Meeting the challenges of automated patch management: Using HFNETCHKPRO Version 4 to Maintain Your Windows Systems

John Walther

GSEC practical assignment version 1.4b, option 1
July 19, 2004

Table of Contents

Documentation Conventions

The following conventions are used throughout this paper. They are based in part on information from the following style guides:

- *Microsoft Manual of Style for Technical Publications (MSTP)*
- *The Chicago Manual of Style*
- *The Associated Press Stylebook and Briefing on Media Law*

- I use the word “click” vs. “select” or “choose” to describe the action of choosing a button, command or a drop-down list menu.
- I use the word “select” to describe the action of highlighting an item.
- I use the word “type” vs. “enter” to describe the action of typing text into a dialog box.
- User input is displayed in lower case.
- I use the word “page” to denote Web pages.
- I use the word “screen” to denote non-Web pages.
- Acronyms are all in uppercase.
- Commands on menus and buttons are in **bold**, with capitalization following what the interfaces displays.
- Options in dialog boxes are in **bold**, with capitalization following what the interface displays.
- Dialog box tiles are in **bold**, using TITLE CAPS.
- UNC naming paths have initial Caps.
- Document names are in *italics* and TITLE CAPS.
- Field names are in **bold**, with capitalization following what the interface displays.
- Field values are in *italics*, with capitalization following what the interface displays.
- File names are in TITLE CAPS.
- File paths are in TITLE CAPS.
- Folder names are in TITLE CAPS.
- Menu names are in TITLE CAPS.
- Program and application names appear in TITLE CAPS.
- URL’s are all in lower case and act as a valid hyperlink to the Web site listed.
- Window names are in TITLE CAPS; unless they are unnamed then they are in lower case.

Abstract

According to the CERT® Coordination Center (CERT®/CC), 95 percent of all network intrusions could be avoided by keeping systems up-to-date.[1] With a statistic like this one, we have to wonder why companies are still failing to do this most critical and complex task.

When it comes to patch management companies are encountering the following challenges:

- Complexity of networking environments. Network professionals are responsible for a wide variety of hardware, operating systems and applications. Even in small environments it can be a challenge to keep up.
- Lack of time. With the typical mandate to "keep everything up and running all the time" day-to-day operations take precedence, and patch management falls by the wayside.
- The number and frequency of patches that are released for hardware, operating systems, and applications. A recent study by CERT®/CC determined that patches are being released on average about every 5.5 days.[2]
- Time to research and determine what vulnerabilities exist, what patches (if any) are available, and if they need to be applied in their network environment. According to a research paper from Intel, "researching each of the 4,200 vulnerabilities published by CERT last year for 10 minutes would have required 17.5 weeks, or 700 hours of a researcher's time.[3]
- Balancing the needs of patch management with the demands of system availability.

Creating a patch management methodology is the first step in resolving these challenges. Evidence suggests that companies understand the importance of staying current with patches and service packs, yet they lack an overall methodology for ensuring the task is done.

A successful patch management methodology includes the following components:

- A detailed inventory of all hardware, operating systems and applications that exist in the network. And the creation of the process to keep the inventory up-to-date.

[1] Schweitzer, Douglas. "Emerging Technology: Patch Me if You Can." *Network Magazine*. 8/5/03

[2] Integrated Information Systems. "Patching Statistics."

[3] Integrated Information Systems. "Patching Statistics."

- A process to identify vulnerabilities in hardware, operating systems and applications.
- Risk assessment and buy-in from management and business owners.
- A detailed procedure for testing patches prior to deployment.
- A detailed process for deploying patches and service packs, as well as a process for verification of deployment.

The second step toward resolving the challenges of patch management is to automate the methodology. There are numerous commercial and open source tools available to help companies automate their patch management methodology. We will be examining HFNETCHKPRO, a commercial product from Shavlik Technologies, to see how it meets the minimum requirements for a patch management tool, and how it can be used to automate the patch management process.

1. Introduction

When it comes to the technology related vulnerabilities of hardware, operating systems and applications, and the exploits of those vulnerabilities, the numbers are not on our side. All you have to do is look at the statistics, read any hacking related Web site, pick up the local paper, or the worst case scenario - be a statistic yourself.

As the number of technology related security incidents grows, it's only a matter of time before you, or your company will be affected. According to the CERT® Coordination Center (CERT®/CC) at Carnegie Mellon, the number of these incidents jumped from 52,658 in 2001 to 82,094 in 2002.[4] That's an increase of 29,436 known vulnerabilities in just one year. So it pays to start being proactive, not only in researching vulnerabilities, but having a plan in place to address them.

Not only is the number of vulnerabilities on the rise, the sophistication and effectiveness of attacks based on vulnerabilities has also increased. In recent testimony by Robert F. Dacey, Director of Information Security Issues for the US General Accounting Office, he states "The sophistication and effectiveness of cyber attacks have steadily advanced. Because automated tools now exist, CERT/CC has noted, attacks that once took weeks or months to propagate over the Internet now take just hours, or even minutes."[5]

Add to the growing number of known vulnerabilities and the variety of threats posed by them as well as the potential costs of having to clean up after a security incident, and you will begin to see the importance of a patch management strategy. As an example, within the first five days of the spread of the SQL Slammer worm, the estimated costs of lost productivity to companies affected was over $1 billion.[6]   Keep in mind that this estimate was only for the first <u>five</u> days.

Director Dacey's testimony to the *Subcommittee on Technology Information Policy, Intergovernmental Relations, and the Census, House Committee on Government Reform* was based in part on information provided by the CERT® Coordination Center. The CERT® Coordination Center (CERT®/CC) is primarily a

[4] NetSupport Solutions Inc. "Beating Hackers to the Patch." Windows Security.com. 10/6/03.

[5] United States General Accounting Office. "INFORMATION SECURITY: Effective Patch Management is Critical to Mitigating Software Vulnerabilities. 9/10/03.

[6] Schweitzer, Douglas. "Emerging Technology: Patch Me if You Can." *Network Magazine*. 8/5/03

federally funded research and development center. Operating out of Carnegie Mellon University's Software Engineering Institute, they serve as a reporting center for Internet related security problems. According to their Web site they do the following:

> "Staff members provide technical advice and coordinate responses to security compromises, identify trends in intruder activity, work with other security experts to identify solutions to security problems, and disseminate information to the broad community. The CERT/CC also analyzes product vulnerabilities, publishes technical documents, and presents training courses."[7]

In one publication, their 2003 Annual Report, CERT®/CC noted "From January through December 2003, the CERT/CC received 542,754 email messages and more than 934 hotline calls reporting computer security incidents or requesting information. We received 3,784 vulnerability reports and handled 137,529 computer security incidents during this period."[8] Statistics like these give you an idea of what we are up against, as well as a glimpse into what CERT®/CC uses to generate their statistics, recommendations and training materials.

CERT®/CC has been tracking vulnerabilities since 1995. According to their statistics, the total number of vulnerabilities they have tracked between 1995 and 2003 is 12,946. Take a good look at the chart below and notice the progression of numbers from year-to-year, especially in the years 2000-2003.

Vulnerabilities reported[9]

1995-1999

Year	1995	1996	1997	1998	1999
Vulnerabilities	171	345	311	262	417

2000-2003

Year	2000	2001	2002	2003
Vulnerabilities	1,090	2,437	4,129	3,784

Total vulnerabilities reported (1995-2003): **12,946**

The numbers are pretty astounding. But not as astounding as knowing that CERT®/CC determined that roughly 95 percent of the vulnerabilities could have been avoided if the appropriate patches had been applied.[10] Imagine that, 95

[7] CERT® Coordination Center (CERT®/CC) "The CERT Coordination Center FAQ." 2/26/04.

[8] CERT® Coordination Center (CERT®/CC) "CERT Coordination Center 2003 Annual Report." 4/5/04.

[9] CERT® Coordination Center (CERT®/CC) "CERT/CC Statistics 1988-2003." 1/22/04.

[10] Schweitzer, Douglas. "Emerging Technology: Patch Me if You Can." *Network Magazine*. 8/05/03

percent of the known vulnerabilities out there can be resolved, or avoided altogether, simply by applying patches!

CERT®/CC is not the only organization that has determined this. According to the FBI, in another sobering statistic, “More than 90% of all security breaches involve a software vulnerability caused by a missing patch that the IT department already knows about.”[11]

If the FBI and CERT®/CC agree that information about vulnerabilities and the patches that fix them are readily available and known, why do we still have companies being so severely impacted? Is it that companies don’t see the need to patch? Or is it something else?

In my personal experience, and anecdotally in information I’ve read, it would appear that companies do understand the need to stay current with service packs and patches. So, they do “get it.” But “getting it” is not translating into accomplishing it. Where is the breakdown occurring between understanding and accomplishing?

Challenges of patch management

One of the biggest barriers to patch management is the increasing complexity of networked environments. Take a moment and look at your own network. Chances are, even if it is relatively small, you will be dealing with a variety of hardware, operating systems and applications. If you are in an enterprise environment, the sheer amount of these can be truly daunting. Add to the complexity of the environment the typical mandate to “keep it all running, all the time” and you will understand why patching never takes place, or takes a back seat to day-to-day operations.

If you are already doing proactive patch management, it is more than likely chewing up a significant portion of your time. Gartner Group estimates that “IT Managers spend an average of 2 hours per day managing patches.”[12] I found this to be true in my job. My company has 45 Windows 2000 servers and I was spending roughly two hours per day using a manual process to keep them updated. And that was just for Critical updates – not updates to Exchange, Office or SQL. If you add those in, I was spending quite a bit more time on the process.

Gartner’s estimates show the impact patch management is having on people’s time; but what about the monetary costs to an organization? A recent survey by the Aberdeen estimates the annual cost of patch management to be $2 billion and above for U.S. businesses.[13] Digex, a Web and Applications hosting

[11] Backman, Alex. “Five Tips for Effective Patch Management.” *Computerworld*. 7/14/03.
[12] Integrated Information Systems. “Patching Statistics.”
[13] Violino, Bob. “Patching Things Up.” *CIO* 8/1/03

company, estimates the cost of manually managing the patch process at $14,000 a year.[14]

The next barrier to effective patch management is both the number and frequency of patches that are released for hardware, operating systems and applications.

According to a study by CERT®/CC, patches are being released on average about every 5.5 days.[15] In 2003 alone, Microsoft released 51 security advisories. That represents an average of nearly one new security patch per week.[16] And that is just for Microsoft products! Obviously, most typical networks are not completely Microsoft based - though they might wish it was so. As someone responsible for a network, the reality is that you might be dealing with upwards of 51 security advisories from Microsoft, along with numerous potential advisories from your firewall manufacturer, flavors of the *NIX operating system on your network, Cisco products, and so on. That's a lot of patches and fixes for the typical network administrator to deal with.

As a network professional you are literally bombarded with information about patches and service packs that are available. Not that all of them should be, or need be applied. It takes time to wade through this information to see what is important. This is the next barrier to patch management. According to a research paper from Intel, "Researching each of the 4,200 vulnerabilities published by CERT last year for 10 minutes would have required 17.5 weeks, or 700 hours of a researcher's time."[17] That's a lot of time and expense spent. And even if you take the time to do the research, there is no guarantee that you will find the information you need to make an informed decision. According to Netsupport Solutions, frequently the information on Microsoft's security site is cryptic, leaving you asking how severe or imminent the threat is.[18] Bottom line – if you don't feel comfortable with the information you have about a patch or service pack, chances are you will decide not to apply it.

Yet another reason companies fail to apply patches is the need to balance availability of systems with the necessary downtime required to install patches. Typically, the goals of uptime are at odds with patch management, and often security as a whole. As someone who is responsible for a network, you may find yourself battling for the time you need to apply patches and fixes.

Perhaps the biggest barrier to effective patch management is that many companies do not have a methodology in place. In other words they "get it"; they

[14] Violino, Bob. "Patching Things Up." *CIO* 8/1/03
[15] Integrated Information Systems. "Patching Statistics."
[16] SecurityStats.com. Most Requested Statistics.
[17] Integrated Information Systems. "Patching Statistics."
[18] NetSupport Solutions Inc. "Beating Hackers to the Patch." Windows Security.com. 10/6/03.

just don’t get to it!   There is no process behind what needs to be done so patch management, if it occurs, is occurring in a haphazard way.

For example, in a large company, it is very possible to have more than one person responsible for patch management. Without an overriding process to determine what each person is doing, or a process to validate that entire organization is up-to-date, it is very possible to wind up with pockets of vulnerable systems that could impact the network as a whole. If it is true that “Computer networks without a comprehensive patch management program are on average 5% to 7% patched”,[19] then this is a problem that needs to be addressed.

If you do not have a process in place, chances are you are winging it, not evaluating or testing patches, have no roll back plan and if you were under the gun, would not be ready to apply critical patches.

Risks and costs

Many companies are under the erroneous impression that just having a firewall protects them from vulnerabilities. From personal experience let me say this is simply not true. When the SQL Slammer worm was wreaking havoc on networks across the world, my company made the decision to mitigate the problem by temporarily relying on our firewall to block the ports that were used to infect servers. Our rationale - a valid one - was that we wanted to test the Microsoft-provided fix prior to installing it. This solution would have worked, except that a contractor brought in a personal laptop, plugged it into our network (something which is expressly forbidden in our signed security policies) and infected us with the worm. It took us hours to determine what was impacting our network performance. We learned the hard way that a firewall is not enough.

So, if you are relying on a firewall as your only source of protection – think again. Eric Schultze**,** chief security architect at Shavlik Technologies agrees. “Firewalls, anti-virus products and IDS’s are excellent solutions for their intended uses. But when combined with patch management, they become a multiple-layered, defense-in-depth strategy, critical to keeping a network secure.”[20] He goes on to say that “IT admins need to view patch management like firewall and anti-virus software-proactive tools to help protect the network from attack.”[21]

[19] Integrated Information Systems. “Patching Statistics.”
[20] Schultze, Eric. “Is Patch Management the best Protection Against Vulnerabilities? Yes.” *NetworkWorldFusion*. 3/29/04.
[21] Cruit, Nadine. “Shavlik Technologies: Patching Up the Security Holes.” *ComputerUser* Local Profiles Minneapolis /.St.Paul. 4/04.

According to statistics gathered from SANS and CERT$^{®}$/CC, companies are taking huge risks by not patching systems. According to them, the average cost of having a security vulnerability exploited, in 2002, was:

> Direct costs - $69,000
> Indirect costs - over $2 million due to lost revenue from intellectual property.[22]

That is a lot of money that could be used elsewhere in an organization, especially in these times of tight budgets. In addition, the money is not being spent proactively. Rather than spending these considerable sums cleaning up after an incident, companies could spend significantly less by devising a patch management strategy and purchasing commercial products to deploy patches and service packs. Ask yourself, which makes more sense?

From a compliance perspective a company puts itself at legal risk by not applying patches. According to Integrated Information, Inc.'s Web site, patch management is a component of several laws including[23]:

- *Sarbanes-Oxley 404* - The Institute of Internal Auditors (IIA) suggests the following as part of being compliant with SOX:
  - Implement processes to ensure security vulnerabilities are quickly identified and corrected
  - Deploy automated software tools to scan the network for workstation vulnerabilities and adherence to standards.
  - Upgrade PC operating systems and other software to stay current with security patches and to ensure continuous vendor support for all software in use.

- *HIPAA* - The Health Insurance Portability and Accountability Act imposes requirements upon Healthcare organizations to guard data integrity, confidentiality, and availability. The 3 categories for HIPAA Security Rule Compliance include Physical Safeguards, Administrative Safeguards, and Technical Safeguards - which include a series of security measures that specify the use of technology to secure protected health information - especially the access to such data.

- *Gramm-Leach-Bliley Act* - Under the Safeguards Rule, enforced by the Federal Trade Commission, the act mandates strict compliance to requirements for financial institutions to have a security plan to protect the confidentiality and integrity of personal consumer information.

[22] Integrated Information Systems. "Patching Statistics."
[23] Integrated Information Systems. "Government Regulations."

- *FDIC* - "A patch management program should be part of an institution's overall computer security program... ...An inadequate patch management program may adversely affect certain components of an institution's overall Information Technology (IT) examination rating*.*

Beyond having to meet the requirements of compliance, you may also find your company has to meet the requirements of business partners. It is possible that business partners may refuse to do business with you if you are not performing patch management. They may see you as potential risk to their business. The reverse is also true. It is an excellent idea to ensure that your trusted business partners meet your own internal mandates for patch management. Be sure to get this in writing and verify that they are actually performing it.

What is patch management?

At its most basic, patch management is a process. The process includes the following steps.

- Reviewing available information about known vulnerabilities and associated patches. This information can be gleaned from vendor security sites, security related Web sites, and mailing lists. Decide which works best for you. I would recommend that you choose a few – you may get duplicate information but you will not miss anything. As part of this review process you should decided how you will keep up-to-date on newly discovered vulnerabilities and patches.

- Identifying hardware, operating systems and applications that are potentially impacted by a vulnerability. Typically this is accomplished by using scanning tools.

- Assessing the risk of the security flaw to your organization. Please keep in mind that not all patches apply to every organization. Perhaps the vulnerability would not impact your company because you do not use a configuration that is at risk. Also, be sure to asses the risk of applying the patch. Remember that it is possible that applying a patch could be detrimental to your organization

- Testing and remediation. It is never a good idea to deploy patches to production systems prior to completely testing them. It is a best practice to create a lab setting with equipment that is identical or similar (be sure to document the differences) to your production hardware, operating systems and applications. You will want to create a testing plan that can be followed for each new patch to be deployed.

- o Deploying. After completing the previous steps you will then choose the method and process that you will use to deploy the patches. Questions to answer here are: 1.) will this be a manual or automated process? 2.) Will you use a single product or multiple products?

- o Verifying. You need to have the ability to verify that the patch was installed and that the patch actually fixed the vulnerability. Most patch management programs will have the capability to perform this. Scanning tools can also be used for verification.

Components of a successful patch management methodology

Previously I listed the challenges that companies face with patch management. According to Douglas Schweitzer, "The key to meeting these challenges lies in establishing policies that will make it easier for administrators to assess their systems' vulnerabilities, prioritize which systems should be patched and when, and establish methods for testing patches before they're released onto the network."[24]

In other words, come up with a methodology that addresses the entire patch management process.

In a recent TechRepublic article Ronni Colville and Mark Nicolett, state that "Patch management is an area in which manual approaches have no chance of being effective."[25] Mr. Schweitzer also agrees, stating "Organizations using manual processes to stay on top of security alerts and patches often fall behind quickly, leaving them vulnerable to attacks such as the Code Red and Slammer worms. A better approach may be to automate the distribution of security patches for workstations and servers, thereby simplifying and shortening the patch management process."[26]

So, if they are correct, what makes up a good patch management methodology?

First and foremost, the methodology itself should be a process that can easily be automated. Patch management lends itself to this because it is a repetitive process. "Effective patch management is more than just plugging holes and hoping for the best. It's an ongoing, systematic process that can benefit from automation"[27] according to Brad Carpenter, author of "Patch Management: Find the Weakest Link."

[24] Schweitzer, Douglas. "Emerging Technology: Patch Me if You Can." *Network Magazine*. 8/05/03

[25] Colville, Ronni Nicolett,Mark. "Patch Management: Surveying the Vendor Landscape." TechRepublic. Tech Perspective. 5/14/03.

[26] Schweitzer, Douglas. "Emerging Technology: Patch Me if You Can." *Network Magazine*. 8/05/03

[27] Carpenter, Brad. "Patch Management: Find the Weakest Link." ZDNet. News Commentary. 2/4/04.

The first step in any good patch management strategy is a full and detailed inventory of all hardware, operating systems and applications that exist in your network. This just makes sense. After all, if you don't know what's on your network how are you going to know what to patch? Some examples of items to include in an inventory would be operating systems and versions, applications and versions, patch status, hardware, who owns the hardware and their contact information. Again, this should be very detailed information. The inventory process is a huge undertaking, even if you are using software to help you compile the information. Invest the time and by all means, keep it updated. It should be a living-breathing document.

With an accurate inventory, you can begin the process of identifying vulnerabilities and patches. The first time you perform this step you will go through the process of examining and acquiring the tools you will use. There are multiple programs and tools that are available. Examples include open source tools like NESSUS, SYSTEM ANALYST INTEGRATED NETWORK TOOL (SAINT), and SECURITY ADMINISTRATOR'S RESEARCH ASSISTANT (SARA). There are also numerous commercial tools available. HFNETCHKPRO is my personal favorite. We will be covering its installation and usage in the following pages. NETRECON, HACKERSHIELD, INTERNET SCANNER, RETINA and STAT are other commercial products that are available. Another available option, if you are using Microsoft products, is the Web-based WINDOWS UPDATE and OFFICE UPDATE sites. From a defense-in-depth perspective, I would recommend using more than one of these tools. You will get more comprehensive results.

During this step you will also need to decide how to stay informed of new vulnerabilities. This is a vital task. There are numerous avenues available including security bulletins from hardware and software vendors, security related Web sites, and various mailing lists. Because this is such a vital task I recommend that you use as many of these information avenues as possible. Never rely on information from just one source – pick a few

After you have identified vulnerabilities, the next step in your methodology is critical - obtain management buy-in. This includes business owners. Business owners include not only owners of the hardware, operating systems and applications, but also those who own any data that resides on these systems. It is very critical to ensure that you have buy-in from the correct people.

You may be asking why this is not the first step in the methodology. Well, if you have not performed an inventory and identified potential vulnerabilities, what information can you bring to the business owners to base their decisions on? How will they perform an accurate risk assessment without detailed information? In discussions with the business owners be sure to discuss the level of acceptable risk, both for applying or not applying patches. From these meetings you will come away with an idea of how your company wants to deal with any potential risks identified.

With sign-off from management and business owners in hand, your next step is to test the patches. As stated before, it is a “best practice” to create a lab setting with equipment that is either identical, or similar (be sure to document the differences) to your production hardware, operating systems and applications. While in theory this is great, it only works if you have the budget. Lacking the necessary budget you could also use a product like VMWare and run virtual machines directly on your production machines. Since the virtual machines would be the “same” as your production equipment, this would give you a valid platform for testing how patches and service packs would work on your production systems. Keep in mind that the reason you want to test each and every patch is that it is not possible for the vendor to test their patches for every possible configuration of hardware and software out there; it is up to you to do this.

The next step is to devise the approach you will take during deployments. Begin by identifying priorities for patching hardware, operating systems and applications. For example, you’d probably want to patch any Internet-connected Web servers before patching Web servers behind your firewalls. Take some time to logically group your machines so that you are not patching your entire network in one evening. And, you will want to devise a plan for how to respond to new vulnerabilities as they are discovered. If you plan on having more than one person responsible for patch management, document the expectations and process for each person. Also, create a plan for recovering from deployments which damage something in your network. It is very important that you take the time to create an action plan you can follow in an emergency. And don’t forget to test how the patch application itself works. You want to know its quirks and limitations prior to an emergency.

After you have mapped out your deployment strategy, you are ready for the final step - deployment and verification. Use the strategy you designed to deploy patches and service packs. After the deployment process, be sure to verify patches have been applied and that vulnerabilities have been fixed.

The ultimate goal of any patch management methodology should be automation. While you are devising your methodology keep asking yourself, “How can this be automated?” Your aim is to create a process that can be repeated easily and consistently. Commercial products, like HFNetCheckPro, allow you to automate the patch management process.

According to Integrated Information Systems, “By replacing manual tasks with automated, system-driven functions, the costs associated with endless hours of security patch implementations are reduced, and there is a much less significant margin for human error, offering IT professionals better peace of mind."[28] Douglas Schweitzer agrees, "When it comes to automating the patch management process, there's no magic bullet. Nevertheless, the right product, coupled with a corporate-wide security plan and sensible policies, can help you develop a successful, comprehensive patch management strategy."[29]

Finally, Eric Schultze, chief security architect at Shavlik Technologies, also agrees, saying "Ensuring network security through patch management is no simple task. It requires diligence to stay informed of available patches, test the patches on non-production systems, deploy the patches to all affected systems and validate that they were installed properly. Automated patch management systems can ease the chores associated with keeping your systems up to date and provide peace of mind that you're safe from associated vulnerabilities."[30]

Minimum requirements for a patch management application:

Now that you have a grasp of the patch management process, you are probably wondering what types of products fit into it. Keep in mind that there are myriad of products available; some use agents, others do not, some are free, others are prohibitively expensive. When researching patch management products look for a program that has these minimum features:

- Keeps itself up-to-date with information about recently discovered vulnerabilities and patches
- Has the ability to scan and identify vulnerabilities on servers and workstations
- Has the ability to schedule and deploy patches to workstations and servers - preferably from a centralized console
- Is flexible and easy to work with and enables you to combine machine attributes and patches attributes for deployments
- Allows you to schedule and automate the process of deployments
- Has strong reporting features including the ability track changes between past and current machine configurations
- Has verification features

So, where do you look for such a product? Well, there are undoubtedly open source tools available, but if you are serious about patch management you will probably want to invest in a commercial product and support. Not surprisingly,

[28] Integrated Information Systems. "Patch Management

[29] Schweitzer, Douglas. "Emerging Technology: Patch Me if You Can." *Network Magazine*. 8/5/03

[30] Schultze, Eric. "Is Patch Management the Best Protection Against Vulnerabilities? Yes." NetworkWorldFusion. 3/29/04.

this matches the view of one company that sells a patching solution. In the opinion of Alex Bakman of Ecora Software Corp, "…the majority of customers will tell you they need a commercial product if you want to get the job done. For companies that want to install something, scan their environment, get the latest and greatest patches and automatically deploy those with the click of a button, they need a commercial product."[31]

One solution to the problem – Shavlik's HFNetChkPro

Let's take a closer look at one application that fits into a patch management methodology, and meets the minimum requirements for a solid patch management application - HFNETCHKPRO from Shavlik Technologies.

HFNETCHKPRO is a Microsoft-only patch management solution. Though at the time of this writing, they are moving toward the ability to scan and patch other operating systems. The program is a more robust version of the technology that is used in the MICROSOFT BASELINE SECURITY ANALYZER, which Shavlik developed for Microsoft.

Shavlik Technologies was founded in 1993 and their goal, according to their Web site, is to provide "Powerful, easy to use security products for the entire computer infrastructure of its customers." [32] To that end they have developed several products and services centered on patch management and security.

President and CEO Mark Shavlik has this to say about their product offerings "…we offer tools for proactive patch and security management, which have eliminated much of the cost, time, and effort required to actually protect systems and networks. Ultimately, proactive patch management can limit successful attacks, network and system failures, lost productivity, privacy, and security breaches and liability risk."[33]

So, how does HFNETCHKPRO stack up against the minimum features you should look for in a product? HFNETCHKPRO meets all of the requirements that we previously discussed.

HFNETCHKPRO uses XML technology to keep a current database of all known and newly discovered vulnerabilities. This patch database is continually updated during the operation of the product. Using an Internet connection you have real-time access to patch information from both Shavlik's and Microsoft's servers. The program also has the ability to automatically download patches as they are needed.

[31] Semilof, Margie. "Managing Patches Manually is Futile, Ecora Exec Says." SearchWin2000.com. Question & Answer. 3/10/03.
[32] Shavlik Technologies. About Shavlik. Shavlik.com
[33] Cruit, Nadine. "Shavlik Technologies: Patching Up the Security Holes." *ComputerUser.* Local Profiles Minneapolis/St.Paul. 4/04.

HFNETCHKPRO has the built in ability, using information in the continually updated patch database, to scan and identify vulnerabilities on both workstations and servers for the following software:[34]

- WINDOWS NT 4.0, 2000, XP AND SERVER 2003
- EXCHANGE SERVER
- SQL SERVER
- MICROSOFT OFFICE INCLUDING OUTLOOK AND OFFICE INSTALLATION POINTS
- JAVA VIRTUAL MACHINE
- INTERNET EXPLORER
- INTERNET INFORMATION SERVICES (IIS)
- WINDOWS MEDIA PLAYER
- MICROSOFT DATA ACCESS COMPONENTS (MDAC)
- ISA SERVER
- COMMERCE SERVER
- .NET FRAMEWORK

HFNETCHKPRO uses a centralized console and patch database. However, you do have the flexibility, depending upon licensing, to have multiple consoles tied to one database.

HFNETCHKPRO is highly flexible. Among other things, you can customize views, the patch database, information regarding vulnerabilities, scanning groups, scanning templates and deployment templates. The program supports drag-and-drop functionality, and there is no scripting language to learn. There are no agents to install, which means you will have less planning and ongoing administration to get the product working. I'll cover these in detail in the following pages. For now just know that there are a wide variety of ways to customize the program, and Shavlik has done a great job of making it extremely user-friendly. You can literally be up and running within a few moments of installation.

HFNETCHKPRO leverages the Windows Scheduler service for automation. After you have created a scanning template you can automate it using settings in the Scheduler service. You can also, if you are really gutsy, automate the entire process of deploying patches and service packs at the same time that scans are performed.

Depending on how you license the product you will have access to a powerful and flexible reporting engine. The reporting engine allows you to do complex reporting using basic filters that are in drop-down lists, or if you prefer, by using a scripting language.

Finally, HFNETCHKPRO has several methods of verification available. Verification is provided during the deployment process, and within the PatchPush^{TM}

[34] Shavlik Technologies. Welcome to HFNetCheckPro 4.2. Help File.

technology which reports the ongoing status (before, during and after) of all deployments.

Let's take a more in-depth look at the product.

2. Installation

System Requirements

As with most software products, prior to installation, you need to meet the vendor's hardware and software requirements. The base hardware requirements to run HFNETCHKPRO are:

- Administrative Console (machine you will install the product on)
    - A system with a 500MHz, or faster, processor
    - A minimum of 256MB of RAM - for better performance 512MB or higher is suggested
    - 60MB of free disk space for the application files
    - 2GB, or more, free disk space for downloaded patches and service packs
    - A monitor that supports a video resolution of 1024 x 768 or higher
    - Though not listed as a requirement, you will need a working Internet connection
- Clients (machines you plan to scan and patch)
    - Free disk space, on the root of the system, equal to five times the size of the patches being deployed

The base operating system requirements to run HFNETCHKPRO are:

- Administrative console
    - WINDOWS 2000 SP3 OR HIGHER
    - WINDOWS SERVER 2003
    - WINDOWS XP
- Clients
    - INTERNET EXPLORER 4.0 or later
    - Supported operating system
        - WINDOWS NT WORKSTATION 4.0 SP4 OR HIGHER.
        - WINDOWS NT SERVER 4.0 SP4 OR HIGHER
        - WINDOWS NT SERVER 4.0, ENTERPRISE EDITION SP4 OR HIGHER
        - WINDOWS NT SERVER 4.0, TERMINAL SERVER EDITION SP4 OR HIGHER
        - WINDOWS 2000 PROFESSIONAL
        - WINDOWS 2000 SERVER
        - WINDOWS 2000 ADVANCED SERVER
        - WINDOWS 2000 DATACENTER SERVER
        - WINDOWS 2000 SMALL BUSINESS SERVER

- WINDOWS XP HOME EDITION (THIS VERSION DOES NOT SUPPORT NETWORKING, ONLY LOCAL SCANS ARE SUPPORTED)
- WINDOWS XP PROFESSIONAL
- WINDOWS XP TABLET EDITION PC
- WINDOWS SERVER 2003 STANDARD EDITION
- WINDOWS SERVER 2003 ENTERPRISE EDITION
- WINDOWS SERVER 2003 WEB EDITION
- WINDOWS SERVER 2003 FOR SMALL BUSINESS SERVER
- WINDOWS SERVER 2003 DATACENTER EDITION

Prerequisites

Beyond meeting the above base hardware and OS requirements, Shavlik also requires the following software components be installed:

- INTERNET EXPLORER 5.5 or later
- MICROSOFT WINDOWS INSTALLER version 2.0
- MICROSOFT DATA ACCESS COMPONENTS (MDAC) 2.7 SP1 or higher
- MICROSOFT XML PARSER 3.0 SP2 or later, or MICROSOFT XML 4.0. - for best performance they recommend installing version 4 and version 3
- MICROSOFT JET 4.0 SP8 or later

Though you can download and install the components yourself, the folks at Shavlik have built a nice feature into their installer. When launched, the installer will determine which components are missing, and give you the opportunity to automatically download and install them.

The installer will download and install English, French or German versions of these components. If you are using another language, you will need to download and install these components for your language, then continue with the installation.

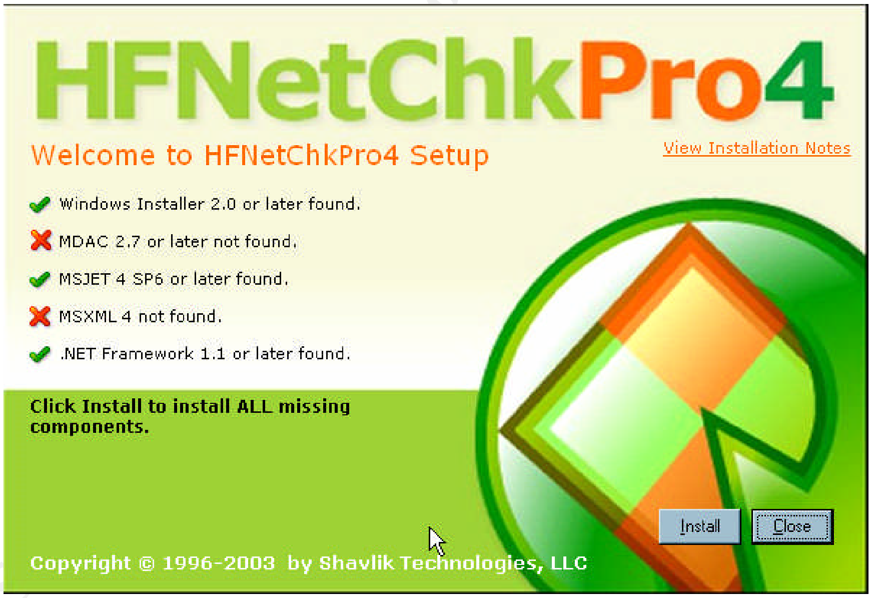
Installation Step-by-step

First off, you will have to obtain the software. HFNETCHKPRO can be downloaded directly from Shavlik's Web site at http://www.shavlik.com/pDownloadForm4.aspx. You will need to fill out a form to download the software. Save the downloaded file to the system you plan to use as the administrative console.

Note, HFNETCHKPRO now supports a SQL backend. For the purposes of this paper I will not be covering that configuration, making the assumption that you are installing a stand-alone administrative console on a Windows 2000 Professional workstation. For more information about installing multiple consoles with one SQL backend, visit http://hfnetchk.shavlik.com/sqlupdater.asp. You must have a separate SQL Enabled license key to use this feature.

After completing the download you are ready to begin the installation. When you first open the Installer you will be presented with the Welcome to Setup screen (Figure 1). This screen allows you to verify which prerequisite components are installed. Components verified as installed on the system have a green checkmark next to them. Missing components have a red "X" next to them. Notice that you can't continue with the installation of the product until these components are installed.

Using the **Install** button you have the option to automatically install all missing components. Keep in mind that this will only install English, French or German versions of these components. If you are using another language you must manually download and install the components before continuing with the installation.



Welcome to HFNetChkPro4 Setup

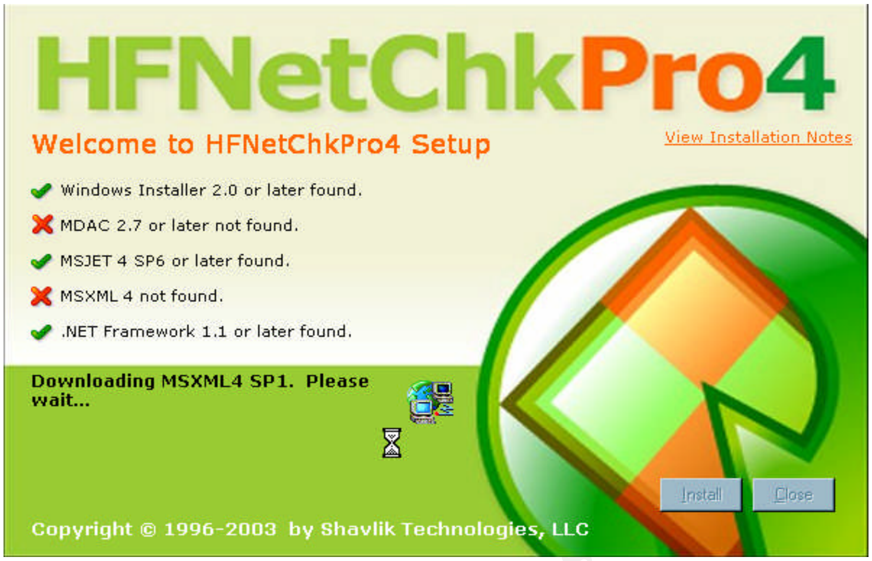
✓ Windows Installer 2.0 or later found.
✗ MDAC 2.7 or later not found.
✓ MSJET 4 SP6 or later found.
✗ MSXML 4 not found.
✓ .NET Framework 1.1 or later found.

Click Install to install ALL missing components.

Copyright © 1996-2003 by Shavlik Technologies, LLC

Figure 1

After clicking **Install**, the Welcome to Setup screen will update you on the process of installing the prerequisites (Figure 2).



Welcome to HFNetChkPro4 Setup

✓ Windows Installer 2.0 or later found.

✗ MDAC 2.7 or later not found.

✓ MSJET 4 SP6 or later found.

✗ MSXML 4 not found.

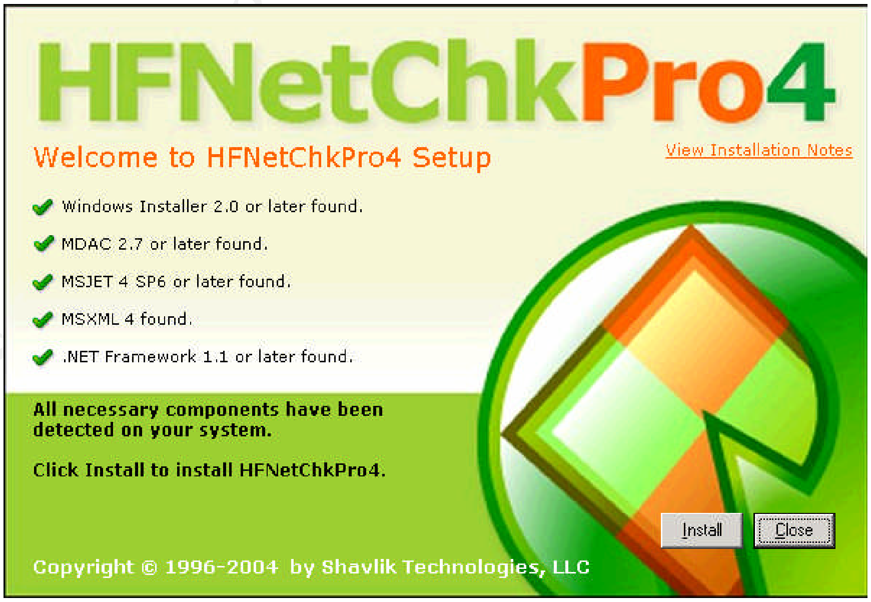
✓ .NET Framework 1.1 or later found.

Downloading MSXML4 SP1. Please wait...

Copyright © 1996-2003 by Shavlik Technologies, LLC

Figure 2

During the installation of missing prerequisites, you might be prompted to restart your machine. This may happen more than once, or not at all, depending upon what components are missing. Just keep re-running the installation until all missing prerequisites are installed. You will then see a screen indicating all components have been detected (Figure 3). Click **Install** and the installation of HFNetChkPro will begin.



Welcome to HFNetChkPro4 Setup

✓ Windows Installer 2.0 or later found.

✓ MDAC 2.7 or later found.

✓ MSJET 4 SP6 or later found.

✓ MSXML 4 found.

✓ .NET Framework 1.1 or later found.

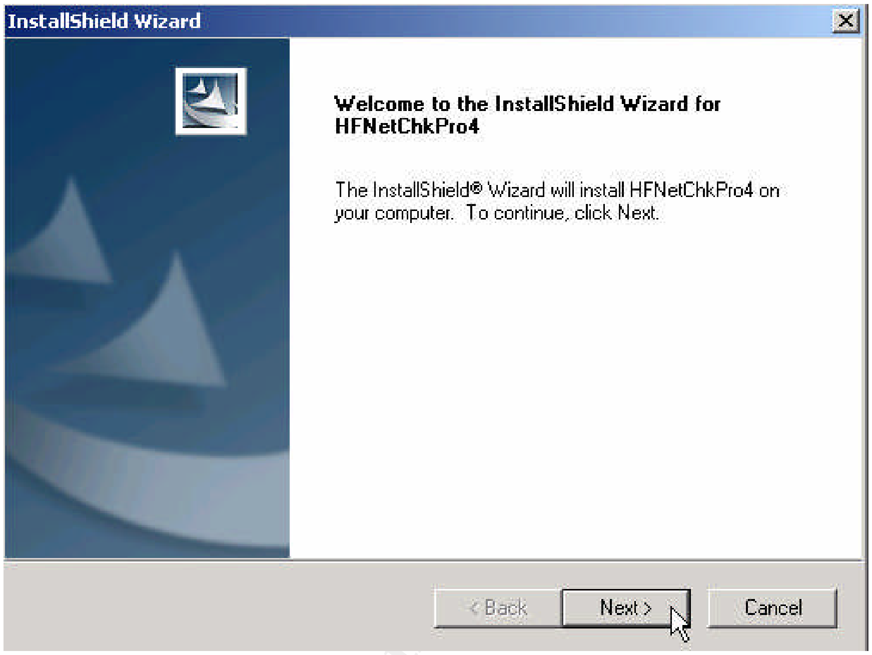
All necessary components have been detected on your system.

Click Install to install HFNetChkPro4.

Copyright © 1996-2004 by Shavlik Technologies, LLC

Figure 3

The first step the INSTALLER will perform is verification that the WINDOWS INSTALLER SERVICE is configured correctly. After that has completed you will be see the WELCOME screen (Figure 4).

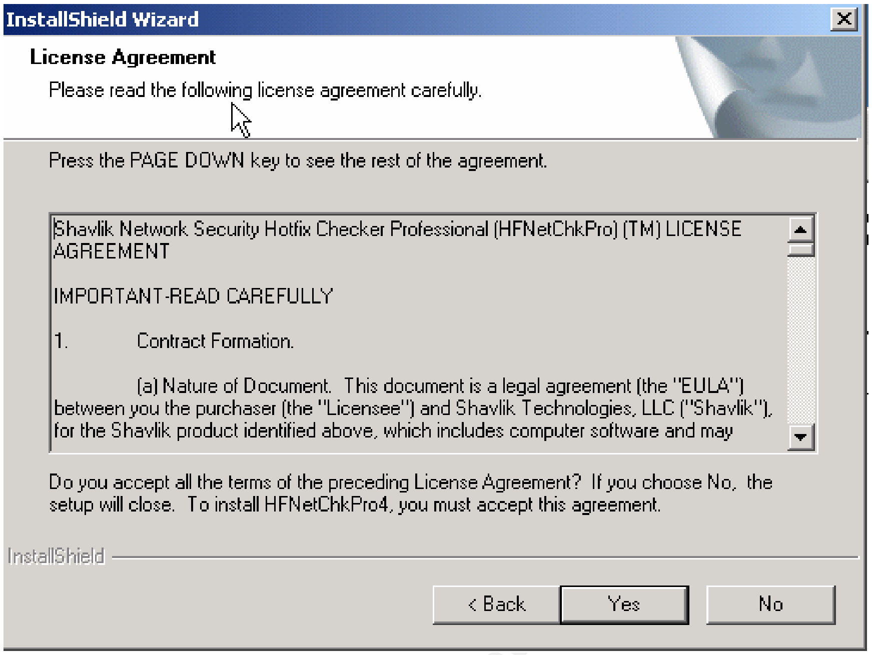


Welcome to the InstallShield Wizard for HFNetChkPro4

The InstallShield® Wizard will install HFNetChkPro4 on your computer. To continue, click Next.

Figure 4

Click **Next** to begin the installation process. The first screen that appears is the LICENSE AGREEMENT. You are asked to read (and I know we all take the time to read these – OK, you can stop laughing now) the *LICENSE AGREEMENT* and accept its terms. Click **Yes** to accept the *LICENSE AGREEMENT* (Figure 5).



Press the PAGE DOWN key to see the rest of the agreement.

Shavlik Network Security Hotfix Checker Professional (HFNetChkPro) (TM) LICENSE AGREEMENT

IMPORTANT-READ CAREFULLY

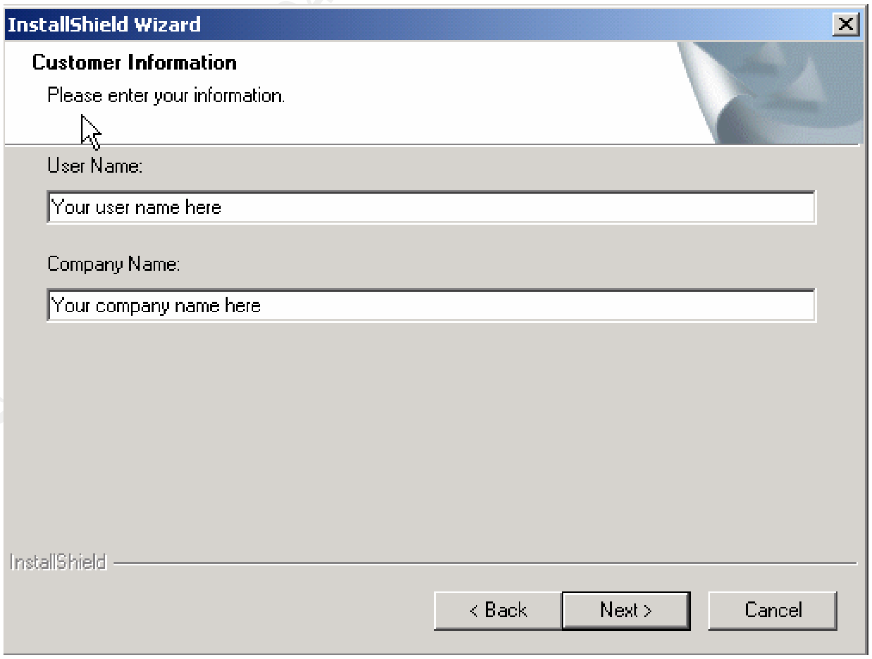
1. Contract Formation.

(a) Nature of Document. This document is a legal agreement (the "EULA") between you the purchaser (the "Licensee") and Shavlik Technologies, LLC ("Shavlik"), for the Shavlik product identified above, which includes computer software and may

Do you accept all the terms of the preceding License Agreement? If you choose No, the setup will close. To install HFNetChkPro4, you must accept this agreement.

Figure 5

The CUSTOMER INFORMATION screen appears next (Figure 6). Type the appropriate information in the **User Name** and **Company Name** fields. Click **Next**.

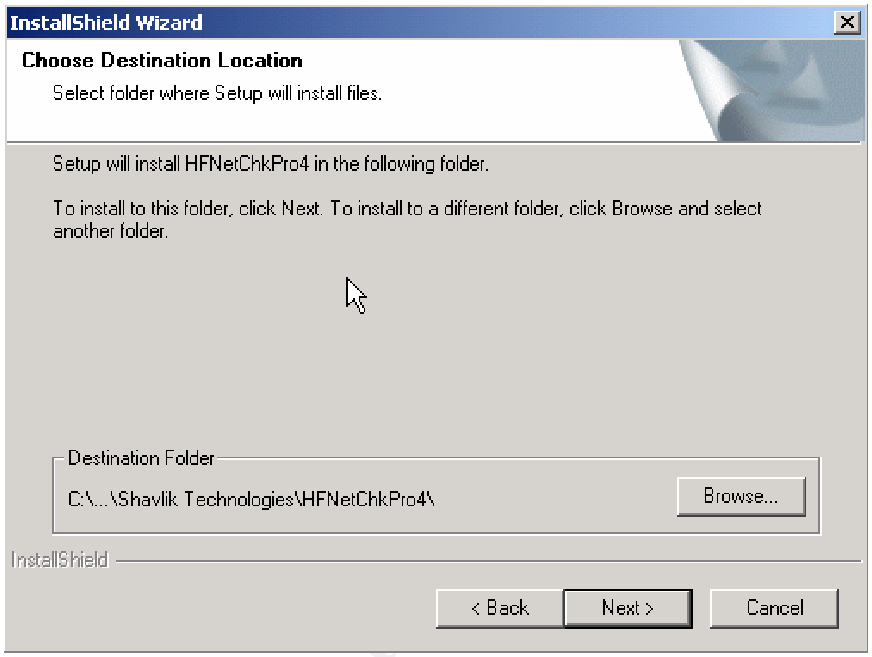


User Name: Your user name here

Company Name: Your company name here

Figure 6

The DESTINATION LOCATION screen is next (Figure 7). Either accept the default or use **Browse** to select another location. I recommend clicking **Next** to accept the default installation location. See my notes in the Best Practices section for my reasons.



Select folder where Setup will install files.

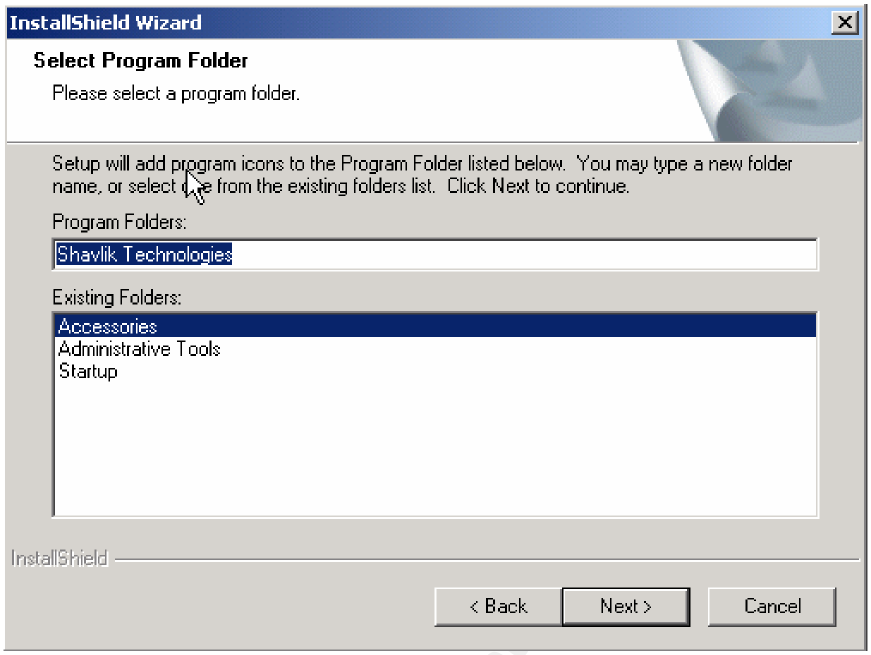
Setup will install HFNetChkPro4 in the following folder.

To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder: C:\...\Shavlik Technologies\HFNetChkPro4\

Figure 7

The PROGRAM FOLDER screen is next (Figure 8). Either accept the default folder name, or type a new one in the **Program Folders** field. This is the name of the folder that will appear within your START menu. Click **Next**.



InstallShield Wizard

Select Program Folder

Please select a program folder.

Setup will add program icons to the Program Folder listed below. You may type a new folder name, or select one from the existing folders list. Click Next to continue.

Program Folders:

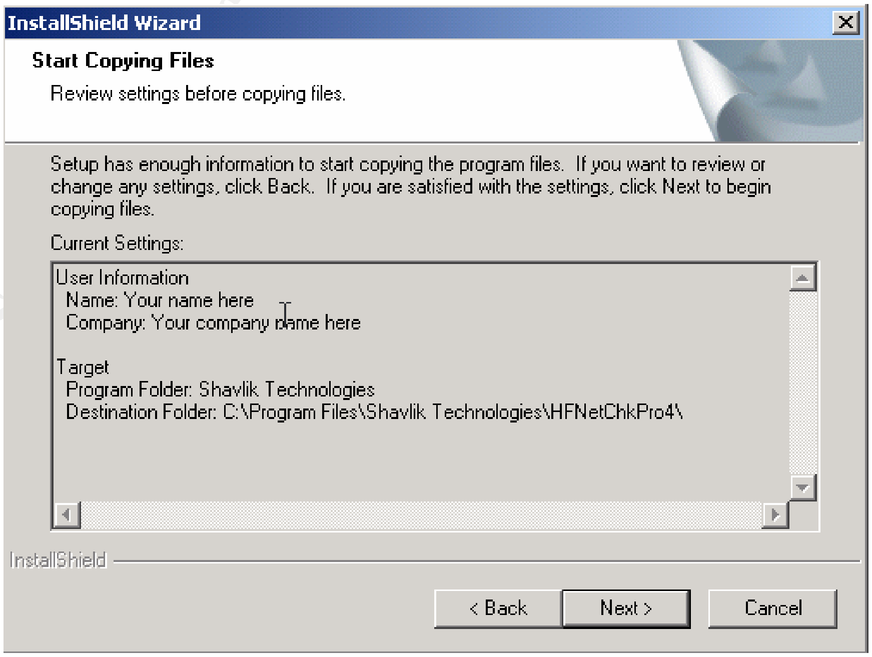
Shavlik Technologies

Existing Folders:

Accessories
Administrative Tools
Startup

Figure 8

The final INSTALLER screen (Figure 9) allows you to review your settings. Click **Back** to make any changes, or if you are happy with your settings click **Next**. Files will be copied to the local drive, and Registry changes will be made (Figure 10). Once this has completed, you will see the INSTALLSHIELD WIZARD COMPLETE screen (Figure 11). Click **Finish** to complete the install process.



InstallShield Wizard

Start Copying Files

Review settings before copying files.

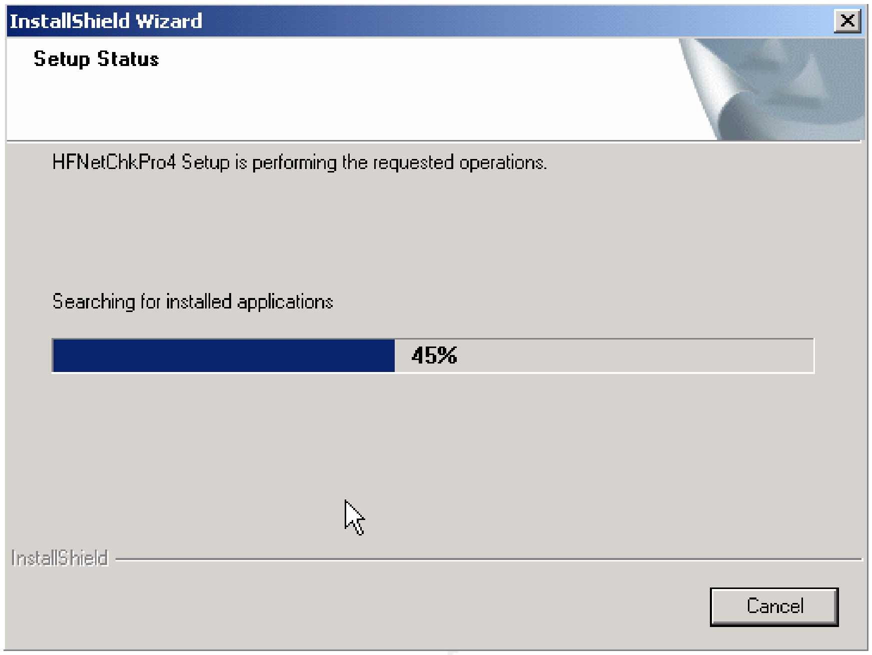
Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.

Current Settings:

```
User Information
  Name: Your name here
  Company: Your company name here

Target
  Program Folder: Shavlik Technologies
  Destination Folder: C:\Program Files\Shavlik Technologies\HFNetChkPro4\
```

Figure 9


InstallShield Wizard

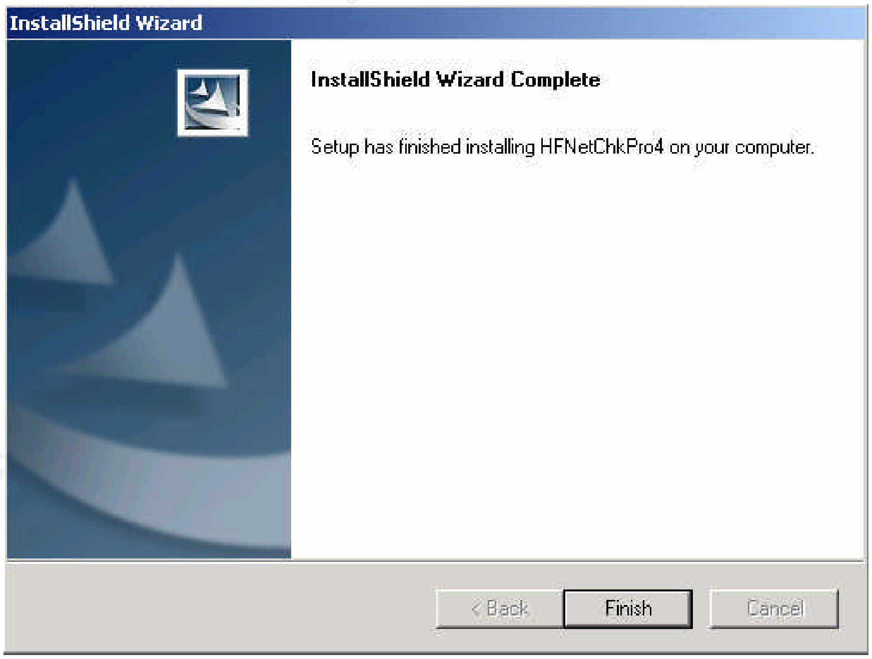
Setup Status

HFNetChkPro4 Setup is performing the requested operations.

Searching for installed applications

45%

Figure 10


InstallShield Wizard

InstallShield Wizard Complete

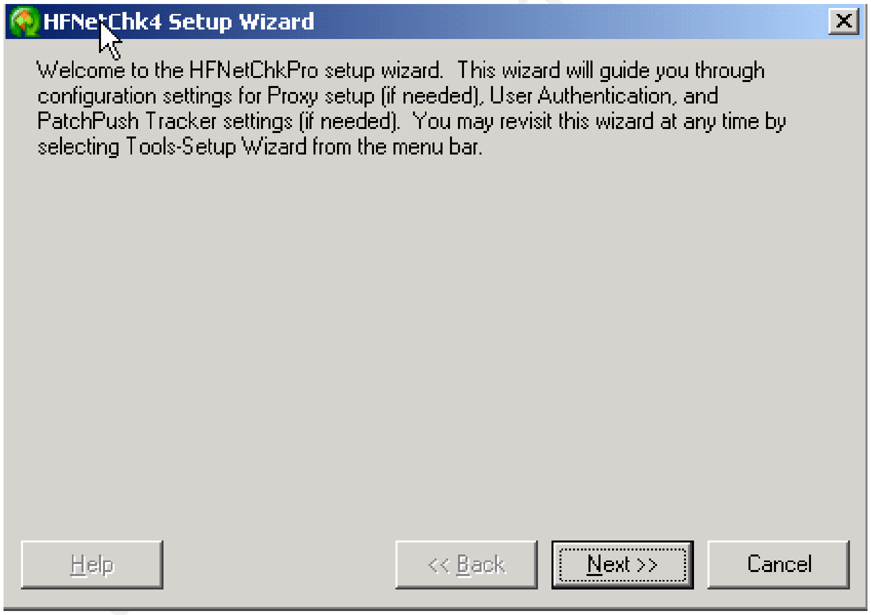
Setup has finished installing HFNetChkPro4 on your computer.

Figure 11

If you want to confirm the installation process was a success, you can look for the following:

- There will now be an icon on your desktop for HFNETCHKPRO4.
- The Shavlik HFNetChkPro Service will be installed and running.
- The program folder you created will show up within your START menu.

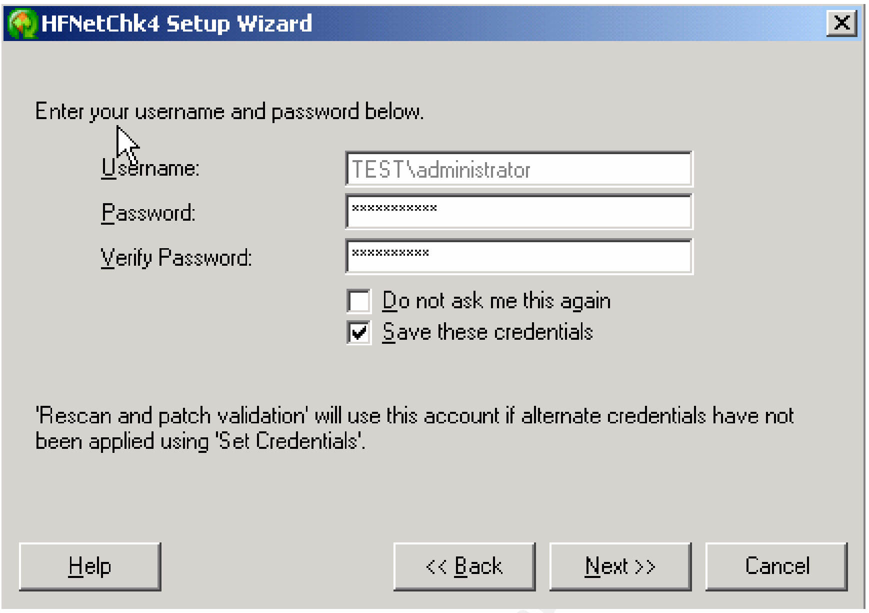
Launch the application to complete the final steps of installation. When you launch the product for the first time the SETUP WIZARD launches. The SETUP WIZARD (Figure 12) prompts for the credentials you will use when scanning and patching systems (see my notes in the Best Practices section) and any proxy settings needed for Internet connectivity. Note that you can always go back in and change these setting by selecting SETUP WIZARD from the TOOLS menu.



Welcome to the HFNetChkPro setup wizard. This wizard will guide you through configuration settings for Proxy setup (if needed), User Authentication, and PatchPush Tracker settings (if needed). You may revisit this wizard at any time by selecting Tools-Setup Wizard from the menu bar.

Figure 12

Type the desired credentials in the *Username* field. Type a password in the *Password* and *Verify Password* fields. Click **Next** (Figure 13). If prompted, type information about your Proxy connection. You have now successfully completed the installation of the product.



HFNetChk4 Setup Wizard

Enter your username and password below.

Username: TEST\administrator

Password: ************

Verify Password: ***********

□ Do not ask me this again

☑ Save these credentials

'Rescan and patch validation' will use this account if alternate credentials have not been applied using 'Set Credentials'.

Figure 13

Best Practices and lessons learned during installation.

- When selecting the directory to install the application to, I would recommend the default directory. You can still change the drive letter that the product is installed to, but accept the default directory path. I recommend this because I encountered issues with the update process when the application was not installed in the default directory.
- You may want to consider installing the application on more than one machine. For example, at my company, we decided to install one console strictly to manage our servers, and a second console to manage our workstations. We chose to do this mainly because different people are responsible for each process, and partly due to performance considerations.
- You should consider creating a specialized account to be used with the product. Make it a domain account with a complex password. With a specialized account you will not be impacted by changes to your other administrative accounts, and you will be able to audit more effectively. This account must have administrative permissions on each machine you plan to manage with this product.

3. Post installation and "customizing" the product

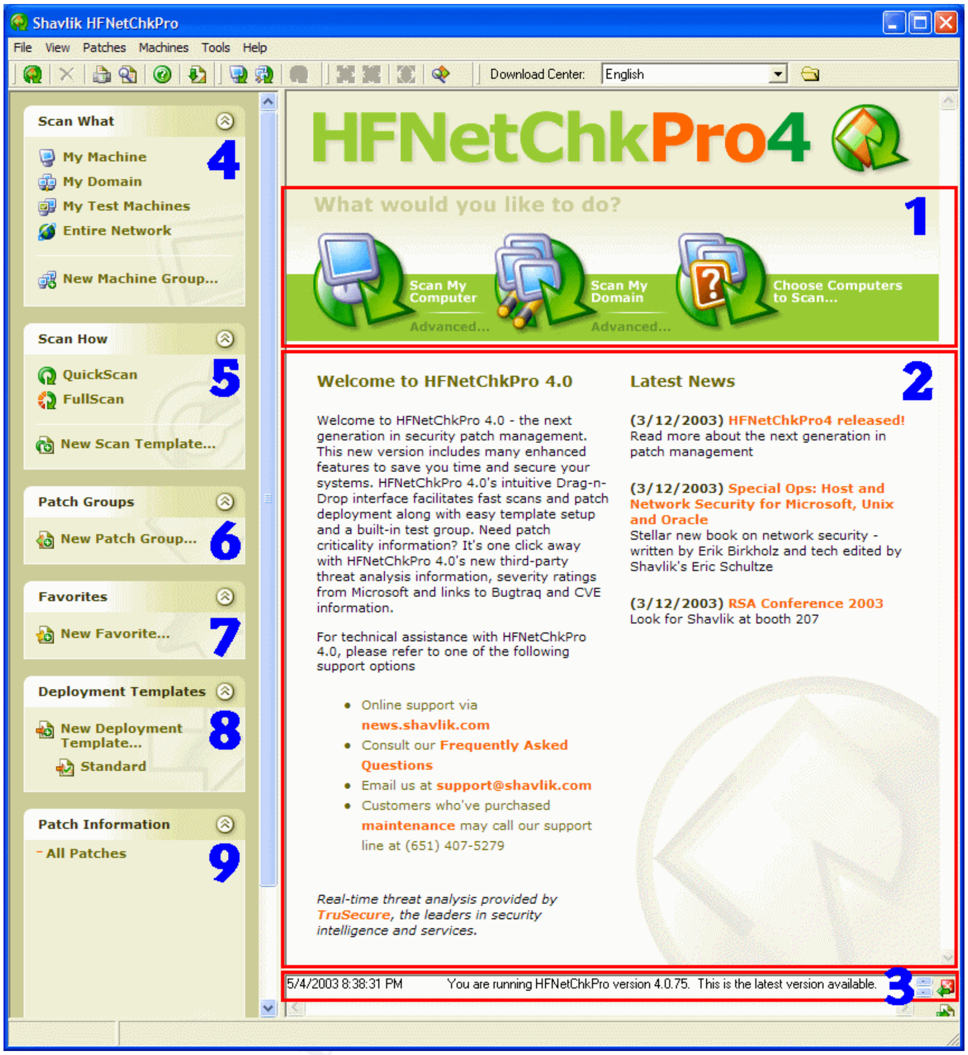
Registration and licensing

When you first download and install HFNetChkPro, it is in an unlicensed state. Depending upon how you want to use the application you have two options:

- HFNETCHKPRO LIMITED EDITION. If you wish to use the product to scan and patch fewer than ten machines and one server, and have minimal interest in generating reports (only one report is available in this edition), all you need to do is register the product with Shavlik. Registering the product gives you a valid license key, allowing your console to connect to the Shavlik network and download application updates and the XML files used during scanning. You do not pay for this option. This would be a good option to choose if you were using WINDOWS XP HOME, which only supports local scanning, or if you are a consultant who needs a quick and dirty way to push out patches to a client's network.
- HFNETCHKPRO PRO EDITION. If you wish to use the product to scan and patch more than ten machines and one server, and have complex reporting needs, you will need to contact a salesperson at Shavlik and license the product based on the number of machines you wish to scan.

Finding your way around - an introduction to the GUI and layout of the program.

When you launch HFNETCHKPRO, you automatically start on the HOME PAGE (Figure 14). The majority of the product features are available from this page, so most of your work will occur here. Let's examine what's on the HOME PAGE.



Welcome to HFNetChkPro 4.0

Welcome to HFNetChkPro 4.0 - the next generation in security patch management. This new version includes many enhanced features to save you time and secure your systems. HFNetChkPro 4.0's intuitive Drag-n-Drop interface facilitates fast scans and patch deployment along with easy template setup and a built-in test group. Need patch criticality information? It's one click away with HFNetChkPro 4.0's new third-party threat analysis information, severity ratings from Microsoft and links to Bugtraq and CVE information.

For technical assistance with HFNetChkPro 4.0, please refer to one of the following support options

- Online support via news.shavlik.com
- Consult our Frequently Asked Questions
- Email us at support@shavlik.com
- Customers who've purchased maintenance may call our support line at (651) 407-5279

Real-time threat analysis provided by TruSecure, the leaders in security intelligence and services.

Latest News

(3/12/2003) HFNetChkPro4 released!
Read more about the next generation in patch management

(3/12/2003) Special Ops: Host and Network Security for Microsoft, Unix and Oracle
Stellar new book on network security - written by Erik Birkholz and tech edited by Shavlik's Eric Schultze

(3/12/2003) RSA Conference 2003
Look for Shavlik at booth 207

5/4/2003 8:38:31 PM You are running HFNetChkPro version 4.0.75. This is the latest version available.

Figure 14[35]

1. **QUICKLAUNCH AREA.** With a single mouse click you can scan:
   a. Your local computer
   b. Your entire domain
   c. A specified set of machine names, IP addresses or a range of IP addresses.

2. **INFORMATION AREA.** Here you will find reminders of where and how to obtain technical support. You will also find information about the latest security threats, advisories and links to other security related news.

[35] http://hfnetchk.shavlik.com/support/hfpro4help/HFNetChk4_user_interface.gif

3. **STATUS MESSAGE AREA**. Displays information about the version you are currently using, notifications of any updates that are available and status messages as you use the product.

NOTE: Areas four through eight are contained in what Shavlik calls the **NAVIGATOR PANEL**.

4. **SCAN WHAT AREA.** – You will make selections here regarding what you'd like to scan. You can select the following:
    a. Your local machine
    b. Your domain
    c. A set of test machines
    d. Your entire network (IP addresses)
    e. Create your own Machine group. We will cover this later.

5. **SCAN HOW AREA**. Use these options to configure how you would like to scan. Later, I'll cover the differences between them in more detail. For now, just be aware that the options are:
    a. Quick Scan
    b. Full Scan
    c. Create your own customized scan

6. **FAVORITES AREA**. Here you can create sets of favorites, which are a collection of machines to scan, and your preferred method of scanning them.

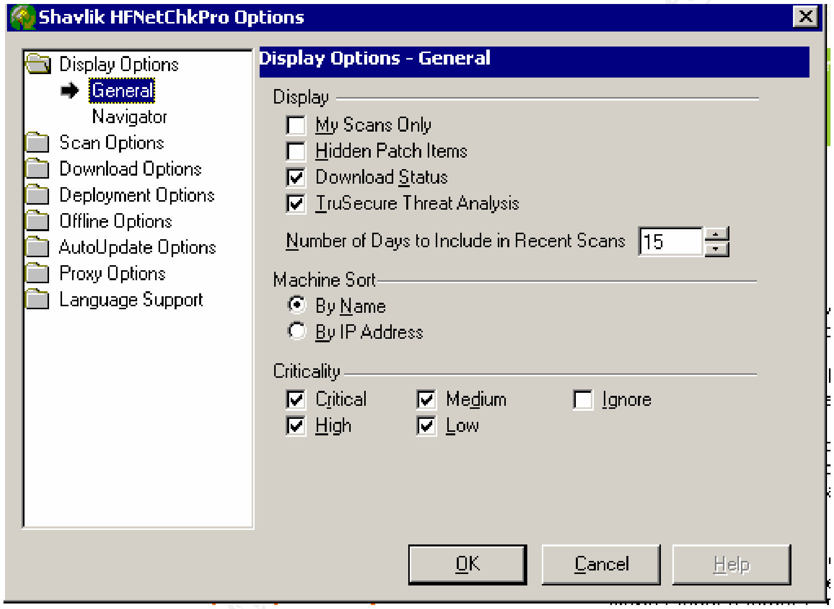
7. **DEPLOYMENTS AREA**. You will use this area to manage and create deployment templates. These templates contain the settings you choose to manage how patches are deployed to machines. I will cover deployment settings later.

8. **PATCH INFORMATION AREA**. You will find detailed information, broken down by product, for patches that are available. For more information about a patch, just click on the "+" sign next to the patch.

The OPTIONS menu – making the product look and run the way that works best for you

Now that you have an idea of what the HOME PAGE looks like, let's look at how you can customize it. Chances are you will not use all of the features Shavlik has built into the product. So, they have given you the ability to customize not only how the HOME PAGE is displayed, but how the application itself will run. You make these changes in the OPTIONS panel, which is located under the TOOLS menu. You have the ability to make changes to eight categories that control application behavior. They are:

- **Display Options** – these options are broken down into two areas. **General** options (Figure 15) allow you to customize what you want to be displayed throughout various screens within the product. **Navigator** options (Figure 16) allow you to specifically configure the display settings of the **NAVIGATOR PANEL.**



Display Options - General

Display

☐ My Scans Only
☐ Hidden Patch Items
☑ Download Status
☑ TruSecure Threat Analysis

Number of Days to Include in Recent Scans 15

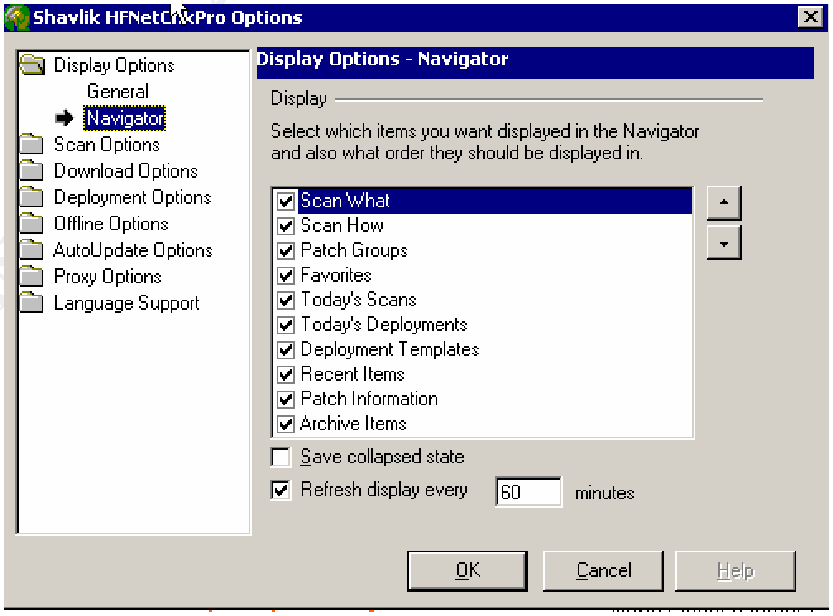
Machine Sort

● By Name
○ By IP Address

Criticality

☑ Critical ☑ Medium ☐ Ignore
☑ High ☑ Low

Figure 15



Display Options - Navigator

Display

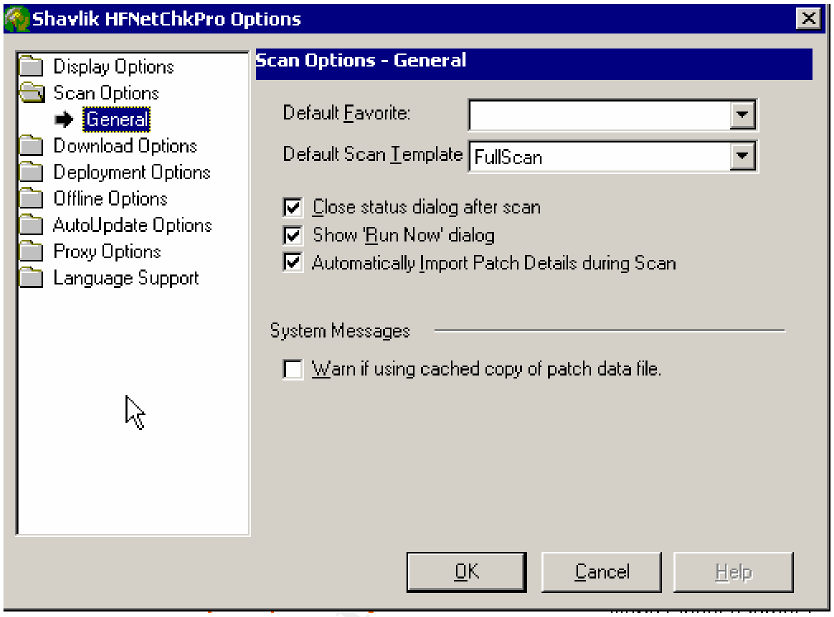
Select which items you want displayed in the Navigator and also what order they should be displayed in.

☑ Scan What
☑ Scan How
☑ Patch Groups
☑ Favorites
☑ Today's Scans
☑ Today's Deployments
☑ Deployment Templates
☑ Recent Items
☑ Patch Information
☑ Archive Items

☐ Save collapsed state
☑ Refresh display every 60 minutes

Figure 16

- **Scan Options** (Figure 17) – these options allow you to set a default *Favorite* and *Default Scan Template*. You can also configure what options appear when you are scanning, such as viewing the status screen.



Scan Options - General

Default Favorite:

Default Scan Template: FullScan

☑ Close status dialog after scan

☑ Show 'Run Now' dialog

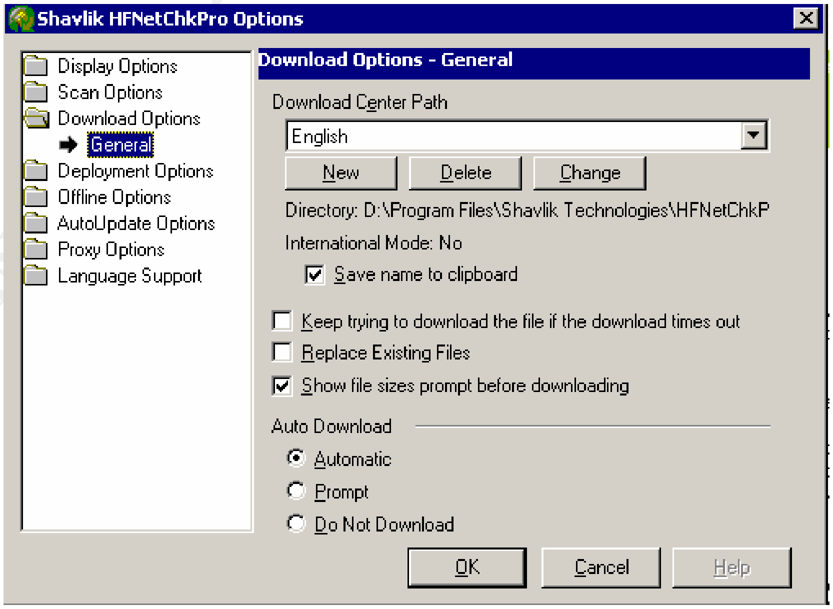
☑ Automatically Import Patch Details during Scan

System Messages

□ Warn if using cached copy of patch data file.

Figure 17

- **Download Options** (Figure 18) – these configuration options control how patches are downloaded, where they are downloaded to and how the download process takes place.



Download Options - General

Download Center Path

English

Directory: D:\Program Files\Shavlik Technologies\HFNetChkP

International Mode: No

☑ Save name to clipboard

□ Keep trying to download the file if the download times out

□ Replace Existing Files

☑ Show file sizes prompt before downloading

Auto Download

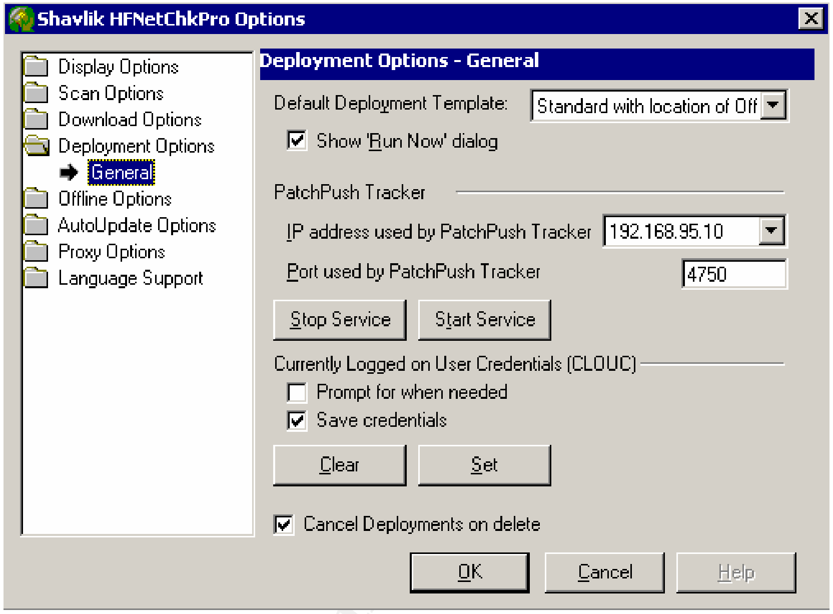
● Automatic

○ Prompt

○ Do Not Download

Figure 18

- **Deployment Options** (Figure 19) – use these options to set a *Default Deployment Template*, set the overall credentials used during patch deployment, and any customizing you want to do to the PATCHPUSH^{TM} TRACKER.



Deployment Options - General

Default Deployment Template: Standard with location of Off

☑ Show 'Run Now' dialog

PatchPush Tracker

IP address used by PatchPush Tracker 192.168.95.10

Port used by PatchPush Tracker 4750

Currently Logged on User Credentials (CLOUC)

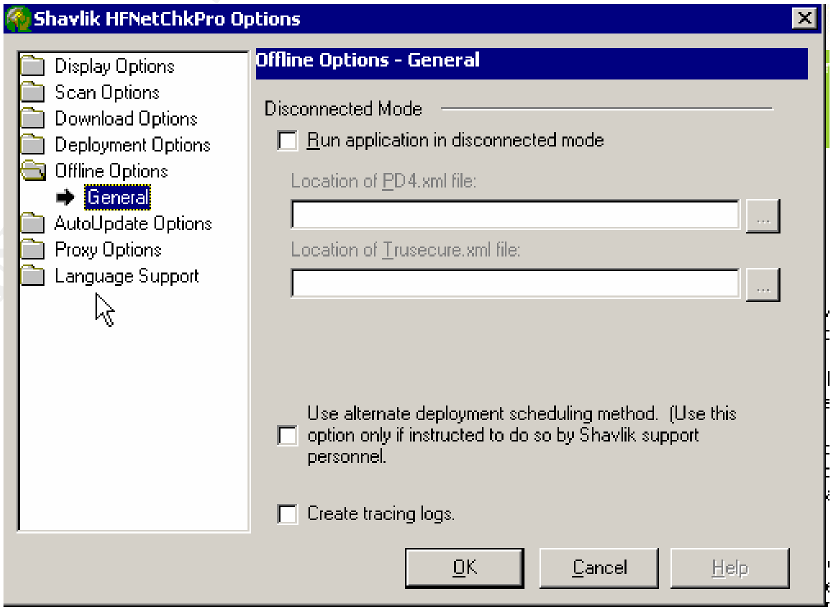
□ Prompt for when needed

☑ Save credentials

☑ Cancel Deployments on delete

Figure 19

- **Offline Options** (Figure 20) – configuration options for running the program in *Disconnected* mode. You can set an alternate path to an XML file, and choose a desired deployment method.



Offline Options - General

Disconnected Mode

□ Run application in disconnected mode

Location of PD4.xml file:

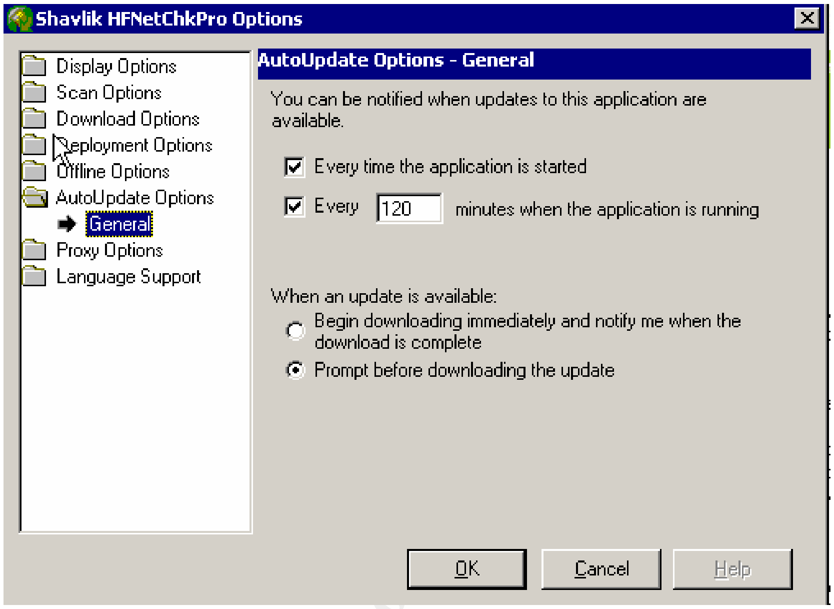
Location of Trusecure.xml file:

□ Use alternate deployment scheduling method. (Use this option only if instructed to do so by Shavlik support personnel.

□ Create tracing logs.

Figure 20

- **AutoUpdate Options** (Figure 21) – these options control when and how you are notified of application updates, and how updates will be performed.



AutoUpdate Options - General

You can be notified when updates to this application are available.

☑ Every time the application is started

☑ Every 120 minutes when the application is running

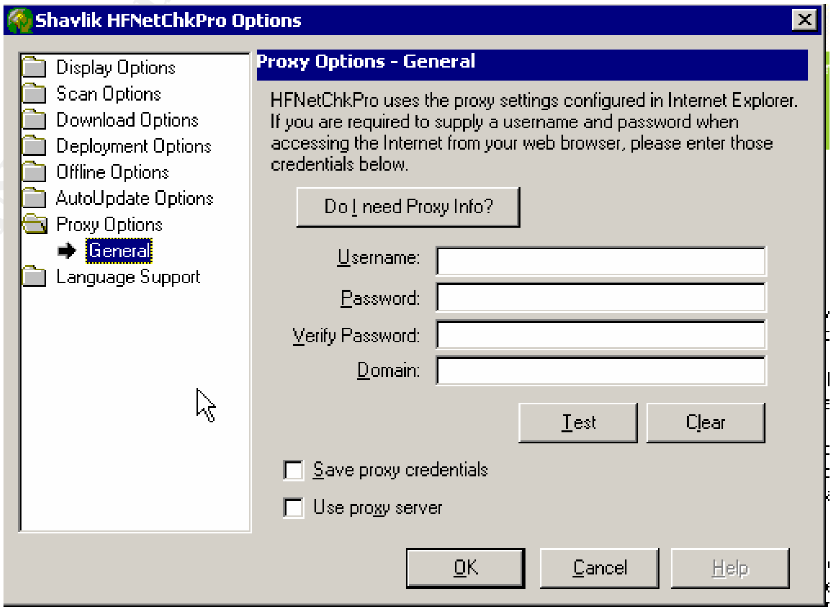
When an update is available:

○ Begin downloading immediately and notify me when the download is complete

● Prompt before downloading the update

Figure 21

- **Proxy Options** (Figure 22) - configure these options if your administrative console connects to the Internet through a proxy server. These settings have nothing to do with scanning a machine through a firewall. They are only settings for how the administrative console connects to the Internet.



Proxy Options - General

HFNetChkPro uses the proxy settings configured in Internet Explorer. If you are required to supply a username and password when accessing the Internet from your web browser, please enter those credentials below.

Username:

Password:

Verify Password:

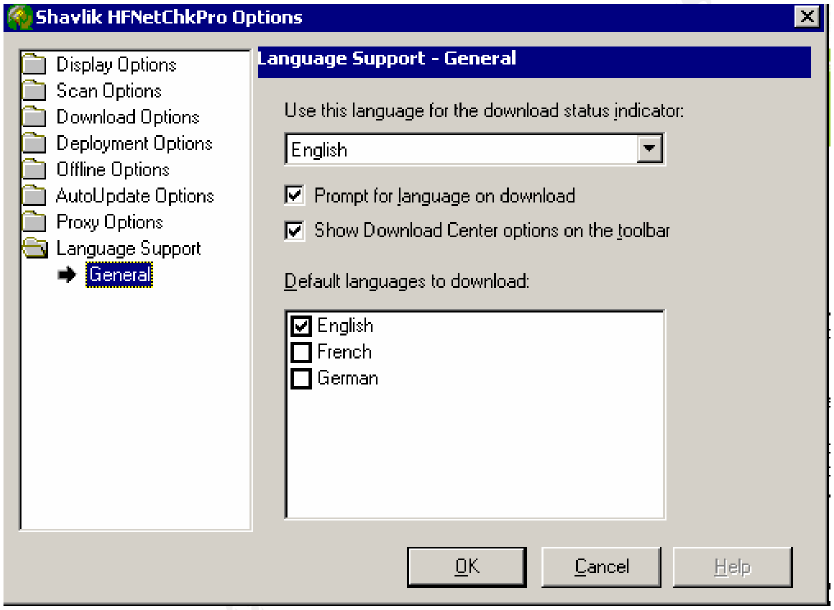
Domain:

☐ Save proxy credentials

☐ Use proxy server

Figure 22

- **Language Options** (Figure 23) – these options configure support for languages other than English, French or German. You must create a new download center to support international languages. For more information on configuring international support, visit the Help file at: http://hfnetchk.shavlik.com/support/hfpro4help/About_international_patches.htm.



Use this language for the download status indicator: English

☑ Prompt for language on download

☑ Show Download Center options on the toolbar

Default languages to download:

☑ English
□ French
□ German

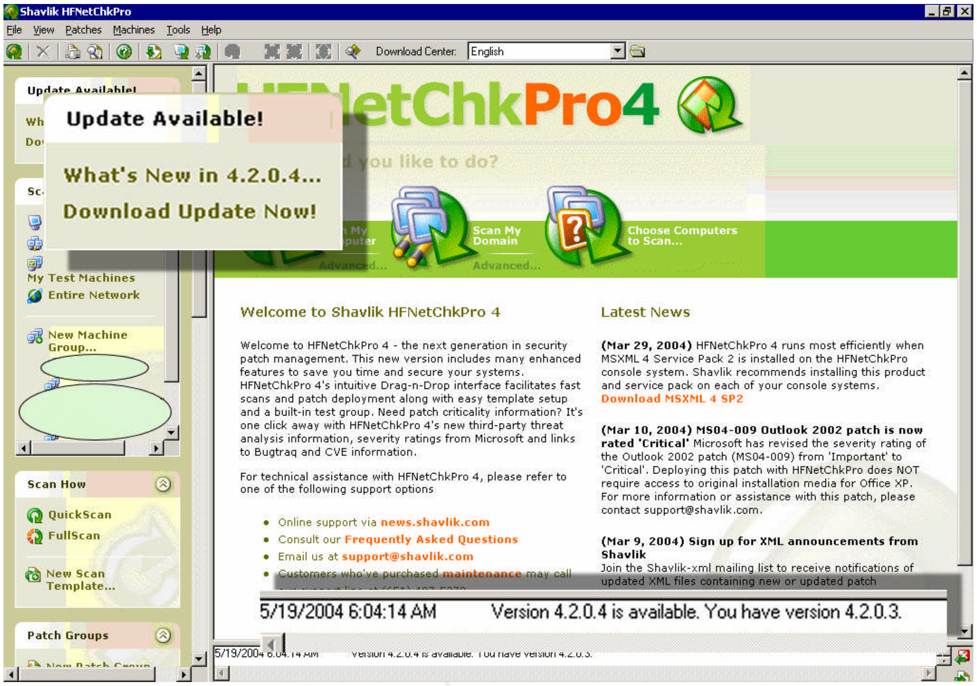
Figure 23

Be sure to take time to review the settings within the Options panel. You will find a lot of ways to customize the program to suit your needs.

Checking for application and software updates

It's probably fairly obvious that this would be a worthless application if it were not being updated on a regular basis. There are actually two ways the product is kept up-to-date: application updates and patch information updates.

Application updates happen on a fairly regular basis as Shavlik adds more functionality and, if necessary, fixes to the product. You are informed about updates in a few ways. Each time you launch the application it will attempt to check and see if you are using the latest version. You must have an active Internet connection for this to work. If you are using the latest version, you will see a statement to that effect in the **Information area** at the bottom of the Home Page. Or, if an update is available, you will see a statement to that effect in the **Information area**. To get the update, click **Update Available** which appears within the Navigator panel. The only time you will see this option is when an update is available; otherwise the "Scan What" option appears at the top of the **NAVIGATOR PANEL** (Figure 24).



Welcome to Shavlik HFNetChkPro 4

Welcome to HFNetChkPro 4 - the next generation in security patch management. This new version includes many enhanced features to save you time and secure your systems. HFNetChkPro 4's intuitive Drag-n-Drop interface facilitates fast scans and patch deployment along with easy template setup and a built-in test group. Need patch criticality information? It's one click away with HFNetChkPro 4's new third-party threat analysis information, severity ratings from Microsoft and links to Bugtraq and CVE information.

For technical assistance with HFNetChkPro 4, please refer to one of the following support options

- Online support via news.shavlik.com
- Consult our Frequently Asked Questions
- Email us at support@shavlik.com
- Customers who've purchased maintenance may call

Latest News

(Mar 29, 2004) HFNetChkPro 4 runs most efficiently when MSXML 4 Service Pack 2 is installed on the HFNetChkPro console system. Shavlik recommends installing this product and service pack on each of your console systems. Download MSXML 4 SP2

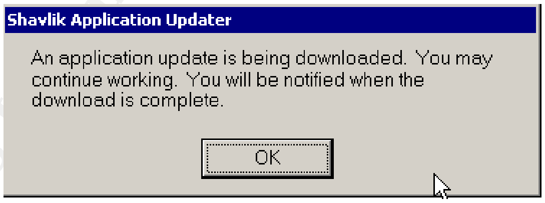
(Mar 10, 2004) MS04-009 Outlook 2002 patch is now rated 'Critical' Microsoft has revised the severity rating of the Outlook 2002 patch (MS04-009) from 'Important' to 'Critical'. Deploying this patch with HFNetChkPro does NOT require access to original installation media for Office XP. For more information or assistance with this patch, please contact support@shavlik.com.

(Mar 9, 2004) Sign up for XML announcements from Shavlik
Join the Shavlik-xml mailing list to receive notifications of updated XML files containing new or updated patch

5/19/2004 6:04:14 AM Version 4.2.0.4 is available. You have version 4.2.0.3.

Figure 24

The download of the new version will begin in the background while you continue working. You will see a dialog box (Figure 25) letting you know that the process is occurring in the background.


Shavlik Application Updater

An application update is being downloaded. You may continue working. You will be notified when the download is complete.

Figure 25

Once the download is complete, you will be prompted to exit the application and restart it. When the application is restarted a few things will happen. A DOS prompt will open, the Shavlik service will stop, the new update will be applied, the service will be restarted and the application will automatically open to the HOME PAGE.

The second way the application is kept up-to-date is patch information updates. Each time you perform a scan, the first step the application performs is a download of new patch information. You must have a working connection to the Internet for downloads to take place. Patch information is contained in the following files:

- MSSECURE.XML - the HFNETCHKPRO engine uses the EXTENSIBLE MARKUP LANGUAGE (XML) in a file that contains information about Microsoft security hotfixes that are available, and which products they are available for. The XML file contains security bulletin names and titles and detailed data about product-specific security hotfixes, including:

  - files in each hotfix package and their file versions and checksums
  - registry keys that were applied by the hotfix installation package
  - information about which patches supersede which other patches
  - related MICROSOFT KNOWLEDGE BASE article numbers
  - third party analysis of the threat posed by a patch's vulnerability
  - links to additional information from BUGTRAQ (BugtraqID) and cross references to the COMMON VULNERABILITIES AND EXPOSURES (CVE) database hosted by Mitre.org (CVEID). [36]

  MSSECURE.XML contains fairly detailed information about each patch, such as the target operating system version and service pack level, corresponding MICROSOFT KNOWLEDGE BASE article and security bulletin reference number, affected product and service pack IDs, Registry key to be created, file version, checksum and location, and reboot requirement.[37]

- PD4.XML – The patch download and deployment XML file. It contains information about each patch including file size, deployment and rollback switches, etc. This file also helps download the file from the vendor.

- COMMANDLINE4.EXE – This is a helper application that launches each patch installation. It interprets specific commands in the installation batch file, assisting with silent installs and rollbacks, as well as sending information back to PATCHPUSH™ TRACKER.

[36] Shavlik Technologies. “Scanning Engine Overview”. Help File.
[37] Policht, Marcin. “An Introduction fo Windows Patch Management.” CrossNodes. 1/20/04.

- TRUESECURE.XML – contains information regarding threat level analysis from the TruSecure Corporation. This 3rd party threat assessment tool is only available in versions prior to 4.0.3. If you are using a newer version, this file is no longer updated.

These files can be manually downloaded at any time by selecting the **Refresh Files** option from the TOOLS menu.

Here is an example of the output you will see in the **DETAILS** screen while a scan is being performed. Everything up to phase one happens each time a scan is performed, then depending upon necessity, phase two will occur.

```
Imports new patch information

Importing new patch information...
Updating the patch table if necessary.
Updating the patch table - phase 1.
Updating the patch table - phase 2 - Please be patient.
Updating patch information for Windows Server 2003, Standard Edition Gold
Updating patch information for Windows Server 2003, Enterprise Edition Gold
Updating patch information for Windows Server 2003, Datacenter Edition Gold
Updating patch information for Windows Server 2003, Web Edition Gold
Updating patch information for Windows Server 2003 for Small Business Server Gold
Updating patch information for Windows XP Home Edition Gold
Updating patch information for Windows XP Home Edition SP1
Updating patch information for Windows XP Professional Gold
Updating patch information for Windows XP Professional SP1
Updating patch information for Windows 2000 Professional Gold
Updating patch information for Windows 2000 Professional SP1
……..
```

Best practices and lessons learned during post installation and customization

- Take time to examine all of the settings in the OPTIONS panel. Customize the program to suit your needs.
- Before you perform your first scan after installing the program, take time to do an initial download of all existing patches. Since the program will not have to download each patch as a part of the deployment process, this up-front download will speed up your first deployment. To do this, go to the **PATCH INFORMATION AREA** and click **All Patches**. Select **Download Patches (All)** from the PATCHES menu. Choose the language you want the patches downloaded in click **OK**. In previous versions, Shavlik allowed you to pick and choose patches only for products you used. Now they force you to download patches for all products. Once you select **Download Patches (All)** go ahead and get a cup of coffee – it can take a while to download.

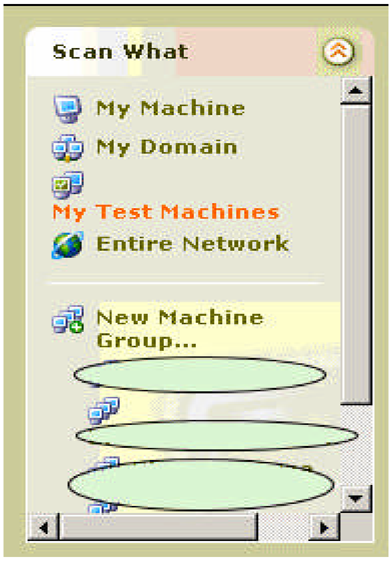
- You should consider creating your own customized deployment template and setting it as the default for all deployments. Why? Well, for example, to deploy MICROSOFT OFFICE updates and service packs, you must create a deployment template that points to the location of the original installation files\media. If you create a default template, and use it for all deployments, you will not forget to configure these settings when deploying OFFICE updates and service packs.
- To avoid having to type credentials for each scan, set default credentials in the OPTIONS panel. These credentials will be used for all scans. If you need to you can always override the default credentials.
- If you have multiple network cards in the administrative console you might want to consider setting the PATCHPUSH^{TM} TRACKER to use the second network card. This will improve performance.

4. Managing Machine Groups – the "Scan What" option

Default options

We have already spent some time discussing a few of the default scan options that are available within the **SCAN WHAT AREA** of the product. They are:

- **My Machine** – the administrative console
- **My Domain** – the domain the administrative console is a member of
- **My Test Machines** – any machines you want to do a quick scan of
- **My Network** – every machine the administrative console can see on the network
- **New Machine group** – create and manage your own groups



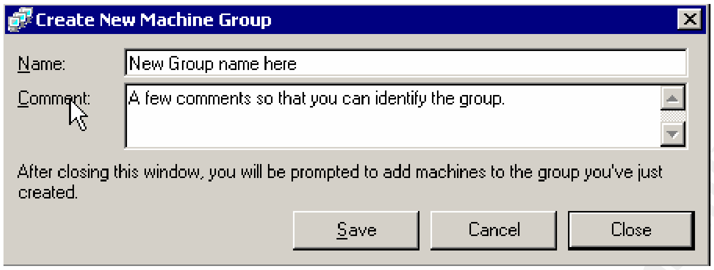
Let's spend some time focusing on the **New Machine Group** option. To use the product effectively you will find yourself creating machine groups. You have complete flexibility to group machines into groupings that make the most sense to you. For example, you can group machines based on:

- Subnet
- Server application (SQL, Exchange, Web servers)

- Active Directory OU
- Location, such as outside a firewall

Creating a new Machine group

To create a new machine group, click **New Machine group**. Type a name and short description in the *Name* and *Comment* fields (Figure 26).



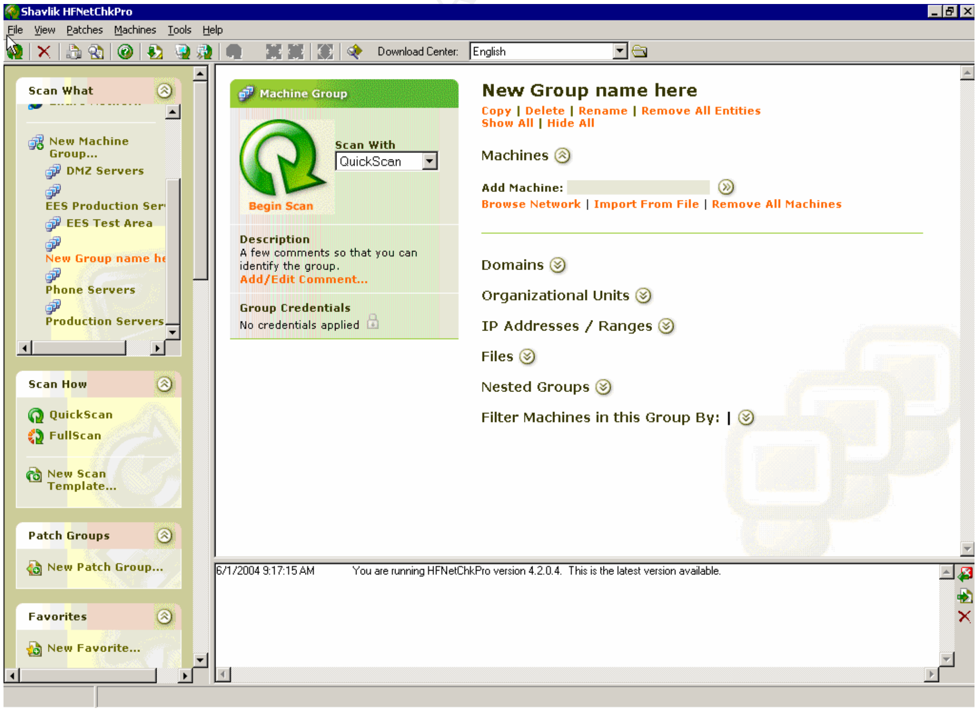
Name: New Group name here

Comment: A few comments so that you can identify the group.

After closing this window, you will be prompted to add machines to the group you've just created.

Figure 26

Once you have created a group you can change various options. Select the group you just created. The **INFORMATION AREA** will change to display options you can modify (Figure 27).



New Group name here

Description
A few comments so that you can identify the group.

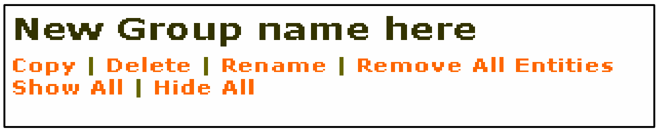
Group Credentials
No credentials applied

6/1/2004 9:17:15 AM You are running HFNetChkPro version 4.2.0.4. This is the latest version available.

Figure 27

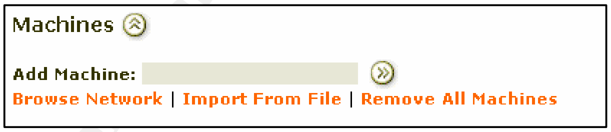
To change the group as a whole, use the options at the top of the **INFORMATION AREA** screen**.** You can do the following to a group:

- Copy it
- Delete it
- Rename it
- Remove members of the group
- Show or hide members of the group

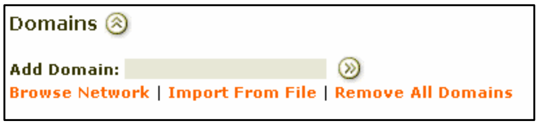


Immediately under these options you will find a list of subcategories describing how objects can be added to a group. Objects can be individual machines, domains, subnets, etc. The ⌃ icon next to each subcategory allows you to show or hide the options for that subcategory. Clicking » will save the object into the subcategory of the group. Let's look at each subcategory in detail.

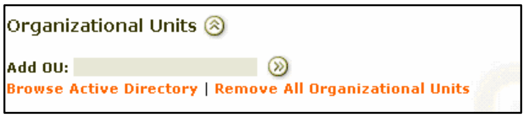
1. **Machines** – use this subcategory to add individual machines to the group by:
   - Typing the machine name in the *Add Machine* field
   - Browsing the network.
   - Importing machine names from a file.



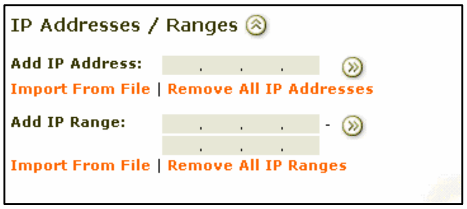
2. **Domains** - Use this subcategory to add machines that exist in domain(s) by:
   - Typing the domain name in the *Add Domain* field
   - Browsing the network for domains.
   - Importing domain names from a file.



3. **Organizational Units** – Use this subcategory to add machines that exist in Active Directory Organizational Units by:
   - Typing the Active Directory OU name in the *Add OU* field
   - Browsing the Active Directory database for OU's.



4. **IP Addresses / Ranges** – Use this subcategory to add machines to the group based on:
   - Individual IP addresses
   - Subnet ranges

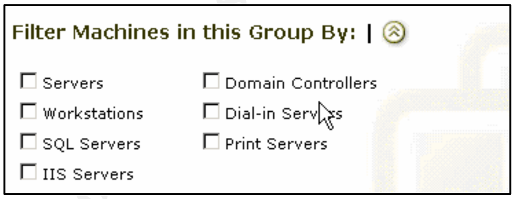

IP Addresses / Ranges
Add IP Address:
Import From File | Remove All IP Addresses
Add IP Range:
Import From File | Remove All IP Ranges

5. **Files** - Use this subcategory to add machines to the group based on any of the following files:
   - Machine files
   - Domain files
   - IP address and range files

6. **Nested Groups** – Use this subcategory to nest groups, within this group, you have already created.

7. **Filter Machines in Group** – Use this subcategory to filter the types of machines that will be in the group. You can filter by any of the following types of machine "values."

   - Server
   - Worstation
   - SQL Server
   - IIS Server
   - Domain Controller
   - Dial-in Server
   - Print Server



Filter Machines in this Group By: |

□ Servers □ Domain Controllers
□ Workstations □ Dial-in Servers
□ SQL Servers □ Print Servers
□ IIS Servers

Perhaps the most powerful feature of the product is that you are not limited to selecting just one of these subcategories per group.

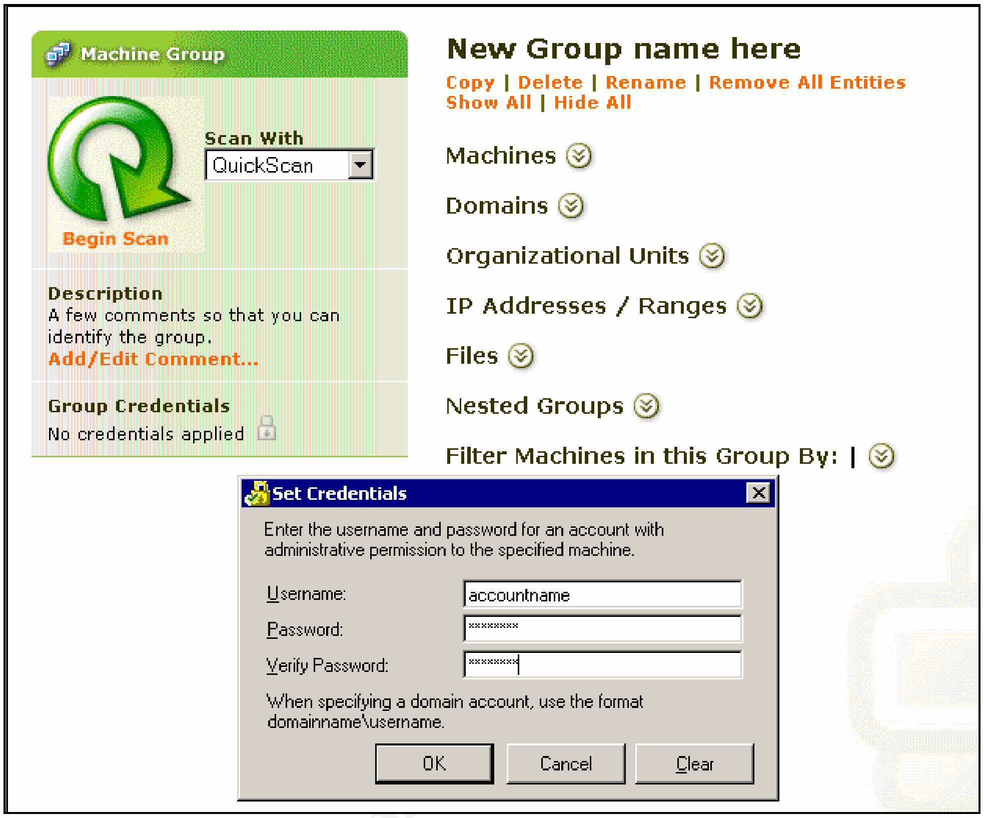
Making changes to existing groups

To make changes to an existing group, all you need to do is select the group from the **Scan What area.** You will see the same options you had when you first created the group.

A few options we did not cover when creating a group are – adding credentials and deleting machines. Deleting any object from a group is straight forward. Just click on the red "x" next to the name of the object and it will be deleted from the group.

Setting credentials has been covered before. As a reminder, if you set credentials in the Options panel, those credentials will be used for all scans. But, if you want to override those settings, say because the machine or domain does not use them, then you can do it per group or individual object in the group.

To set credentials for the group itself, select the grayed-out lock icon under **Group Credentials** (Figure 28). Type an account and password in the provided fields. Click **OK**. The icon will change to a solid lock with a green checkmark next to it.



Scan With: QuickScan

Description
A few comments so that you can identify the group.
Add/Edit Comment...

Group Credentials
No credentials applied

Enter the username and password for an account with administrative permission to the specified machine.

Username: accountname
Password: ********
Verify Password: ********

When specifying a domain account, use the format domainname\username.

Figure 28

To set credentials for any object within a group, select the grayed-out lock icon next to the object (Figure 29). Type an account and password in the provided fields. Click **OK**. The icon will then change to a solid lock with a green checkmark next to it.

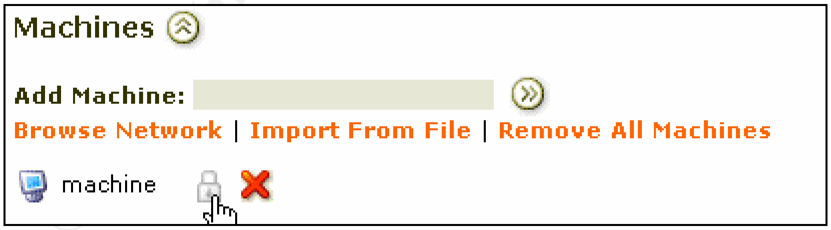
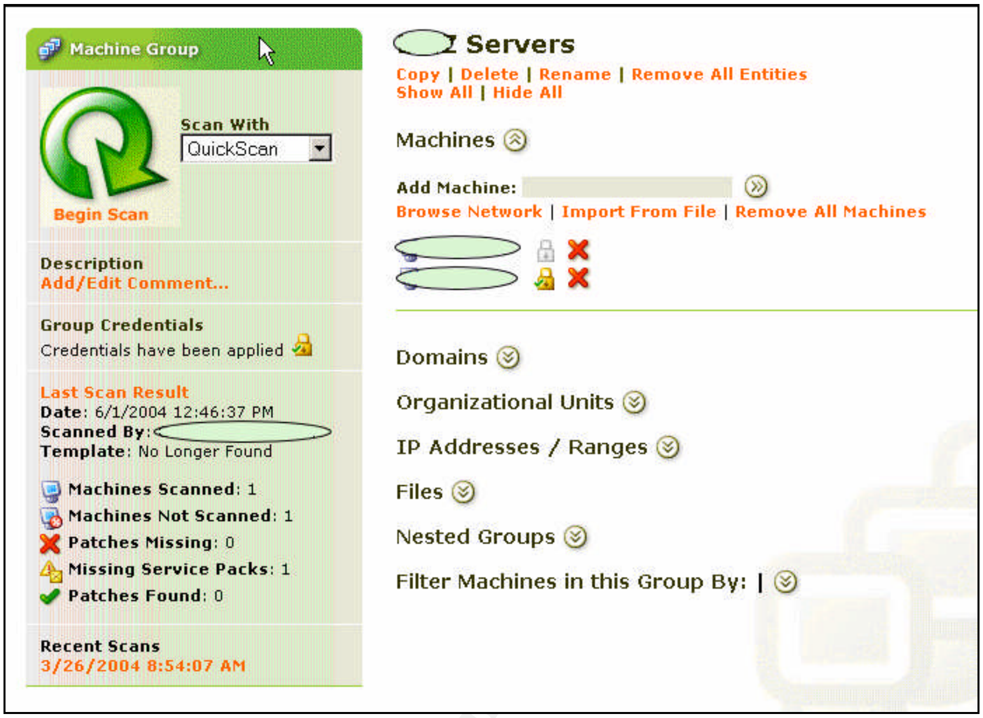


Figure 29

Before we move on to scan templates, let's look at some other information within a group's properties. If the group has been used to perform a scan, you will see the past results of the previous scan listed on the left-hand side of the properties of the group (Figure 30). Notice that you get a summary of the last scan including when it was performed, who performed it, the number of machines in the group that were scanned and not scanned, the number of found and missing patches and, finally, the number of missing service packs. Keep in mind this information is for the group as a whole, not individual machines.



Description
Add/Edit Comment...

Group Credentials
Credentials have been applied

Last Scan Result
Date: 6/1/2004 12:46:37 PM
Scanned By: [redacted]
Template: No Longer Found

Machines Scanned: 1
Machines Not Scanned: 1
Patches Missing: 0
Missing Service Packs: 1
Patches Found: 0

Recent Scans
3/26/2004 8:54:07 AM

Figure 30

5. Managing scan templates – the "Scan How" option

Default options

Now that we have delved into how groups are created, let's examine how to create and modify scanning templates. By default there are three scanning options available in the **SCAN HOW AREA** of the **NAVIGATOR PANEL.** Each one has a different option, and works in a different way.

- **Quick Scan** – scans a machine for both missing and installed patches, but does not use checksums.
- **Full Scan** – scans a machine for both missing and installed patches and uses checksums when evaluating. Full scans also display notes and warnings in the **SCAN STATUS** dialog box.
- **New Scan Template** – allows you to create your own scanning settings.

Creating a new scan template

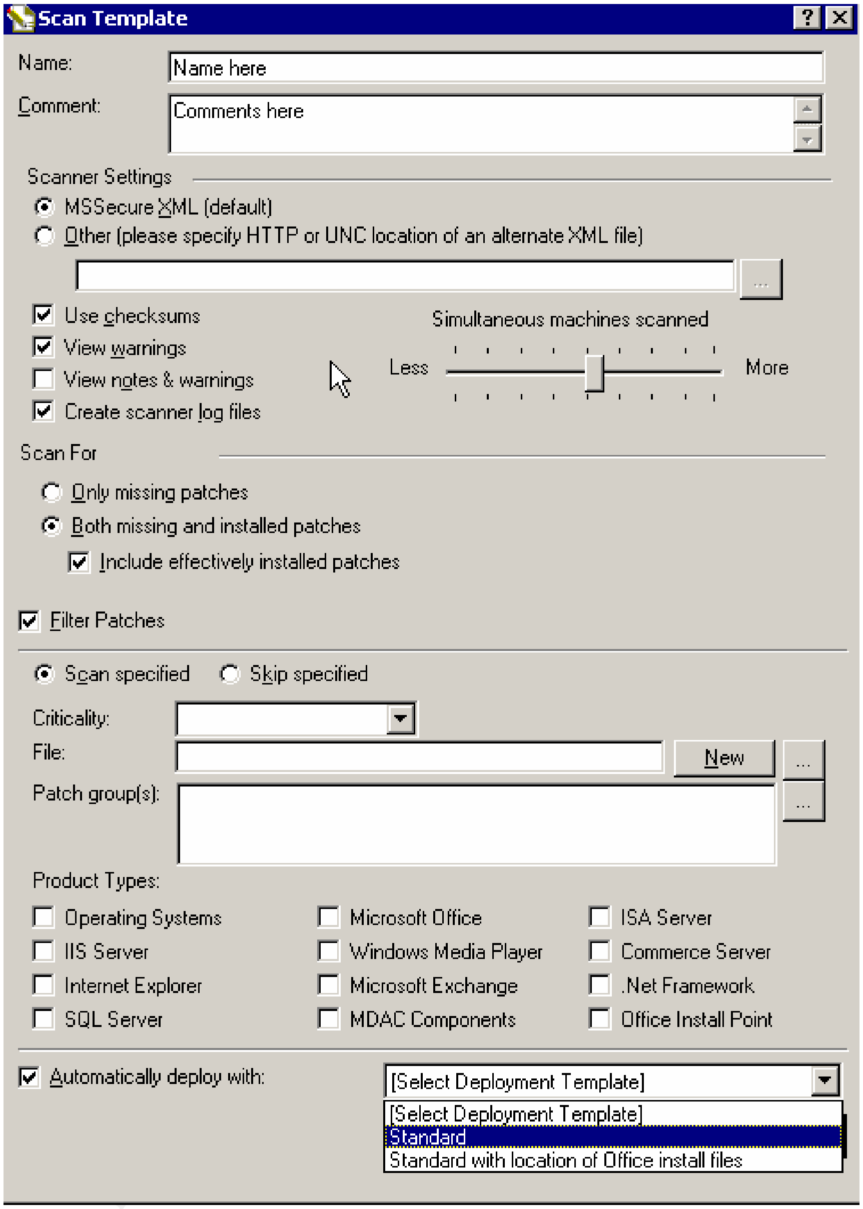
To create a new scanning template, select **New Scan Template**. Type a name and short description in the *Name* and *Comment* fields. You now have a few options you can set within the template preferences (Figure 31).

- **Scanner Settings**
  - You can use the default XML file hosted on the Shavlik servers. Or, if you are operating in *Disconnected* mode, you can point to a location on your own machine or network.
  - You have the choice of using, or not using, checksums to validate downloads.
  - You can choose to view, or not view, any errors generated during the scanning process.
  - For troubleshooting purposes you can create a log file.
  - Using the slider bar, you can set the simultaneous number of machines that can be scanned. You can scan up to 64 machines at one time. Keep in mind though, that the more simultaneous scans you perform, the more potential impact to your network.

- **Scan for**
  - You can scan for missing or installed patches, or both if you prefer.
  - You have the choice of scanning or not scanning for "Effectively" installed patches. These patches, though not specifically installed, are still shown as installed. They are actually "installed" by patches that came after them. In Shavlik terminology this is the premise of superscedence.

- **Filtering Patches.** Use these checkboxes and pull down lists to filter your scans based on numerous criteria.

- **Automatically deploy with**. Be VERY, VERY careful with this option. If you check this you are asking the application to automatically deploy any, and all, patches that it finds missing. Always test patches and service packs before you deploy them. Use this option only if you are absolutely sure that what you are deploying will not break anything. Note that, by design, this automated deployment option does not work with scheduled scans. It will only be available during manual scans.



Name: Name here

Comment: Comments here

Scanner Settings

● MSSecure XML (default)

○ Other (please specify HTTP or UNC location of an alternate XML file)

☑ Use checksums

☑ View warnings

☐ View notes & warnings

☑ Create scanner log files

Scan For

○ Only missing patches

● Both missing and installed patches

☑ Include effectively installed patches

☑ Filter Patches

● Scan specified ○ Skip specified

Criticality:

File:

Patch group(s):

Product Types:

☐ Operating Systems ☐ Microsoft Office ☐ ISA Server

☐ IIS Server ☐ Windows Media Player ☐ Commerce Server

☐ Internet Explorer ☐ Microsoft Exchange ☐ .Net Framework

☐ SQL Server ☐ MDAC Components ☐ Office Install Point

☑ Automatically deploy with: [Select Deployment Template]

[Select Deployment Template]
Standard
Standard with location of Office install files

Figure 31

Best practices and lessons learned when creating and using scan templates

- If you do not have any spare machines around to test patches on, buy a copy of VMWare and test patches on virtual machines.
- Be sure to review all of the information within the product help file if you plan to create your own scanning templates.
- You more than likely will not be creating your own scanning templates unless you plan to use the product in *Disconnected* mode.

- Where the ability to create your own scan templates is powerful, is when you have the need to look for specific patches that either are, or are not, installed. For example, using the filter options to scan for the latest security threat, while ignoring all other missing patches. But why do this when you can create a patch group instead?

6. Managing patch groups

What are they?

Suppose it’s Tuesday and Microsoft released a series of critical patches for Web services. The list includes a patch that was released three months ago, but with a different criticality level. Now it is listed at a higher level. So you read up on the issues related to the patch and determine it needs to be installed.

But you’re not sure if you installed it already or not. Sound familiar?

Now, you could just scan all your machines and slog through the information that is returned, or you could create a patch group that only looks for the patch, and only on Web servers at that!

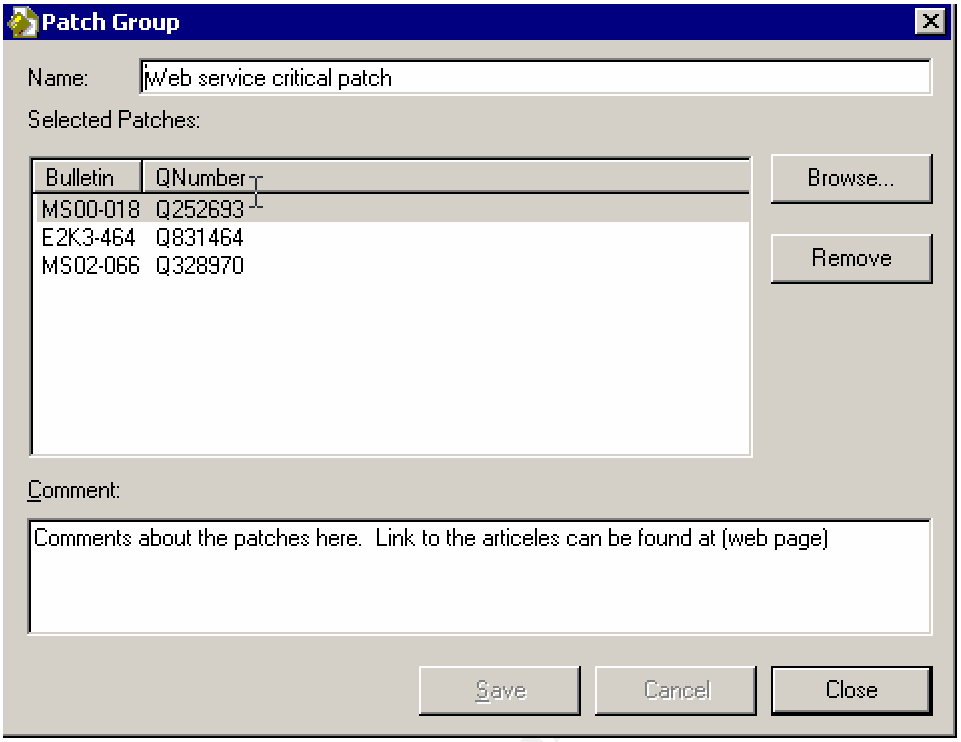
That is what patch groups do. They organize, and can then be used to scan for specific “Q” articles and their related patches. In the scenario above you’d create a patch group containing the “Q” article associated with the patch, then scan your Web servers. You’d then be able to see which servers did or did not have the patch installed.

Another great use for patch groups is using them to prove to management the value of patch management, as well as that the process is being done in a timely manner. When was the last time you got an e-mail from your boss asking if you had such and such a patch installed? Create a patch group, do the scan and give them a report.

Creating a new patch group

There are actually several ways to create a patch group within the product.

The quickest way is to select **New Patch Group** from the Navigator panel. Enter a name for the Patch group, then use the **Browse** button to locate the “Q” article number associated with the patch, or patches, you want to scan for. If you desire, add a comment, then click the **Save** button to create the group (Figure 32).



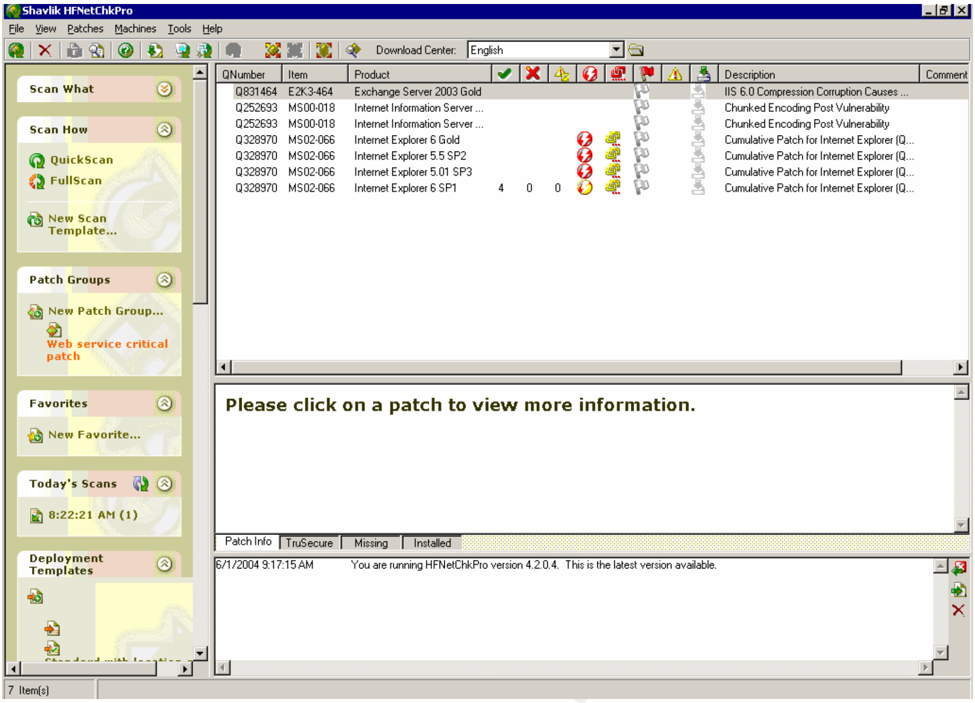
Web service critical patch

Bulletin	QNumber
MS00-018	Q252693
E2K3-464	Q831464
MS02-066	Q328970

Comments about the patches here. Link to the articeles can be found at (web page)

Figure 32

Notice something interesting here. I only selected three "Q" articles in my patch group. Yet this screen shows seven (Figure 33). What's going on here? Well if you look closely, you will see that one of the "Q" articles actually references five separate products – all of them a version of Internet Explorer.



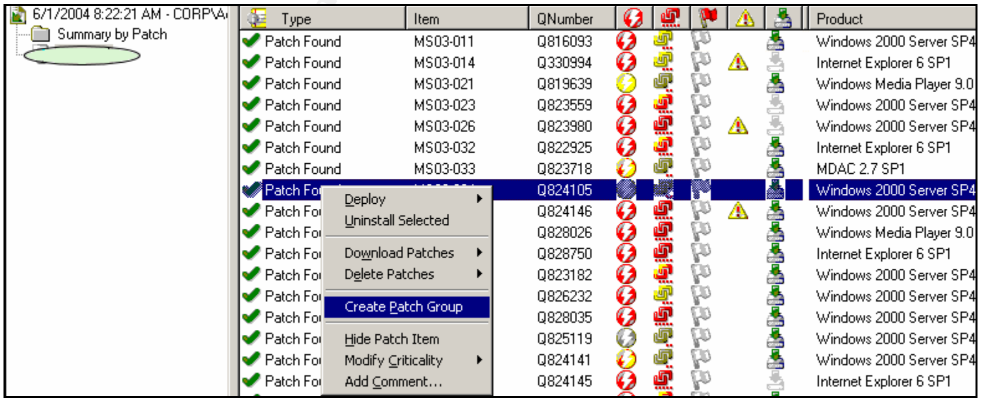
QNumber	Item	Product	✓	✗							Description	Comment
Q831464	E2K3-464	Exchange Server 2003 Gold									IIS 6.0 Compression Corruption Causes ...	
Q252693	MS00-018	Internet Information Server ...									Chunked Encoding Post Vulnerability	
Q252693	MS00-018	Internet Information Server ...									Chunked Encoding Post Vulnerability	
Q328970	MS02-066	Internet Explorer 6 Gold									Cumulative Patch for Internet Explorer (Q...	
Q328970	MS02-066	Internet Explorer 5.5 SP2									Cumulative Patch for Internet Explorer (Q...	
Q328970	MS02-066	Internet Explorer 5.01 SP3									Cumulative Patch for Internet Explorer (Q...	
Q328970	MS02-066	Internet Explorer 6 SP1	4	0	0						Cumulative Patch for Internet Explorer (Q...	

Please click on a patch to view more information.

```
6/1/2004 9:17:15 AM        You are running HFNetChkPro version 4.2.0.4.  This is the latest version available.
```

Figure 33

The other way to create a patch group is available after you have completed a scan. Once you see the results of your scan, you can right-click (SHIFT/CTRL click to select multiples) on a missing or installed patch, then select **Make Patch Group** from the resulting menu (Figure 34).



Type	Item	QNumber	Product
Patch Found	MS03-011	Q816093	Windows 2000 Server SP4
Patch Found	MS03-014	Q330994	Internet Explorer 6 SP1
Patch Found	MS03-021	Q819639	Windows Media Player 9.0
Patch Found	MS03-023	Q823559	Windows 2000 Server SP4
Patch Found	MS03-026	Q823980	Windows 2000 Server SP4
Patch Found	MS03-032	Q822925	Internet Explorer 6 SP1
Patch Found	MS03-033	Q823718	MDAC 2.7 SP1
Patch Fo		Q824105	Windows 2000 Server SP4
Patch Fo		Q824146	Windows 2000 Server SP4
Patch Fo		Q828026	Windows Media Player 9.0
Patch Fo		Q828750	Internet Explorer 6 SP1
Patch Fo		Q823182	Windows 2000 Server SP4
Patch Fo		Q826232	Windows 2000 Server SP4
Patch Fo		Q828035	Windows 2000 Server SP4
Patch Fo		Q825119	Windows 2000 Server SP4
Patch Fo		Q824141	Windows 2000 Server SP4
Patch Fo		Q824145	Internet Explorer 6 SP1

Figure 34

Using Patch Groups

Now that you have created a patch group, you can use it to scan any previously created machine group. Just click on the patch group you created and drag and drop it on a machine group. The **Run Scan** dialog box will appear. Select your options and run the scan. The results will show only the information related to the specific “Q” articles you selected as part of your patch group.

Best practices and lessons learned when creating and using patch groups

- When you create your patch groups you may want to put the “Q” article and a short summary in the name field. This makes it much easier to identify what the patch group is used for.
- You may want to consider putting a Web link to the “Q” article in the comment field of patch groups.

7. Managing deployment templates

What are they?

Deployment templates are nothing more than the collection of your desired settings for determining how patches are deployed. They include the actions that occur prior to, and after, patch installation.

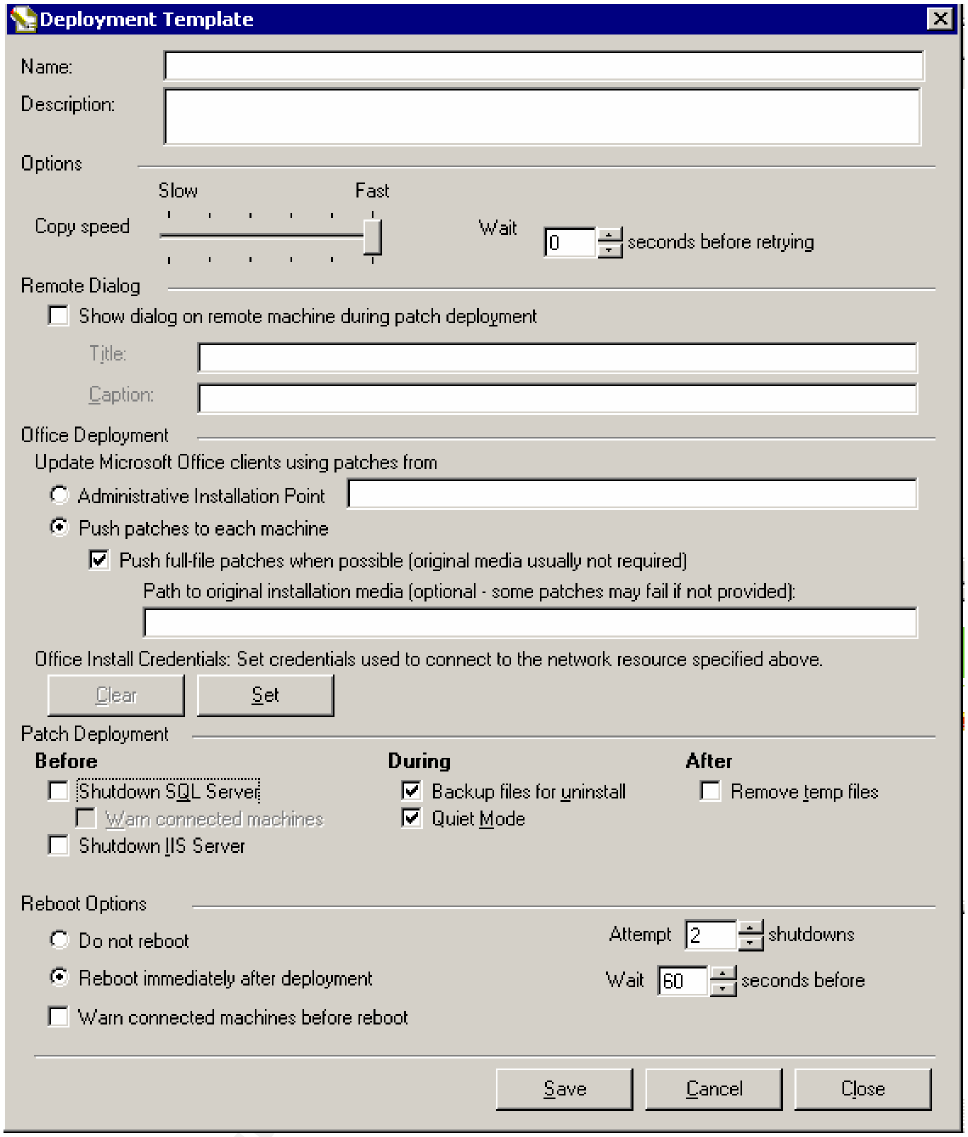
Creating a new deployment template

To create a new deployment template click **New Deployment Template.** Within a template you can configure the following (Figure 35):

- **Copy speed**. This setting controls the speed that files are copied to the target machine. Settings range from one to five, with five being the fastest. Remember the faster the copy speed, the more network bandwidth you will consume.
- **Retry period**. If the patch copy fails, this setting will configure a pause before the patch copy is attempted again. Values range from zero to 100 seconds.
- **Remote dialog**. Here you can type information that will appear within the pop-up dialog box on the target machine. Type a title for the pop-up box, and any text you want to display to your users.
- **Office Deployment options.** MICROSOFT OFFICE patches are handled differently than other patches. You need to have access to the original installation files/media when deploying OFFICE updates. You can do this via an Administrative installation point, or by pushing “full-file patches” to each machine. If you opt for the “full-file patches”, then you need to provide the UNC path to the original OFFICE installation files.

- **Office Install credentials** – If you are using the “full-file patches” option, you also need to provide credentials that the program will use to access the UNC path.
- **Patch deployment options**. Configure the before, during, and after actions of patch deployment. Options are grouped into the following areas:
  - **Before** – Shut down services.
  - **During** – Backup files so the patch can be uninstalled. If you choose, you can send out patches in quite mode, which gives no warning or visual clues to anyone using the remote machine.
  - **After** – Remove temporary files after installation.

- **Reboot options**. Configure the actions that take place after patches are installed. You can choose not to reboot, force a reboot or force a reboot with a warning to users. You can also set the number of attempted shutdowns.



Deployment Template

Name:

Description:

Options

Copy speed: Slow — Fast

Wait 0 seconds before retrying

Remote Dialog

□ Show dialog on remote machine during patch deployment

Title:

Caption:

Office Deployment

Update Microsoft Office clients using patches from

○ Administrative Installation Point

● Push patches to each machine

☑ Push full-file patches when possible (original media usually not required)

Path to original installation media (optional - some patches may fail if not provided):

Office Install Credentials: Set credentials used to connect to the network resource specified above.

Patch Deployment

Before

□ Shutdown SQL Server

□ Warn connected machines

□ Shutdown IIS Server

During

☑ Backup files for uninstall

☑ Quiet Mode

After

□ Remove temp files

Reboot Options

○ Do not reboot

● Reboot immediately after deployment

□ Warn connected machines before reboot

Attempt 2 shutdowns

Wait 60 seconds before

Figure 35

Best practices and lessons learned when creating and using deployment templates

- Always leave the **Backup Files for Uninstall** option selected. You want a way to back out your changes right?
- You may want to consider removing temporary files after each deployment. This does not impact the ability to remove any installed patches; it just cleans up disk space.
- Create a template with the path to your MICROSOFT OFFICE files. Use this template as your default template for all scans (set it in the OPTIONS panel).

8. Performing scans

Prerequisites

Before you can begin patching machines you need to ensure you have met the following requirements.

- Local Machine
  - You must be an Administrator.
  - You must be able to obtain the patch XML database file from the Internet, or locally on the network if you are running in *Disconnected* mode.
  - The Workstation service must be running.
- Remote machines
  - You must have local administrative rights, and the ability to log onto each machine.
  - File and Print Sharing must be turned on.
  - You must be able to access the remote machine using NetBIOS (TCP port 139) or Direct Host (TCP port 445.) These are critical ports to have opened if you plan to patch machines through a firewall.
  - The Server service must be running.
  - The Remote Registry service must be running.
  - The %systemroot% share must be available.

If you are at all concerned about having the Server service and Remote Registry services running on your remote machines see Shavlik's white paper entitled *Scanning Secured Machines Using IPSec Ports* at http://hfnetchk.shavlik.com/support/ipsec/ipsec_scan.htm.

Testing deployment – ensuring you can communicate with the selected machine(s)

How are you going to ensure you have met the above requirements? On the local machine it's easy. But on remote clients it might be a bit trickier. You could go to each machine and see the settings, or you could use **Test Deployment to…** to test your access – then fix any issues per machine.

The **Test Deployment to…** option is located under the TOOLS menu. When prompted, type an IP address or a machine name. Click **OK**, type the credentials you want to use, then click **OK** to begin the test. When the test is completed you will receive a report with the results. Information in the report looks like this:

```
Test Deployment

Good: Localhost is running the Workstation Service
Good: Localhost is running NetBios or Direct Host services enabled

********** Test machine name **********

Test 1) machine name- Good: You are an administrator on this computer using specified
credentials.
Test 2) machine name - Good: remote computer is running Remote Registry Service
Test 3) machine name - Good: remote computer is running Server Service
Test 4) machine name - Good: remote computer is running Workstation Service
Test 5) machine name - Good: remote computer is running NetBIOS or Direct Host
services.
Test 6) machine name - Good: You can access the remote registry on this computer
Test 7) machine name - Good: You can access the remote computer's Workstation
Information
Test 8) machine name - Note: User(s) logged in on the remote computer:
        >user name
        >user name
Test 9) machine name - Good: the Scheduler is running on the remote computer.
Test 10) machine name - Good: created remote directory for copying test updates
Test 11) machine name - Good: copied test update files
Test 12) machine name - Good: remote task was successfully scheduled.
Test 13) machine name -   Scheduler Log:
*****
machine name - Overall grade of Pass.  Patch installation is possible.
```

Review the report and, when necessary, correct any errors. The report always gives clues how to resolve any issues it finds.

Performing a Scan

Let's go ahead and perform our first scan. You can do this a couple of ways.

HFNETCHKPRO supports drag-and-drop functionality, which we have seen used with patch groups. The process is much the same for starting a scan. To start a scan of a machine group simply drag-and-drop a scan method (Quick, Full, one you created) onto an existing machine group (Figure 35). You can also do the opposite, drag the machine group to the scan method. After doing that you will see the **RUN SCAN** dialog box.

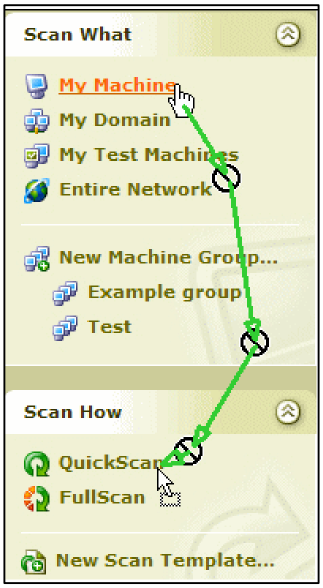
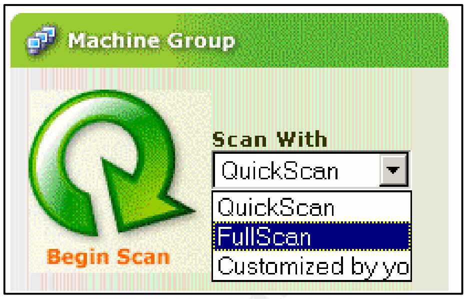


Figure 35[38]

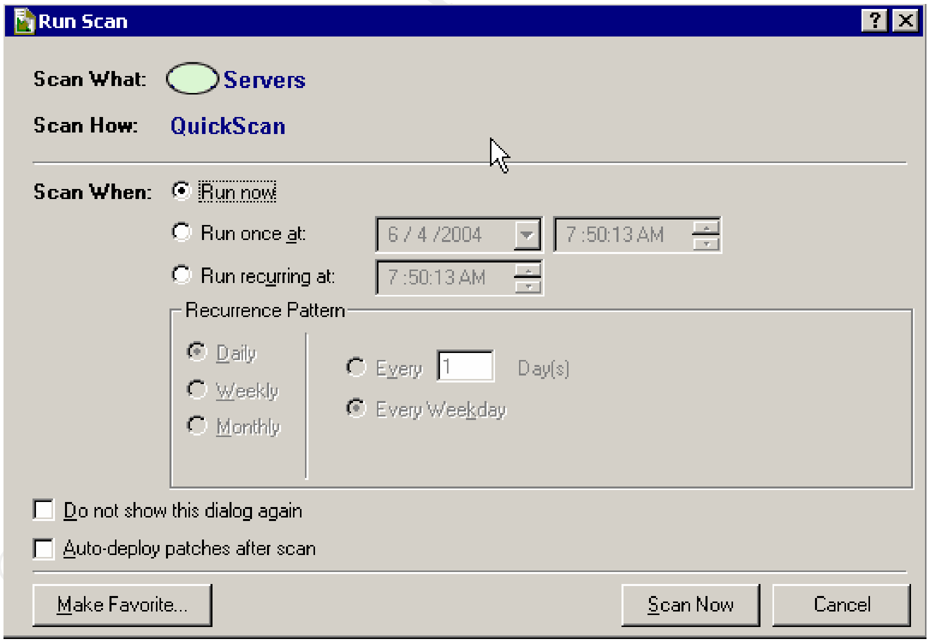
[38] http://hfnetchk.shavlik.com/support/hfpro4help/Drag_and_drop_scanning_sample.gif

The other way to start a scan is to select a machine group from the **NAVIGATOR PANEL**. The **INFORMATION AREA** will display the properties of the machine group. To run a scan, use the drop-down list to select a scan method (Quick, Full, one you created.) Click **Begin Scan**. You will now see the **RUN SCAN** dialog box.



The **RUN SCAN** dialog box (Figure 36) gives you a few options to choose from.

- **Run Now** – Begin the scan immediately using the **Scan Now** button. Note that you can auto deploy patches by clicking the checkbox.
- **Run Once At** – Use this option to schedule a one time scan.
- **Run Recurring at** – Schedule a job based on reoccurrence patterns (see automating the process below).



Run Scan

Scan What: Servers

Scan How: QuickScan

Scan When: ● Run now

○ Run once at: 6 / 4 /2004 7 :50:13 AM

○ Run recurring at: 7 :50:13 AM

Recurrence Pattern

● Daily ○ Weekly ○ Monthly

○ Every 1 Day(s)

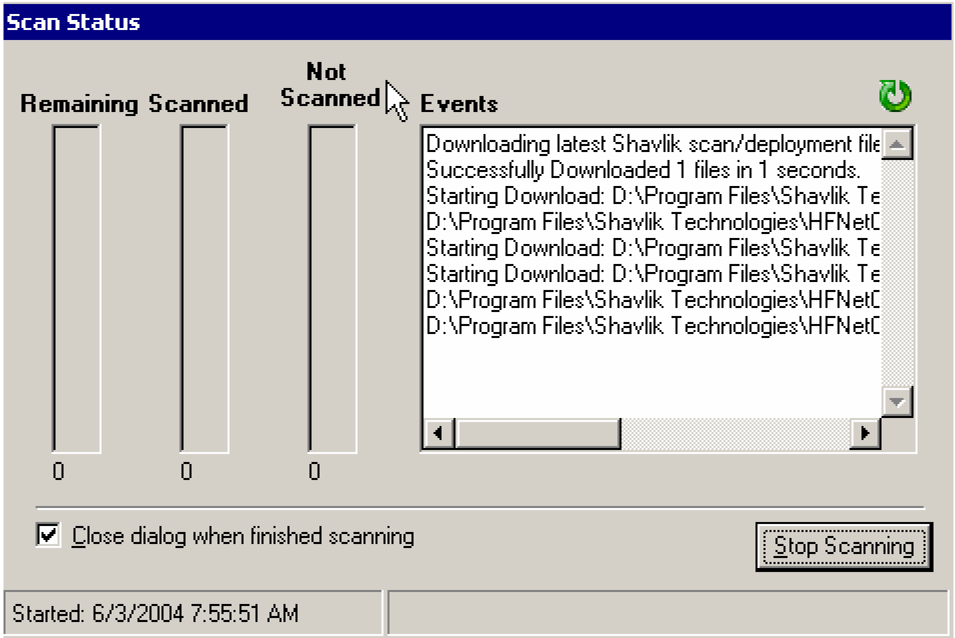
● Every Weekday

□ Do not show this dialog again

□ Auto-deploy patches after scan

Figure 36

After clicking **Scan Now**, you will see the **Scan Status** dialog box (Figure 37). This box shows you the processes occurring during the scan.



```
Downloading latest Shavlik scan/deployment file
Successfully Downloaded 1 files in 1 seconds.
Starting Download: D:\Program Files\Shavlik Te
D:\Program Files\Shavlik Technologies\HFNetC
Starting Download: D:\Program Files\Shavlik Te
Starting Download: D:\Program Files\Shavlik Te
D:\Program Files\Shavlik Technologies\HFNetC
D:\Program Files\Shavlik Technologies\HFNetC
```

Started: 6/3/2004 7:55:51 AM

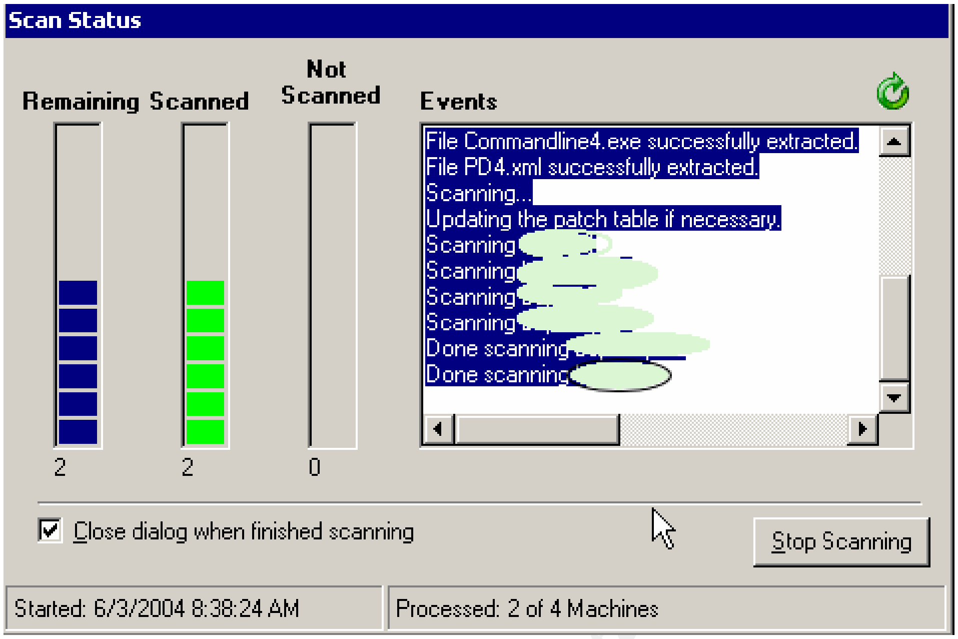
Figure 37

The **Events** area details what is happening in the background. Information that occurs here looks like this:

```
Downloading latest Shavlik scan/deployment files...
Successfully Downloaded 1 files in 1 seconds.
Starting Download: D:\Program Files\Shavlik
Technologies\HFNetChkPro4\Patches\en-us\hftoolver.txt
D:\Program Files\Shavlik Technologies\HFNetChkPro4\Patches\en-
us\hftoolver.txt
Starting Download: D:\Program Files\Shavlik
Technologies\HFNetChkPro4\ShavlikDataFiles\Commandline4.cab
Starting Download: D:\Program Files\Shavlik
Technologies\HFNetChkPro4\ShavlikDataFiles\PD4.cab
D:\Program Files\Shavlik
Technologies\HFNetChkPro4\ShavlikDataFiles\Commandline4.cab
D:\Program Files\Shavlik
Technologies\HFNetChkPro4\ShavlikDataFiles\PD4.cab
File Complete: D:\Program Files\Shavlik
Technologies\HFNetChkPro4\ShavlikDataFiles\Commandline4.cab
File: Commandline4.cab successfully downloaded.
File Complete: D:\Program Files\Shavlik
Technologies\HFNetChkPro4\ShavlikDataFiles\PD4.cab
File: PD4.cab successfully downloaded.
File Commandline4.exe successfully extracted.
File PD4.xml successfully extracted.
Scanning...
Updating the patch table if necessary.
Updating the patch table - phase 1.
Updating the patch table - phase 2 - Please be patient.
Updating patch information for Windows Server 2003, Standard Edition Gold
Updating patch information for Windows Server 2003, Enterprise Edition Gold
Updating patch information for Windows Server 2003, Datacenter Edition Gold
Updating patch information for Windows Server 2003, Web Edition Gold
Updating patch information for Windows Server 2003 for Small Business Server Gold
Updating patch information for Windows XP Home Edition Gold
Updating patch information for Windows XP Home Edition SP1
Updating patch information for Windows XP Professional Gold
Updating patch information for Windows XP Professional SP1
Updating patch information for Windows 2000 Professional Gold
Updating patch information for Windows 2000 Professional SP1
Updating patch information for Windows 2000 Professional SP2
Updating patch information for Windows 2000 Professional SP3
Updating patch information for Windows 2000 Professional SP4
Updating patch information for Windows 2000 Server Gold
Updating patch information for Windows 2000 Server SP1
Updating patch information for Windows 2000 Server SP2
Updating patch information for Windows 2000 Server SP3
Updating patch information for Windows 2000 Server SP4
Updating patch information for Windows 2000 Advanced Server Gold
Updating patch information for Windows 2000 Advanced Server SP1
Updating patch information for Windows 2000 Advanced Server SP2
Updating patch information for Windows 2000 Advanced Server SP3
Updating patch information for Windows 2000 Advanced Server SP4
Updating patch information for Small Business Server 2000 Gold
Etc……
```

The first set of downloads and extracts happens each time you perform a scan. The next step, updating the patch table, only happens when necessary. So, you may not see it each time.

The left-hand side of the **Scan Status** box displays the status of the machines being scanned. The colored bars represent machines that are remaining to be scanned, those that are completed and those that were not scanned. The **Events** area will also show you this information in text form (Figure 38).



File Commandline4.exe successfully extracted.
File PD4.xml successfully extracted.
Scanning...
Updating the patch table if necessary.
Scanning
Scanning
Scanning
Scanning
Done scanning
Done scanning

Started: 6/3/2004 8:38:24 AM
Processed: 2 of 4 Machines

Figure 38

Automating the process – using the Windows Scheduler service

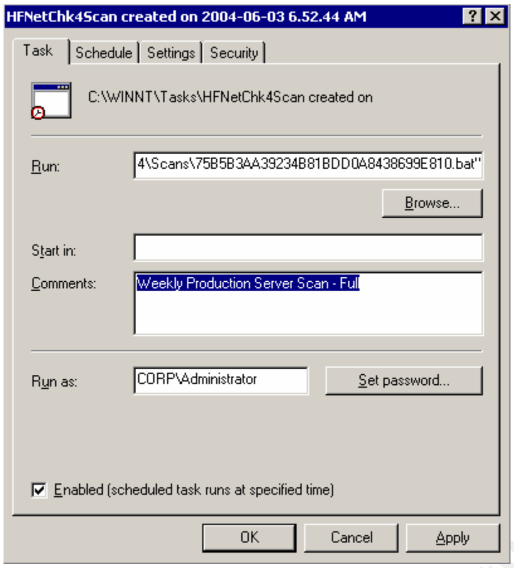
A simple, yet powerful automation ability exists within the product. HFNETCHKPRO leverages the capabilities of the Windows Scheduler service to automate the scanning process. Doing this is fairly straightforward.

First off, you have to have created a machine group. Select the machine group you want to schedule a scan for. From the properties window of the group, select a method for scanning (Quick, Full or a customized scan). Click **Begin Scan**. This will bring up the familiar **RUN SCAN** dialog box.

To schedule a scan, select either the **Run Once At**, or the **Run Recurring at** options. With either option selected, you now have the ability use the Schedule button at the bottom of the **RUN SCAN** dialog box.

You will be prompted to create the scan as a Favorite. Type a descriptive name in the provided fields, and then click **OK**. Type the credentials you want the scan to run with, and then click **OK.** You are notified that the scan has successfully been scheduled, and that to review settings, you will need to open SCHEDULED TASKS. SCHEDULED TASKS is found under the CONTROL PANELS applet.

Let's open SCHEDULED TASKS and examine our scan. You can see the scan listed within the SCHEDULED TASKS window. Right-click on the task, select **Properties**. Notice that you can change the account that runs the scheduled task (Figure 39). If the account that you are using has a password change, be sure to come back in here and change the password, or your automated scans will not work. Using the **Schedule tab** you can modify how often the task will run (Figure 40). It is possible to make changes to any previously created scheduled task.



HFNetChk4Scan created on 2004-06-03 6.52.44 AM

C:\WINNT\Tasks\HFNetChk4Scan created on

Run: 4\Scans\75B5B3AA39234B81BDD0A8438699E810.bat"

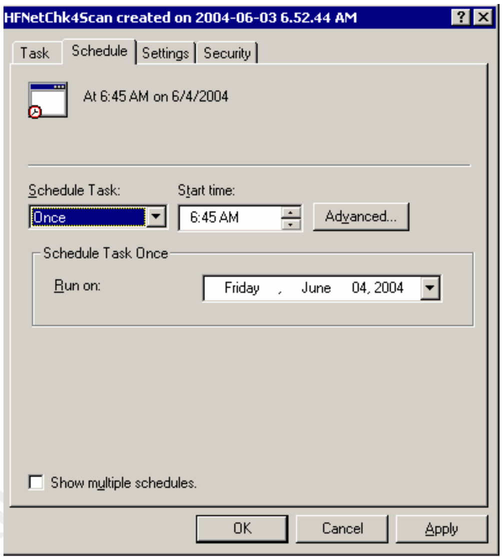
Start in:

Comments: Weekly Production Server Scan - Full

Run as: CORP\Administrator

☑ Enabled (scheduled task runs at specified time)

Figure 39



HFNetChk4Scan created on 2004-06-03 6.52.44 AM

At 6:45 AM on 6/4/2004

Schedule Task: Once

Start time: 6:45 AM

Schedule Task Once

Run on: Friday , June 04, 2004

☐ Show multiple schedules.

Figure 40

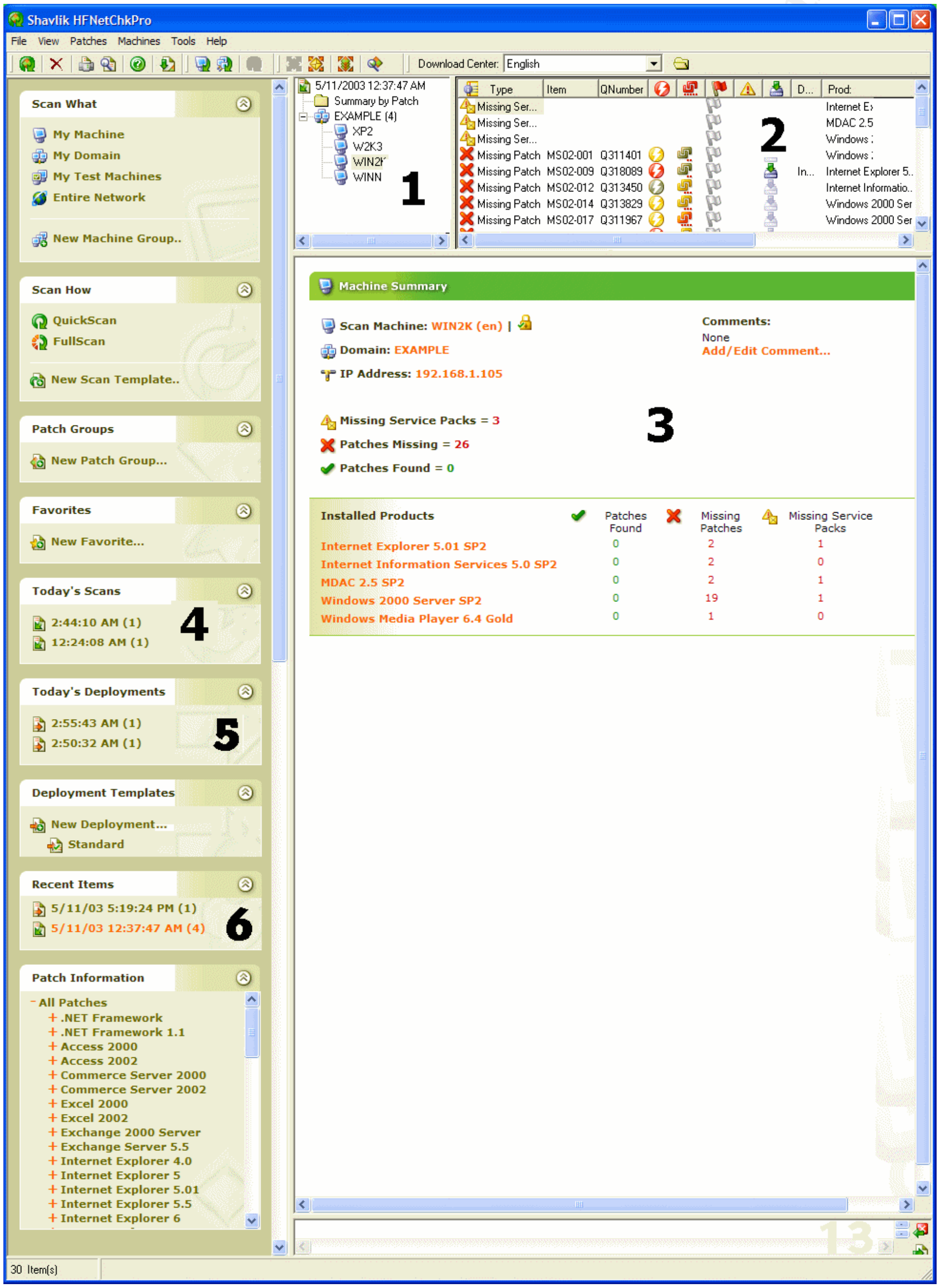
Best practices and lessons learned during scans

- Use the COMPUTER MANAGEMENT MMC console to connect to remote Windows machines and enable any prerequisite services. Or, use customized login scripts to enable critical services.
- Leverage the power of automation. Windows Scheduler is your friend. With it you can perform nightly scans and have the results waiting for you when you return the next day.
- By default the Scheduler service only states that a job was scheduled by HFNETCHKPRO. It does not really give you any details about the scan itself. Open the properties of the scan and type information about the scan in the *comments* field. You will also want to rename the scheduled task itself. When you have a list of scheduled jobs this becomes important, otherwise they all say "HFNetChk4Scan created on …"
- Practice Defense-in-Depth. HFNETCHKPRO is a powerful product. But you should never rely on just one product, or process, to stay current with patches and service packs. In my experience, occasionally, the product will report incorrectly that a patch has been applied, even though it has not. So, have a backup plan. Use another product to validate that patches are installed. I have found that using a combination of WINDOWS UPDATE and NESSUS works well.

9. Interpreting results

The Scanning Interface

When a scan has completed, the view will change from the HOME PAGE to the SCANNING INTERFACE. Let's examine what is shown in this view (Figure 41).



Type	Item	QNumber	D...	Prod:
Missing Ser...				Internet E›
Missing Ser...				MDAC 2.5
Missing Ser...				Windows :
Missing Patch	MS02-001	Q311401		Windows :
Missing Patch	MS02-009	Q318089	In...	Internet Explorer 5..
Missing Patch	MS02-012	Q313450		Internet Informatio..
Missing Patch	MS02-014	Q313829		Windows 2000 Ser
Missing Patch	MS02-017	Q311967		Windows 2000 Ser

Machine Summary

Scan Machine: WIN2K (en) |

Domain: EXAMPLE

IP Address: 192.168.1.105

Comments:
None
Add/Edit Comment...

Missing Service Packs = 3

Patches Missing = 26

Patches Found = 0

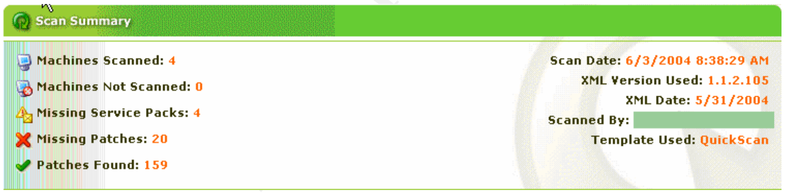
Installed Products	✓ Patches Found	✗ Missing Patches	Missing Service Packs
Internet Explorer 5.01 SP2	0	2	1
Internet Information Services 5.0 SP2	0	2	0
MDAC 2.5 SP2	0	2	1
Windows 2000 Server SP2	0	19	1
Windows Media Player 6.4 Gold	0	1	0

Figure 41[39]

1. **Summary of scanned machines** – There are two possible ways to view information in this pane. They are covered in more detail below
   - Summary by patch
   - Summary by machine

2. **Summary details** – Information in this view changes depending upon what you have selected in the SUMMARY OF SCANNED MACHINES pane. If you select:

   - **Scan summary** (Figure 42) – This shows a summary of <u>all</u> the machines within the group that were scanned. Information here includes: when the scan occurred, the date of the XML file used, how many machines were scanned and not scanned, the number of missing service packs, missing patches and patches that were found.



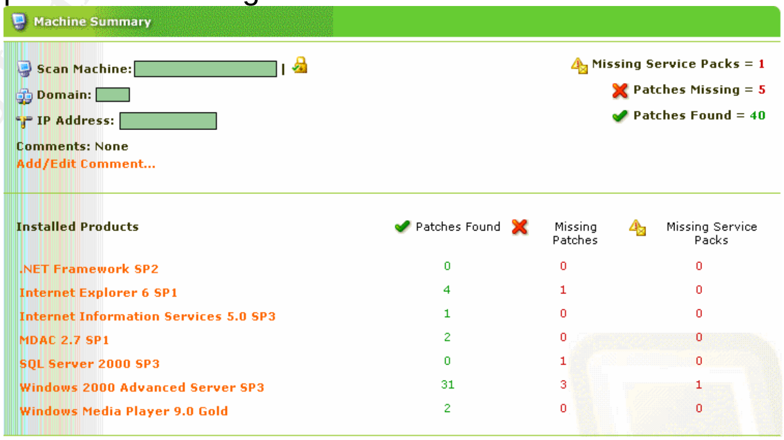
Scan Summary

Machines Scanned: 4
Machines Not Scanned: 0
Missing Service Packs: 4
Missing Patches: 20
Patches Found: 159

Scan Date: 6/3/2004 8:38:29 AM
XML Version Used: 1.1.2.105
XML Date: 5/31/2004
Scanned By: [redacted]
Template Used: QuickScan

Figure 42

   - **Machine summary** (Figure 43) – This shows a summary of a specific machine. Information here includes: the machine name and IP address, who scanned it, a graphic detailing what patches were found or are missing, and what service packs are missing.



Machine Summary

Scan Machine: [redacted] |
Domain: [redacted]
IP Address: [redacted]
Comments: None
Add/Edit Comment...

Missing Service Packs = 1
Patches Missing = 5
Patches Found = 40

Installed Products	✓ Patches Found	✗ Missing Patches	Missing Service Packs
.NET Framework SP2	0	0	0
Internet Explorer 6 SP1	4	1	0
Internet Information Services 5.0 SP3	1	0	0
MDAC 2.7 SP1	2	0	0
SQL Server 2000 SP3	0	1	0
Windows 2000 Advanced Server SP3	31	3	1
Windows Media Player 9.0 Gold	2	0	0

Figure 43

[39] http://hfnetchk.shavlik.com/support/hfpro4help/Scanning_interface.gif (NOTE: Image has been modified with new numbers.)

3. **Today's scans** – Provides a link to each scan you have performed today. This is where any automated scans would appear.

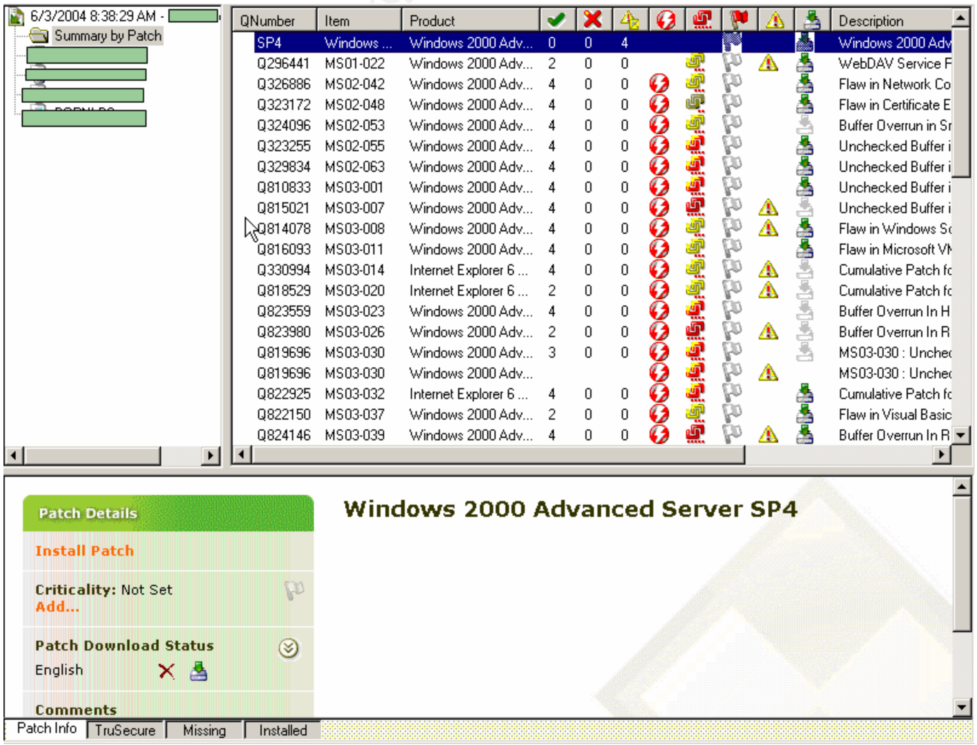
4. **Today's Deployments** – Provides a link to each deployment you have made today.

5. **Recent Items** – contains links to any scans or deployments that occurred in the past.

Summary by patch

When you select **SUMMARY BY PATCH**, you get detailed information about patches and service packs for the entire group. The key point to remember here is that you are not examining the results for one machine, but the group as a whole.

Here is an example of the **SUMMARY BY PATCH** screen for a scan of four servers (Figure 44). The servers that were scanned are listed on the left-hand side of the screen. The SUMMARY pane contains a list of all patches and service packs related to the scanned machines. Selecting a service pack, or patch, from this list changes the PATCH DETAILS pane at the bottom of the screen. Now specific details about the selected item are displayed.



6/3/2004 8:38:29 AM -
Summary by Patch
[redacted]

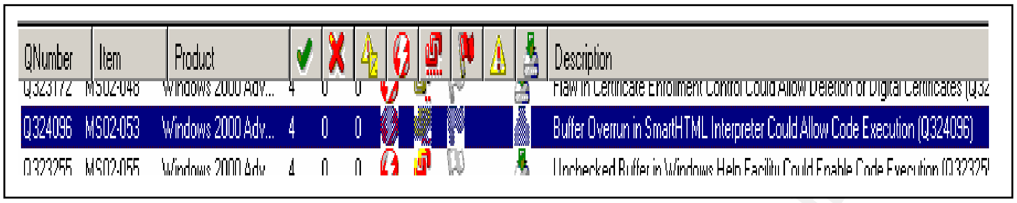
QNumber	Item	Product	✓	✗		⚠	Description
SP4	Windows ...	Windows 2000 Adv...	0	0	4		Windows 2000 Adv
Q296441	MS01-022	Windows 2000 Adv...	2	0	0	⚠	WebDAV Service F
Q326886	MS02-042	Windows 2000 Adv...	4	0	0		Flaw in Network Co
Q323172	MS02-048	Windows 2000 Adv...	4	0	0		Flaw in Certificate E
Q324096	MS02-053	Windows 2000 Adv...	4	0	0		Buffer Overrun in Sr
Q323255	MS02-055	Windows 2000 Adv...	4	0	0		Unchecked Buffer i
Q329834	MS02-063	Windows 2000 Adv...	4	0	0		Unchecked Buffer i
Q810833	MS03-001	Windows 2000 Adv...	4	0	0		Unchecked Buffer i
Q815021	MS03-007	Windows 2000 Adv...	4	0	0	⚠	Unchecked Buffer i
Q814078	MS03-008	Windows 2000 Adv...	4	0	0	⚠	Flaw in Windows Sc
Q816093	MS03-011	Windows 2000 Adv...	4	0	0		Flaw in Microsoft VI
Q330994	MS03-014	Internet Explorer 6 ...	4	0	0	⚠	Cumulative Patch fc
Q818529	MS03-020	Internet Explorer 6 ...	2	0	0	⚠	Cumulative Patch fc
Q823559	MS03-023	Windows 2000 Adv...	4	0	0		Buffer Overrun In H
Q823980	MS03-026	Windows 2000 Adv...	2	0	0	⚠	Buffer Overrun In R
Q819696	MS03-030	Windows 2000 Adv...	3	0	0		MS03-030 : Unchec
Q819696	MS03-030	Windows 2000 Adv...				⚠	MS03-030 : Unchec
Q822925	MS03-032	Internet Explorer 6 ...	4	0	0		Cumulative Patch fc
Q822150	MS03-037	Windows 2000 Adv...	2	0	0		Flaw in Visual Basic
Q824146	MS03-039	Windows 2000 Adv...	4	0	0	⚠	Buffer Overrun In R

Patch Details
Install Patch
Criticality: Not Set
Add...
Patch Download Status
English ✗
Comments

Windows 2000 Advanced Server SP4

Figure 44

Let's take a look at the information that is displayed when we select a specific patch from the SUMMARY pane. In the following example I've selected Q324096 from the list of patches (Figure 45).



QNumber	Item	Product	✓	✗							Description
Q323172	MS02-048	Windows 2000 Adv...	4	0	0						Flaw in Certificate Enrollment Control Could Allow Deletion of Digital Certificates (Q32
Q324096	MS02-053	Windows 2000 Adv...	4	0	0						Buffer Overrun in SmartHTML Interpreter Could Allow Code Execution (Q324096)
Q323255	MS02-055	Windows 2000 Adv...	4	0	0						Unchecked Buffer in Windows Help Facility Could Enable Code Execution (Q32325

Figure 45

Across the top of the SUMMARY DETAILS pane you see a toolbar with a series of icons. Information in each row below the icons represents details about the items that are listed.

- QNumber – This column displays the "Q" number that Microsoft has assigned the patch or service pack. "Q" articles are found online in the MICROSOFT KNOWLEDGEBASE. Using this number, you can search the Knowledgebase for more information related to the patch or service pack.

- Item – This column displays the Security Bulletin ID number that Microsoft has assigned to the patch or service pack.

- Product – This column displays the name of the product that the patch or service pack affects.

- ✓ - The value in this column represents the number of times a patch was found installed on the machines in the group.

- ✗ - The value in this column represents the number of times a patch was determined missing from the machines in the group.

- ⚠ - The value in this column represents the number of times a service pack was determined to be missing from the machines in the group.

- ⚡ - Icons in this column display the level of severity that Microsoft assigned to the patch or service pack. Severity levels will be one of the following:
  - Critical
  - Important
  - Moderate

Low

- ⚑ - Icons in this column represent the criticality value that you, or your company, have defined for this patch or service pack. Severity levels will be one of the following:

  Critical
  High
  Medium
  Low
  Ignore
  Criticality not set

- ⚠ - The icon in this column lets you know that Shavlik's technicians have provided important information about the patch or service pack. To display the notes, "hover" your mouse over the icon.

- - The icon in this column displays whether the patch has been downloaded. If the icon is green, the patch has been downloaded. If the icon is grayed-out, then the patch has not been downloaded. Icons are only green if the downloaded patch has been digitally signed by Microsoft.

As you can see, you can glean a huge amount of information about patches and service packs, just by examining the information in the columns of the SUMMARY DETAILS pane.

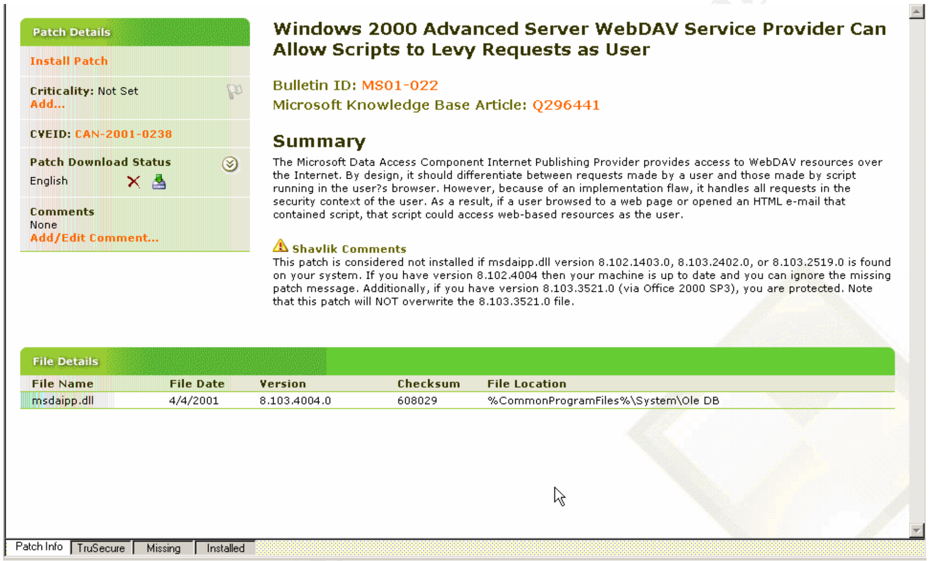
But, if you want to delve a bit deeper into the details of a specific patch or service pack, you need to examine the information shown in the PATCH DETAILS pane. When you select a particular patch, or service pack, comprehensive information about it is shown in the PATCH DETAILS pane. The PATCH DETAILS pane has three tabs along the bottom to display a variety of information.

By default the PATCH DETAILS pane opens to the **Patch Info** tab (Figure 46). This tab contains the following information, about the selected patch or service pack.

- **Bulletin ID** – The Security Bulletin ID number that Microsoft has assigned to the patch or service pack. Clicking the number will open an Internet connection to the article on TECHNET.
- **Microsoft Knowledgebase Article** – The "Q" number that Microsoft has assigned the patch or service pack. Clicking the Q

number will open an Internet connection to the Microsoft Knowledgebase.

- **Criticality** – The criticality value that you, or your company, have defined for this patch or service pack. Click **Add** to assign your own criticality level.
- **Patch Download Status** – Displays whether the patch has been downloaded, and if it has, what language(s) are available. You can download the file by clicking **Download**.
- **Comments** – You have the ability to add any of your own comments about the patch or service pack.



Patch Details

Install Patch

Criticality: Not Set
Add...

CVEID: CAN-2001-0238

Patch Download Status
English ✕

Comments
None
Add/Edit Comment...

Windows 2000 Advanced Server WebDAV Service Provider Can Allow Scripts to Levy Requests as User

Bulletin ID: MS01-022
Microsoft Knowledge Base Article: Q296441

Summary

The Microsoft Data Access Component Internet Publishing Provider provides access to WebDAV resources over the Internet. By design, it should differentiate between requests made by a user and those made by script running in the user?s browser. However, because of an implementation flaw, it handles all requests in the security context of the user. As a result, if a user browsed to a web page or opened an HTML e-mail that contained script, that script could access web-based resources as the user.

⚠ Shavlik Comments
This patch is considered not installed if msdaipp.dll version 8.102.1403.0, 8.103.2402.0, or 8.103.2519.0 is found on your system. If you have version 8.102.4004 then your machine is up to date and you can ignore the missing patch message. Additionally, if you have version 8.103.3521.0 (via Office 2000 SP3), you are protected. Note that this patch will NOT overwrite the 8.103.3521.0 file.

File Details

File Name	File Date	Version	Checksum	File Location
msdaipp.dll	4/4/2001	8.103.4004.0	608029	%CommonProgramFiles%\System\Ole DB

Figure 46

Just a quick note here about the screen shot. At the time I was writing this, Shavlik released a major version upgrade. The newest version (4.3.0 at the time of writing) removes the following functionality that you see listed on the screen shot.

- **Information from TruSecure** – 3rd party assessment of threat levels.
- **CVEID** - the CVE number assigned to the problem the patch or service pack is addressing. CVE "is a list of standardized names for vulnerabilities and other information security exposures - CVE aims to standardize the names for all publicly known vulnerabilities and security exposures."[40] Clicking the CVE number opened an Internet connection to the CVE database.
- **Bugtraq ID** – the Bugtraq number assigned to the problem the patch or service pack is addressing. Bugtraq "is a high volume, full disclosure mailing list for the detailed discussion and

[40] Common Vulnerabilities and Exposures. About CVE. 2/4/04.

> announcement of computer security vulnerabilities."[41] Clicking the ID number opened an Internet connection to the Security Focus Web site.

As an editorial comment I'll say that I'm disappointed that this information was dropped from the interface. I understand how company agreements can change, so the loss of TruSecure is understandable. But having CVE and BUGTRAQ information was very useful form a research perspective. Of course, you can still get this information, but it was easier when the links were right in the product. My hope is that they will add this information back in with future updates.

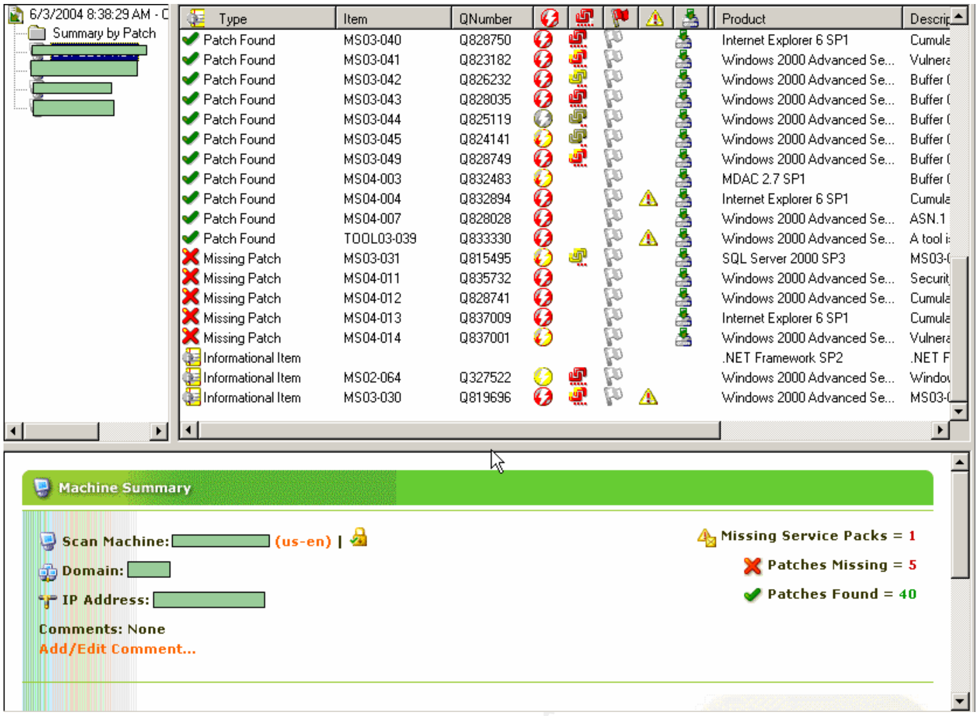
The remaining two tabs in the patch details pane are **Missing** and **Installed**. As you might have guessed from their names, both tabs show a detailed list of which machine(s) have the patch installed or not installed.

Summary by specific machine

When you select **SUMMARY BY MACHINE**, you get details for a specific machine, not the entire group. The views change a bit, but as you will see, the information is relatively similar.

Here is an example of the **SUMMARY BY MACHINE** screen. I've used the same machine group of four servers that I used before (Figure 47). Note the similarities to the **SUMMARY BY PATCH** view. The servers that were scanned are still listed on the left-hand side of the screen. The difference though, (and it might be hard to see because I covered the server name to protect the innocent, or guilty if you prefer) is that I have selected only one of the servers. The SUMMARY pane now contains details about all of patches and service packs related to that machine. Notice that we still have the familiar icons across the top of the window; they are just in a different order.

[41] Security Focus.



6/3/2004 8:38:29 AM - C
Summary by Patch
[redacted]

Type	Item	QNumber	⚠	Product	Descrip
✓ Patch Found	MS03-040	Q828750		Internet Explorer 6 SP1	Cumula
✓ Patch Found	MS03-041	Q823182		Windows 2000 Advanced Se...	Vulnera
✓ Patch Found	MS03-042	Q826232		Windows 2000 Advanced Se...	Buffer (
✓ Patch Found	MS03-043	Q828035		Windows 2000 Advanced Se...	Buffer (
✓ Patch Found	MS03-044	Q825119		Windows 2000 Advanced Se...	Buffer (
✓ Patch Found	MS03-045	Q824141		Windows 2000 Advanced Se...	Buffer (
✓ Patch Found	MS03-049	Q828749		Windows 2000 Advanced Se...	Buffer (
✓ Patch Found	MS04-003	Q832483		MDAC 2.7 SP1	Buffer (
✓ Patch Found	MS04-004	Q832894	⚠	Internet Explorer 6 SP1	Cumula
✓ Patch Found	MS04-007	Q828028		Windows 2000 Advanced Se...	ASN.1
✓ Patch Found	TOOL03-039	Q833330	⚠	Windows 2000 Advanced Se...	A tool i:
✗ Missing Patch	MS03-031	Q815495		SQL Server 2000 SP3	MS03-(
✗ Missing Patch	MS04-011	Q835732		Windows 2000 Advanced Se...	Securit
✗ Missing Patch	MS04-012	Q828741		Windows 2000 Advanced Se...	Cumula
✗ Missing Patch	MS04-013	Q837009		Internet Explorer 6 SP1	Cumula
✗ Missing Patch	MS04-014	Q837001		Windows 2000 Advanced Se...	Vulnera
Informational Item				.NET Framework SP2	.NET F
Informational Item	MS02-064	Q327522		Windows 2000 Advanced Se...	Windov
Informational Item	MS03-030	Q819696	⚠	Windows 2000 Advanced Se...	MS03-(

Machine Summary

Scan Machine: [redacted] (us-en) |
Domain: [redacted]
IP Address: [redacted]
Comments: None
Add/Edit Comment...

⚠ Missing Service Packs = 1
✗ Patches Missing = 5
✓ Patches Found = 40

Figure 47

The only real difference between this view, and the SUMMARY BY PATCH view, is that there is a new column called **Type**. This column displays the following information:

- ⚠ Missing Service Pack – Notifies you that this Service Pack is missing from the system. Unless you modify the display order, service packs are always at the top of the list.

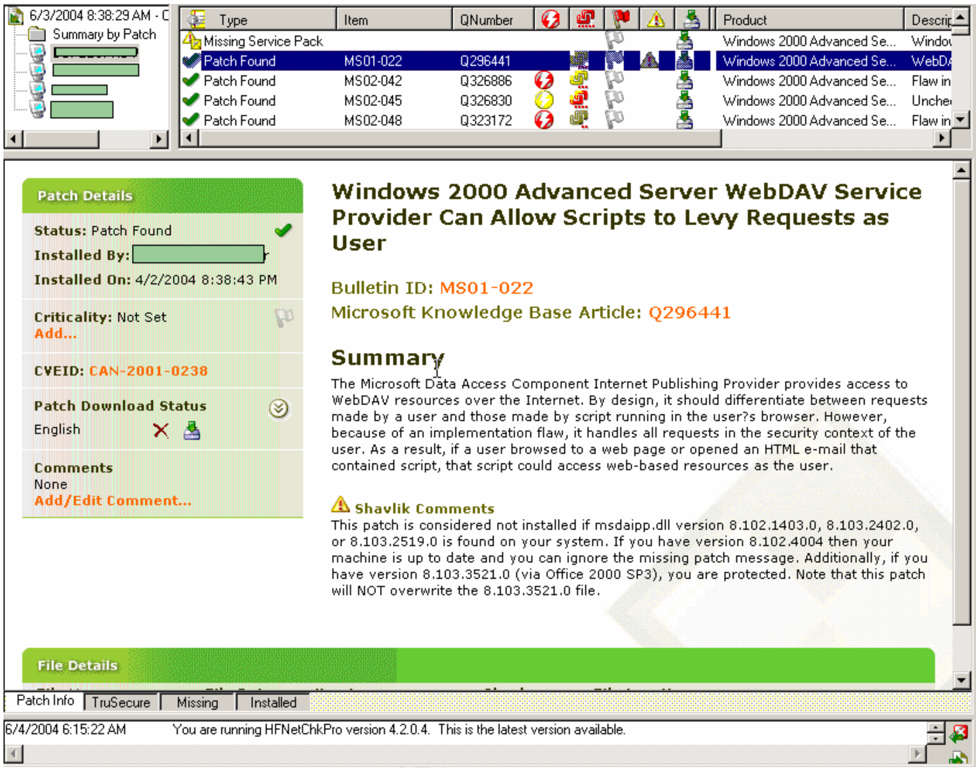
- ✓ Patch Found – Notifies you that this patch was found on the system.

- ✗ Missing Patch – Notifies you that this patch was not found on the system.

- Informational Item – Just what they say they are. For example, you might see an informational item letting you know that the default permissions for the machine could potentially allow a Trojan Horse program access, with directions how to fix the issue.

At the bottom of the screen, the MACHINE SUMMARY pane replaces the PATCH DETAILS pane. With a machine selected, you get a high level overview of number of patches that are either missing or found, and the number of missing service packs.

Selecting a specific patch, or service pack, from the SUMMARY pane changes the view from MACHINE SUMMARY, to the familiar PATCH DETAILS pane.



6/3/2004 8:38:29 AM - C
Summary by Patch
[redacted]
[redacted]
[redacted]
[redacted]

Type	Item	QNumber	Product	Descrip
Missing Service Pack			Windows 2000 Advanced Se...	Windo
Patch Found	MS01-022	Q296441	Windows 2000 Advanced Se...	WebD
Patch Found	MS02-042	Q326886	Windows 2000 Advanced Se...	Flaw in
Patch Found	MS02-045	Q326830	Windows 2000 Advanced Se...	Unche
Patch Found	MS02-048	Q323172	Windows 2000 Advanced Se...	Flaw in

Patch Details

Status: Patch Found ✓
Installed By: [redacted]
Installed On: 4/2/2004 8:38:43 PM

Criticality: Not Set
Add...

CVEID: CAN-2001-0238

Patch Download Status
English

Comments
None
Add/Edit Comment...

Windows 2000 Advanced Server WebDAV Service Provider Can Allow Scripts to Levy Requests as User

Bulletin ID: MS01-022
Microsoft Knowledge Base Article: Q296441

Summary
The Microsoft Data Access Component Internet Publishing Provider provides access to WebDAV resources over the Internet. By design, it should differentiate between requests made by a user and those made by script running in the user?s browser. However, because of an implementation flaw, it handles all requests in the security context of the user. As a result, if a user browsed to a web page or opened an HTML e-mail that contained script, that script could access web-based resources as the user.

⚠ Shavlik Comments
This patch is considered not installed if msdaipp.dll version 8.102.1403.0, 8.103.2402.0, or 8.103.2519.0 is found on your system. If you have version 8.102.4004 then your machine is up to date and you can ignore the missing patch message. Additionally, if you have version 8.103.3521.0 (via Office 2000 SP3), you are protected. Note that this patch will NOT overwrite the 8.103.3521.0 file.

File Details

6/4/2004 6:15:22 AM You are running HFNetChkPro version 4.2.0.4. This is the latest version available.

Figure 48

Best practices and lessons learned during scans

- As you can see from the above discussion and screens shots, there are lots of options, and information, that is presented when performing scans. Be sure to read the help file to understand all the options that are available to you.
- If you don't like the layout of the menu bar along the top of the different views, just right-click on the menu bar and then select, deselect or reorder the items.
- When you are examining whether a patch should be applied, and what its impact will be, be sure to use all of the tools that are available within the product. There is a wealth of information from Microsoft, TruSecure, Bugtraq and Shavlik that you can peruse when making decisions on whether to apply patches. Some of these tools are no longer available within the product – but are still accessible outside of the product.

10. Deploying patches

Prerequisites

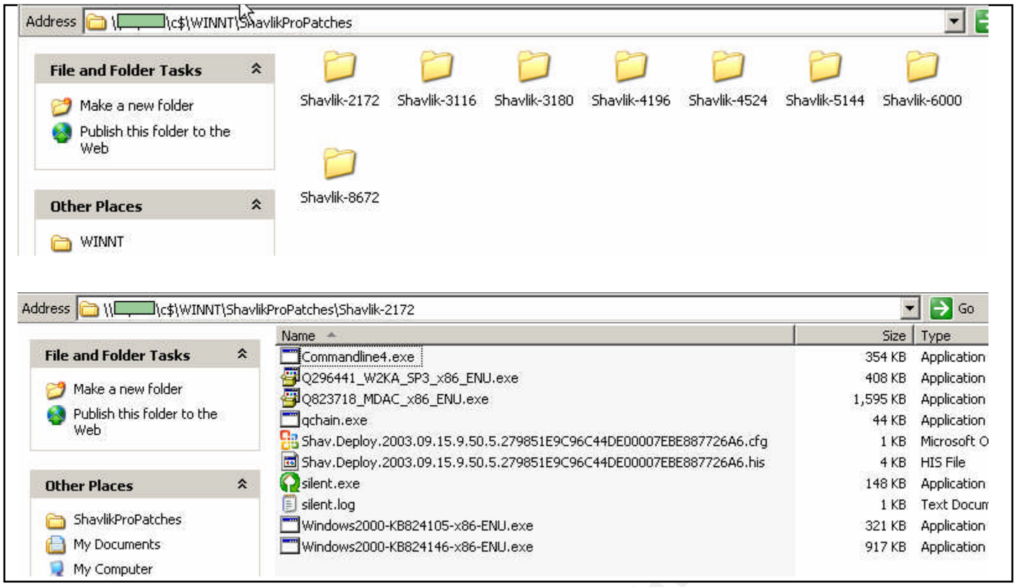
Beyond meeting the previously listed prerequisites for scanning, before you deploy patches and service packs, you must also enable the Scheduler service on each remote workstation.

Overview of the deployment process

Once you have completed a scan, you can then begin deploying patches and service packs to machines. When you deploy patches to a remote machine, each patch goes through three security validations, including validating the signature from Microsoft during the initial download of the patch. Each patch is then stored on the remote machines local drive, with strict permissions assigned.

The patch copy process to the remote system will not occur at all unless the patch itself has been signed. This is to ensure that the patch is valid, and that no one inserted a non-validated patch into the product's DOWNLOAD CENTER. After the patch has been copied to the machine, depending on how it is scheduled, it is quite possible that it will reside locally for an extended time period. So, to prevent possible tampering, the patch is once again checked for signature validity before actual installation.

During the deployment process, files are copied to the local machine in the \\ip address\C$\WINNT\ShavlikProPatches\deployment number directory structure (Figure 49). Where the *deployment number* directory is different for each deployment you create. Only the LOCALSYSTEM account and Administrator accounts have access to this directory. Again, this is to prevent tampering.



Address \\[redacted]\c$\WINNT\ShavlikProPatches

Address \\[redacted]\c$\WINNT\ShavlikProPatches\Shavlik-2172

Name	Size	Type
Commandline4.exe	354 KB	Application
Q296441_W2KA_SP3_x86_ENU.exe	408 KB	Application
Q823718_MDAC_x86_ENU.exe	1,595 KB	Application
qchain.exe	44 KB	Application
Shav.Deploy.2003.09.15.9.50.5.279851E9C96C44DE00007EBE887726A6.cfg	1 KB	Microsoft O
Shav.Deploy.2003.09.15.9.50.5.279851E9C96C44DE00007EBE887726A6.his	4 KB	HIS File
silent.exe	148 KB	Application
silent.log	1 KB	Text Docum
Windows2000-KB824105-x86-ENU.exe	321 KB	Application
Windows2000-KB824146-x86-ENU.exe	917 KB	Application

Figure 49

Once the patch file(s) are copied to the machine, the patch process is either executed, or the patch process is scheduled with the remote machine's Scheduler service.

There are several methods to deploy patches to machines, let's look at each in detail.

Deploy patches to all machines

The first method allows you to deploy patches to all machines that are part of a machine group. Once the scan has completed, right-click the date that is shown in the SUMMARY DETAILS pane. You have two deployment options to choose from:

- **All missing patches** – this option will deploy ALL patches that are identified as missing to ALL machines in the group (Figure 50).

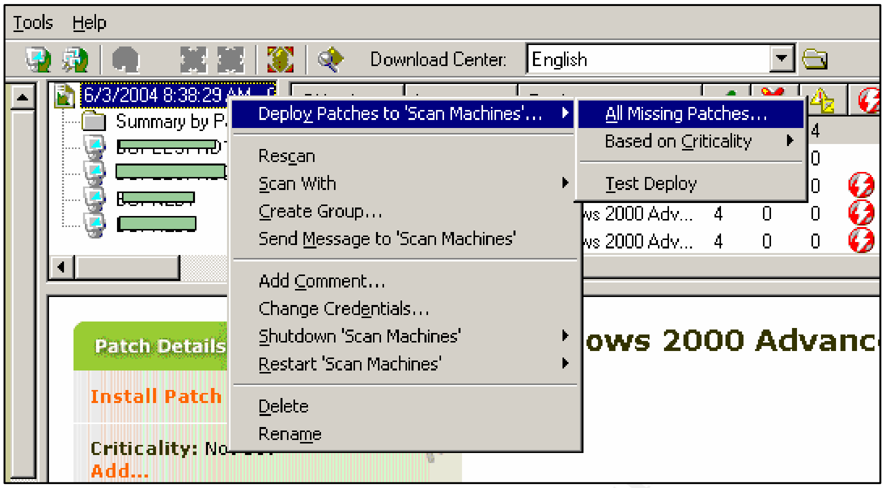


Figure 50

- **Based on Criticality** – this option will deploy only those patches that match your choice for criticality (Figure 51).

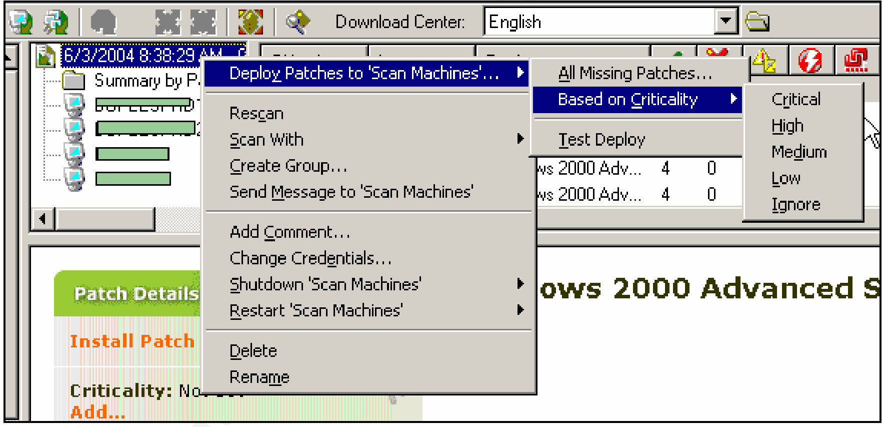


Figure 51

Deploy Patches to a selected machine

Deploying to a selected machine is not much different than deploying to the group as a whole. You right-click the machine name, then choose from the same two deployment options listed above. In addition to those options, you can also individually select patches from the list (SHIFT/CTRL click to select multiples) and deploy them by selecting **Deploy – Selected Patches** (Figure 52).

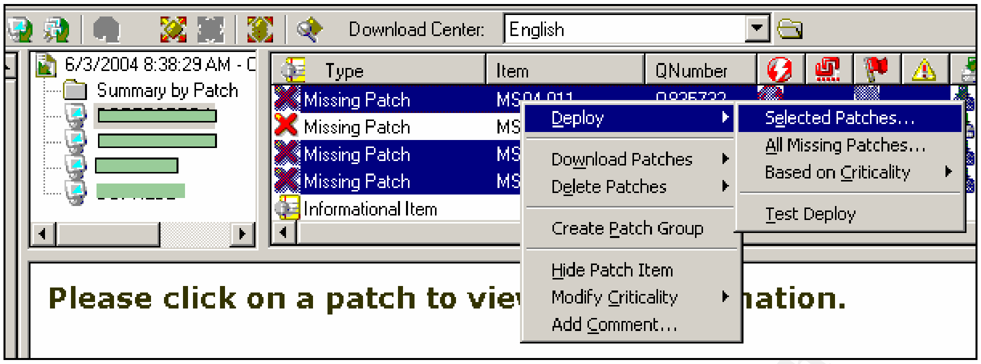


Figure 52

Deploy Service Packs

Service packs are treated a bit differently by the deployment process. The product will not allow you to send out service packs at the same time as patches. Microsoft recommends that service packs be applied separately, and prior to patches. So, this is how the product works. Also, it is not possible to deploy service packs to a group as a whole using the **Deploy to all machines** option. There is a work around to this which I will cover in a moment.

Deploying missing service packs is similar to deploying missing patches. Right-click the missing service pack and select **Deploy - Latest Service pack…** (Figure 53).

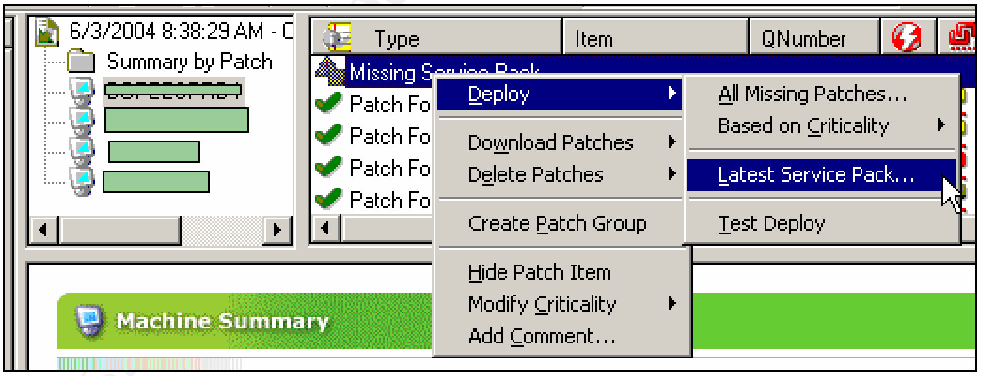
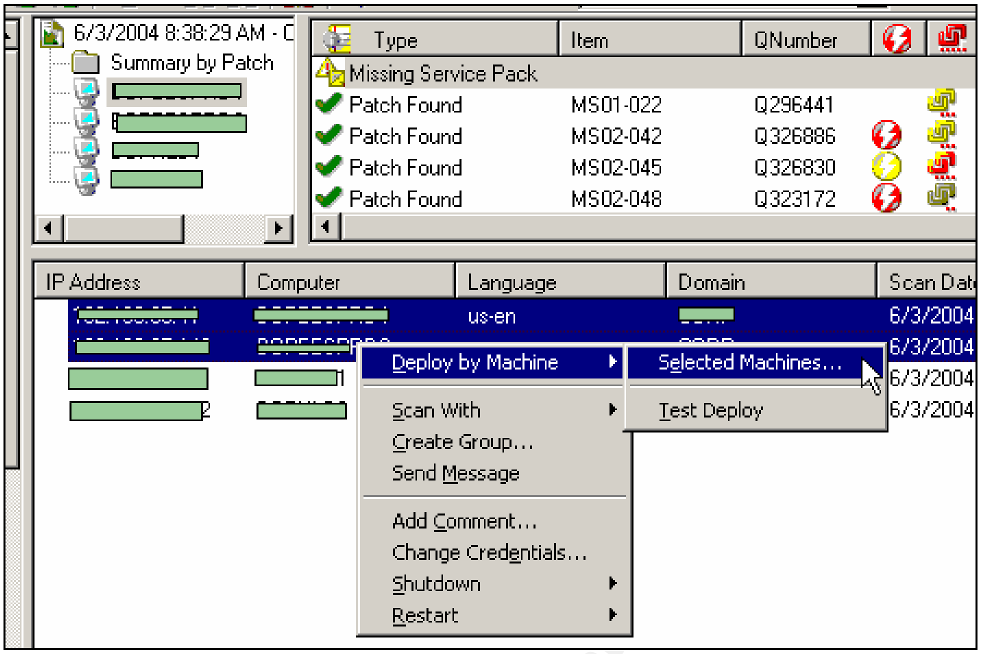


Figure 53

The workaround for sending out service packs to multiple machines takes a few steps. First, select the missing service pack from the SUMMARY pane. You will have to select a machine to do this. Now, click the **Missing** tab at the bottom of the PATCH DETAILS pane. Use your mouse to select one or more machines from the list. Once they are selected, right-click on one of them, then select **Deploy by machine – selected machines** (Figure 54).



Type	Item	QNumber
Missing Service Pack		
Patch Found	MS01-022	Q296441
Patch Found	MS02-042	Q326886
Patch Found	MS02-045	Q326830
Patch Found	MS02-048	Q323172

IP Address	Computer	Language	Domain	Scan Date
[redacted]	[redacted]	us-en	[redacted]	6/3/2004
[redacted]	[redacted]		[redacted]	6/3/2004
[redacted]	[redacted]			6/3/2004
[redacted]	[redacted]			6/3/2004

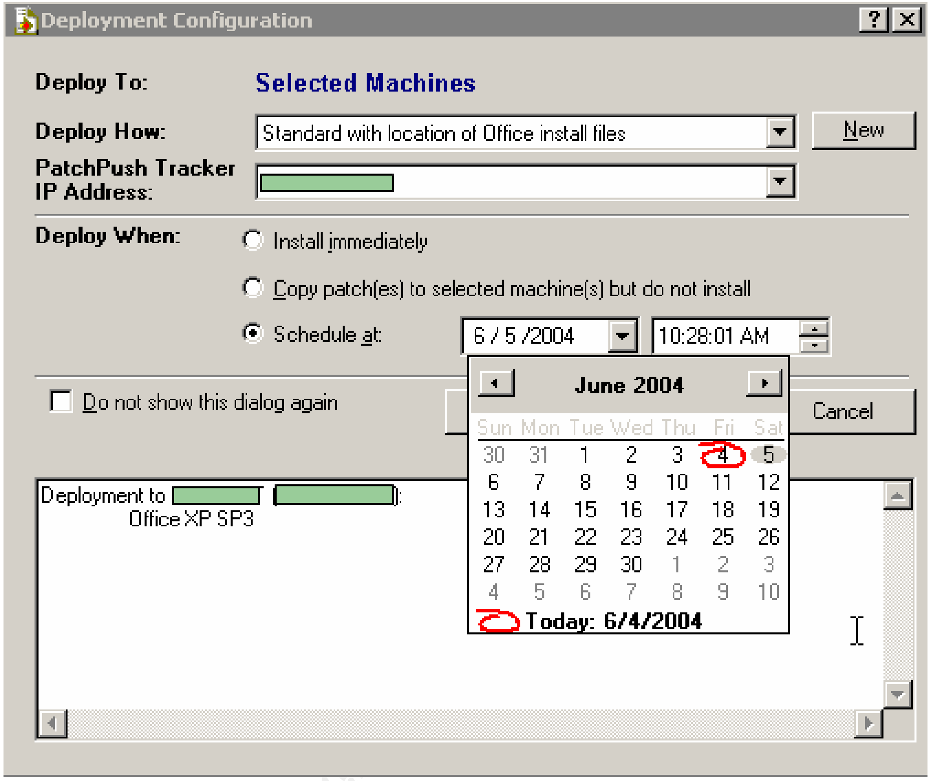
Figure 54

The deployment dialog box

For each of the above deployment methods, the next step is the same. The **Deployment Configuration** dialog box appears (Figure 55). This is where you will make decisions about how deployment will occur. The options you can select are:

- **Deploy how**: Use the drop-down list to select a deployment template or, use the **New** button to create a deployment template.
- **PatchPush^{TM} Tracker** – Select the IP address that serves this function. Typically this is the IP address of the administrative console. But, if you have multiple NIC's, or a centralized tracker, enter type IP address here.
- **Deploy when** – Use the radio button to select you preferred method of scheduling. The options are:
  - **Immediately** – patches are pushed and installed immediately.
  - **Copy patches to machine but do not install** – useful if you want the files on the machine but you want to manually install them. For example, a MICROSOFT SQL SERVER update.
  - **Schedule at** – Use the provided *calendar* and *time* fields to schedule when patches will be applied. During deployment, files will be copied and scheduled for later installation.

- **Details** – Click this button to see more detail about which machines are being patched, and what patches are being applied.
- **Deploy** – Click this button to begin the actual deployment.



Deployment Configuration

Deploy To: Selected Machines

Deploy How: Standard with location of Office install files

PatchPush Tracker IP Address: [redacted]

Deploy When:

○ Install immediately

○ Copy patch(es) to selected machine(s) but do not install

● Schedule at: 6 / 5 /2004 10:28:01 AM

June 2004

Sun	Mon	Tue	Wed	Thu	Fri	Sat
30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	1	2	3
4	5	6	7	8	9	10

Today: 6/4/2004

□ Do not show this dialog again

Deployment to [redacted] [redacted]:
Office XP SP3

Figure 55

Best Practices and lessons learned during deployment

- Always deploy service packs prior to deploying patches.
- Internet Explorer service packs (not patches) can be problematic. These are the only service packs that Microsoft releases that require Administrative rights to complete. Don't get burned by this. I speak from experience when I say that your technical support staff will be very unhappy if you do not take this into account and push out service packs to your desktops that users have no administrative rights to.
- Even though you can push out patches and service packs to Microsoft Exchange Server and Microsoft SQL Server, you may want to install them manually using the **Copy to machine but do not install** option. I've seen issues with Microsoft SQL Server patches not installing correctly because the Shavlik product does not have the ability to shut down any applications that were actually using the SQL server. Patching a SQL server while applications are using the SQL database is a very bad idea – be prepared, at a minimum, to spend

some time with Microsoft support, or rebuilding and restoring the server if you do this.
- Be very careful when pushing out patches and service packs to applications that reside on a cluster. Again, you may want to do this manually.

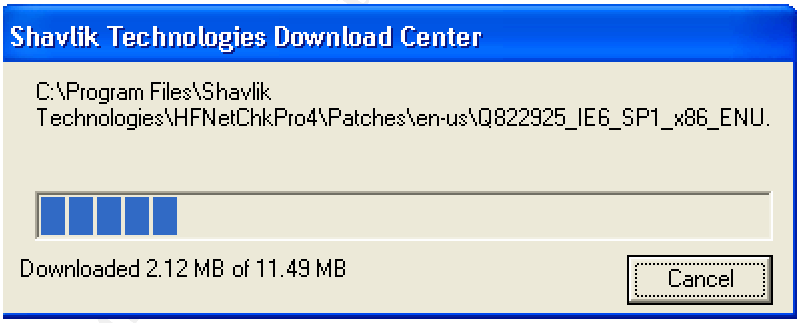
11. Validating Deployment

Monitoring deployment

OK, so we have deployed patches to machine(s) and we want to ensure that the push happened, and that the application of the updates happened. There are a couple of ways to do this.

The first approach is to watch what happens when you click the **Deploy** button. As the deployment progresses, you will be notified about the steps taking place. During a typical deployment this is what you will see:

- First, if any patch you selected has not been downloaded, the download will occur.

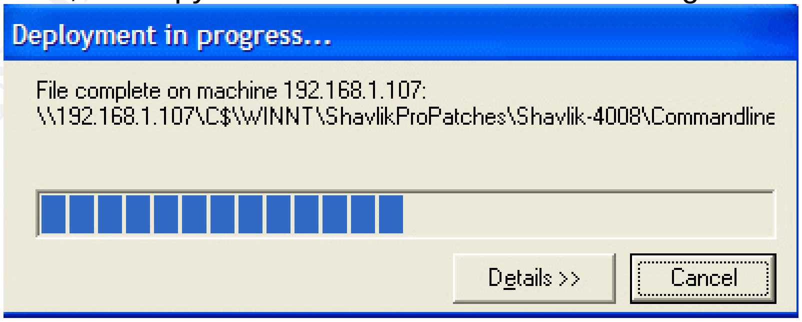


Shavlik Technologies Download Center

C:\Program Files\Shavlik Technologies\HFNetChkPro4\Patches\en-us\Q822925_IE6_SP1_x86_ENU.

Downloaded 2.12 MB of 11.49 MB

- Next, the copy of files to the remote machine begins.



Deployment in progress...

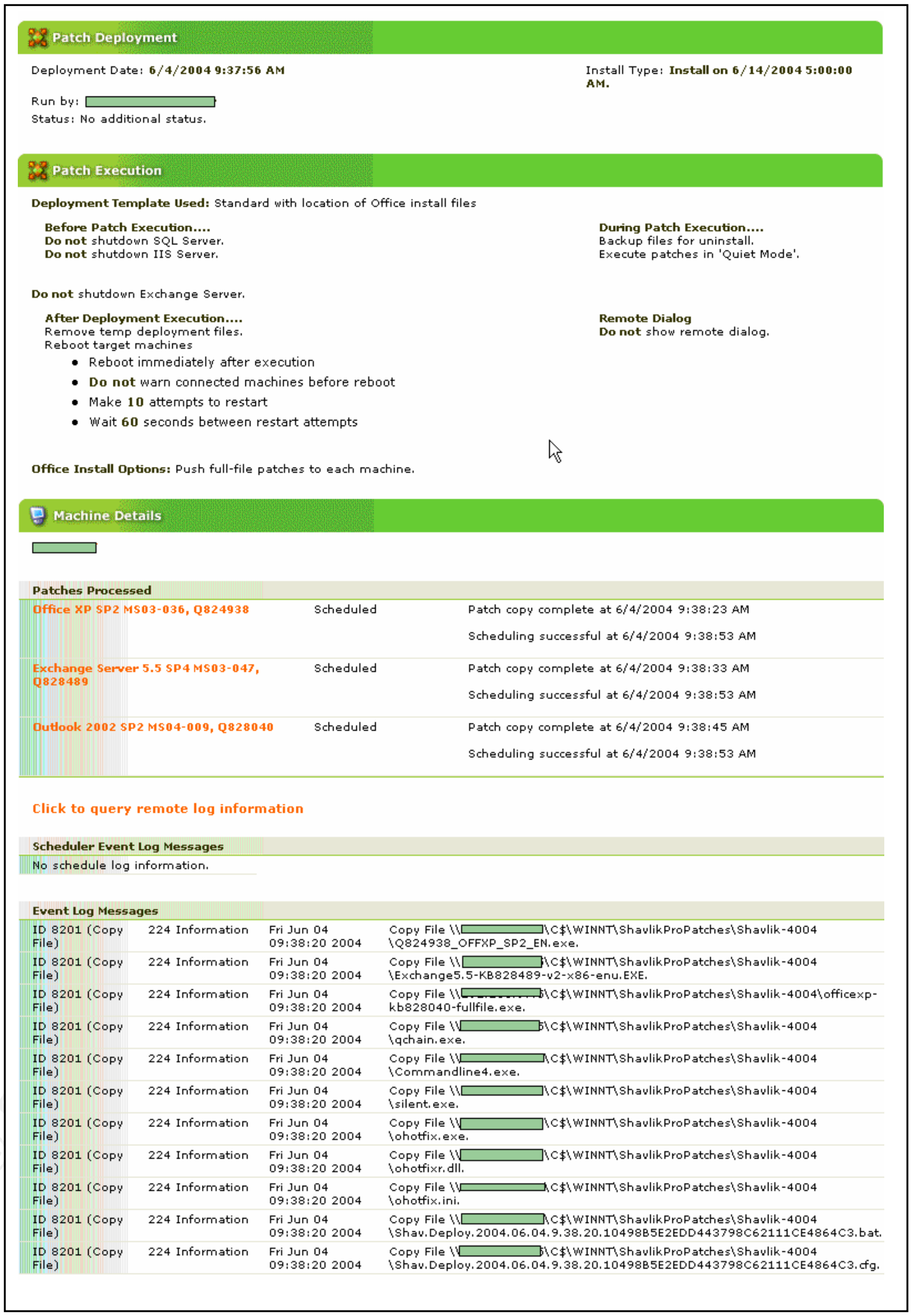
File complete on machine 192.168.1.107:
\\192.168.1.107\C$\WINNT\ShavlikProPatches\Shavlik-4008\Commandline

[42]

- After all of the files have been copied, the PATCHPUSH™ TRACKER will launch. More on this later.

[42] http://hfnetchk.shavlik.com/support/hfpro4help/Deployment_installation_status.gif

- Finally, your screen will change to a PATCH DEPLOYMENT details screen. Here you can see which patches were sent, when they were scheduled and what the execution options were that you selected. Clicking on the **Remote log** feature gives you very detailed information about the file copy process (Figure 56).



Patch Deployment

Deployment Date: **6/4/2004 9:37:56 AM**

Install Type: **Install on 6/14/2004 5:00:00 AM.**

Run by: [redacted]

Status: No additional status.

Patch Execution

Deployment Template Used: Standard with location of Office install files

Before Patch Execution....
Do not shutdown SQL Server.
Do not shutdown IIS Server.

During Patch Execution....
Backup files for uninstall.
Execute patches in 'Quiet Mode'.

Do not shutdown Exchange Server.

After Deployment Execution....
Remove temp deployment files.
Reboot target machines

- Reboot immediately after execution
- **Do not** warn connected machines before reboot
- Make **10** attempts to restart
- Wait **60** seconds between restart attempts

Remote Dialog
Do not show remote dialog.

Office Install Options: Push full-file patches to each machine.

Machine Details

[redacted]

Patches Processed		
Office XP SP2 MS03-036, Q824938	Scheduled	Patch copy complete at 6/4/2004 9:38:23 AM Scheduling successful at 6/4/2004 9:38:53 AM
Exchange Server 5.5 SP4 MS03-047, Q828489	Scheduled	Patch copy complete at 6/4/2004 9:38:33 AM Scheduling successful at 6/4/2004 9:38:53 AM
Outlook 2002 SP2 MS04-009, Q828040	Scheduled	Patch copy complete at 6/4/2004 9:38:45 AM Scheduling successful at 6/4/2004 9:38:53 AM

Click to query remote log information

Scheduler Event Log Messages

No schedule log information.

Event Log Messages			
ID 8201 (Copy File)	224 Information	Fri Jun 04 09:38:20 2004	Copy File \\[redacted]\C$\WINNT\ShavlikProPatches\Shavlik-4004 \Q824938_OFFXP_SP2_EN.exe.
ID 8201 (Copy File)	224 Information	Fri Jun 04 09:38:20 2004	Copy File \\[redacted]\C$\WINNT\ShavlikProPatches\Shavlik-4004 \Exchange5.5-KB828489-v2-x86-enu.EXE.
ID 8201 (Copy File)	224 Information	Fri Jun 04 09:38:20 2004	Copy File \\[redacted]\C$\WINNT\ShavlikProPatches\Shavlik-4004\officexp-kb828040-fullfile.exe.
ID 8201 (Copy File)	224 Information	Fri Jun 04 09:38:20 2004	Copy File \\[redacted]\C$\WINNT\ShavlikProPatches\Shavlik-4004 \qchain.exe.
ID 8201 (Copy File)	224 Information	Fri Jun 04 09:38:20 2004	Copy File \\[redacted]\C$\WINNT\ShavlikProPatches\Shavlik-4004 \Commandline4.exe.
ID 8201 (Copy File)	224 Information	Fri Jun 04 09:38:20 2004	Copy File \\[redacted]\C$\WINNT\ShavlikProPatches\Shavlik-4004 \silent.exe.
ID 8201 (Copy File)	224 Information	Fri Jun 04 09:38:20 2004	Copy File \\[redacted]\C$\WINNT\ShavlikProPatches\Shavlik-4004 \ohotfix.exe.
ID 8201 (Copy File)	224 Information	Fri Jun 04 09:38:20 2004	Copy File \\[redacted]\C$\WINNT\ShavlikProPatches\Shavlik-4004 \ohotfixr.dll.
ID 8201 (Copy File)	224 Information	Fri Jun 04 09:38:20 2004	Copy File \\[redacted]\C$\WINNT\ShavlikProPatches\Shavlik-4004 \ohotfix.ini.
ID 8201 (Copy File)	224 Information	Fri Jun 04 09:38:20 2004	Copy File \\[redacted]\C$\WINNT\ShavlikProPatches\Shavlik-4004 \Shav.Deploy.2004.06.04.9.38.20.10498B5E2EDD443798C62111CE4864C3.bat.
ID 8201 (Copy File)	224 Information	Fri Jun 04 09:38:20 2004	Copy File \\[redacted]\C$\WINNT\ShavlikProPatches\Shavlik-4004 \Shav.Deploy.2004.06.04.9.38.20.10498B5E2EDD443798C62111CE4864C3.cfg.

Figure 56

What is PATCHPUSH^{TM} TRACKER?

PATCHPUSH^{TM} TRACKER is a centralized console for viewing the status of deployments. Think of it as a validation tool. The TRACKER gets its messages from the HFNETCHKPRO service, which by default listens on TCP port 4750. For machines outside a firewall, this is another port you might need to have open.

Each line in the TRACKER shows the status for a separate patch or service pack that has been deployed to a machine. The state of deployments can be any of the following (represented by colored dots).

- Green: The patch was deployed without any problems
- Yellow: The rescan of the system, after installation of the patch or service pack, failed because of bad credentials.
- Red: Deployment failed.
- Blue: Patching is in process and has not completed yet.

12. Reporting

What's Available?

Before we discuss reporting, I want to remind you that if you are using HFNETCHKPRO LIMITED EDITION, you only have the *Condensed Patch Listing* report available. If you have the HFNETCHKPRO PRO EDITION, you have 13 reports to choose from. For a complete listing of reports see the product help file at:

http://hfnetchk.shavlik.com/support/hfpro4help/Overview_of_reports.htm.

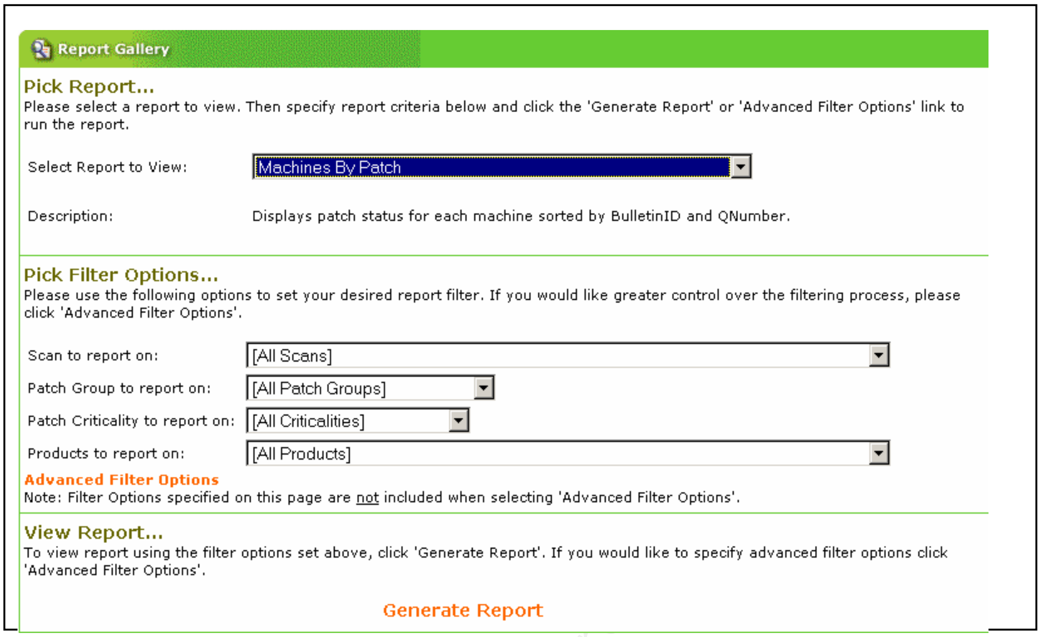
Creating and customizing a report

I'm not going to spend too much time discussing reporting, there are just too many options to choose from. So, I'll let you discover the reporting features for yourself. I'll just quickly mention that the reporting engine allows you to do complex reporting with the use of basic filters within drop-down lists, and complex filters using scripting language (Figure 57). For a better description of reporting features see the product help file at:

http://hfnetchk.shavlik.com/support/hfpro4help/Basic_filtering.htm

and

http://hfnetchk.shavlik.com/support/hfpro4help/Advanced_filtering.htm



Report Gallery

Pick Report...

Please select a report to view. Then specify report criteria below and click the 'Generate Report' or 'Advanced Filter Options' link to run the report.

Select Report to View: Machines By Patch

Description: Displays patch status for each machine sorted by BulletinID and QNumber.

Pick Filter Options...

Please use the following options to set your desired report filter. If you would like greater control over the filtering process, please click 'Advanced Filter Options'.

Scan to report on: [All Scans]

Patch Group to report on: [All Patch Groups]

Patch Criticality to report on: [All Criticalities]

Products to report on: [All Products]

Advanced Filter Options

Note: Filter Options specified on this page are not included when selecting 'Advanced Filter Options'.

View Report...

To view report using the filter options set above, click 'Generate Report'. If you would like to specify advanced filter options click 'Advanced Filter Options'.

Generate Report

Figure 57

13. Troubleshooting

Uninstalling patches

Life being what it is, you may encounter patches and service packs that break functionality in your network. So, you better have the ability to back them out. There are actually two ways to do this, one within the product and one within the OS.

Within the product, some patches that are listed as found can be uninstalled. Simply right-click on the patch and, if it is available, select the **Uninstall Selected** option (Figure 58). Keep in mind that not all patches have the ability to be uninstalled – so don't be surprised if this option is unavailable.

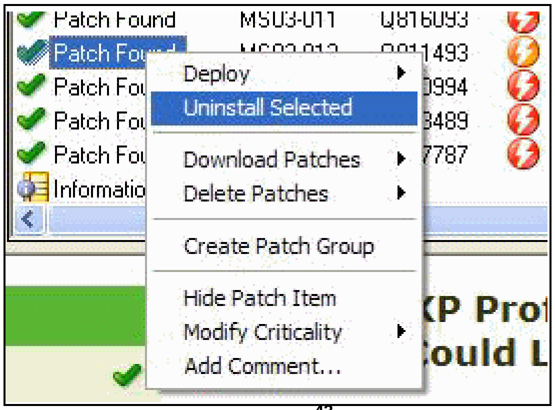
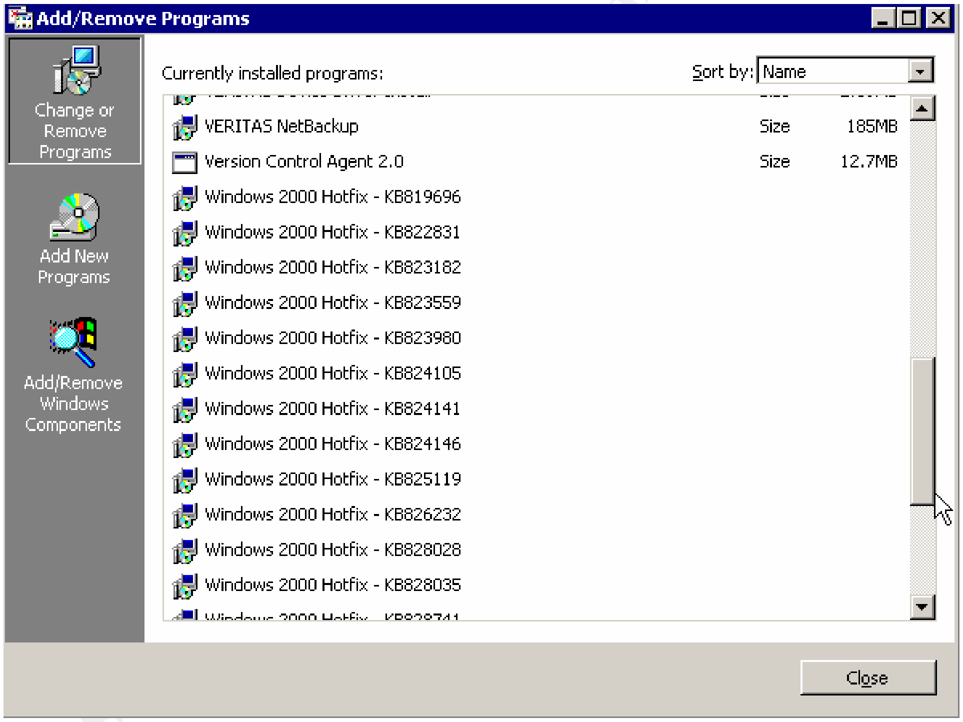


Figure 58[43]

Within the OS, you can uninstall patches if they appear in the **Add|Remove** programs applet. Patches that appear here are listed by their KNOWLEDGEBASE (KB) article numbers (Figure 59).



Currently installed programs:

VERITAS NetBackup	Size	185MB
Version Control Agent 2.0	Size	12.7MB
Windows 2000 Hotfix - KB819696		
Windows 2000 Hotfix - KB822831		
Windows 2000 Hotfix - KB823182		
Windows 2000 Hotfix - KB823559		
Windows 2000 Hotfix - KB823980		
Windows 2000 Hotfix - KB824105		
Windows 2000 Hotfix - KB824141		
Windows 2000 Hotfix - KB824146		
Windows 2000 Hotfix - KB825119		
Windows 2000 Hotfix - KB826232		
Windows 2000 Hotfix - KB828028		
Windows 2000 Hotfix - KB828035		

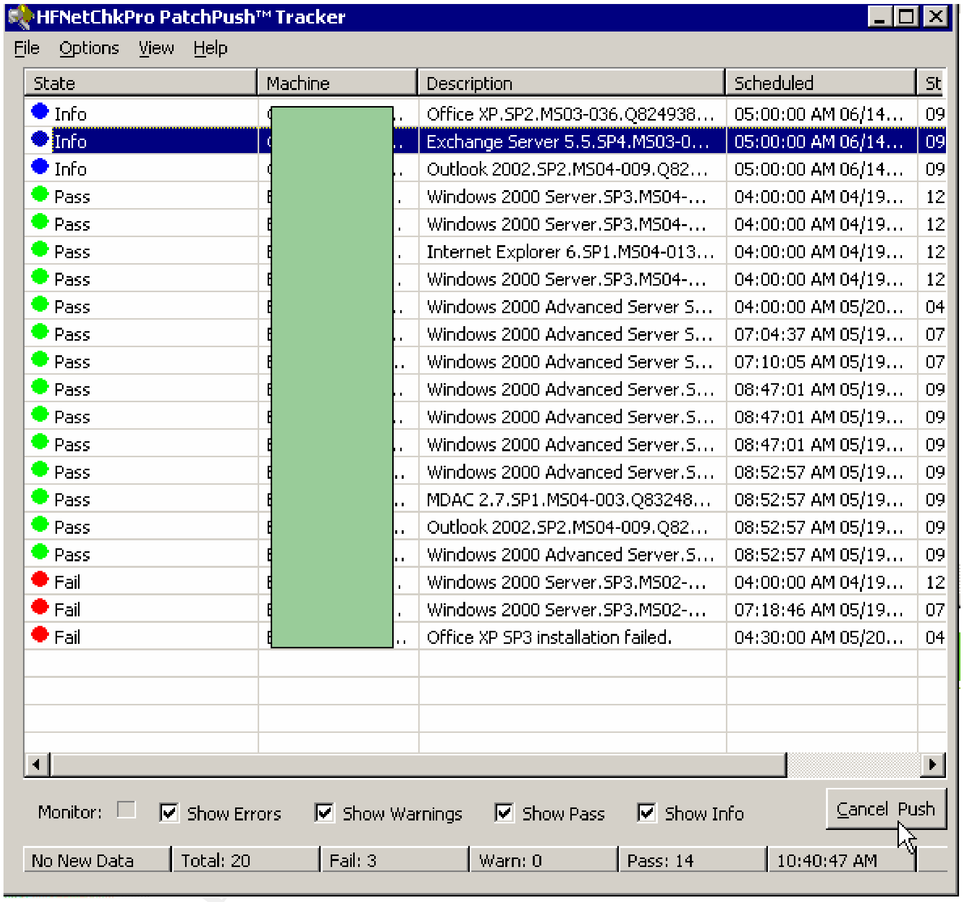
Figure 59

Obviously, in terms of best practice, it is a good idea to test all patches and service packs BEFORE you deploy them. You never want to get yourself into a situation where you can't back patches and service packs out.

Canceling deployment

[43] http://hfnetchk.shavlik.com/support/hfpro4help/Uninstall_Selected.gif

It is possible to cancel any deployment that has not finished. Simply click the **Cancel** button. Or, if the deployment has finished, but not been applied, you can use PATCHPUSH^{TM} TRACKER to cancel the deployment. Within the TRACKER, select the line that contains the deployment of the patch or service pack you want to cancel, and then click the **Cancel Push** button (Figure 60).



State	Machine	Description	Scheduled	St
🔵 Info	[redacted]	Office XP.SP2.MS03-036.Q824938...	05:00:00 AM 06/14...	09
🔵 Info	[redacted]	Exchange Server 5.5.SP4.MS03-0...	05:00:00 AM 06/14...	09
🔵 Info	[redacted]	Outlook 2002.SP2.MS04-009.Q82...	05:00:00 AM 06/14...	09
🟢 Pass	[redacted]	Windows 2000 Server.SP3.MS04-...	04:00:00 AM 04/19...	12
🟢 Pass	[redacted]	Windows 2000 Server.SP3.MS04-...	04:00:00 AM 04/19...	12
🟢 Pass	[redacted]	Internet Explorer 6.SP1.MS04-013...	04:00:00 AM 04/19...	12
🟢 Pass	[redacted]	Windows 2000 Server.SP3.MS04-...	04:00:00 AM 04/19...	12
🟢 Pass	[redacted]	Windows 2000 Advanced Server S...	04:00:00 AM 05/20...	04
🟢 Pass	[redacted]	Windows 2000 Advanced Server S...	07:04:37 AM 05/19...	07
🟢 Pass	[redacted]	Windows 2000 Advanced Server S...	07:10:05 AM 05/19...	07
🟢 Pass	[redacted]	Windows 2000 Advanced Server.S...	08:47:01 AM 05/19...	09
🟢 Pass	[redacted]	Windows 2000 Advanced Server.S...	08:47:01 AM 05/19...	09
🟢 Pass	[redacted]	Windows 2000 Advanced Server.S...	08:47:01 AM 05/19...	09
🟢 Pass	[redacted]	Windows 2000 Advanced Server.S...	08:52:57 AM 05/19...	09
🟢 Pass	[redacted]	MDAC 2.7.SP1.MS04-003.Q83248...	08:52:57 AM 05/19...	09
🟢 Pass	[redacted]	Outlook 2002.SP2.MS04-009.Q82...	08:52:57 AM 05/19...	09
🟢 Pass	[redacted]	Windows 2000 Advanced Server.S...	08:52:57 AM 05/19...	09
🔴 Fail	[redacted]	Windows 2000 Server.SP3.MS02-...	04:00:00 AM 04/19...	12
🔴 Fail	[redacted]	Windows 2000 Server.SP3.MS02-...	07:18:46 AM 05/19...	07
🔴 Fail	[redacted]	Office XP SP3 installation failed.	04:30:00 AM 05/20...	04

Monitor: □ ☑ Show Errors ☑ Show Warnings ☑ Show Pass ☑ Show Info

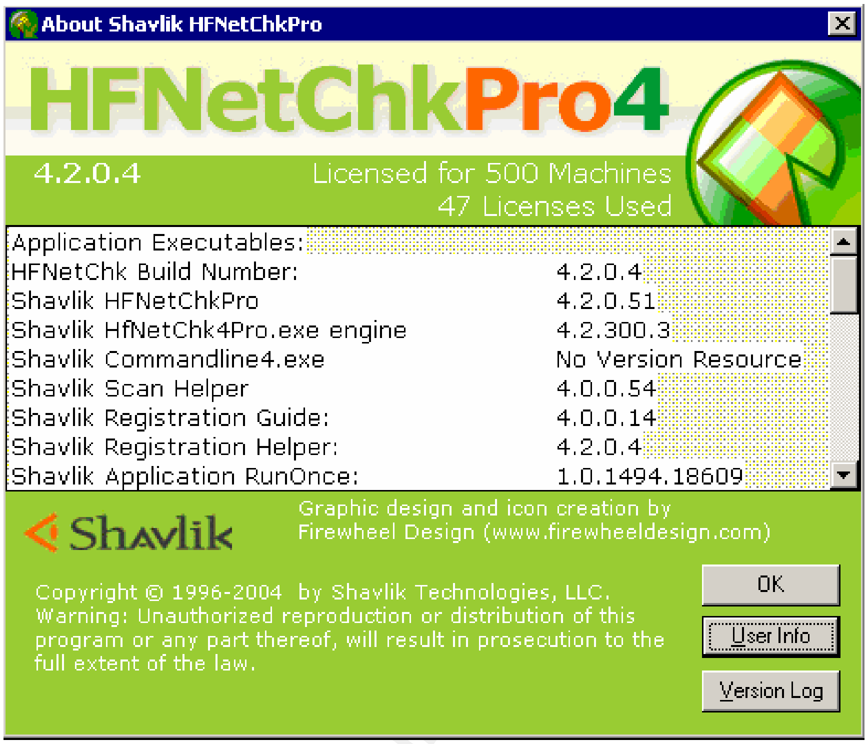
No New Data | Total: 20 | Fail: 3 | Warn: 0 | Pass: 14 | 10:40:47 AM

Figure 60

Log files and where they are located

There are numerous locations within the product HELP screen and in log files, which can be used to troubleshoot problems.

- If you need to view information about the versions of files that make up the product open, HELP|ABOUT. The **System information** button and **Version log** buttons will show you detailed information about each of the components that are being used by the product (Figure 61).



4.2.0.4

Licensed for 500 Machines
47 Licenses Used

```
Application Executables:
HFNetChk Build Number:               4.2.0.4
Shavlik HFNetChkPro                  4.2.0.51
Shavlik HfNetChk4Pro.exe engine      4.2.300.3
Shavlik Commandline4.exe             No Version Resource
Shavlik Scan Helper                  4.0.0.54
Shavlik Registration Guide:          4.0.0.14
Shavlik Registration Helper:         4.2.0.4
Shavlik Application RunOnce:         1.0.1494.18609
```

Graphic design and icon creation by
Firewheel Design (www.firewheeldesign.com)

Copyright © 1996-2004 by Shavlik Technologies, LLC.
Warning: Unauthorized reproduction or distribution of this program or any part thereof, will result in prosecution to the full extent of the law.

Using JET database

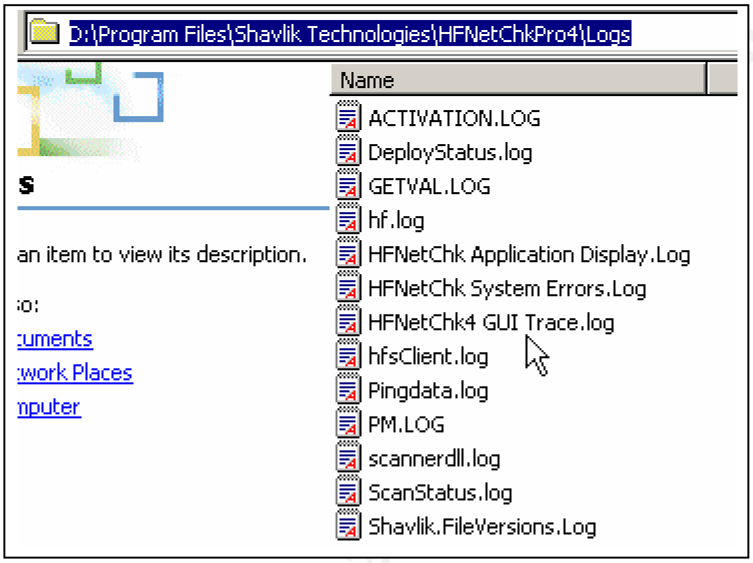
****Versions****
Application Executables:
Shavlik HFNetchk Build: 4.2.0.4
Shavlik HFNetChkPro 4.2.0.51
Shavlik HfNetChk4Pro.exe engine: 4.2.300.3
Shavlik Commandline4.exe : No Version Resource
Shavlik Scan Helper: 4.0.0.54
Shavlik Registration Guide: 4.0.0.14
Shavlik Registration Helper: 4.2.0.4
Shavlik Application RunOnce: 1.0.1494.18609
Shavlik Application Updater: 1.1.0.29636
Microsoft qchain.exe: 5.0.2195.6666

ActiveX Components:
Shavlik RegistryAid Tool: 1.0.0.10
Shavlik SubClasser Tool: 1.0.0.49
Shavlik Type Library: 4.0.0.60
Shavlik Scan Components: 4.2.0.41
Shavlik Deployment Components: 4.2.0.45
Shavlik XML Parser: 4.0.0.58
Shavlik PatchEngine: 4.2.0.4
Shavlik HFNetChk4 Reports: 4.2.0.39
Shavlik Report Architecture: 1.0.0.4
MS Scripting Runtime: 5.6.0.6626
MS ADODB: 2.71.9030.0
MS Windows Scripting Host: 5.6.0.6626
MS XML DOM 4.0: 4.20.9818.0

ActiveX Controls:
Shavlik Criteria Builder: 2.1.0.51
MS Common Controls: 6.0.81.5
MS Internet Controls: 6.0.2800.1106
Data Dynamics ActiveReports: 2.0.0.1130

Figure 61

If these are not helpful, there are also several logs that can be found within the logs folder (Figure 62). These will be very useful when you are troubleshooting, or working with Shavlik technical support.



D:\Program Files\Shavlik Technologies\HFNetChkPro4\Logs

Name
ACTIVATION.LOG
DeployStatus.log
GETVAL.LOG
hf.log
HFNetChk Application Display.Log
HFNetChk System Errors.Log
HFNetChk4 GUI Trace.log
hfsClient.log
Pingdata.log
PM.LOG
scannerdll.log
ScanStatus.log
Shavlik.FileVersions.Log

Figure 62

Event log information and codes

HFNetChkPro logs events directly to the operating system event log. A list of events can be found in the HELP file for the product at:

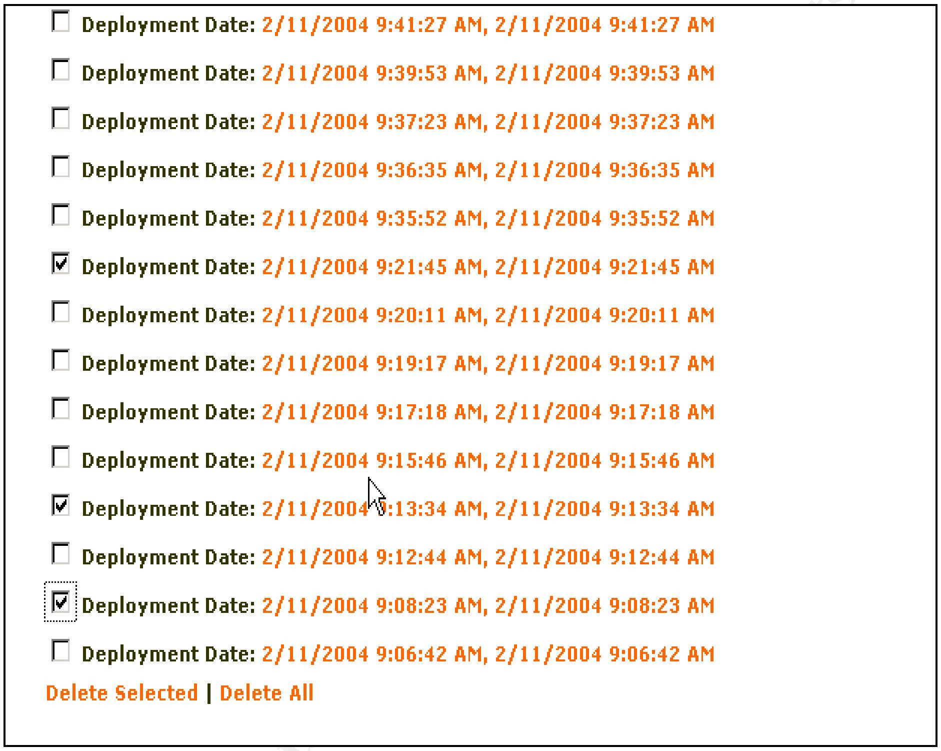
http://hfnetchk.shavlik.com/support/hfpro4help/Error_messages.htm

Using this information, it is possible to build alert rules within products like Microsoft Operations Manger or Tivoli.

Maintaining the product database

Finally, from a maintenance perspective, it is a good idea to clean out and compress the program's database. As you use the product it continues to keep track of all previous scans and deployments. This information fills up the database rather quickly and will cause the program to run slowly, or stop working altogether.

To fix issues with the database, follow this two step process. First, clean out any information related to previous scans and deployments. Delete what you do not want to keep. To do this, select **Manage Items** from the TOOLS menu. Place a checkmark before each entry you'd like to delete, and then click **Delete Selected** (Figure 63).



□ Deployment Date: 2/11/2004 9:41:27 AM, 2/11/2004 9:41:27 AM

□ Deployment Date: 2/11/2004 9:39:53 AM, 2/11/2004 9:39:53 AM

□ Deployment Date: 2/11/2004 9:37:23 AM, 2/11/2004 9:37:23 AM

□ Deployment Date: 2/11/2004 9:36:35 AM, 2/11/2004 9:36:35 AM

□ Deployment Date: 2/11/2004 9:35:52 AM, 2/11/2004 9:35:52 AM

☑ Deployment Date: 2/11/2004 9:21:45 AM, 2/11/2004 9:21:45 AM

□ Deployment Date: 2/11/2004 9:20:11 AM, 2/11/2004 9:20:11 AM

□ Deployment Date: 2/11/2004 9:19:17 AM, 2/11/2004 9:19:17 AM

□ Deployment Date: 2/11/2004 9:17:18 AM, 2/11/2004 9:17:18 AM

□ Deployment Date: 2/11/2004 9:15:46 AM, 2/11/2004 9:15:46 AM

☑ Deployment Date: 2/11/2004 9:13:34 AM, 2/11/2004 9:13:34 AM

□ Deployment Date: 2/11/2004 9:12:44 AM, 2/11/2004 9:12:44 AM

☑ Deployment Date: 2/11/2004 9:08:23 AM, 2/11/2004 9:08:23 AM

□ Deployment Date: 2/11/2004 9:06:42 AM, 2/11/2004 9:06:42 AM

Figure 63

After you have cleaned out unnecessary or older information, the next step is to select the **Compact\Repair database** option from the TOOLS menu. A warning will appear letting you know that the process might take some time. Click **Yes** to begin the process. The HFNETCHKPRO service will stop, the database will be compacted and the service will be restarted.

Summary

Meeting the challenges of patch management is not easy. It takes a lot of front-end work to devise a strategy and keep it up-to-date. With vulnerabilities, and the sophistication of attacks based on vulnerabilities, on the rise, evidence suggests it is worth the up-front time to develop a patch management methodology – especially when viewed against the potential back-end time and expense cleaning up after a security incident. If you automate your methodology, you will have taken the steps necessary to ensure your entire organization is up-to-date, aware of new vulnerabilities as they are discovered and moved from a reactive stance to a proactive stance. Toward that end, HFNETCHKPRO is an easy product to use, fits well within a patch management methodology, and meets the minimum recommendations for an automated solution.

References

Schweitzer, Douglas. “Emerging Technology: Patch Me if You Can.” Network Magazine. 8/05/2003
URL: http://www.networkmagazine.com/shared/article/showArticle.jhtml?articleId=13000049

NetSupport Solutions Inc. “Beating Hackers to the Patch.” Windows Security.com. 10/06/03.
URL: http://secinf.net/Patch_Management/Beating_Hackers_to_the_Patch.html

United States General Accounting Office. “INFORMATION SECURITY: Effective Patch Management is Critical to Mitigating Software Vulnerabilities.” 9/10/03.
URL: http://www.gao.gov/new.items/d031138t.pdf

CERT® Coordination Center (CERT®/CC.) “The CERT Coordination Center FAQ.” 2/26/04.
URL: http://www.cert.org/faq/cert_faq.html#A1

CERT®Coordination Center (CERT®/CC.) “CERT Coordination Center 2003 Annual Report.” 4/5/04.
URL: http://www.cert.org/annual_rpts/cert_rpt_03.html

CERT® Coordination Center (CERT®/CC.) “CERT/CC Statistics 1988-2003.” 1/22/04.
URL: http://www.cert.org/stats/cert_stats.html

Violino, Bob. “Patching Things Up.” CIO 8/1/03
URL: http://www.cio.com/archive/080103/et_article.html

Backman, Alex. “Five Tips for Effective Patch Management.” Computerworld. 7/14/03.
URL:
http://www.computerworld.com/securitytopics/security/story/0%2C10801%2C82458%2C00.html

Integrated Information Systems. “Patching Statistics.”
URL: http://www.iis.com/default.aspx?pageid=4

Integrated Information Systems. “Patch Management.”
URL: http://www.iis.com/default.aspx?pageid=35

Security Stats.com. Most Requested Statistics.
URL: http://www.securitystats.com

Schultze, Eric. “Is Patch Management the best Protection Against Vulnerabilities? Yes.” NetworkWorldFusion. 3/29/04.
URL: http://www.nwfusion.com/columnists/2004/0329faceoffyes.html

Cruit, Nadine. “Shavlik Technologies: Patching Up the Security Holes.” ComputerUser Local Profiles Minneapolis /.St.Paul. 4/04.
URL: http://computeruser.com/articles/2304,10,66,1,0401,04.html

Integrated Information Systems. “Government Regulations.” URL:
http://www.iis.com/default.aspx?pageid=5

Colville, Ronni Nicolett,Mark. “Patch Management: Surveying the Vendor Landscape.” TechRepublic. Tech Perspective. 5/14/03.
URL: http://techrepublic.com.com/5100-6264-5034938.html

Carpenter, Brad. “Patch Management: Find the Weakest Link.” ZDNet. News Commentary. 2/4/04.
URL: http://zdnet.com.com/2100-1107-5152602.html

Semilof, Margie. “Managing Patches Manually is Futile, Ecora Exec Says.” SearchWin2000.com. Question & Answer. 3/10/03.
URL: http://searchwin2000.techtarget.com/qna/0,289202,sid1_gci884779,00.html

Shavlik Technologies. About Us.
URL: http://www.shavlik.com/pAbout_Shavlik.aspx

Shavlik Technologies. Help File.
URL: http://hfnetchk.shavlik.com/support/hfpro4help/Welcome_to_HFNetChk_4.htm

Policht, Marcin. “An Introduction fo Windows Patch Management.” CrossNodes. 1/20/04.
URL: http://networking.earthWeb.com/netsysm/article.php/10954_3301151_3

Common Vulnerabilities and Exposures. About CVE. 2/4/04.
URL: http://www.cve.mitre.org/about/

Security Focus.
URL: http://www.securityfocus.com/corporate/company/index.shtml