at 2:00 AM, so you'll have a scan to review in the mornings.
- 11. Click Apply.
- 12. Click **OK**.
- 13. Click Close.
- Tip: Tomorrow morning, choose File... Open... to load the scheduled scan. Be sure to click on the

**Policy** view button to see the results of your scan with your policy applied.

ielect Systems				
Groups Available		Systems in group	testgroup	
Group Name	Selected	Windows (25)	Unix (0)	
All Systems	No	Sustem	NT Domain	
estgroup	Yes	AL BANY	FCOBAQA	Windows 2000
		BACH	ECOBAGA	Windows 2003
		BOSTON	ECORAQA	Windows 2000
				<u> </u>
	· · · · · · · · · · · · · · · · · · ·	i    L		
			ement Discover Su	vstems Select
	<u>S</u> elect			
Group\System	<u>Select</u>	June Systems Manage	License	
Group\System estgroup	<u>S</u> elect Type GroupObject		License N/A	
Group\System estgroup	Type GroupObject	Systems <u>M</u> anagi	License N/A	
Group\System estgroup	Type GroupObject		License N/A	
Group\System sstgroup <u>R</u> emove	Type GroupObject	JJ Systems <u>M</u> anag	License N/A	Selected

🐴 Task

General Name:

Scan Settings

2

Sure-Scan

B

Rapid-Scan

<u>H</u>elp

Production Scan

Description: All production systems - weekly

Sure-Scan: analyzes systems using file integrity verification

Rapid-Scan: analyzes systems without using the file integrity verification.

OK

Cano

Evaluation Scan			? ×	Evaluation
Task Schedule Sett	ings			Task
	S\Tasks\Evaluation S	can.job		1. At 2:
<u>B</u> un: r 3.0\	bin\EcoraPatchManag	jer.exe" -b "Evalı	uation Scan''	
			Browse	<u>S</u> chedu Daily
S <u>t</u> art in:				Schee
<u>C</u> omments: Task	scheduled by Ecora S	oftware		Ever
Ryn as: ECOF	)A\admin	<u>S</u> et pas	sword	
Enabled (scheduled	I task runs at specified	time)		☑ Sho
	ОК	Cancel	Apply	

Evaluation Scan			? ×
Task Schedule Settings			
1 At 2:00 AM summiday, she		12	
T. At 2:00 AM every day, sta	arding 10/27/200	13	
		New	<u>D</u> elete
<u>S</u> chedule Task: Sta Daily ▼ 2 Schedule Task Daily Every 1 ▲ da	ut time: :00 AM ay(\$)	Advance	ed
	ОК	Cancel	Apply

? ×

### **Schedule Agent Scans**

Let's schedule recurring scans for the agents (if you deployed any).

Select a view C All Agent Sys C Filtered	tems V Criteria	gent Version Status — Iersion Status atest Agent Version	Up-To-Date 1.01.113	-			
Diomain	System	Status	Version	Version Status	Last Communicated	Scheduled	Last Analyzed
2KDC1CHILD	2K/DC1	Online	1.01.112	Up-To-Date	2005-02-17 13:36:16	Every day at 19:00	2005-02-17 12:04:4
2KDC1CHILD	CHICAGO	Online	1.01.112	Up-To-Date	2005-02-17 13:35:25	Every day at 19:00	2005-02-17 12:04:4
2KDC1CHILD	MEMPHIS	Online	1.01.112	Up-To-Date	2005-02-17 13:36:08	Every day at 19:00	2005-02-17 12:04:4
2KDC1CHILD	MILWAUKEE	Online	1.01.112	Up-To-Date	2005-02-17 13:36:05	Every day at 19:00	2005-02-17 12:04:4
CHILD	CHILDDC1	Online	1.01.112	Up-To-Date	2005-02-17 13:35:28	Every day at 19:00	2005-02-17 12:04:4
ECORA	ALIEX88	Online	1.01.112	Up-To-Date	2005-02-17 13:35:38	Every day at 19:00	2005-02-17 12:04:4
ECORAQA	AQDEVSERVER	Online	1.01.112	Up-To-Date	2005-02-17 13:35:25	Every day at 19:00	2005-02-17 12:04:4
ECORAQA	BE NLEYXP	Online	1.01.112	Up-To-Date	2005-02-17 13:35:28	Every day at 19.00	2005-02-17 12:04:4
ECORADA	BOSTON	Online	1.01.112	Up To-Date	2005-02-17 13:36:22	Every day at 19.00	2005-02-17 12:04:4
ECORAQA	DAYTON	Online	1.01.112	Up-To-Date	2005-02-17 13:36:15	Every day at 19:00	2005-02-17 12:04:4
ECORAQA	MALACHI:2K3	Online	1.01.112	Up-To-Date	2005-02-17 13:35:38	Every day at 19:00	2005-02-17 12:04:4
ECORAQA	MLAMI	Online	1.01.112	Up-To-Date	2005-02-17 13:35:31	Every day at 19:00	2005-02-17 12:04:4
ECORAQA	MV/WIN2003	Online	1.01.112	Up-To-Date	2005-02-17 13:36:2+	Every day at 19:00	2005-02-17 12:04:4
ECORAQA	MV-XPSP2	Online	1.01.112	Up-To-Date	2005-02-17 13:36:05	Every day at 19:00	2005-02-17 12:04:4
ECORADA	NASHUA	Online	1.01.112	Up To-Date	2005-02-17 13:35:40	Every day at 19:00	2005-02-17 12:04:4
Help	Uninstall Agent	Update Agent	Schedule Analysis	Befresh	Properties	Select All	Close

- 1. Choose **Tools... Agents...** or click on the **Agent** button.
- 2. Locate and select the agent you wish to schedule.
- 3. Click the **Schedule Analysis...** button and set the frequency for automatic analysis on a recurring basis.

📲 Schedule Scan	<u>? ×</u>
-Schedule Scan	
<b>⊠</b> Enable	
Daily	
<u>○</u> <u>₩</u> eekly	On: Thursday 🗸
Monthly	On the: 1-st
✓ Sure-Scan	At: 00:00
Help	<u>C</u> ancel <u>O</u> K

- 4. Click in the checkbox to **Enable** scheduled analysis.
- 5. Choose **Daily**, **Weekly**, or **Monthly** for the frequency of automatic analysis.
- 6. Set the start date, day, and/or time for recurring scans.
- 7. Click **OK**.

## **Use the Online Reporting Center**

The reporting center is a website interface created by Ecora to provide an intuitive way to query the Patch Manager database. The URL can be accessible to anyone in an environment who can access the share on which you installed the reporting center. CIOs or auditors can see a report of Policy Compliance across all systems; IT staff might be interested in the Patch History of a machine.

- Click on the **Reports** button to access the online reporting center (installed on an IIS server during setup).
- 2. If prompted, enter your login and password and

#### click OK.

- Select the Missing Patches report from the drop-down list.
- 4. Click in the checkbox for the test group.
- 5. Click **Go**.
- Browse the resulting report. Verify that there are no instances of the IE patch 828750 missing.
- Change the report to Pushed Patches and the group to All Systems.
- 8. Click Go.
- Browse the resulting report for IE patch 828750 installed on test group systems.



## **Congratulations!**

You have implemented Ecora Patch Manager conducted a security patch analysis of hosts in your environment, and responded immediately to detected vulnerabilities by deploying a high-exposure patch - all from your desk! If you proceeded with the optional exercises, you have also tried the Test Center, approved a patch for deployment, established a model patch policy, compared your systems to it, and scheduled a scan and an alert. Patch Manager enables you to immediately reduce your infrastructure's risk and to proactively maintain security on an ongoing basis.

## **Customer Support**

Ecora Sales representatives are available to answer your questions about product features and pricing at 1.877.923.2672 or email sales@ecora.com.

Ecora technical support representatives are available to help resolve any technical issues at 1.877.923.2672 ext 771 or email support@ecora.com.

Don't forget to read the User Manual, available in fully hyperlinked format in the online help system as well as in printable (PDF) format at: (http://www.ecora.com/ecora/um/patchmanager/5.0/user\_manual-patchmanager5.0.pdf).