Ecora Patch Manager 5.0
Evaluation Guide

Table of Contents

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® 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.

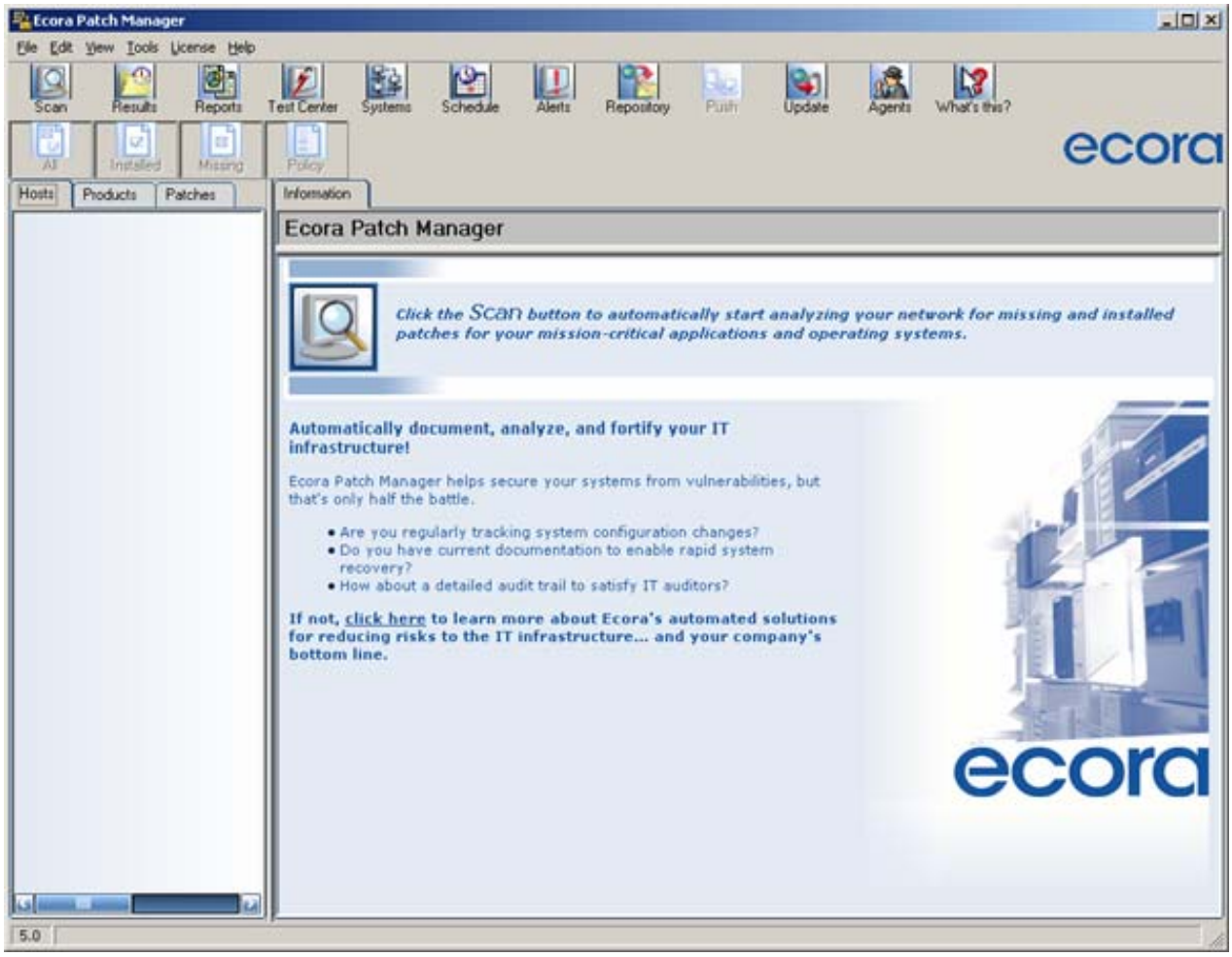
International Language Support – Supports international versions of Microsoft and Sun operating systems, including: Danish, Dutch, French, Finnish, German, Italian, Japanese, Norwegian, Portuguese, Spanish, Swedish, and United Kingdom.

Install the Software

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

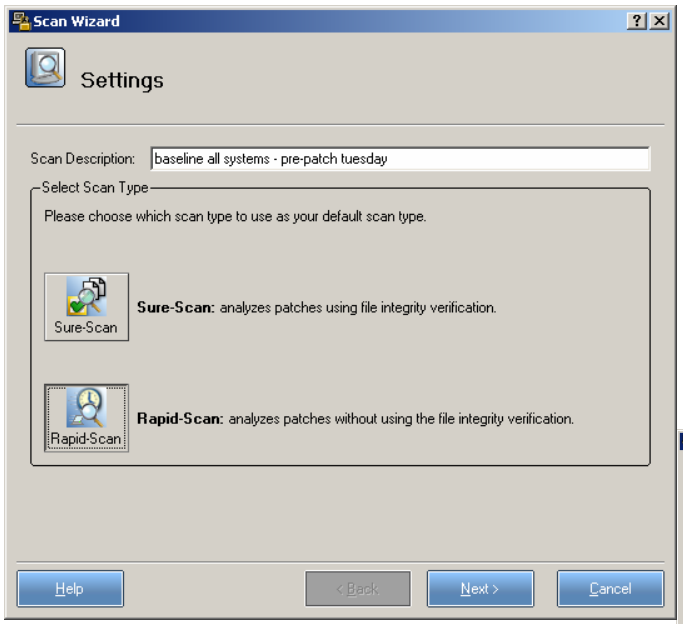
- If you have not, please refer to the **Start-up Guide**, located on Ecora's Support webpage (http://www.ecora.com/ecora/um/patchmanager/5.0/startup_guide-patchmanager5.0.pdf).

You should be here…

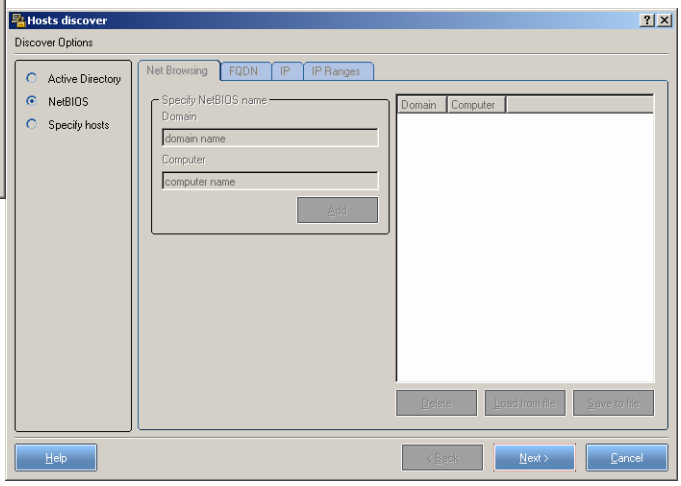


The main user interface of Patch Manager.

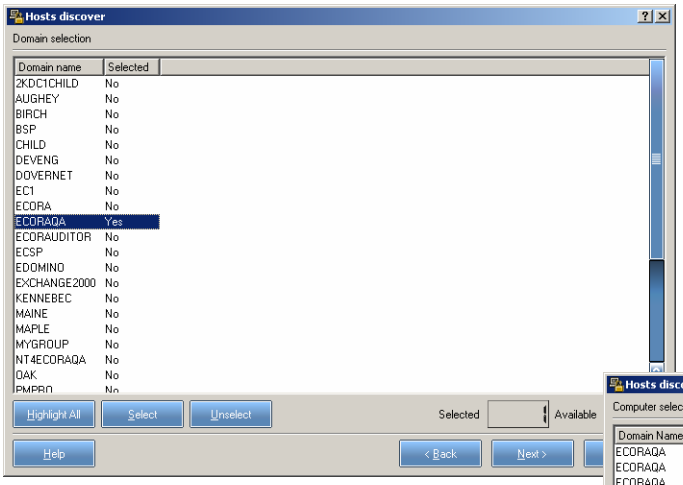
Discover, Group, & Scan



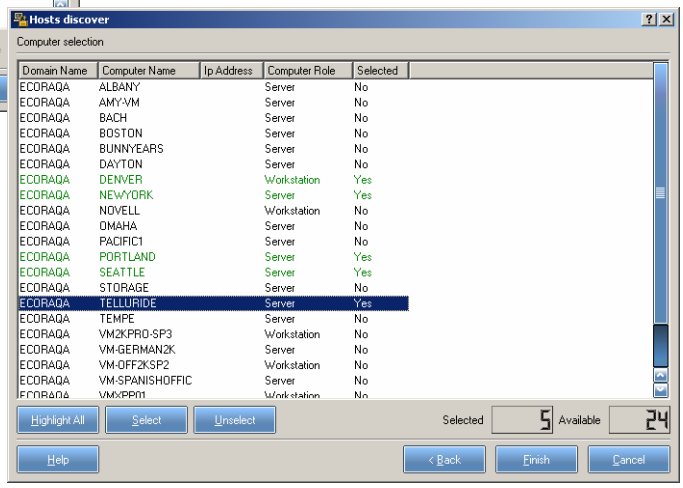
1. Click on the **Scan** button.
2. Choose the Scan Type: **Sure Scan** or **Rapid Scan** and click **Next >**.
   Sure Scan - analysis includes file integrity (MD5 checksum) verification for greatest accuracy and security.
   Rapid Scan - analysis skips file integrity check for greater speed and faster results display.
3. Click on the **Discover Systems** button.



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



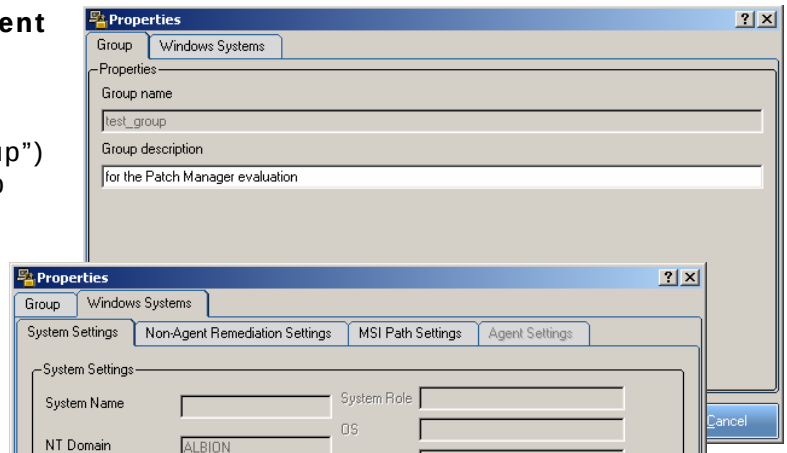
5. Click on the **Next >** button.
6. Double-click to select the domain(s) to discover and click **Next >**.
7. Double-click to select a few (3-5) systems and click **Finish**.

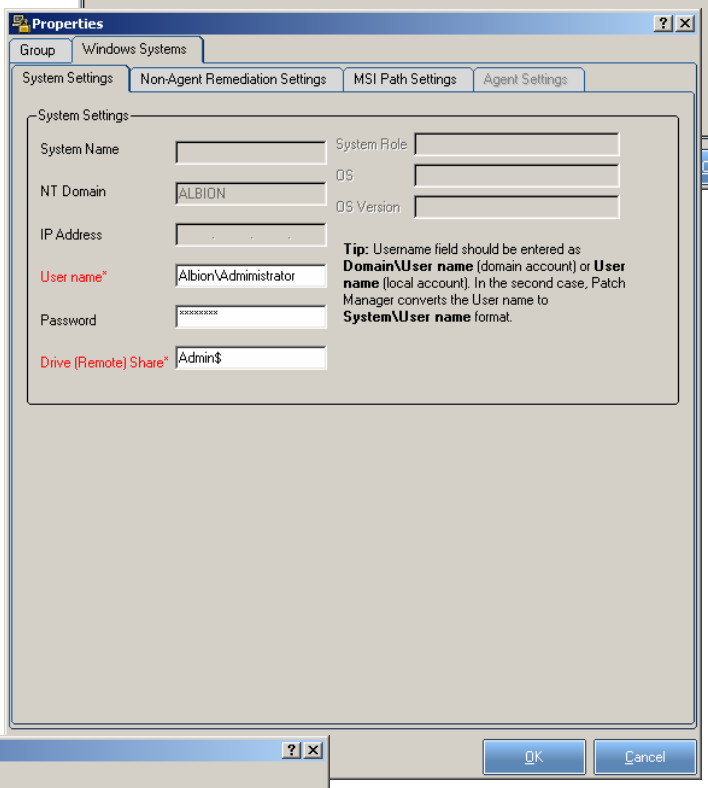


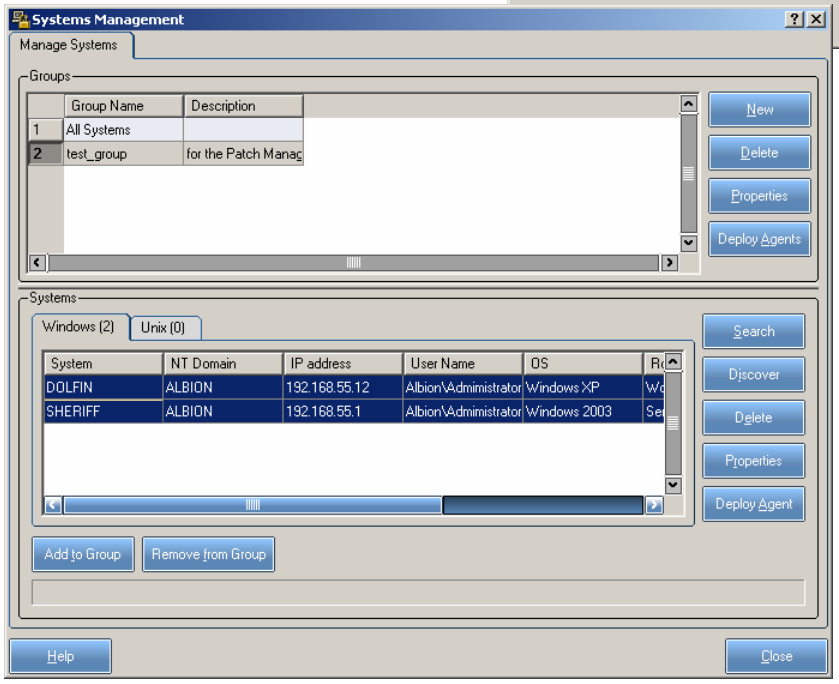
Tip: If possible, select devices in a test lab or non-production capacity. The following sections include the deployment of a patch, which should always be "tested" in a minimum-risk situation.

Tip: If you wish to use agents, the Start-up Guide includes a section on deploying agents from this dialog box.

8. Click on the **Systems Management** button.
9. Click on the **New** button.
10. 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.





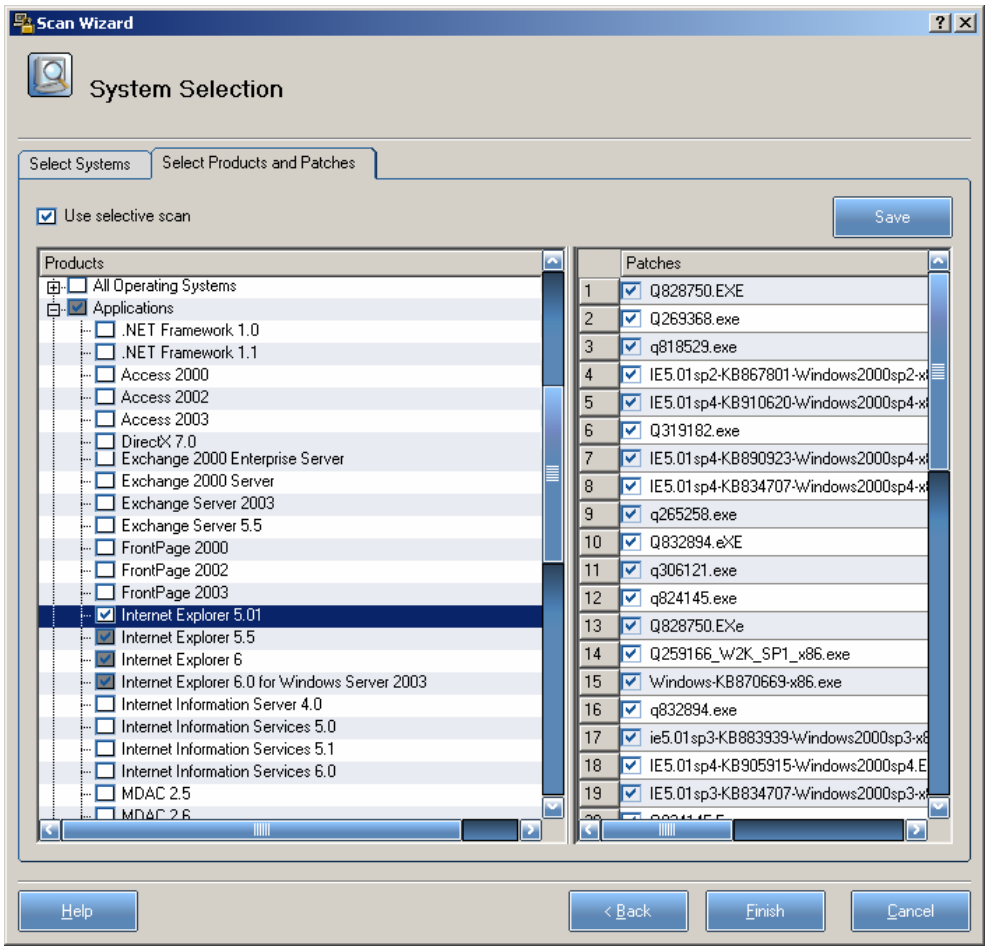


18. Select the test group.

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.



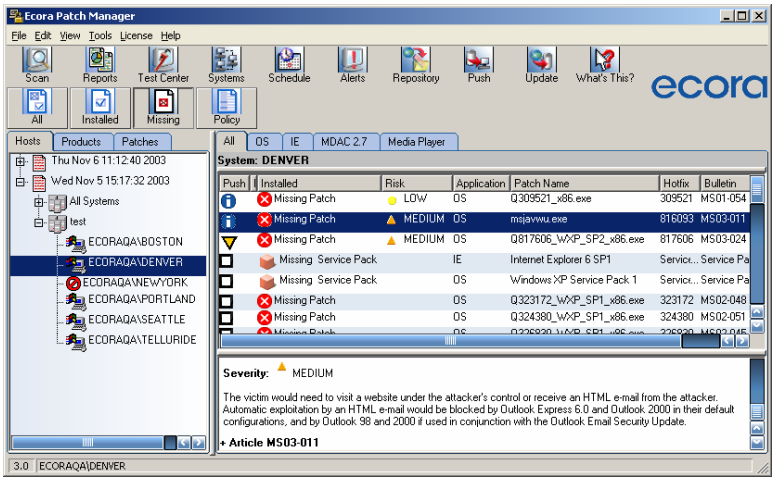
22. In the right pane, locate and select the patch(es) to analyze.
    For this evaluation, leave all selected.

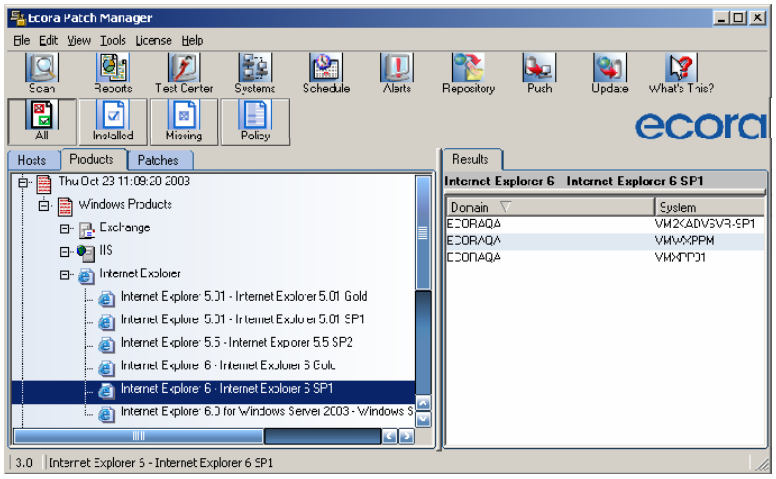
23. Click **Finish** to begin scanning systems for patches.

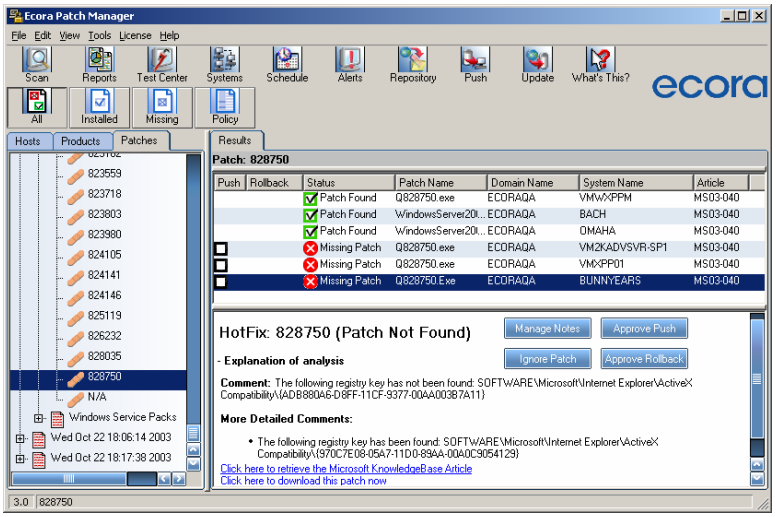
24. Enter a Scan Description and click **OK**.

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.
2. 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.
3. 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.
6. We are looking for a specific patch, so click on the **Patches** tab.
7. Click on the **All** button (for all information; installed and missing patches and service packs).
8. 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:
   http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-040.asp
   http://www.ciac.org/ciac/bulletins/o-002.shtml

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.

    Patch was not detected as installed.

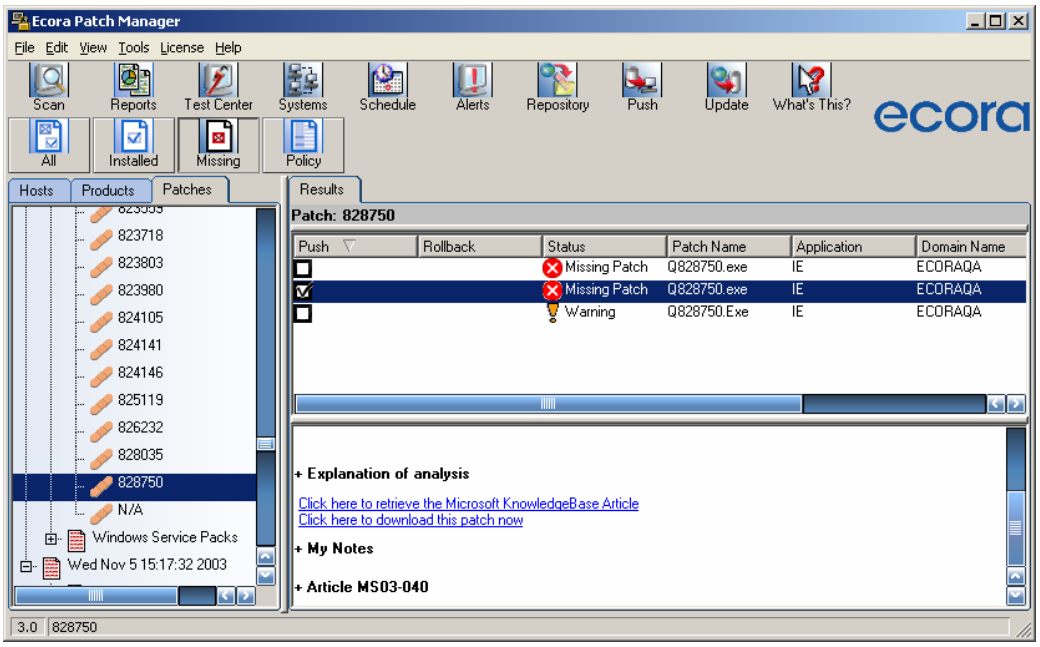
11. Click on the **Missing** button to filter out machines with the patch installed. The result is a list of machines that need to have 828750 installed.

    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

CAUTION:
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. 



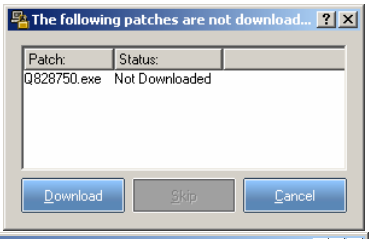
Note: If the patch is not already downloaded perform these steps:

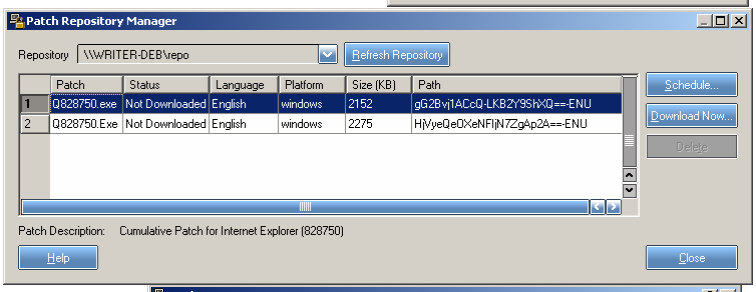
a. Click **Download** to download patches selected for push.

b. In the repository dialog, select the patch and choose **Download Now…** (vs. scheduling for later).

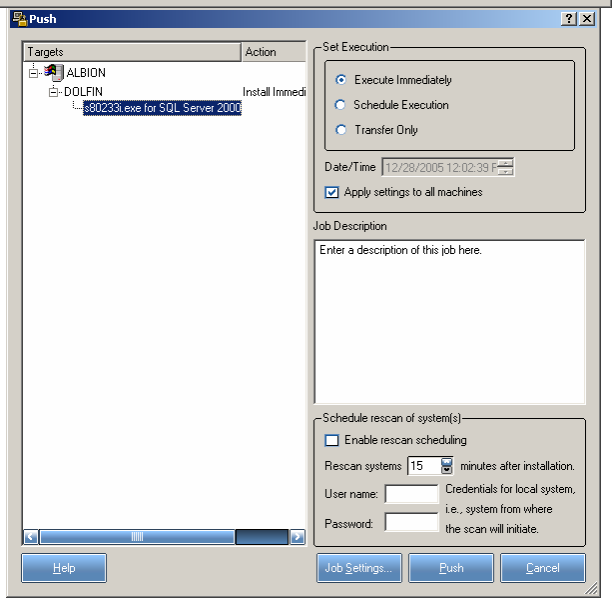
c. Click **OK**.

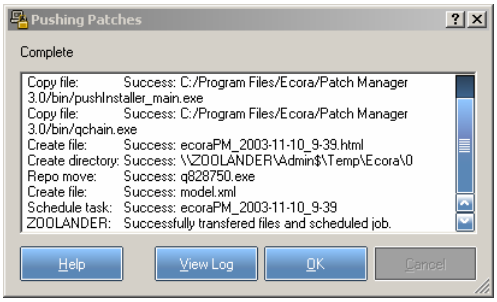
d. Once the patch has successfully downloaded, click **Close**.





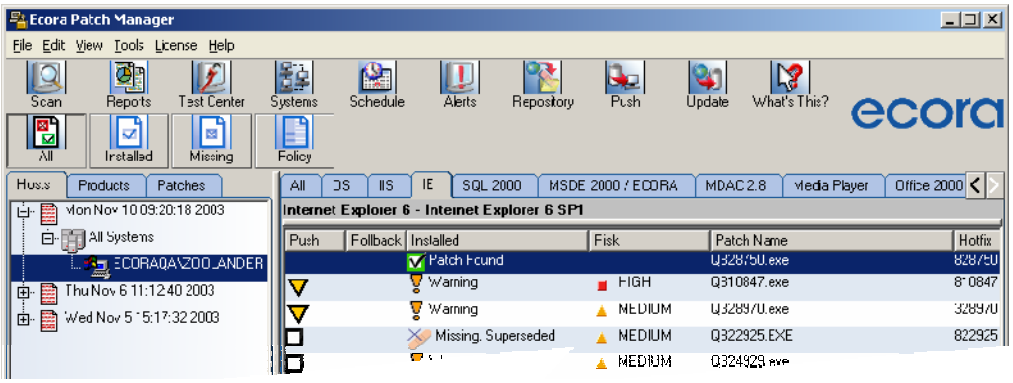
5. In the Push dialog box, verify that the host and patch are correct.
6. Enable the **Execute Immediately** option to install now (vs. scheduling for later).
7. Enter a job description.
8. Click **Push**.
9. Click **OK** to accept the job global settings (without any overrides).
10. Once the push has finished, click **OK**.





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.
6. Verify that the host you updated shows patch 828750 as installed.



Optional Exercises – for Added Value!

Approvals & Notes

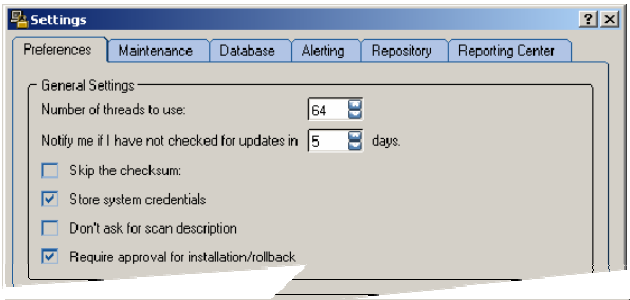
Patch Manager provides the ability to add notes and conditions to each patch. This allows you to record your test findings or comments, approve patches for approval or rollback, and set certain patches to be ignored in analysis.

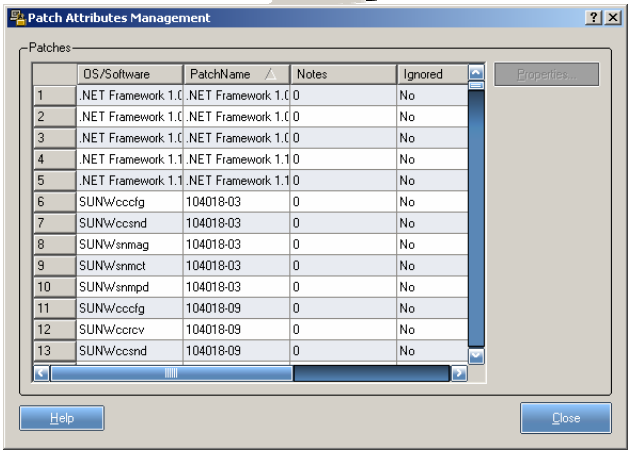
We have verified successful installation of patch 828750 and will now approve it for distribution and enable required approvals. Combined with policies (next section), required approvals further tighten security controls.

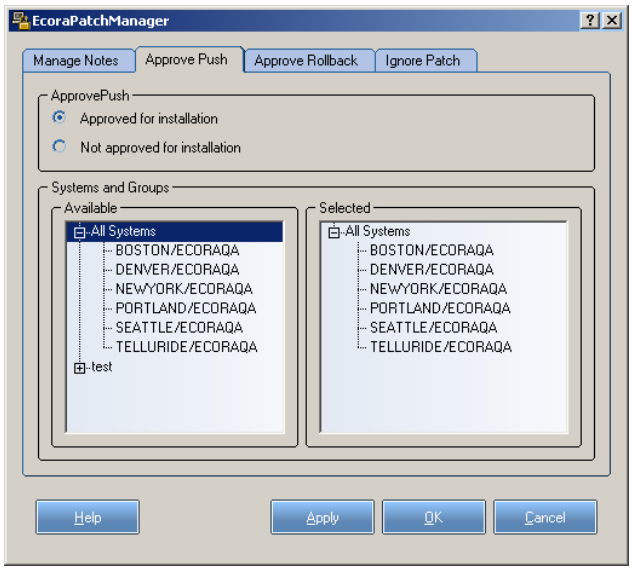
1. To enable approvals, choose **File... Settings...**
2. Click in the **Require approval for installation / rollback** checkbox and click **OK**.
3. Choose **Tools... Patch Attributes Management...**from the main menu.
4. Click on the **Patch Name** column head to sort by the patch name.
5. Scroll to 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**.
9. 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.





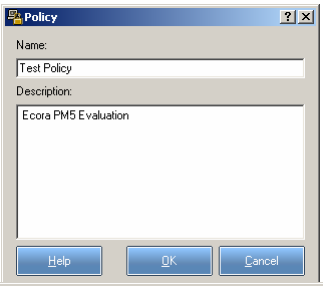


Using Policy Manager

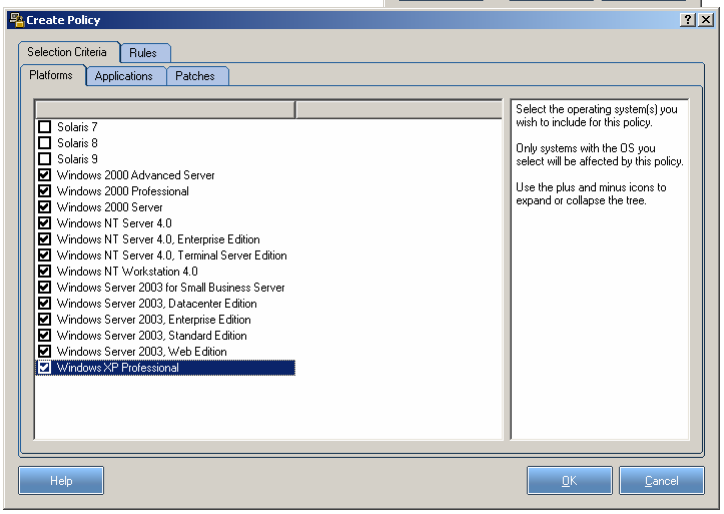
Create a Policy

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.

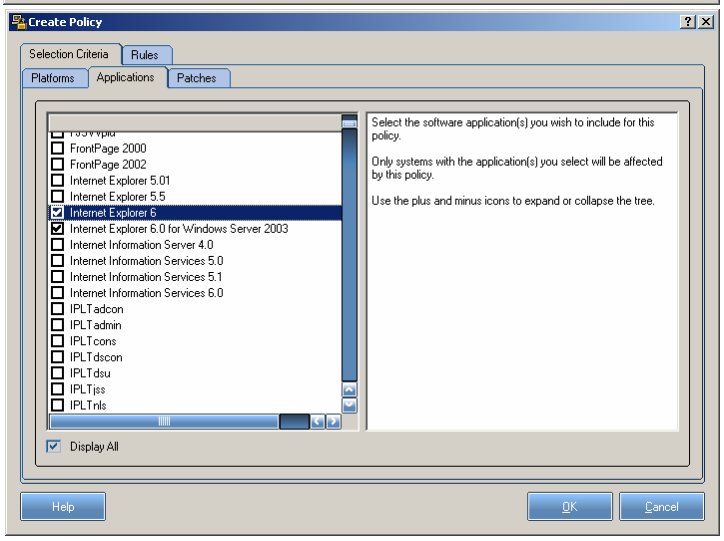
Since we've tested patch 828750 and approved it for distribution, let's create a policy that all systems in the test group must have 828750 installed to be in compliance.



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**.



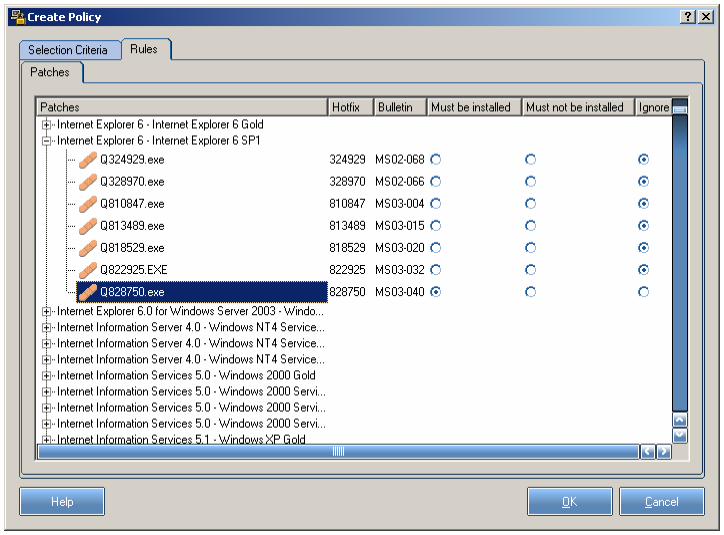
4. In the Create Policy dialog box, on the Selection Criteria tab, click on the **Platforms** tab.
5. Click in the checkbox for each Windows OS version.
6. Click on the **Applications** tab.
7. Click in the **Display All** checkbox.
8. Click in the checkbox for the relevant version(s) of Internet Explorer (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.

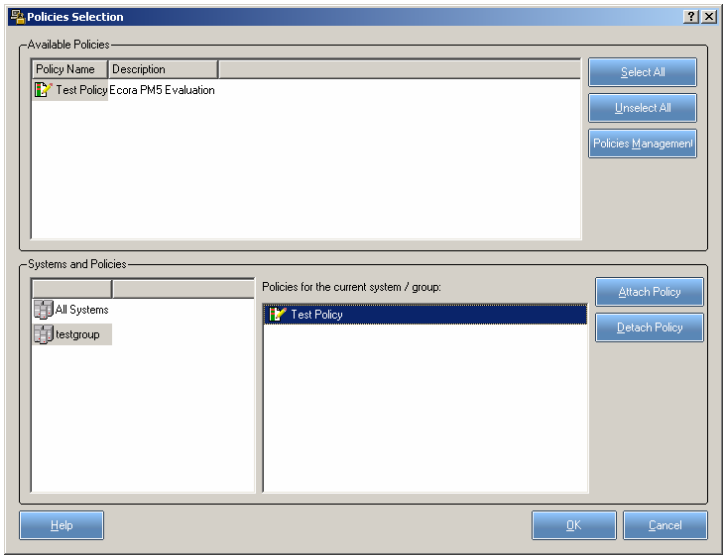
10. Click on plus signs to expand the tree by application to see patches. In this case, leave all patches set to **Ignore** so the policy applies regardless of installed status. You could choose to have a policy apply ONLY if a given patch was installed or not installed. Systems are displayed in Policy view only if they meet the selected criteria.

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.



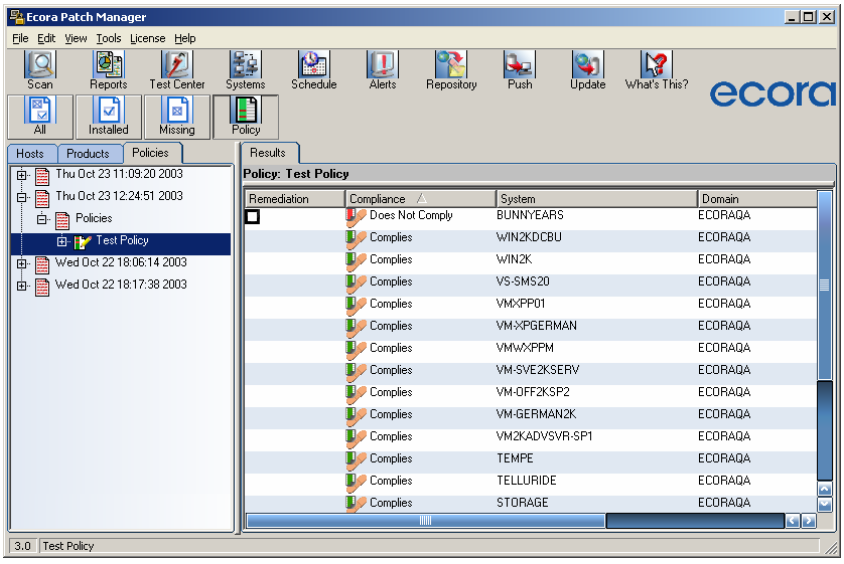
Apply the Policy

1. 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.
2. 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.

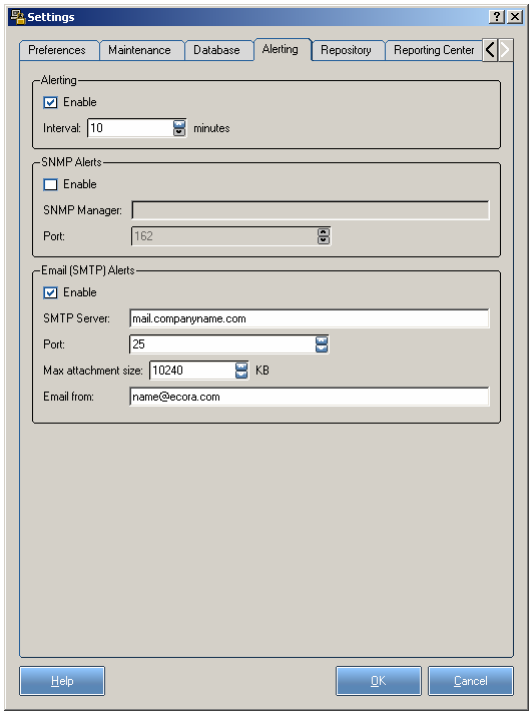


Tip: Notice that any systems that do NOT comply have a checkbox for remediation (which includes both installation and rollback, if necessary, to bring the system into compliance with the policy). If you want to remediate by policy, select the checkbox, click **Push**, and follow the Patch Installation 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.

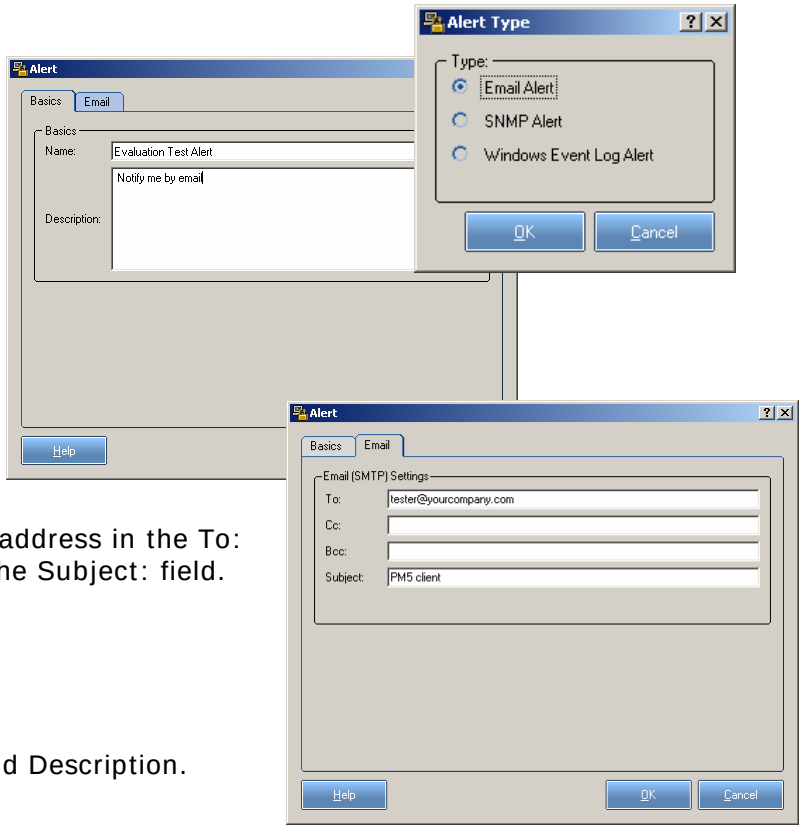
Enable Alerts & Triggers



1. 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**.

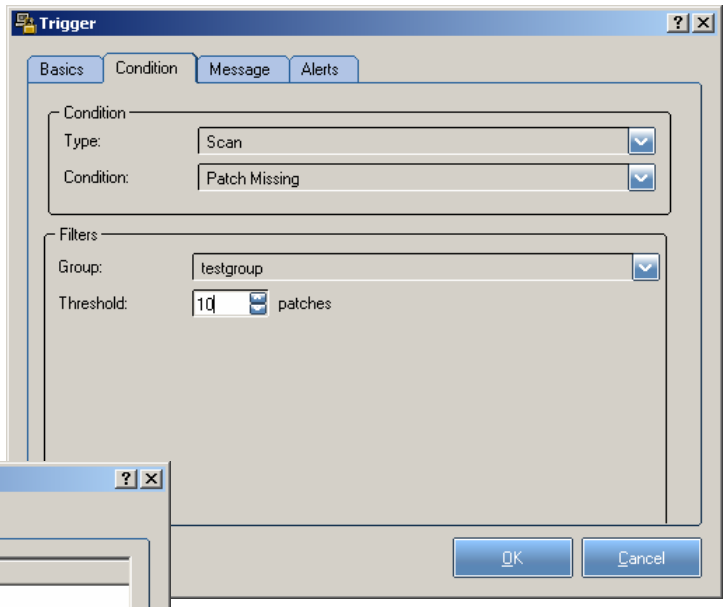
Set an Alert

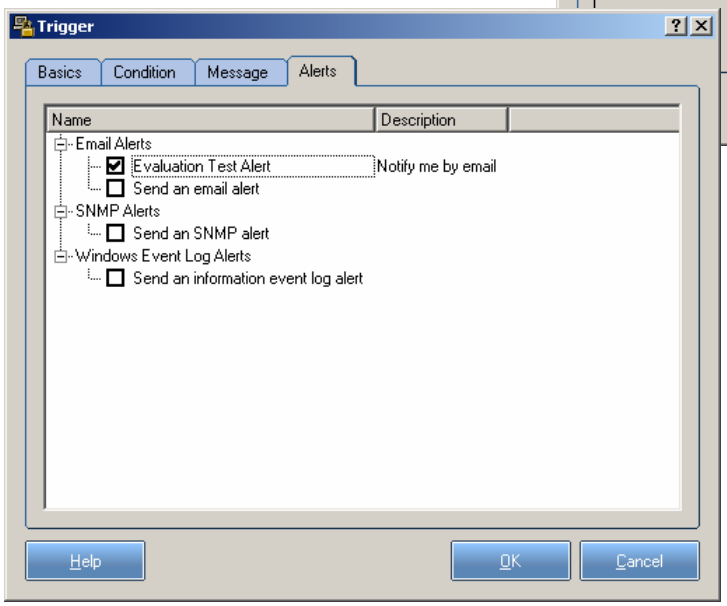
We'll create an alert for too many missing patches.



1. Choose **Edit... Alerts & Triggers...** from the menu.
2. Click on the **Alerting** tab.
3. Click **New…**.
4. Select **Email Alert** and click **OK**.
5. 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.

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**.



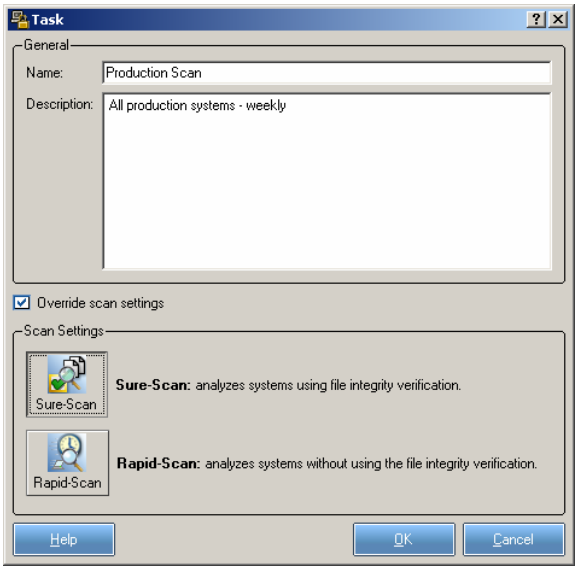


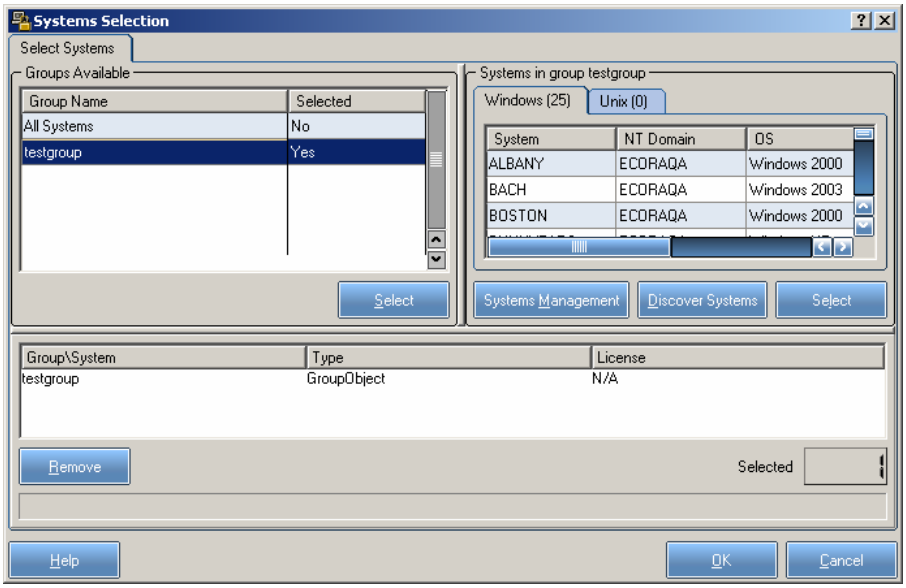
Schedule a Scan

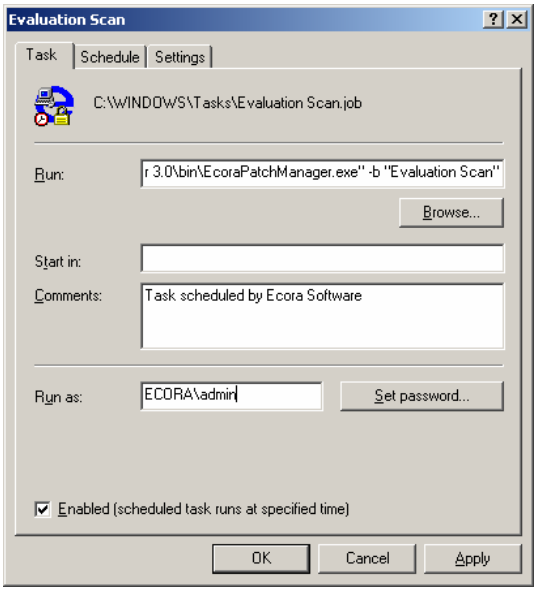
Let's schedule a scan for overnight for you to review in the morning.

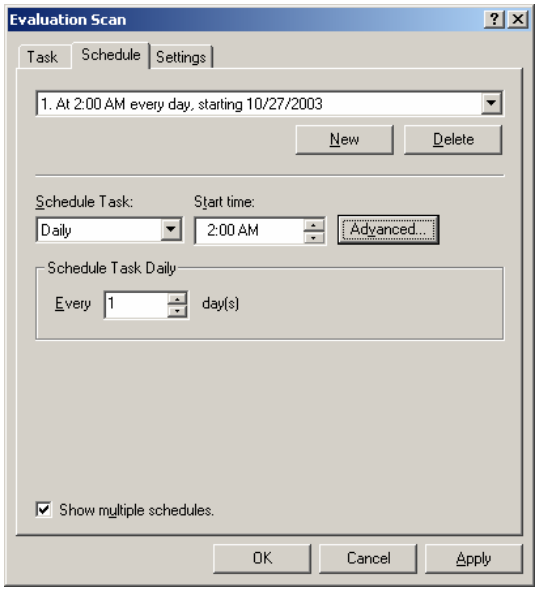
1. Click on the **Schedule** button.
2. Click on the **New…** button.
3. Enter a name (such as "Evaluation Scan") and a description for the task.
4. Click **OK**.
5. Highlight your group and click the **Select** button.
6. Click **OK**.
7. On the Task tab, use the **Run as** field and use the **Set Password…** 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.



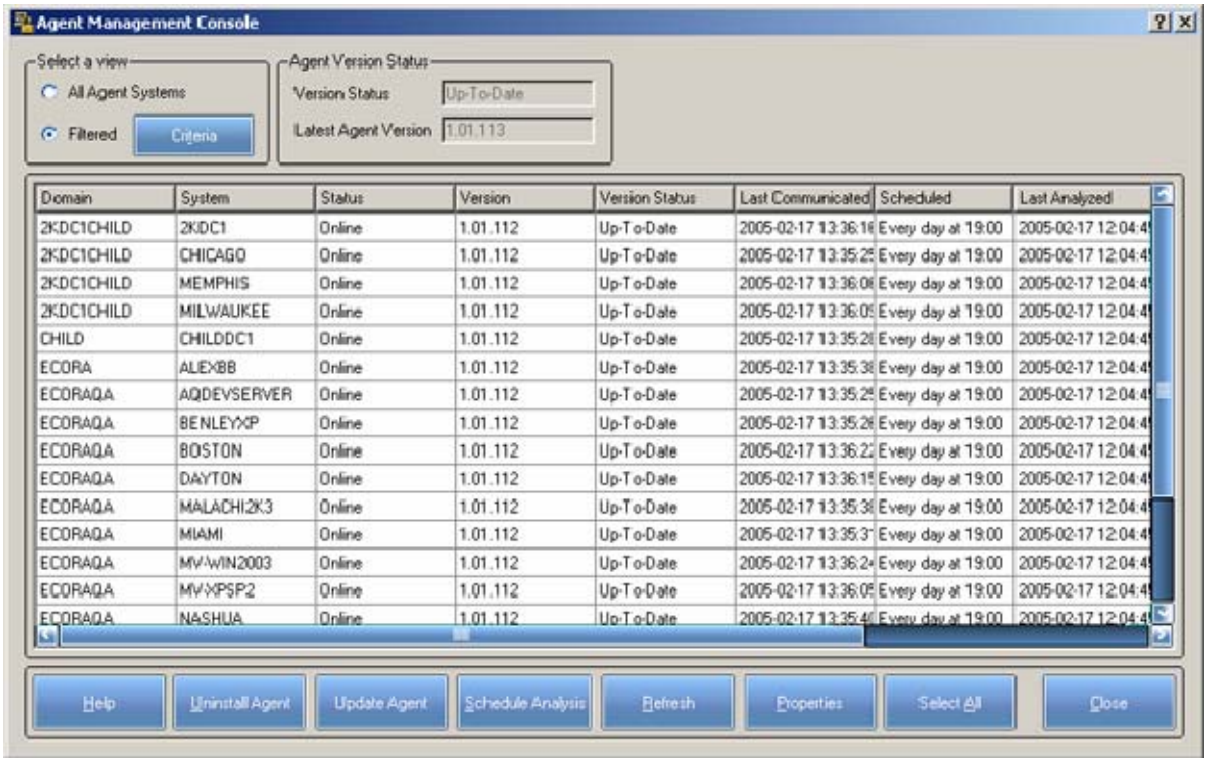




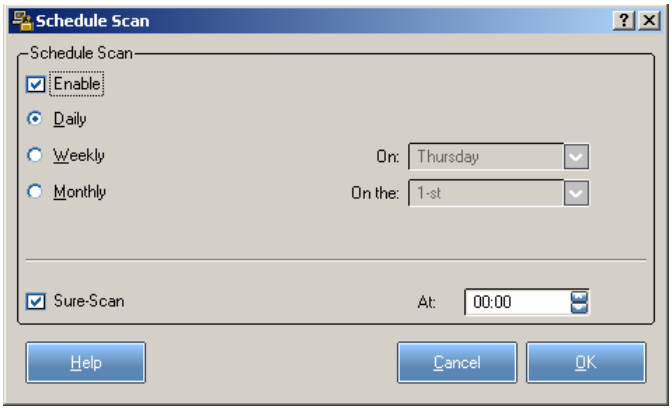


Schedule Agent Scans

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



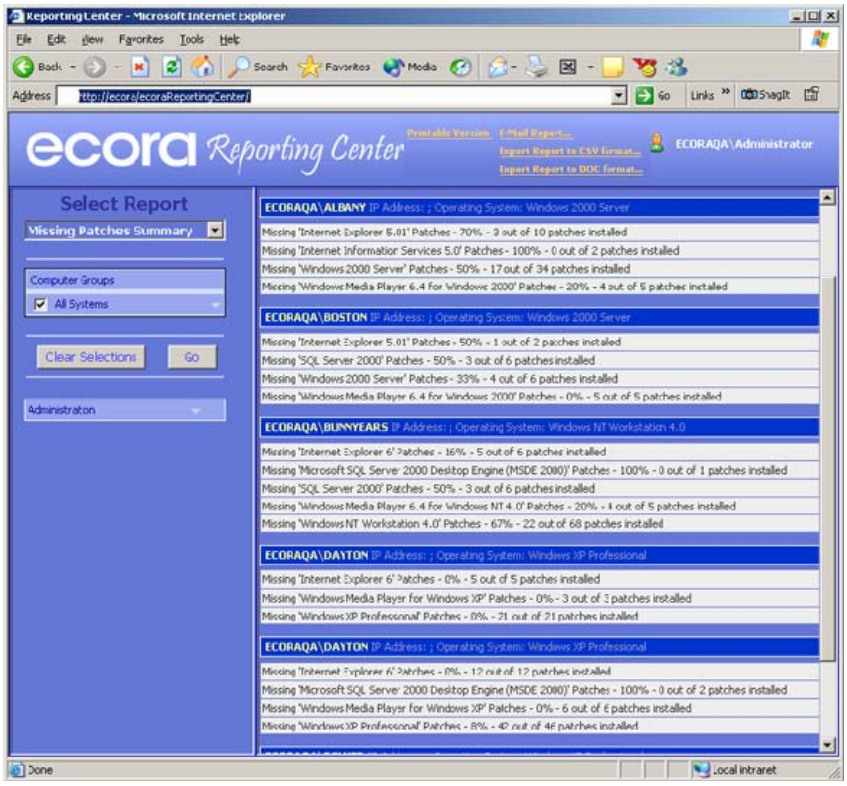
1. Choose **Tools... Agents...** or click on the **Agent** button.
2. Locate and select the agent you wish to schedule.
3. Click the **Schedule Analysis...** button and set the frequency for automatic analysis on a recurring basis.



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.



1. 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**.
3. Select the **Missing Patches** report from the drop-down list.
4. Click in the checkbox for the test group.
5. Click **Go**.
6. Browse the resulting report. Verify that there are no instances of the IE patch 828750 missing.
7. Change the report to **Pushed Patches** and the group to **All Systems**.
8. Click **Go**.
9. 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).