

My Temporary Passwords

Note: Please remember to change these passwords as soon as you have decided on or chosen more secure versions.

See the following packet page for a guide to creating a secure password.

My Temporary Personal Account Password is: _____

My Temporary localmgr password is: _____

My Temporary Network password is: _____

Quick Guide to Creating a Secure Password

The passwords chosen by students at Rose-Hulman protect a range of services, including financial aid, course registration, email, and personal data storage. With freely available cracking programs usable even to the average person, cracking a simple password has never been easier. Choosing a secure password will help to prevent password cracking, and adds a layer of defense against electronic intrusion.

Your network password must include at least 3 of the 4 following sets and be 8 to 20 characters long:

- Lowercase characters
- Uppercase characters
- Numeric characters
- Special characters such as punctuation or alt characters

DON'T:

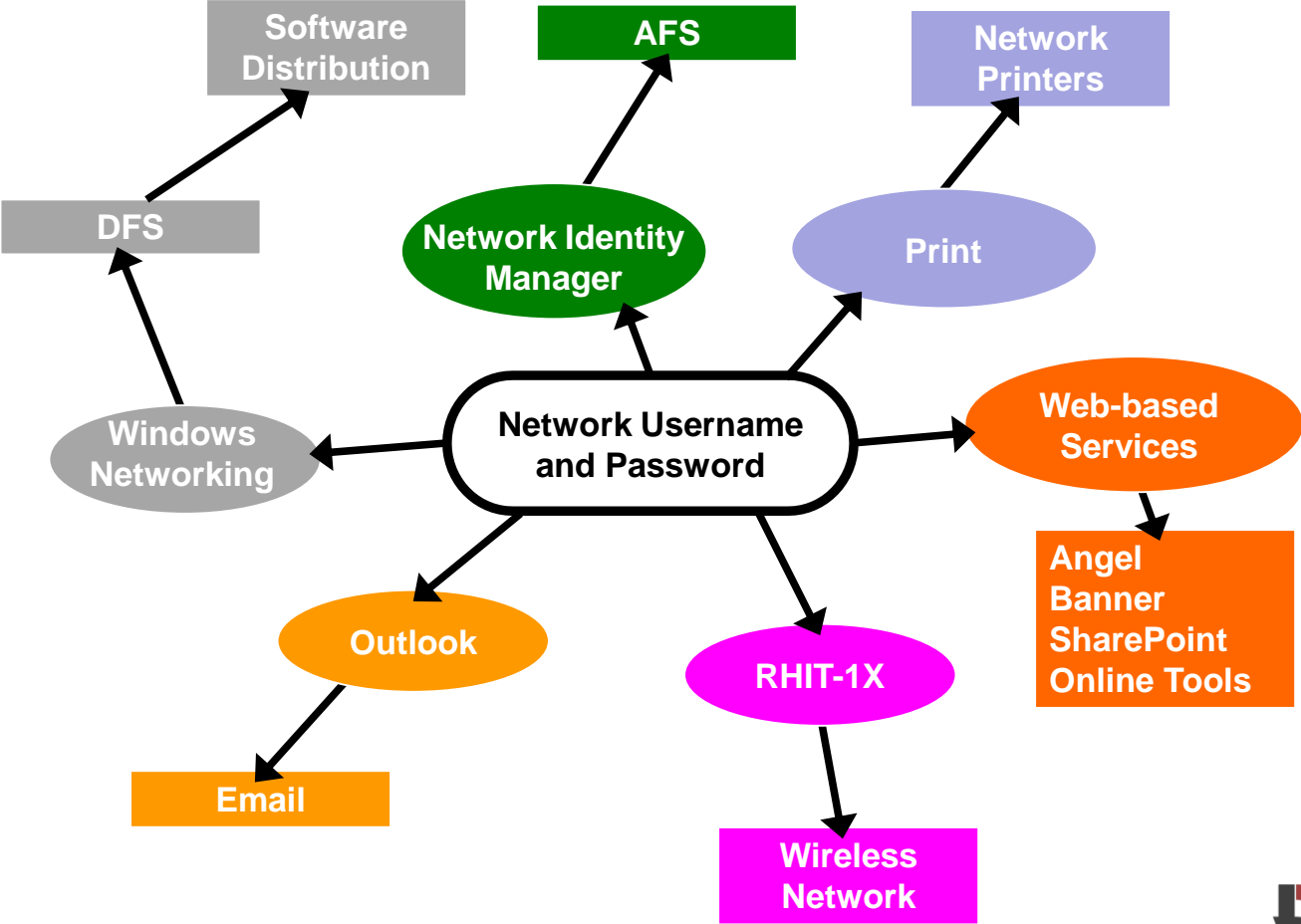
- Use dictionary words, English or foreign
- Use personal information such as birthday, birth year, names of friends or family, or pets' names
- Use ordinary words written backwards
- Just add numbers to a dictionary word

DO:

- Use unusual misspellings of words, made-up words, or unusual phrases
- Change your passwords often
- Consider using alt characters such as †, ě, and ć

Once your password is created, never share it with anyone, including employees of Rose-Hulman IAIT. If someone else needs to use your computer, log in for them or consider temporarily changing your password.

Network Services Overview



Quick Guide to Rose-Hulman's Computing Services

How do I contact the Help Desk for technical support?

Location: G108 on the first floor of Crapo Hall
Phone: x8989
Email: helpdesk@rose-hulman.edu
Web: <http://www.rose-hulman.edu/TSC>

Note: For problems with your laptop's hardware, please bring it to the Help Desk. We can't fix a broken screen on the phone, with email, or on the web.

Where do I take my laptop if it has a problem?

The Help Desk

Where is the Help Desk / Technical Service Center web site?

<http://www.rose-hulman.edu/TSC>

How do I change my password?

Network password (choose one of the following):

- Press Ctrl-Alt-Del, click Change Password, change the "Log on to" field to ROSE-HULMAN, then fill in the password fields
- Go to <http://password.rose-hulman.edu>

Local laptop password: Press Ctrl-Alt-Del and click Change Password

What do I do if I forget my password?

Come to the Help Desk with your student ID.

Where can I get software?

Double click My Network Places → Go to DFS Root, log in with your username and network password if asked, then go to Software folder.

Where can I check my email by using a web browser?

<http://webmail.rose-hulman.edu>

How can I check my email / Exchange quota?

<http://www.rose-hulman.edu/TSC/tools/quota>

What are Rose-Hulman's email servers and their settings?

See <http://www.rose-hulman.edu/TSC/services/email/exchange/>

How do I check or change my Barracuda Spam Firewall settings?

<https://rhspam.rose-hulman.edu>

How can I register a new network card or change an existing one?

Connect the device to the network and open a web browser if available. If you are not prompted with a registration page or the device does not have a web browser, contact the Helpdesk.

How can I check how much bandwidth I've used?

https://www.rose-hulman.edu/TSC/tools/network_usage_tool/

Where do I go to access the Angel course management system?

<http://angel.rose-hulman.edu>

How do I access Banner?

Use Quick Links from <http://www.rose-hulman.edu>

Where can I access the VPN client?

<http://sslvpn.rose-hulman.edu>

What are the addresses of Rose-Hulman's public UNIX servers accessible through SSH?

addiator.rose-hulman.edu

How do I reset my voice mail password if I have forgotten it?

Come to the Help Desk with your student ID.

How do I add a printer?

Click Start → Run, then type [\\print](#), then double-click the printer.

How do I manage a mailing list?

[http://mailman.rose-hulman.edu/mailman/admin/\(list name\)](http://mailman.rose-hulman.edu/mailman/admin/(list_name))

What online tools does IAIT provide?

Many are located at <http://www.rose-hulman.edu/TSC/tools/>

Quick Guide to DFS and AFS Network Storage

Rose-Hulman provides a network file storage services called DFS and AFS. Using these services, it is possible to create remote backups of important files, share data between users, and create websites. DFS and AFS are also used by some courses as a way to turn in electronic homework or test files.

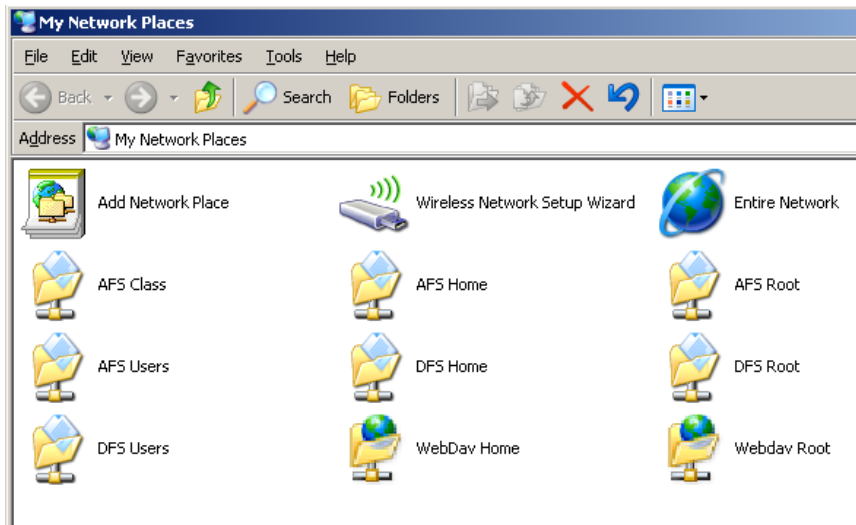
You have 500 MB of space in your DFS directory. You have 100MB of Public space in your AFS directory, and 100MB of space for the remainder of the directory.

To Access DFS:

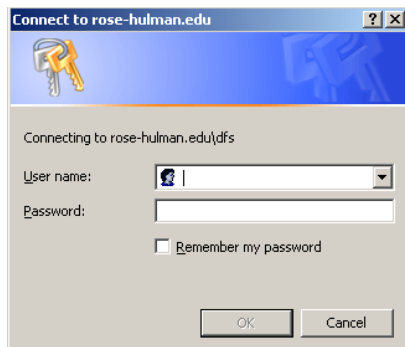
1. Open My Network Places



2. Double click the DFS location you want to access.



3. Enter username (i.e. username@rose-hulman.edu) and network password if asked.



To Access AFS:

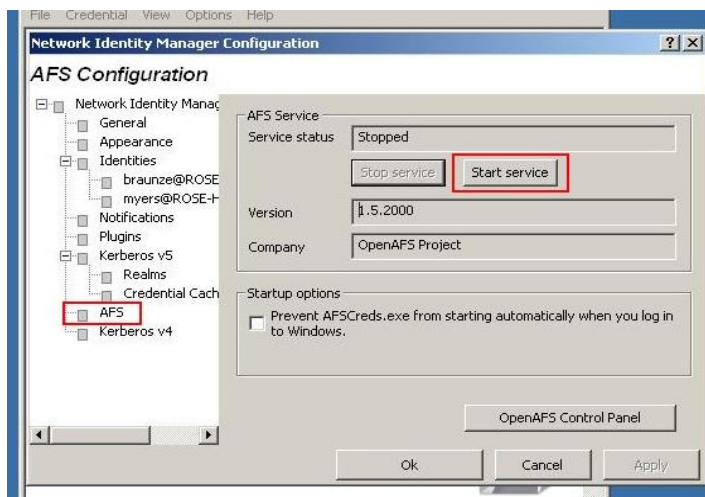
1. Open the **Network Identity Manager** via the icon (shown below) on your desktop.



2. Next, click on **Options** and **AFS** as shown below:



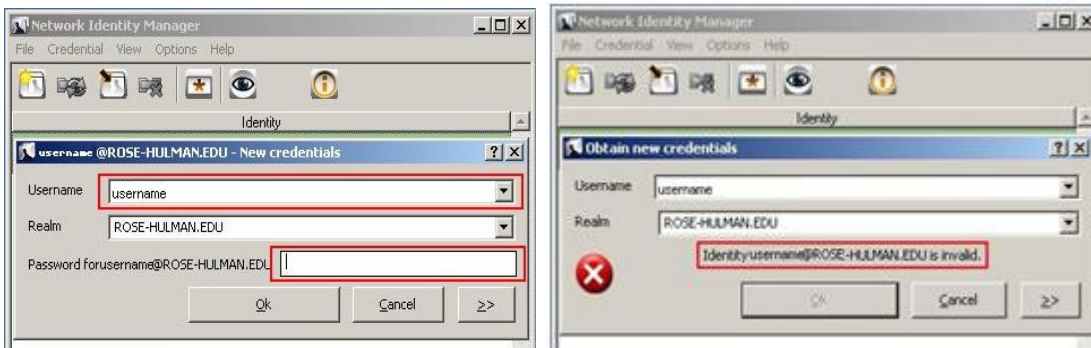
3. This will open the dialog shown below. Select **AFS** then click **Start Service**. Once the Start Service button turns grey, click **OK**.



4. Now, back at the main Network Identity Manager screen, click **Credential** and **Obtain New Credentials** as shown below.



5. The dialog shown on the below left should now appear. Enter your username in the first highlighted field and your **password** in the second and click **OK**. **If you see an error "Identity [name] is invalid,"** as shown on the right, **double-check** your username and try again.



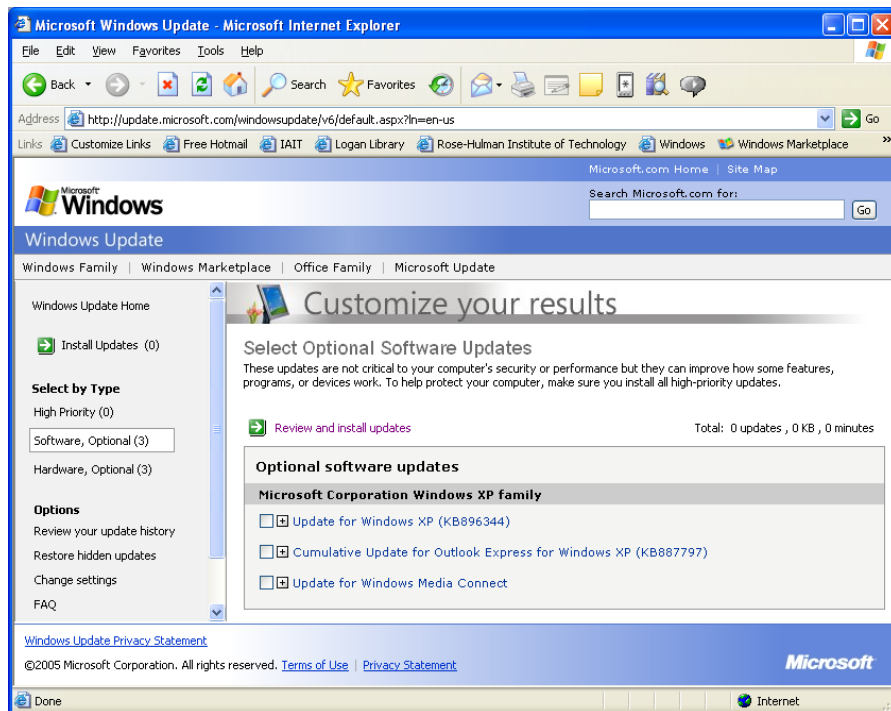
6. Your network drives will now be accessible by opening **My Network Places** via the icon (shown below) on your desktop.



Running Windows Update

Login as LocalMgr. Click Start -> All Programs -> Windows Update. This will open Internet Explorer. If you are prompted to install an ActiveX component from Microsoft, it is safe to do so (Microsoft is a trusted source). Click “Custom”.

Select all High Priority updates. On the left side there is a “Select by Type” section, click “Software, Optional”. Again select all the Software updates. We do NOT recommend selecting the Hardware, Optional updates for laptops. Most of these are drivers and can cause problems on laptops.

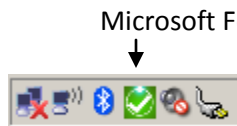


Click “Review and install updates”. Click “Install Updates”. The updates will now install.

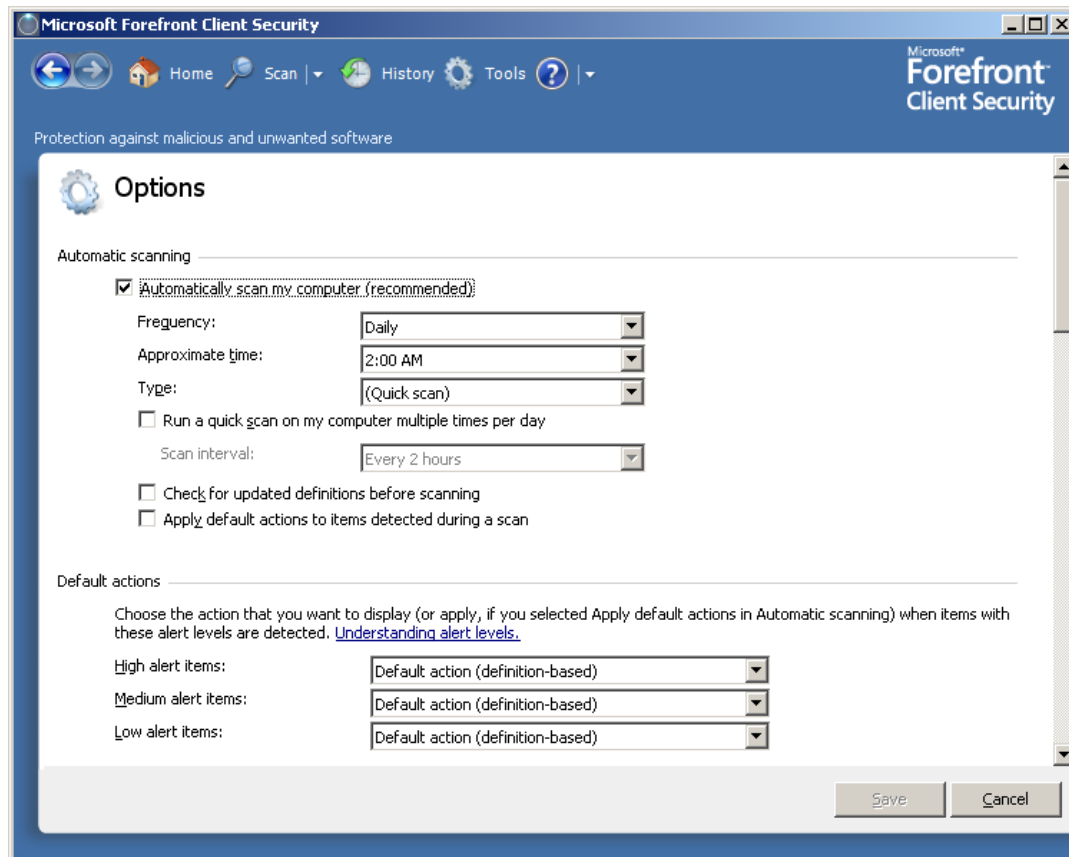
Changing Microsoft Forefront Scan Time

By default, Forefront will perform a Quick scan at 2:00AM. This is not very resource intensive as it only scans running programs and the most likely places for malware to hide. However, you may choose to adjust the time when the Quick scan runs or schedule a Full scan instead. Note: A Full scan is resource intensive, which slows processing, and should be scheduled when it will not affect use of your laptop.

1) In your System Tray, located in the lower right of your screen, double click on the Microsoft Forefront Icon.



2) Click Tools and then Options. Change the Approximate time to the time you wish for your computer to be scanned.



Ways to Extend Battery Life

1. Turn down the LCD brightness.
 - a. Press the Fn and F9 keys simultaneously to decrease Brightness
 - b. Press the Fn and F10 keys simultaneously to increase Brightness
2. Use built-in Windows power management.
 - a. Power Options within the Control Panel
 - b. Using this dialog, you can tell the computer to turn off the monitor and/or hard drive after a certain amount of time; or tell the entire computer to stand-by (minimal power usage) or hibernate (no power usage)
3. Turn off wireless Ethernet when not in use.
 - a. Turn wireless network card on or off by lightly touching the wireless icon by the power button
4. Set screen blanking to 1 or 2 minutes.
 - a. Right click on the desktop
 - b. Click 'Properties'
 - c. Set 'Screen Saver' to 'Blank' via the pull down menu
 - d. Set 'wait' to 1 or 2 minutes
5. Close unused programs.
6. Do NOT fully drain, and then recharge lithium ion batteries every few months. They do not exhibit memory issues.
7. Remove unused notebook powered USB devices.
8. Don't watch DVDs and don't play graphics-intensive games on battery power.

Three ways to Prevent Hard Disk Damage and Data Loss

1. When powering off the laptop you should shut down Windows. Do not just hold down the power button.
2. Don't move or carry your laptop while it is running.
 - a. If the laptop will not shutdown, hold the power button down for approximately five seconds. This will power off the laptop, wait 10 seconds before moving.
3. It is always wise to make a backup copy of your 'My Documents' folder.
 - a. We suggest at least once a week that you back up your data. You can create DVD or CD backups with your laptop. External hard drives and USB Thumb drives provide quick and easy backup.
 - b. Important class work can be backed up to your DFS network space (the DFS Home Folder in My Network Places). Your data on DFS is automatically backed up by IAIT.

Helpful Guide to Malware Removal

There are many good tools to use to clean malware infections. The Help Desk recommends the use of a combination of Microsoft Forefront, AdAware and Spybot - Search & Destroy. These four programs offer the most comprehensive malware removal if they are installed, setup, used, and updated properly. Below are the instructions for installing, configuring, and using each of the cleaning tools.

Installation:

1. Log in as localmgr:

It is important that you use the **localmgr** account rather than a different account with administrative privileges. The **localmgr** account is often less infected and is easier to use to install and update programs.

2. Download the programs:

- **Spybot - Search and Destroy:** Found at <http://www.download.com>
- **AdAware:** Found at <http://www.download.com>

The following are already included on any laptop imaged by IAIT:

- **Microsoft Forefront:** Found at <http://www.microsoft.com>

3. Installation:

- **Microsoft Forefont:** Already installed on your computer.
- **Spybot - Search & Destroy:** Accept the defaults presented by the installer until you get to the "Select Components" portion of the install. Uncheck the "Additional Languages" and the "Skins to change appearance" boxes. On the "Select Additional Tasks" portion of the install, uncheck all boxes and start the installation. Uncheck the "Run Spybot.exe" option on the last part of the installer.
- **AdAware:** Accept the default options presented by the installer, but stop the automatic scan that occurs after AdAware finishes installing.

Setup:

Note that you will not run any scans yet and that you must have an Internet connection for this stage.

1. Microsoft Forefront:

- Microsoft automatically downloads new virus and malware definitions each day.

2. Spybot – Search & Destroy:

- Start Spybot – Search & Destroy.
- If any compatibility warnings pop up, close them.
- Select "Next" on the first page of the "Spybot-S&D Wizard."
- On the second page of the wizard, select "Search for updates."
- Once updates are found, select "Download all available updates."
- Spybot may restart (don't worry if it doesn't).
- Click next in the wizard until you get to step 7.
- At step 7, select "Start using this program."
- In the main Spybot window, go to "Mode->Advanced Mode."
- Select "Yes" to the warning message that pops up.
- On the left side of the Spybot window, select the "Settings" tab.
- In the new menu that pops up, select the "Ignore Products" button.
- Right click in the new window with all of the check boxes and select "Deselect All."
- Scroll down the list of products to "MITBand(CrystalsMedia)" and check its box. This will prevent Spybot from removing AFS/Leash from your system.
- Close Spybot.

3. AdAware:

- Start AdAware.
- Click "Check for updates now."
- In the update window, select "Connect."
- Download any updates.
- Select "Finish."
- Close AdAware.

4. Disable System Restore:

- Right click on "My Computer" and select "Properties" to bring up "System Properties."
- Select the "System Restore" tab .
- Check "Turn off System Restore."
- Click "OK" to close "System Properties" and click "Yes" on the dialogue box that pops up.
- We will turn System Restore back on after we have cleaned the system.

6. Safe Mode:

The next thing you need to do is restart into Windows XP Safe Mode. To do this restart and press the "F8" key several times right after the manufacturer's splash screen (the Compaq/HP/Dell logo) screen. This should display the Windows boot options menu. If the screen asks you to select an operating system press "F8" again to display the Windows boot options menu. On this menu, select "Safe Mode;" make sure you do not select the "Safe Mode (with networking)" option to avoid having a network connection for the first part of the cleaning process.

Cleaning:

1. Accounts:

You will have to run all of the scans in each of the following modes (in order); Safe Mode, localmgr, your user account, and any other accounts on the system. Every account on the system must be cleaned one-at-a-time to prevent re-infection. It is important that you run the scans in this order.

2. Scans:

Make sure you have configured and updated all of the tools as directed in the last section before you continue any farther. This handy grid will help you keep track of where and under which account(s) you have scanned; check each box after you have completed the step (*a larger version is provided at the end of this document*):

Account/Tool	Microsoft Forefront	Spybot	AdAware
Safe Mode			
Localmgr			
User Acct.			
Other Accts.			

3. Microsoft Forefront:

- Open Microsoft Forefront
- Click the downward-pointing arrow next to "Scan" and select "Full Scan"
- After the cleaning is finished, close Windows Defender

4. Spybot – Search & Destroy:

- Click "Check for problems" and let the scan run
- Ensure all of the found items are checked
- Click "Fix selected problems" to start the cleaning
- If Spybot says it will need to start after a restart, select "No"
- After the cleaning is finished close Spybot

5. AdAware:

- Click "Start" and ensure that "Perform full system scan" is the type of scan selected
- Click "Next" to start the scan
- Once the scan has completed, right click somewhere in the list of malware found and choose the "Select All" option
- Click "Next" and select "Yes" on the warning message
- After the cleaning is finished, close AdAware

6. Move to the next account in the checklist and repeat steps 3-6:

7. Enable "System Restore":

- Right click on "My Computer" and select "Properties" to bring up "System Properties"
- Select the "System Restore" tab
- Uncheck "Turn off System Restore" and click "OK" to close "System Properties"

8. Pay Attention to the way your machine performs over the next few days. If you still notice problems, you should read the "Your Options If Your Machine Still Isn't Working" section of this paper.

Options If Your Machine Still Isn't Working:

If you have cleaned your system and it is still not working, you have the following options:

1. Try cleaning again; more problems may be fixed the second time around.
2. Bring the machine to the Help Desk for a reload. If you choose to do this, make sure all of your important files are located in the "My Documents" folder; the "C:\Documents and Settings" folder (and its subfolders) is the only folder the Help Desk will backup. Depending on the size of your "My Documents" folder, the reload may take as long as 6 hours. Reload requests must be submitted to the Help Desk no later than 10AM if you require same-day return of your laptop. A reload is the only guaranteed way to remove all malware from a system.

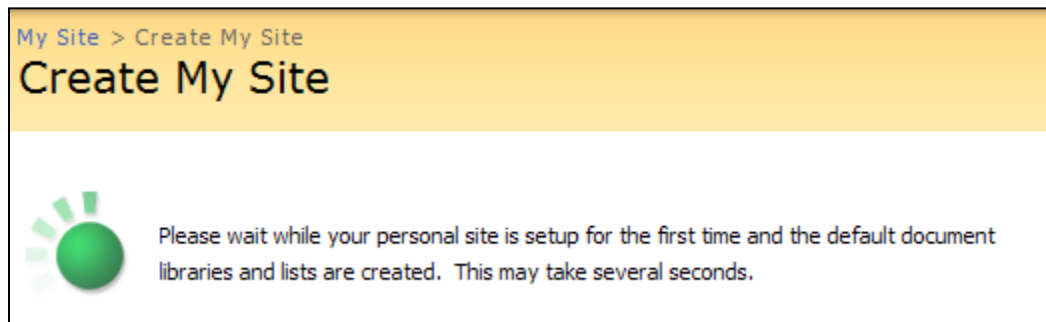
The Help Desk will attempt to answer any questions about this process.

Account \ Tool	Microsoft Forefront	Spybot	AdAware
Safe Mode			
Localmgr			
User Acct.			
Other Accts.			

Creating your Personal SharePoint Site

Your personal site is called a *My Site*. It will be created the first time you access it.

1. Navigate to <http://myrhit.rose-hulman.edu>.
2. Click the *Sign In* link in the upper-right corner of the page.
3. When prompted, enter *[your username]@rose-hulman.edu* and your network password.
4. Click the *My Site* link.
5. You will see the following message and will then be redirected to your site when it is ready.



What can you do with your My Site

These are just a few of the things you can do with your My Site:

- Create a portal storing your favorite links and RSS feeds
- Store and share documents and pictures
- Create additional pages
- Create a discussion forum to communicate with friends
- Create a Blog

Introduction to your My Site

Your *My Site* is pre-configured with a few default lists such as the *Personal Documents* library and the *Shared Pictures* library. These can be accessed by using the menu on the left.

In the center of the page, you will see several blocks of content called web parts. You can modify the layout of the page by clicking the **Site Actions** button and selecting *Edit Page*. From here, you will be able to add, remove and modify the web parts that are displayed on your page. When complete, click the *Exit Edit Mode* link just below the **Site Actions** button.

To add more content to your *My Site*, click the **Site Actions** button and choose *Create*. From here, you can create many things for your site including a forum, additional pages and sub-sites.

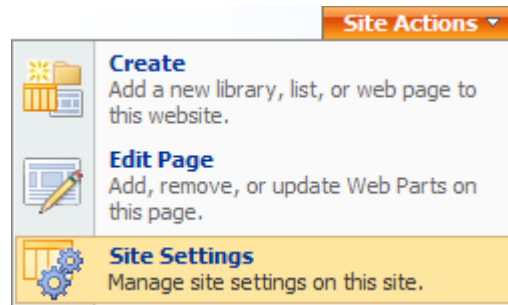
Creating your Blog site

Click the **Create Blog** button to automatically set up your Blog site. The first post on your Blog will explain how to get started creating posts.

Granting Anonymous Access to your Blog

Navigate to your Blog site

Click the Site Actions button and select 'Site Settings'

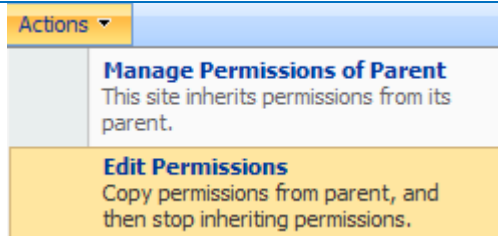


In the 'Users and Permissions' section, select 'Advanced permissions'

Users and Permissions

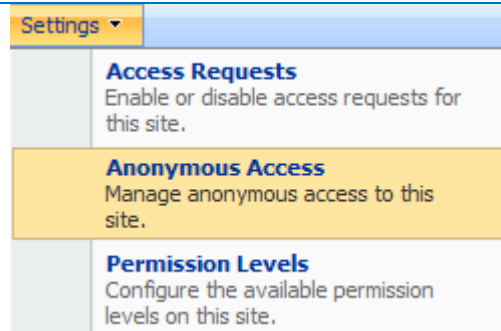
- People and groups
- Advanced permissions

From the 'Actions' menu, select 'Edit Permissions'



Click 'OK' when prompted.

From the Settings menu, select 'Anonymous Access'



Select the 'Entire Web site' option and click 'OK'

Anonymous users can access:

- Entire Web site
- Lists and libraries
- Nothing

Anonymous users can now read your Blog but they will not be able to post comments.