

Georgia Institute of Technology

Patch Management Deployment and Support

March 3, 2004
Last Updated January 11, 2005

Patch Management Deployment and Support

- I. Patching Process
 - a. Analyze (Research)
 - b. Plan (Rate and Rank)
 - c. Test
 - d. Scan
 - e. Deploy
 - f. Validate and Report
 - g. Monitor

- II. Deployment Options/Models
 - a. Option A-Distributed
 - i. Diagram
 - b. Option B-Central Support
 - i. Diagram
 - ii. Availability
 - iii. Standards and Controls
 - iv. Expectations of CSR/CSS/Users
 - v. Expectations of OIT-ITS
 - vi. How to request patching by OIT-ITS
 - c. Option C-Mixed-Central and Distributed Patching
 - i. Diagram
 - ii. Expectations
 - iii. Support
 - d. Option D-Mixed-Central Server with Distributed Patching
 - i. Diagram
 - ii. Expectations
 - iii. Support

- III. Support Sources

- IV. Timeline

Patch Management Implementation Plan

This document addresses the general patching process to be used by OIT-ITS and serves as a model for how departments should manage their own patching processes. The patching process and options may apply to different software tools used for patch management. Option A, the totally distributed model described below, is already in place for some departments as they already have patch management software in place. OIT-ITS plans to use HFNetChkPro for Option B, C, and D.

Items in Bold, Italics, and Underlined indicate where resources may be affected and possibly to the point of requiring additional resources to support the patch management process.

I. **Patching process** - Management of patch deployment is based on Critical and Standard releases from Microsoft. Critical OS and Security patches require immediate research and testing prior to mass deployment. For OIT-ITS this evaluation cycle is done within 1 business day of notification from OIT Information Security (generally within 24 hours). This evaluation cycle is recommended for Departments supporting their own patch program. Standard patches are evaluated monthly following Microsoft's new release schedule and should be deployed within 5 business days.

a. **Analyze (Research)**

- i. Review new patches that have been released. The person tasked with patching machines should be a member of the CERT, Microsoft Security, or other advisory list that sends notification when new patches have been released. For links to organizations that send out notices refer to <http://security.gatech.edu/information/> under the following sections: Advisory and Security News Sites and Security Organizations and Security Related Websites.
- ii. Review all documentation. Before applying any service pack, hot fix or security patch, all relevant documentation should be read. As the documentation is read, look for the following:
 1. Is the update relevant and will it resolve an outstanding issue?
 2. Will adopting the update cause other problems resulting in a compromise of the system?
 3. Are there dependencies relating to the update? (For example, certain features being enabled or disabled for the update to be effective.)
 4. Are any actions needed prior to deploying the update?
- iii. Search Microsoft Support. As well as examining the documentation released with the updates, search the Microsoft support Web site for any additional post-release information on the update. These materials supply critical information that must be referenced.

b. **Plan (Rate and Rank)**

OIT-ITS generally releases patch bundles after individual patch testing & bundled testing is completed. OIT-ITS test against the standard administrative desktop suite.

- i. Identify which patches should be deployed to deter the potential threats and vulnerabilities.
- ii. Determine which patches are critical and must be deployed immediately.
- iii. Determine which patches are non-critical and are specific to your area.
- iv. Rank the patches in priority or prerequisite order.

c. **Test**

- i. Test machines should include computers representative of all of the functions performed within the department or groups being scanned or patched. As a minimum for patch management purposes, you must know what systems are in your environment:
 1. Hardware configuration
 2. OS, Including version
 3. Patch level already in place (Service Pack version, Hot fixes, and other modifications)
 4. Function (desk top, Server, data base, etc.)
 5. Applications
- ii. It is suggested that test machines be non-production machines. However, users within certain groups could be requested to be volunteers to have their machines be the test machines for that group. Also one or two machines in the back of a cluster could be test machines for computer labs.
- iii. Test all patches that have been identified to make sure they will work within your environment without any negative side effects. As with any software, patches may not work perfectly in every environment. Ideally, all patches to be installed in your environment should be thoroughly tested. The following list shows the testing that should be performed for each patch.
 1. Deploy patch(es) to test machines.
 2. Verify that it performs as planned. Use the checklists that you have created. One should be created for each software or system that is tested. An example is at <http://www.itac.gatech.edu/desktop-management/patch-deploy/computer-operation-checklist.doc>
 3. If a patch is suspected of breaking an application, the following tests should be done to help resolve.

- a. If the patch is un-installed, does the problem go away?
 - b. If the patch is installed on another machine with the same software, does the same problem occur?
4. Check the uninstall procedure.
 5. Send information that the patch/patches did not work to patchmanagement@lists.gatech.edu and to CSR list. For successful patch deployment send to CSR list. If problems with deployment, the e-mail should include the following:
 1. Vendor
 2. Software the patch is for
 3. Version of the software the patch is for
 4. Patch reference number(s)
 5. Patch common name
 6. Did the patch break any applications?
 7. if so, which one?
 8. if so, what version of the application
 9. other comments or issues?
- iv. OIT-ITS will follow up with OIT-ITS Standard application vendors when necessary. The list of OIT-ITS' standard applications is at:
http://www.oit.gatech.edu/css_csr/desktop/standard_suite_image.cfm
 - v.
CSR/CSS or official departmental contact for departmental specific software will be responsible for following up with those specific software vendors if a particular patch breaks their application.
 - vi. OIT-ITS will post the results to CSR list and the patch testing web page.
- d. **Scan** – To determine which machines require specific patches, OIT-ITS and the departments should scan their respective machines.
 - e. **Deploy**
 - i. Deploy the right patches to make environment secure.
 - ii. **OIT-ITS deploys patches to those machines “registered” with them to be patched. See the Central patching option below on availability, requirements, and on how to request central support from OIT-ITS.**
 - iii. Department deploys its patches.

f. **Validate and Report**

- i. Rescan and run reports to ensure all machines received the desired patches and that they were deployed properly.

g. **Monitor**

- i. Check all systems after deploying patches to make sure there are no undesired side effects. One week is recommended to identify any problems that occur, or other time frame based on the unit's environment.
- ii. OIT-ITS can meet with CSR/CSSs who report problems with an OIT-ITS standard application, assess risk of rolling back and tradeoffs of rolling back on "registered" machines, as necessary. Departments will be responsible for local roll back decisions on their systems.

II. **Deployment Options** - Four options are available for setting up HFNetChkPro. A departmental CSR/CSS should determine which option best fits their department. Departments can switch between those architectures at any time by meeting the requirements needed for each.

a. **Option A – Distributed Support** - In this model, departments run their own "server" for patch management, and are responsible for all support aspects of their patch management system. To get started, see the "HFNetChkPro Initial Server Setup and Scans" document. It is recommended that a patch management process be used. The "patching process," section I, has a good recommended process. Assistance can be obtained through the various methods outlined in "support sources," section III. Departments can change from Option A to Option B, C or D by meeting the requirements of those sections.

- i. **Diagram** – See <http://www.itac.gatech.edu/desktop-management/patch-deploy/option-A-distributed.pdf> for the diagram of Option A. The diagram for Option A shows that each distributed department has set up their own patch server either with or without SQL server where the department patches their own systems.

NOTE: This model already exists on campus with some departments using HFNetChkPro and some using Patchlink.

b. **Option B (Central Support)** – In this model, departments receive their patches directly from the central patching server, which is located in the Rich machine room. Patches can be deployed to workstations and servers. This model would be beneficial for departments that have standard administrative applications such as PeopleSoft and Banner, etc... However if it is desired to have your servers and non-standard desktops patched in this manner, there is a risk associated with not having a test environment to test patches before deployment to machines.

- i. Diagram - See <http://www.itac.gatech.edu/desktop-management/patch-deploy/option-B-central.pdf> for the diagram of Option B. ***Machines with OIT-ITS standard administrative applications in departments can be opted in for patching by OIT-ITS.*** This is also seen in the diagram of Option C, but guidelines for this are explained in this section. ***In the Option B diagram, CSR/CSS/Users can opt to have their machines patched by OIT-ITS¹.*** Holes may need to be opened in departmental firewalls to allow the OIT-ITS patch server to support the patching process. Those are described in the “HFNetChkPro Initial Server Setup and Scans” document.
- ii. Availability
OIT-ITS can patch machines for departments if so requested The department requesting central patch support must request the appropriate number of licenses for the number of machines. See below for details on how to obtain OIT-ITS patch support. The departmental CSR/CSS/user will be responsible for performing initial troubleshooting on any applications that break. They should give feedback to OIT-ITS via the patchmanagement@lists.gatech.edu community, if it is determined that a patch breaks any application.
- iii. Standards and controls
 1. OIT-ITS has a list of OSs and standard applications that are tested and validated. This link is located at the following link:

http://www.oit.gatech.edu/css_csr/desktop/standard_suite_image.cfm
 2. OIT-ITS is not responsible for any data loss, time down, or catastrophic failure of any machine(s). ***The CSR/CSS/User will be responsible for re-installing the machine or for any data that is/was on the machine in any necessary event. The department should have some back up mechanism in place to protect against data lost.***
- iv. Expectations of CSR/CSS/Users
 1. ***OIT-ITS must have an administrator level account & password on all machines that are patched by OIT’s central patch management service*** This account will be established with each subscribing department. Each department user or CSR/CSS must create the account on the machine before patching can begin.
 - a. OIT-ITS may request a change of the “Patch Management Administrator” password. This would occur in the event of Central staff changes, system compromises, etc.
 - b. Department CSR/CSS may request a change of the “Patch Management Administrator” password for their unit. This would occur in the event of department staff changes, system compromises, etc.

¹ [*Additional OIT Staff may be required*](#)

- c. All “Patch Management Administrator” password changes must be coordinated between the CSR/CSS and OIT-ITS.
 - d. Whenever there is a need to add or remove clients or to reinstall or reimage an existing machine under your patch management subscription an E-Mail must be sent to <http://www.remedy.gatech.edu/ITS/campus/patchmgt-change.html>
 2. Desktops patched by OIT-ITS should have the same OS and application software versions as those tested by OIT –ITS
http://www.oit.gatech.edu/css_cs/desktop/standard_suite_image.cfm
 3. Department CSR/CSS must accept the risk of patches breaking their OS or applications if OS and software version differences exist between OIT-ITS Standard test configurations and department machines.
 4. In order for OIT-ITS to patch Microsoft Office applications, Office must be installed from an Office Installation Point specified by OIT-ITS. This location will be specified by OIT-ITS when a department requests to have some machines patched by OIT-ITS. This will require that the CSR/CSS/User uninstall and re-install office from the installation point or the Office patch update can be done locally by the department.
 5. Should a patch cause catastrophic failure of a machine(s), the CSR/CSS/User will be responsible for re-installing the machine and for any data that is/was on the machine.
 6. The departmental CSR/CSS/User will be responsible for performing initial troubleshooting on any applications that break. They should give feedback to OIT-ITS if it is determined that a patch breaks any application. See “testing” in section I for testing methods to determine if a patch has broken an application. Send E-Mail of results to patchmanagement@lists.gatech.edu
- v. Expectations of OIT-ITS
 1. Patches deployed by OIT-ITS will be scheduled for deployment. There may be staggered times deployment will be done. This is dependant on an agreement between Department and OIT-ITS.
 2. Critical Microsoft Patches will be tested against OIT-ITS standard administrative desktop suite within 1 business day of notification from OIT Information Security (generally within 24 hours).
 3. Standard patches are evaluated monthly following Microsoft’s new release schedule and should be deployed within 5 business days.
 4. OIT-ITS will communicate all results to the CSR list and issues with any patches to the patchmanagement@lists community. When changes occur to the OIT-ITS Standard software or versions this will also be communicated to both list.
- vi. Request Process for Patch Service by OIT-ITS
 1. Request desired number of seats needed for your department, either during the initial request, or during subsequent request.
 2. Submit request to <http://www.remedy.gatech.edu/ITS/campus/patchmgt-setup.html>

to add machines to OIT Central Patch Management Service. Send the following information about each machine or group of machines you want to add:

- a. Department
 - b. CSR/CSS Name
 - c. Phone number
 - d. E-mail
 - e. List of IP addresses or I.P. range for machines to be patched
 - f. List of all software outside of the standard & OS running on the machines to be patched, including versions
 - g. Identify time window for scheduled patch deployment to your systems
3. OIT-ITS will verify receipt of your request by sending a confirmation E-Mail.
 4. OIT-ITS will contact department CSR/CSS within 2 days of receipt of request to schedule a consultation meeting.
 5. OIT-ITS will add your machine(s) to the appropriate patch group within 5 business days of the consultation meeting and send confirmation via E-Mail when completed.
 6. After successful scanning of designated machines in department, you are now a registered patch recipient.
- c. **Option C-Mixed -Central and Distributed Patching-** This model is a combination of Option B, central management, and Option A, distributed management. The department patches most of its machines; OIT-ITS patches those department machines that conform to the requirements stated in Option B for Central Patch Management.
- i. Diagram-See <http://www.itac.gatech.edu/desktop-management/patch-deploy/option-C-mixed.pdf> for the diagram of Option C.

Some of the features of this architecture apply to all architectures. One feature is that the computers can be grouped by the physical hardware, i.e. desktops, laptops, and servers, or they can be grouped by the function or software used on those machines in a functional patch group, i.e. for Computer Aided Engineering Software, Peoplesoft, etc.

Another feature is that for each group, a test machine is designated to represent that group. This is a best practice, but not a requirement, as costs may prohibit this.

A third feature is test groups can be merged into a larger group. Thus the patches can be deployed on the entire test groups with a single deploy command. To do this, see the "HFNetChkPro Initial Setup and Scans" document.

Lastly, see that a department can be behind a firewall and maintain a connection to the OIT-ITS patch server.

There are two things indigenous to Option C. One is that machines running the standard administrative applications can be put under the administration of OIT-ITS for patch scanning and deployment.

The second thing unique is that each department will run and maintain its own patching “server.” These “servers” include a copy of the HFNetChkPro software and a copy of the HFNetChkPro patch repository. They may also include an Office installation point, and a SQL server. See the “HFNetChkPro Initial Setup and Scans” document.

- ii. Expectations - The expectations outlined in Option B, Central Support, apply for any machines that a department would want OIT-ITS to patch.
- iii. Support
 - 1. The only support provided by OIT-ITS will be the support outlined in Option B, Central Support, for machines that are eligible to be patched by OIT-ITS.
 - 2. See section III, Support Sources, for where to go for help.
- d. **Option D-Mixed-Central Server-Distributed patching-** This model is similar to Option C, except machines will not be patched by OIT-ITS, but a department with its own patch management console/computer will connect to OIT’s central server to obtain patches and store patch scanning and deployment information.
 - i. Diagram-See <http://www.itac.gatech.edu/desktop-management/patch-deploy/option-D-limited-mixed.pdf> for the diagram of Option D.

There are two things indigenous to Option D. First note that OIT-ITS doesn’t patch any machines for the departments. Secondly note that the department runs its own HFNetChkPro console, which is attached to OIT’s central server. The patches and scanning data reside on OIT’s server.

- ii. Availability

Departments can run their own console and attach to the OIT patch server if so requested. A department requesting this option must request the appropriate number of licenses for the number of machines. The departmental CSR/CSS will be responsible for running the console and performing initial troubleshooting on any applications that break. They should give feedback to OIT-ITS via the patchmanagement@lists.gatech.edu community, if it is determined that a patch breaks any application.

This option is not available to individual users or small departments with no CSR/CSS support. Individual users or small departments with no support should use Option B.
- iii. Standards and controls
 - 1. OIT-ITS has a list of OSs and standard applications that are tested and validated. This link is located on the patch management page http://www.oit.gatech.edu/css_csr/desktop/standard_suite_image.cfm

2. OIT-ITS is not responsible for any data loss, time down, or catastrophic failure of any machine(s). **The CSR/CSS will be responsible for re-installing the machine or for any data that is/was on the machine in any necessary event. The department should have some back up mechanism in place to protect against data lost.**
- iv. Expectations of CSR/CSS
1. In order for the CSR/CSS to use their console to patch Microsoft Office applications, Office must be installed from an Office Installation Point specified by OIT-ITS. This location will be specified by OIT-ITS when a department requests to have a console connected to OIT's patch server. This will require that the CSR/CSS uninstall and re-install office from the installation point or the Office patch update can be done locally by the department.
 2. The CSR/CSS will provide a list of machines to OIT-ITS and what groups are needed for the CSR/CSS to appropriately group their machines. This will be done at the time of the consultation and updated with the addition of new machines.
 3. The CSR/CSS will agree to not scan or patch systems in other departments, only theirs.
 4. Should a patch cause catastrophic failure of a machine(s), the CSR/CSS will be responsible for re-installing the machine and for any data that is/was on the machine.
 5. The departmental CSR/CSS will be responsible for performing initial troubleshooting on any applications that break. They should give feedback to OIT-ITS if it is determined that a patch breaks any application. See "testing" in section I for testing methods to determine if a patch has broken an application. Send E-Mail of results to patchmanagement@lists.gatech.edu
 6. Whenever there is a need to add or remove clients or to reinstall or reimage an existing machine under your patch management subscription an E-Mail must be sent to <http://www.remedy.gatech.edu/ITS/campus/patchmgt-change.html>
- v. Expectations of OIT-ITS
1. OIT-ITS will provide the CSR/CSS with an account to access the OIT-patch administration server and an appropriate license code for their department.
 2. OIT-ITS will create a group or groups in the central database, so that the CSR/CSS can patch those machines.
 3. Critical Microsoft Patches will be tested against OIT-ITS standard administrative desktop suite within 1 business day of notification from OIT Information Security (generally within 24 hours). Results will be posted to the patch management page http://www.oit.gatech.edu/css_csr/microsoft_windows_patch_testing/overview.cfm and communicated to the CSR list.

- vi. Request Process for running a console connected to OIT's server
 1. Request desired number of seats needed for your department, either during the initial request, or during subsequent request.
 2. Submit request to <http://www.remedy.gatech.edu/ITS/campus/patchmgt-setup.html> to request a console for your department. The request should include the following
 - a. Department
 - b. CSR/CSS Name
 - c. Phone number
 - d. E-mail
 - e. List of groups names for the patch groups
 - f. List of IP addresses or I.P. range for machines to be patched
 3. OIT-ITS will verify receipt of your request by sending a confirmation E-Mail.
 4. OIT-ITS will contact department CSR/CSS within 2 days of receipt of request to schedule a consultation meeting.
 5. OIT-ITS will create groups and send the required information within 5 business days of the consultation meeting and send confirmation via E-Mail when completed
 6. You are now registered to set up and install HFNetChkPro to patch your machines.

III. Support Sources

- a. **Trial Software** – to help in the decision to request HFNetChkPro, trial software can be downloaded from <http://www.shavlik.com/pDownloadForm4.aspx>.
- b. **Tutorial** – A tutorial is available in HFNetChkPro. Under the “help” menu select “contents” and then choose the “Welcome to HFNetChkPro” icon in the top middle of the window. Use the “next” and “previous” button to navigate through the tutorial.
- c. **Training** - Training will be scheduled early in the initial deployment. Training classes will be taught each semester, if there is a minimum of 10 participants. Some additional training sessions may be offered by OIT.
- d. **Initial Server Setup and Scans** - Use the “HFNetChkPro Initial Setup and Scans” document as a good “getting started, best practices” guide.
- e. **OIT-ITS web site of tested patches** - This is located at http://www.oit.gatech.edu/css_csr/microsoft_windows_patch_testing/overview.cfm
- f. **Listserv lists** - patchmanagement@lists.gatech.edu has been created for discussion of issues related to patching.
- g. **CSRs** - E-mail the CSR mail list, csr@lists.gatech.edu , if issues still cannot be resolved. The campus has a lot people who may have tried what you are trying to do.

- h. **Request for console, licenses and/or central patch service -**
<http://www.remedy.gatech.edu/ITS/campus/patchmgt-setup.html>
- i. **OIT-ITS** – CSR/CSSs can contact OIT-ITS for problems related to standard applications by submitting a request to
<http://www.remedy.gatech.edu/ITS/campus/patchmgt-help.html>
- j. **OIT-ITS** – CSR/CSS must report when they re-image, rebuild, add and/or remove machines from the patching process by submitting information at
<http://www.remedy.gatech.edu/ITS/campus/patchmgt-change.html>
- k. **Direct communication with vendors** - The vendor contact information will be posted to the list and may be used if the issues still cannot be resolved.

IV. Timeline

- April 2004 - Presentation at CSR meeting officially announcing OIT opt-in support for patching departmental computers.
- March 2004 - Finalization and approval of implementation and support plans
- Jan.-Feb. 2004 - Initial HFNetChkPro setup and refinement of implementation and support plans.
- December 2003 - Training class was held.
- November 2003 - Bid selection was completed and software purchased.
- October 2003 - Initial draft of implementation, purchasing and support plan was created.
- September 2003 - RFQ was finalized and sent out for bid