



HyBlue Patch Quick Start

Patch Management and System Monitoring

Patch is unique in that it combines the benefits of patch management with detailed systems management including real-time alerting and historical reporting. The following sections discuss how you interact with HyBlue, first with system monitoring and then patch management.

System Monitoring

Patch automatically monitors your systems at a very detailed level, alerting you when a change occurs that requires your attention. The monitoring section of Patch goes to work immediately upon installation of the Patch software and requires no configuration. The sections below discuss this in more detail.

Real-time Alerting Patch will automatically alert you when conditions occur that indicate a problem or a potential problem with your systems. These alerts are prioritized as **Critical**, **Important** or **Minor**.

Critical and **Important** alerts should be reviewed as they arrive as they are indicators of issues that are likely impacting or about to significantly impact your users' ability to get work done. **Minor** alerts should be reviewed when they occur frequently as they are then indicators of potential problems.

Critical and **Important** alerts are sent via email and critical alerts are sent via text message to cell phones if the technical contact has listed their cell phone number and carrier. The alerts are intended to help direct technical staff to quick resolution of the issue noted. HyBlue suppresses repeat alerts so that you are not alerted over and over about the same issue.

Minor alerts are not sent but are recorded on HyBlue's website.

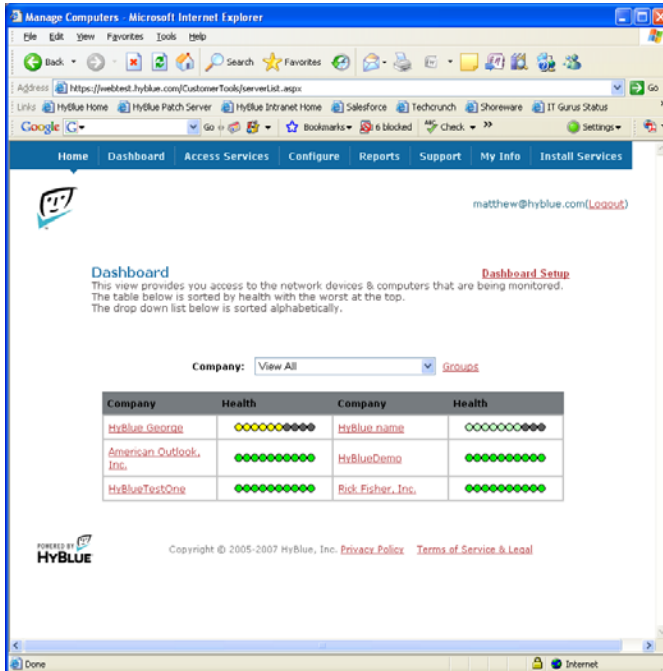
Daily Summary HyBlue also sends an email each morning totaling the alerts that have occurred in the previous 24 hours. This email is sorted by

HyBlue Inc. 5 West Harrison. Seattle, WA 98119
206 838 1907, Sales@HyBlue.com www.HyBlue.com



customer, then server and lists the events and the number of times each event occurred.

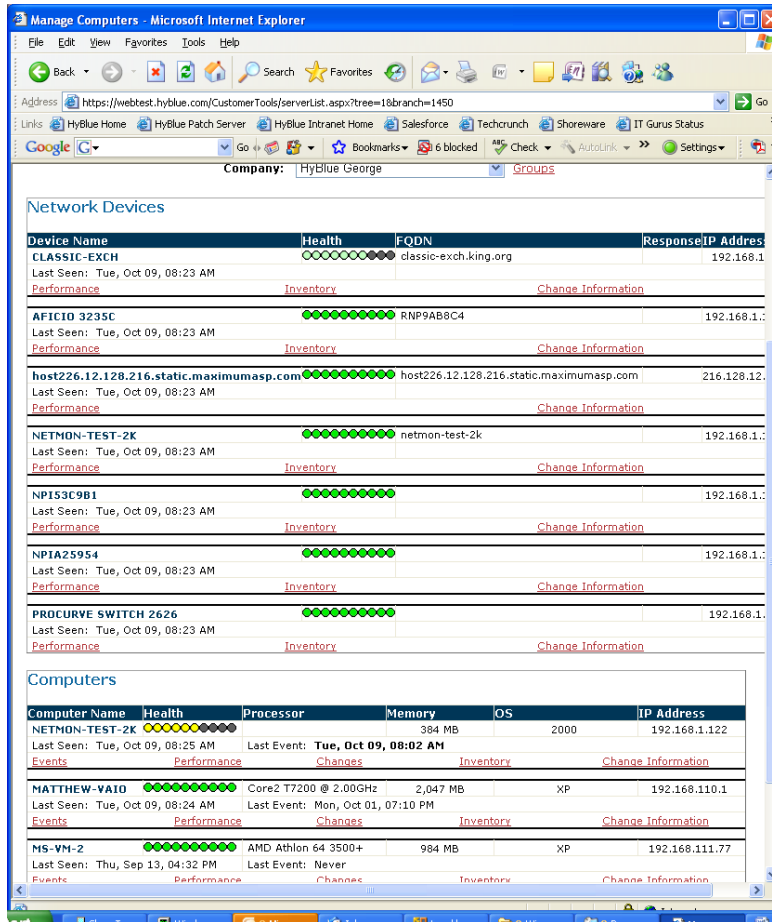
The Dashboard When you first login to the HyBlue Portal, you will see the company names of your customers. You will also see a health indicator that shows the health of each customer.



In the example above, the company HyBlue George has one or more computers that have had an important event within the last 24 hours. HyBlue name has had some minor alerts, Rick Fisher Inc and American Outlook have no problems with his computers.

Clicking on a customer name gives you a health view of all the customer's network devices and computers.

HyBlue Inc. 5 West Harrison. Seattle, WA 98119
206 838 1907, Sales@HyBlue.com www.HyBlue.com



The top group of devices are monitored by HyBlue's Network Performance Monitor service, the lower group are monitored by Windows Monitor, a component of Patch.

Currently, no devices are showing down or red. Netmon-test-2k has had an Important alert. Green indicates the computer is operating normally. Note that each monitored device shows details about the device or computer as well as when it last checked in with HyBlue and when it last sent in an event.

You can click on any link below a computer to drive into Event history, Performance history, Changes or see an Inventory view of that computer. You can also click on Change Information to update specific information on that device or computer including the Computer Name used and technician. You can also remove a device from service from the Change Information page.

HyBlue Inc. 5 West Harrison. Seattle, WA 98119
206 838 1907, Sales@HyBlue.com www.HyBlue.com



Clicking on Events will show you the events that have occurred during the current and previous day.

Home Dashboard Access Services Configure Reports Support My Info Install Services

matthew@hyblue.com (Logout)

Error Log for Computer: CLUSTER-1

The following tables show the events that occurred on this computer during the timeframe below.

From: 5/1/2007 To: 5/2/2007 Filter

[Server Up/Down](#) [Security](#) [Application/System](#) [Performance](#)

Server Up/Down Events

First - Last Occurrence	Number	Priority	Description	Actions
-------------------------	--------	----------	-------------	---------

[Back to top](#)

Security Events

First - Last Occurrence	Number	Priority	Description Event ID/Source	Actions
-------------------------	--------	----------	--------------------------------	---------

[Back to top](#)
[Export](#)

Application/System Events

First - Last Occurrence	Number	Priority	Description Event ID/Source	Actions
5/1/2007 10:10 AM	1	Important	1309 ASP.NET 2.0.50727.0	View Details View All Events

Performance Events

First - Last Occurrence	Number	Priority	Description	Actions
-------------------------	--------	----------	-------------	---------

Copyright © 2005-2007 HyBlue, Inc. [Privacy Policy](#) [Terms of Service & Legal](#)

You can also look at events over a 30 day period by changing the From and To dates. Clicking on an event gives you details of the alert that was sent via email. Note that events can be shown for Up/Down of servers, Security (the Windows Audit log), Application and Performance alerts. Each of these alerts is sent in real-time via email but you can view the history here.

You can also run reports while logged in, both the **Network Audit Report** and **Inventory Report**.

HyBlue Inc. 5 West Harrison. Seattle, WA 98119
206 838 1907, Sales@HyBlue.com www.HyBlue.com



The Network Audit Report gives you a complete history of all events that occurred over the previous 30 days or a previous calendar month. It includes a listing of events, alerts, performance counter and some inventory. Click on Network Audit Report, select the customer and time frame and an email will be sent to you with a link. Click on the link and the report will be displayed.

The report has been formatted to paste directly into Word so you can add comments, remove items you don't require and then print out on your letterhead.

The **Inventory Report** gives a detailed listing of all hardware, software and services for every computer in the customer's network. Like the **Network Audit Report**, it starts with a summary and then shows complete detail for each computer. To display the report, simply click on **Inventory Report**, select the customer you want the report on and a window will pop up. This report has also been formatted to copy and paste into word or print directly to your printer.

Patch Management Operation

Patch does the hard and time-consuming work traditionally performed by an IT professional. It gathers information from your systems, organizes it, and compares it to Microsoft's and other vendors' update-information databases. Once you decide which patches are required for your situation, which machines should receive them, when the patches should be applied, and what should happen if computer needs rebooting, Patch handles the distribution automatically. Patch can be used for a single computer, a network of computers, or computers across multiple networks.

Once the client is installed, it will take a complete inventory of each computer. This operation may take up to an hour, and upon completion the computers will be visible on the Patch Management's **Devices** menu.

To view a computer's patch status, log into the HyBlue portal and select Patch under **Access Services** in the menu bar. A new window will open which will allow access into the Patch Management System.

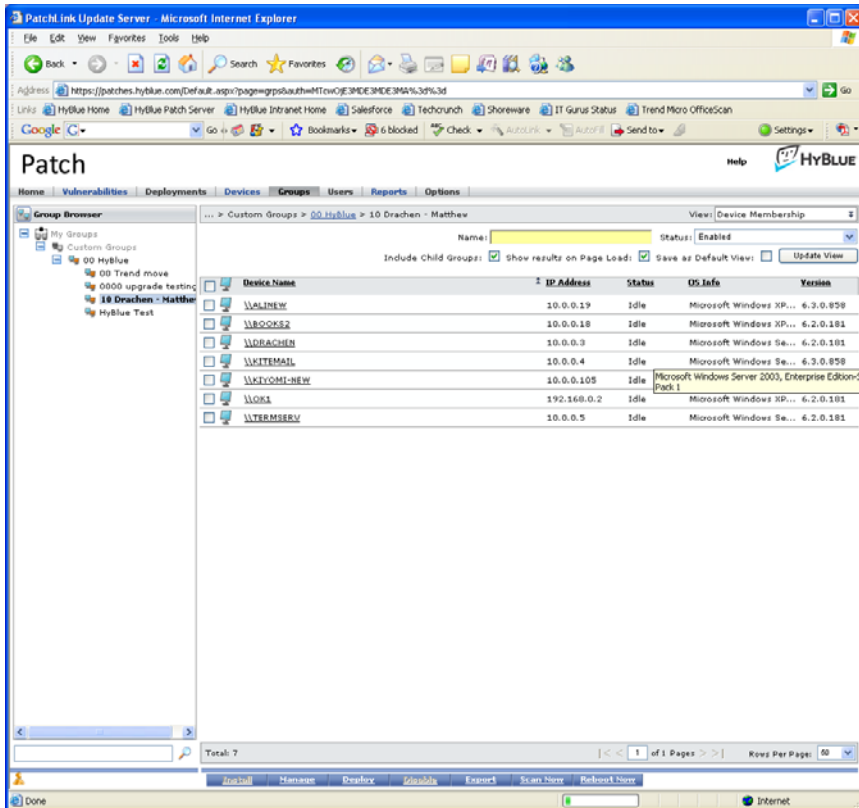
The features of the Patch Management System are discussed below, beginning with the **Top Level Menus** found at the top of the popup window.

HyBlue Inc. 5 West Harrison. Seattle, WA 98119
206 838 1907, Sales@HyBlue.com www.HyBlue.com



Groups

The Groups screen is the first that is displayed when accessing the Patch Management System.



The Groups or companies screen is split between the group listing on the left and the details on the right. In the example above, HyBlue has 4 companies under management.

The details screen has a variety of views, currently shown is the Device Membership view. The views for the details screen break down into 7 major views with specific settings for each view.

The views are:

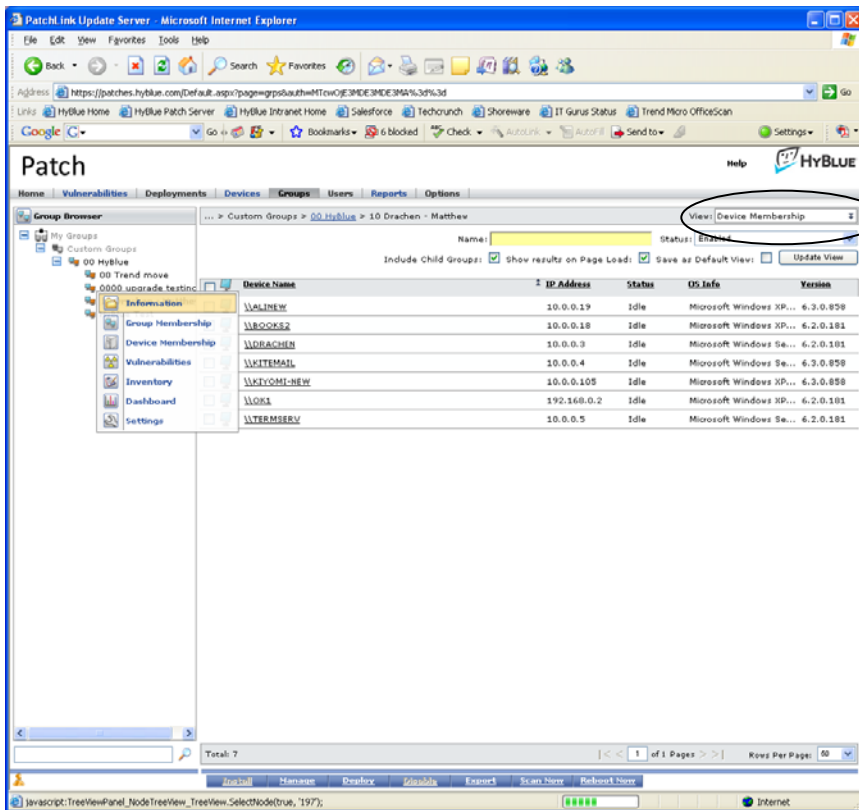
- Information
- Group Membership
- Device Membership
- Vulnerabilities
- Inventory
- Dashboard
- Settings

HyBlue Inc. 5 West Harrison. Seattle, WA 98119
206 838 1907, Sales@HyBlue.com www.HyBlue.com



Each of these views has options for viewing information in them. These options are generally available via the drop down menus in the upper right hand corner.

You can change between views two ways, one by right clicking on a group on the left side.



Or selecting with the View drop down menu circled above.

Views show the following

- **Information** displays general global data for the group.
- **Group Membership** shows which groups are in the group
- **Device Membership** shows which computers are in the group
- **Vulnerabilities** shows which patches are required for this group of computers. You can apply patches directly to computers from this screen by clicking on the desired vulnerability (patch) and following the steps for deployment found below in the **Deployment** section.
- **Inventory** categorizes the group's computers by operating system, software, hardware, and services.

HyBlue Inc. 5 West Harrison. Seattle, WA 98119
206 838 1907, Sales@HyBlue.com www.HyBlue.com



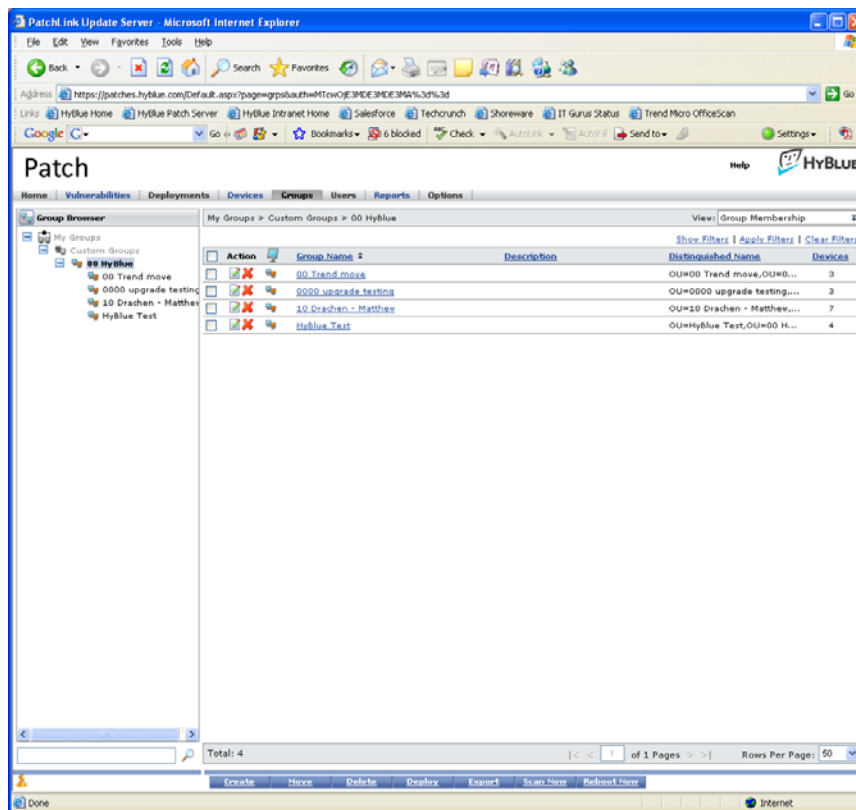
- **Dashboard** gives a quick chart view of patch status
- **Settings** shows some internal technical settings

Information

Information is rarely used, it simply shows specifications for the group

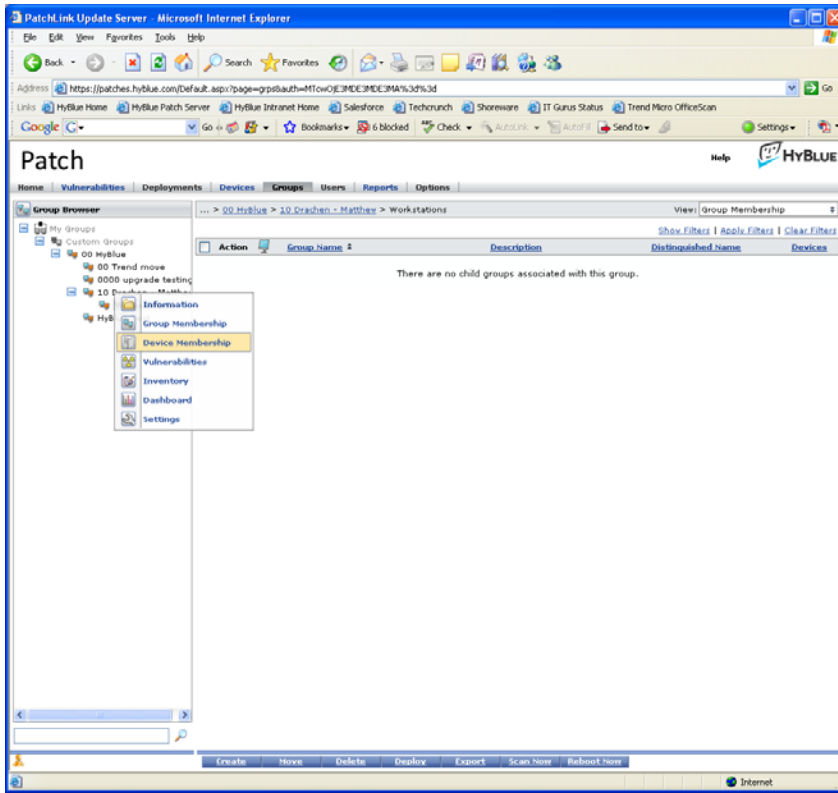
Group Membership

This is the section that allows you to create custom groups. If you select your company name and look at Group Membership you will see each customer below your company.



You should not change your company groups but you can create new groups either at this level or inside of a company. For example, you may want to only patch workstations in a company. Do easily do this you would select the company, for example 10 Drachen – Matthew and then create a group by clicking on the Create button in the bottom of the screen. Then opening that group and selecting Device Membership takes you to the screen shown below.

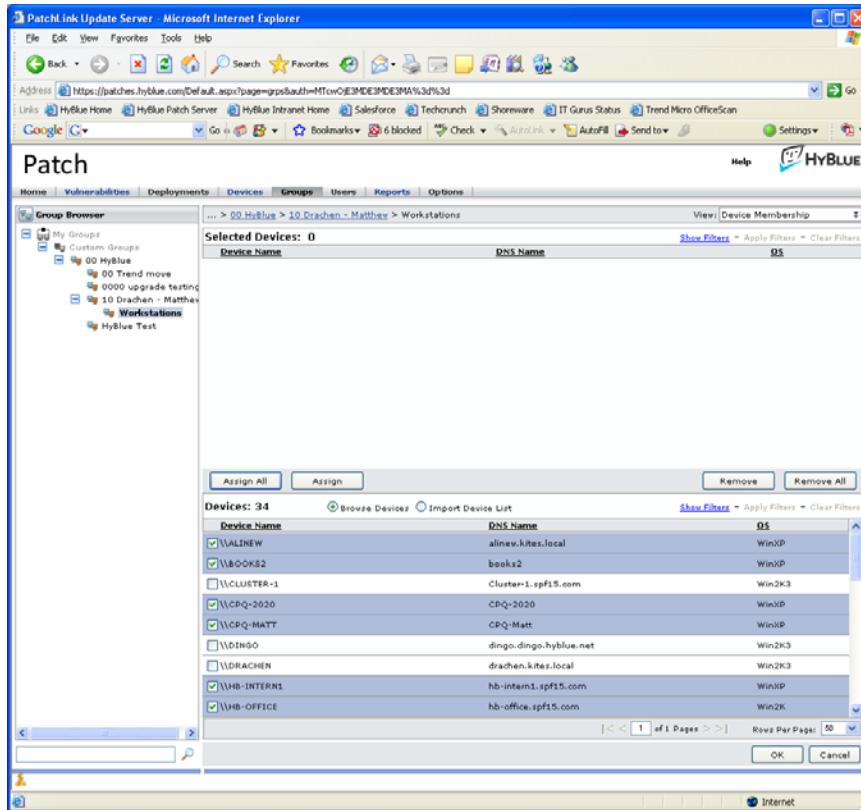
HyBlue Inc. 5 West Harrison. Seattle, WA 98119
206 838 1907, Sales@HyBlue.com www.HyBlue.com



Now click on the Manage button at the bottom of the screen and you will see all computers you manage. You select computers you want to put in the group:

HyBlue Inc. 5 West Harrison. Seattle, WA 98119
206 838 1907, Sales@HyBlue.com www.HyBlue.com

© 2007 HyBlue, Inc. All Rights Reserved. HyBlue and the HyBlue logo are registered trademarks of HyBlue, Inc. All other trademarks and registered trademarks are the property of their respective owners.

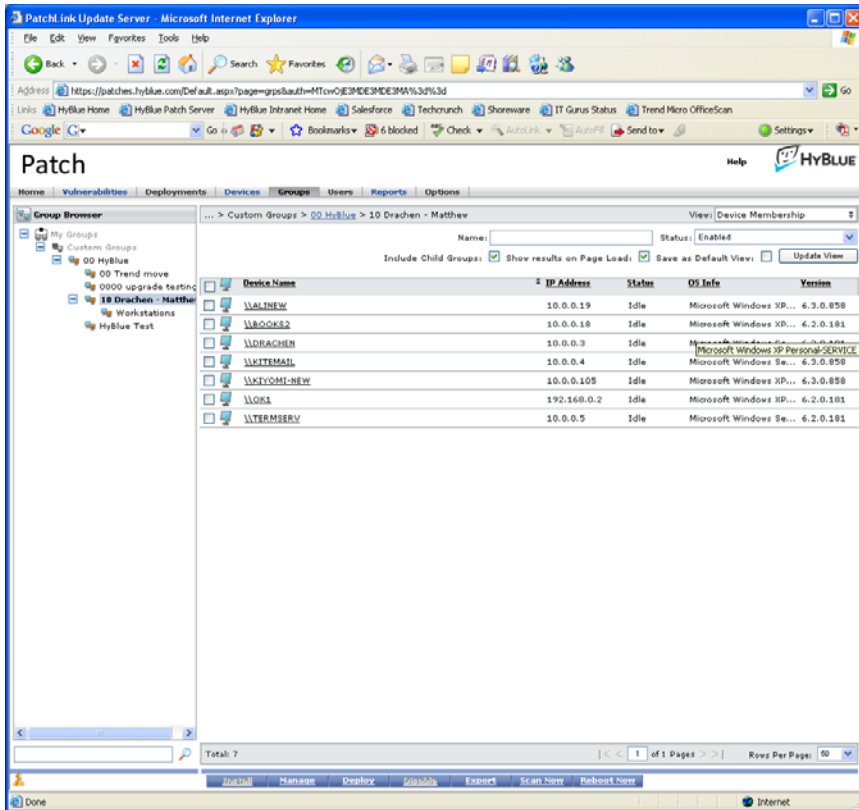


Then click OK. These computers are now a member of the workstations group. You can easily apply patches only to them or to any other group in your control.

Device Membership

The Device Membership screen shows all of the computers that are listed in a particular group. Clicking on a computer name will show you details about that device. We changed from Group Membership to Device Membership in the graphic above.

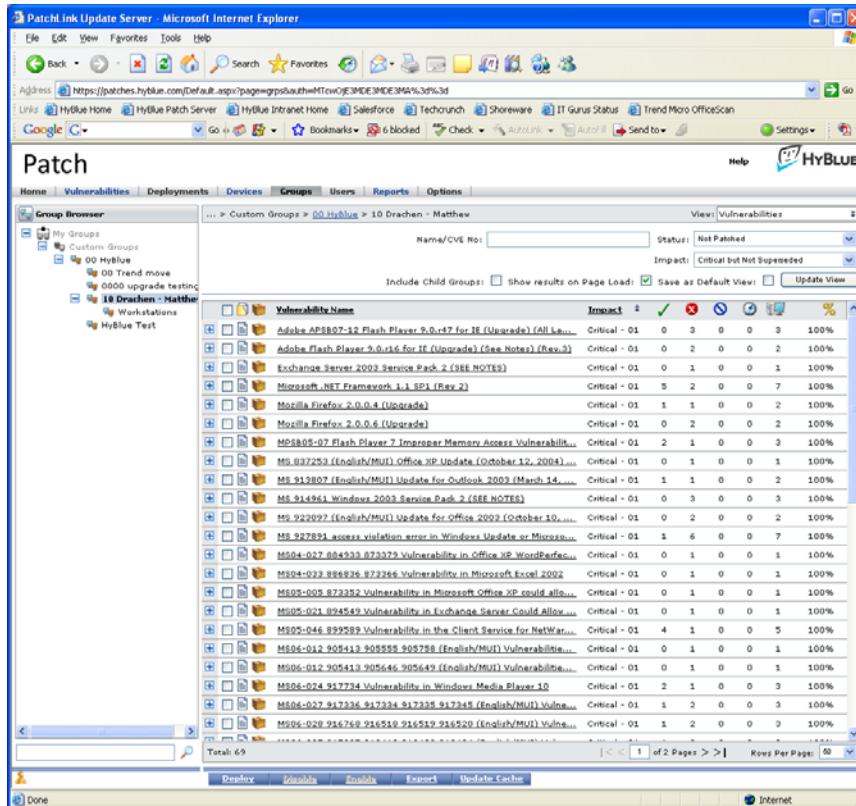
HyBlue Inc. 5 West Harrison. Seattle, WA 98119
206 838 1907, Sales@HyBlue.com www.HyBlue.com



Vulnerabilities

The Vulnerabilities screen shows you a global listing of all patches that are required by the computers in the group. From this screen you can quickly deploy a patch or patches to all the computers in the group.

HyBlue Inc. 5 West Harrison. Seattle, WA 98119
206 838 1907, Sales@HyBlue.com www.HyBlue.com



In the example above, the group 10 Drachen Matthew shows a number of patches that are required. From this screen, simply selecting the Vulnerabilities and clicking Deploy at the bottom of the screen will initiate a wizard that will walk you through deployment of patches to each computer in the group.

In the detail section of this screen you will see the vulnerabilities listed by name. Clicking on the vulnerability name will show you which computers requiring the patch have not yet received it.

To the right are columns detailing the patch status of your computers for that vulnerability. This information includes how many computers have the patch or still need the patch, the number that are in an error mode or are still checking to see what is needed, and the total number of devices. Hovering your mouse over the column symbol will show a description of the data in that column.

To deploy a patch, simply check the box next to one or more vulnerabilities and click the Deploy button at the bottom of the screen. Patch will only

HyBlue Inc. 5 West Harrison. Seattle, WA 98119
206 838 1907, Sales@HyBlue.com www.HyBlue.com



apply the patch to computers that need it. For more information on deploying patches, see the **Deployment** section below.

Filters There are a variety of filters that can be applied to the information on the Vulnerabilities page, using the dropdown menus at the top of the screen. The default **Status** is set to "Not Patched", which is often the information you are seeking as you prepare for a deployment. The default Status is "All", but selecting Patch Vulnerabilities will provide the best view as to what patches are required.

To save a particular combination of filter settings as your default, select the dropdown items desired, then check the box for "Save as Default View" before clicking the Update View button.

Impact Labels Vulnerabilities are labeled with an Impact rating. These are summarized below.

- **Patch Vulnerabilities** This shows all vulnerabilities regardless of the status described below.
- **Other Vulnerabilities** is blank in our implementation
- **Non-Vulnerabilities** shows software that can be distributed by Patch including Acrobat, Flash and other free packages.
- **Critical but Not Superseded** Marked as critical by the manufacturer and not superseded by any newer updates
- **Critical Patches (New)** Marked as critical by the manufacturer and released less than 30 days ago.
- **Critical Patches older than 30 days** Marked as critical by the manufacturer and released more than 30 days ago.
- **Critical but Superseded** Marked as critical by the manufacturer but have been superseded by newer patches.
- **International Patches** are patches created for non English versions of software
- **Recommended** Service packs Recommended by Microsoft are not listed as critical. For this reason, it is important to page through the list of Vulnerabilities to find the service packs.
- **Software Installers** This Impact is shown only if you are filtering on All. This is software that can be installed directly from Patch. This software includes Acrobat, Firefox, Java JRE, Quicktime, .NET Framework, and other Microsoft updates. Note that the software may only download, not install. This information will be noted by the software itself.
- **Tasks** are specific tasks that can be performed and include USB storage blocker and IE7 blocker

HyBlue Inc. 5 West Harrison. Seattle, WA 98119
206 838 1907, Sales@HyBlue.com www.HyBlue.com



Inventory

The Inventory screens in Patch break inventory down into groups of Operating Systems, Hardware, Software and Devices.

Dashboard

The Dashboard is a new view that gives you a graphical representation of patches required and status of the agents.

Deployment

This section describes how to implement patches on the computers. In **Patch**, this is referred to as a Deployment. Deployments can occur on a single computer or on multiple computers, even if they have differing operating systems. HyBlue will never implement a patch that is incompatible with the computer's operating system, so deploying a patch to a broad computer group is a safe operation.

The deployment process is very easy and is available from several locations within the Patch Management System. From the Devices, Groups, or Vulnerabilities screens you can make selections and then click the Deploy button. The software will guide you through the steps, ending in the deployment of the patch or patches. Modifications to selections are available throughout the process.

The following process illustrates deploying patches to all of the computers in a group. Remember, you can select any group to view Vulnerabilities and by selecting "Include Child Groups" you can deploy to all computers in the sub groups as well.

Note that the steps will be exactly the same to deploy a patch to a single computer or to all of the computers you manage; only the starting point will be different.

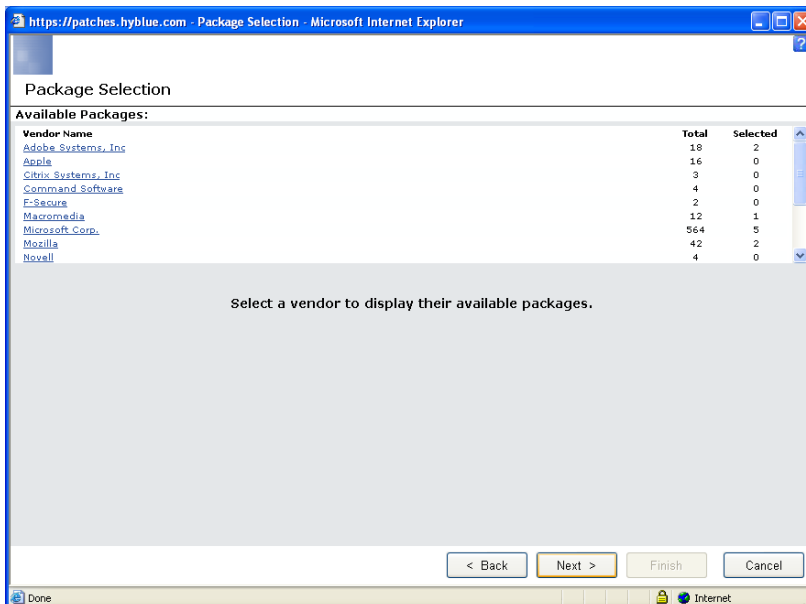
Steps

- Select the Group to patch
- Select the Vulnerabilities view by right clicking on the group name
- Select which patches to deploy by checking the boxes next to the Vulnerability names. Make sure the filters are set to display the Vulnerabilities you want to see.
- Click the Deploy button at the bottom of the screen

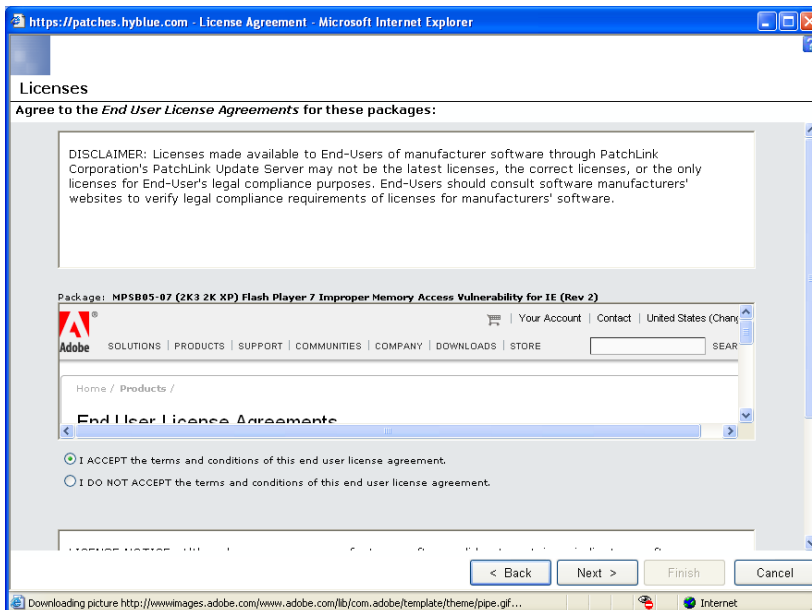
HyBlue Inc. 5 West Harrison. Seattle, WA 98119
206 838 1907, Sales@HyBlue.com www.HyBlue.com



- Review the selection of computers or groups to patch



- Review the packages selected and the manufacturers providing the patches



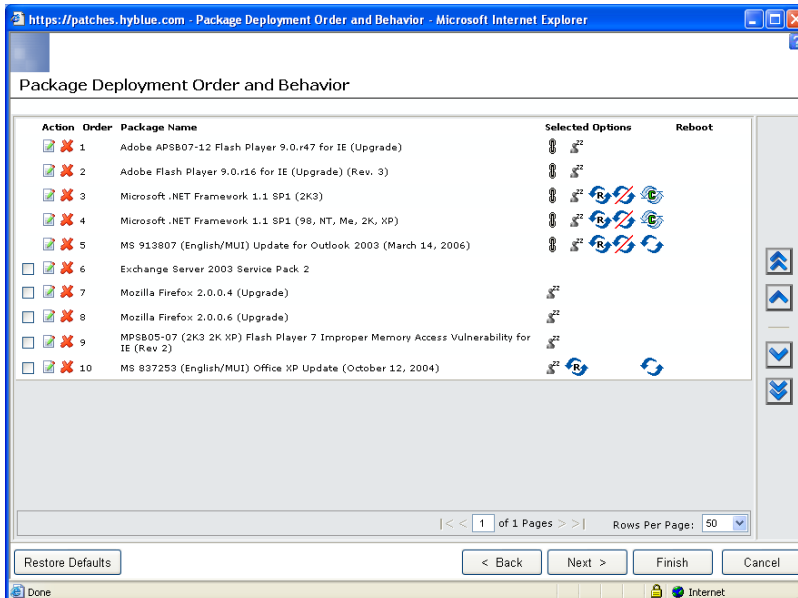
- Accept the End User License Agreement (EULA). If you are deploying patches from multiple vendors, each will require a EULA acceptance. Use the right-hand scroll bar on the window to view all EULAs.

HyBlue Inc. 5 West Harrison. Seattle, WA 98119
206 838 1907, Sales@HyBlue.com www.HyBlue.com

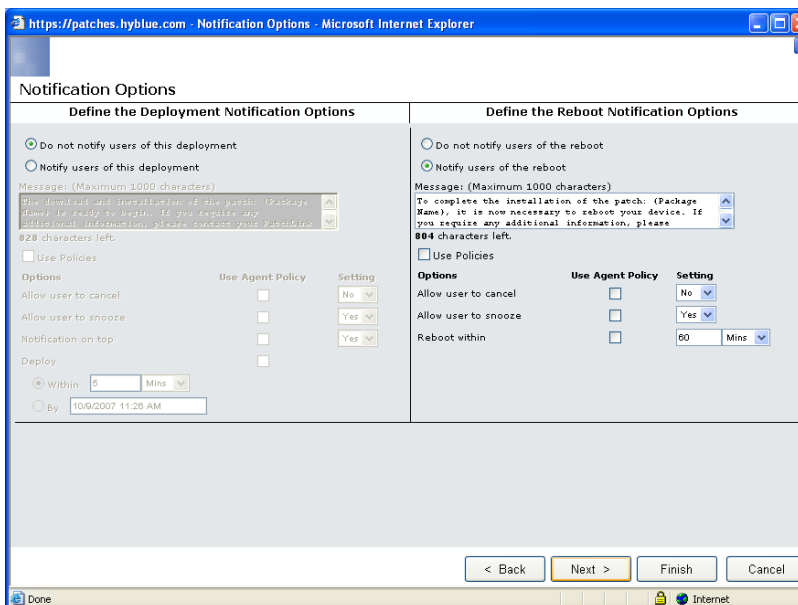


- Select deployment options, which include
 - Deployment name
 - Start time
 - Distribution options
 - Concurrent deployment
 - Number of computers patched at one time
 - Consecutive deployment
 - Error handling
 - Allow overwrite of existing patch
 - Notes

HyBlue Inc. 5 West Harrison. Seattle, WA 98119
206 838 1907, Sales@HyBlue.com www.HyBlue.com



- Select package deployment order and behavior
 - Manipulate the order and options for consecutive installation of patches, if desired.
 - Change reboot options, if desired. Patch automatically suppresses individual reboots whenever possible.
 - In most cases you will not need to change anything on this page.

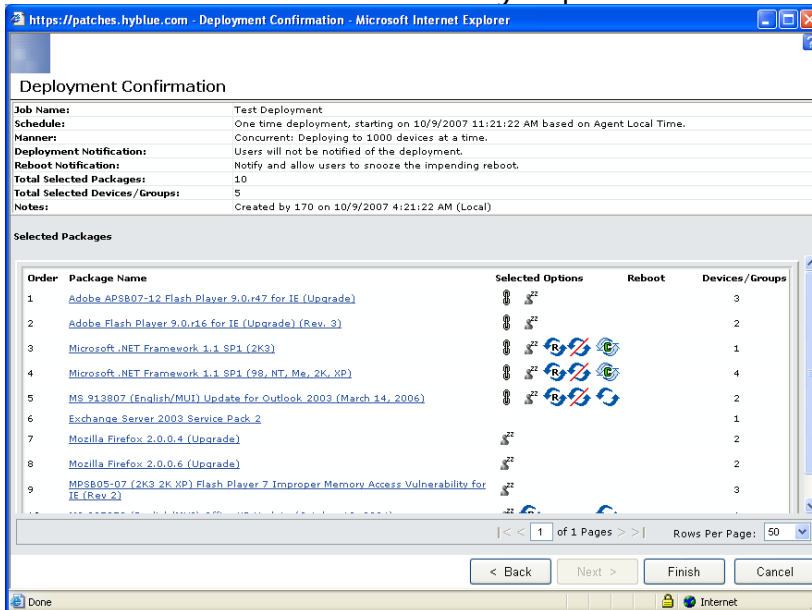


- Select notification options
 - Control whether users are notified of the update as well as how the reboot is accomplished, if a reboot was required.

HyBlue Inc. 5 West Harrison. Seattle, WA 98119
206 838 1907, Sales@HyBlue.com www.HyBlue.com



- If notification is selected, users may be given the options to cancel or put the patch on snooze, and to set a deadline for the installation.
- If a reboot is required and notification is selected, users may be given the options to cancel or put the reboot on snooze, and to set a window for the reboot.
- Policies are not currently implemented.



- Review deployment summary
 - This screen gives you a summary of the deployment description and options. Click the Finish button to launch the deployment.

Once the deployment has started, you can monitor it at the group level or the device level by clicking on the desired item and then clicking on the Deployments tab. After the deployment has run, you may also look at reports detailing which deployments succeeded and which failed. This is done by clicking on the Reports top-level menu item, then selecting the desired report.

In some cases, patches may not be on HyBlue's local server and will need to be downloaded from the main patch server. This may add a few minutes to your deployment time. The system handles this automatically.

Support

If you have further questions on the use of Patch, please contact HyBlue Support at 206.838.7238 or email support@hyblue.com.

HyBlue Inc. 5 West Harrison. Seattle, WA 98119
206 838 1907, Sales@HyBlue.com www.HyBlue.com