

# Quick Reference Guide Table of Contents

<b>QUICK REFERENCE GUIDE TABLE OF CONTENTS.....</b>	<b>1</b>
<b>OVERVIEW .....</b>	<b>4</b>
<i>Being a “Reasonable Person” .....</i>	<i>4</i>
<i>Sharing Computing Resources .....</i>	<i>4</i>
<i>General Computer Information .....</i>	<i>5</i>
<b>HOW TO LOGIN.....</b>	<b>6</b>
<i>SCS Authentication.....</i>	<i>6</i>
<i>Logging on to Windows .....</i>	<i>6</i>
<b>PASSWORD OVERVIEW.....</b>	<b>8</b>
KERBEROS PASSWORDS.....	8
<i>If you require the use of iPass or VPN, use the instance creation page to create this Kerberos instance or contact the SCS Help Desk. ....</i>	<i>8</i>
<i>Refer also to Changing Your Kerberos Password .....</i>	<i>8</i>
OTHER PASSWORDS .....	9
<i>Changing Passwords .....</i>	<i>9</i>
<i>Changing Your Kerberos Password .....</i>	<i>10</i>
<i>How to Use the SCS webISO instance tool to Create New Kerberos Instances .....</i>	<i>11</i>
<i>Windows Passwords .....</i>	<i>12</i>
<i>How to Change Your SCS Domain Password.....</i>	<i>12</i>
<i>Using Jeeves to Administer Your Accounts .....</i>	<i>12</i>
<i>How to use Jeeves to Change AFS Quotas .....</i>	<i>14</i>
<i>How to Use World Wide Web Functions in Jeeves.....</i>	<i>14</i>
<i>How to Use Jeeves to Create an Oracle Calendar Server Account .....</i>	<i>14</i>
<i>Creating the Oracle Calendar Client Account in Jeeves.....</i>	<i>15</i>
<b>SCS EMAIL.....</b>	<b>16</b>
MANAGING YOUR EMAIL ADDRESSES .....	16
<i>Managing Your Email Forwarding Address .....</i>	<i>18</i>
<i>Modifying Your Email Local Addresses .....</i>	<i>18</i>
<i>Modifying Your SCS Preferred Email Address .....</i>	<i>19</i>
<i>Grey Listing .....</i>	<i>19</i>
<i>Discard Spam.....</i>	<i>20</i>
<b>MAILING LISTS .....</b>	<b>20</b>
<i>Email Etiquette .....</i>	<i>21</i>
<b>SCS IMAP EMAIL STORE .....</b>	<b>21</b>
<i>Webmail.....</i>	<i>22</i>
<i>Message Auto-Expiration.....</i>	<i>23</i>
SIEVE SCRIPTING INFORMATION.....	25
<i>Sieve Scripts .....</i>	<i>25</i>
<i>How to Create and Activate a Sieve Script Using the Web Sieve Interface:.....</i>	<i>26</i>
<i>Setting up an “Out of Office” Message with the Web Sieve Interface:.....</i>	<i>26</i>
<b>PRINTING .....</b>	<b>27</b>
<i>Printing Etiquette.....</i>	<i>27</i>
<i>Getting Help.....</i>	<i>27</i>

<i>Lists of Printers</i> .....	27
<b>NETWORKING IN SCS</b> .....	<b>28</b>
NETWORK USE POLICIES .....	28
<i>Introduction</i> .....	28
<i>Connecting Hosts to the Network</i> .....	28
<i>Naming Policy</i> .....	29
DOMAINS AND VIRTUAL HOSTING.....	29
<i>Domain hosting</i> .....	29
<i>Virtual Web Hosting on the SCS Web server</i> .....	30
<i>Network Usage Restrictions</i> .....	30
<i>Running Network Services</i> .....	31
REMOTE ACCESS.....	31
<i>VPN</i> .....	31
<i>iPass</i> .....	32
<i>iPass Tips</i> .....	32
WIRELESS NETWORKING (CMU COMPUTING SERVICES) .....	34
<i>Restrictions on Using Wireless Connections</i> .....	34
<b>AFS</b> .....	<b>35</b>
AUTHENTICATION .....	35
<i>Windows</i> .....	35
<i>Linux</i> .....	36
VOLUMES.....	37
<i>Requesting Volumes &amp; Quotas</i> .....	37
AUTHORIZATION.....	39
<i>Permissions &amp; Access Control Lists</i> .....	40
<i>Show the ACL</i> .....	40
<i>Add or Remove Users &amp; Groups on ACLs</i> .....	42
MANAGING PTS GROUP MEMBERSHIPS .....	43
<i>Negative Permissions</i> .....	44
BACKUPS & RESTORES.....	46
<b>SCS COMPUTING FACILITIES SUPPORT</b> .....	<b>47</b>
SCS UBUNTU LINUX SUPPORT .....	47
MICROSOFT WINDOWS SUPPORT .....	48
<i>Hardware Support</i> .....	48
<i>Software Environment &amp; Support</i> .....	49
<i>Backups</i> .....	49
MAC .....	50
<i>What Apple Hardware and Software Do You Support?</i> .....	50
<i>I Want to Upgrade My Mac to the Latest OS How Can I Do This?</i> .....	50
<i>What Apple Computer Do You Recommend I Buy?</i> .....	50
<i>Printing from a Mac</i> .....	50
<i>What Software Do You Support for the Mac?</i> .....	51
ALL FACILITIZED MACS WILL BE DEPLOYED WITH THE FOLLOWING BASELINE SOFTWARE: .....	51
<i>What if I Want to Run Microsoft Windows on My Mac?</i> .....	51
<i>Backups &amp; Restores</i> .....	51
MAC .....	52
<i>Mac Default Disk Partitioning</i> .....	52
<i>SCS Baseline Configuration for Mac Hosts</i> .....	52
HARDWARE SUPPORT .....	53
BACKUPS.....	53

RESTORES .....	54
LOCATING PEOPLE .....	54
<i>Finger</i> .....	54
<b>SECURITY .....</b>	<b>55</b>
<b>WINDOWS AND MAC MALWARE PROTECTION.....</b>	<b>56</b>
<i>Attachments &amp; Trojans</i> .....	56
<i>Symantec Management Console</i> .....	56
<i>Keeping virus definitions up-to-date</i> .....	57
<i>Dealing with a malware infection</i> .....	57
<i>Symantec Endpoint Protection FAQ</i> .....	58
<i>Contents</i> .....	58
<i>Frequently Asked Questions</i> .....	58

# Overview

Welcome to the Carnegie Mellon University School of Computer Science. The purpose of this document is to provide a quick start reference guide for new SCS users. This is not a comprehensive set of instructions but an aid to utilizing the SCS Computing Facilities. A complete documentation set can be found at

<http://www.cs.cmu.edu/~help/downloads/introduction/Quick-Reference-Guide-2011.pdf>

You can also refer to the SCS Computing Facilities Help pages at

<http://www.cs.cmu.edu/~help>

Throughout this guide we will provide the appropriate links for a deeper understanding of the subject matter that is being presented.

## Being a “Reasonable Person”

The Departmental Review Committee long ago developed a list of rules and customs for behavior generally considered acceptable by others in the Department. The list, based on what’s referred to as “The Reasonable Person Principle,” suggests ways to conserve and share public resources and in general how to be a reasonable and responsible member of the SCS community. Violators of the Reasonable Person Principle are not punished in any formal way, but they may feel the disappointment or anger of those they have affected. We present here some guidelines to help you get off to a good start.

## Sharing Computing Resources

### **Help keep our computing Facilities efficient:**

- Keep your account and its password private. You are responsible for anything done from your account.
- Notify SCS Computing Facilities in advance and read the section on Network Usage Policy before connecting anything to our network.
- If you need multiple copies, use a photocopier. Print large documents at off-peak hours or use the high-speed printers. See our web page for printing at:

<http://www.cs.cmu.edu/~help/printing/index.html>

- Close unnecessary machine connections: When you finish with a machine or Ethernet connection, be sure to log off or close the connection to ensure others efficient access.
- Do not play games during peak hours.
- Please respect others’ privacy.
- Do not read someone else’s files unless you know it’s okay: if in doubt, ask for permission, even if that person has not employed any file protection mechanisms.
- Consider printer output private.
- Make sure that your Windows computer(s) have the current patches.

There are socially-acceptable ways of using digital communications:

- Keep messages short
- Don't send anonymous messages or hate mail. These actions can result in the loss of your account privileges
- It is illegal to use government-sponsored equipment and resources or to post messages outside of SCS for commercial gain

## General Computer Information

Most departments in the School of Computer Science will provide incoming students with a desktop or a laptop computer that is facilitated by SCS Computing Facilities. SCS Computing Facilities provides remote access to both Windows and Linux services. Windows services are provided by the Windows Terminal Services system, and Linux services are provided by a cluster of Linux systems.

The Linux General Purpose (GP) services are accessed via a SCS Computing Facilities-provided telnet or SSH client. The preferred access method is via SSH - all Facilitized Windows systems come with the SSH client "putty" installed by default. To access the Linux GP services, connect to the machine "linux.gp.cs.cmu.edu".

The Linux GP cluster can be used for access to command-line or X-Windows based applications, but there are several limitations:

- You cannot set your mail forwarding to the Linux GP cluster. You can, however, use a mail client that reads your mail from another machine.
- You will not have a home directory on the local disk. You should use your AFS home directory to store any files. AFS (the Andrew File System) is a distributed, client-server, file system used to provide most file-sharing services in SCS
- Programs that use large amounts of memory or CPU cycles are discouraged, as this is a shared resource.

Access to Windows services (on an occasional-use basis) from a Facilitized Linux host is through a service known as "Windows Terminal Services". As described on the SCS Computing Facilities help pages.

[http://www.cs.cmu.edu/~help/unix\\_linux/terminal.services.html](http://www.cs.cmu.edu/~help/unix_linux/terminal.services.html)

You may request access to Windows Terminal Services through the SCS Help Desk. You may use the Linux "rdesktop" client to connect to the Windows Terminal service. The syntax for the rdesktop command is `/usr/local/bin/ts std` for standard services.

# How to Login

## SCS Authentication

There are many different username / password combinations that are used in the SCS computing environment, but the three most common are Kerberos, Mail, and if requested, Windows.

When your SCS account is created you will receive the following:

- A Kerberos username and password; these have been sent to you via email.
- A Mail password, unless you are having your SCS mail forwarded to another system.
- A Windows domain password (if requested) would have also been emailed to you.

**Note:** The username for all of these are normally the same, only the passwords would vary.

## Logging on to Windows

On a Windows-based machine, you will be prompted to press ctrl-alt-del to log in. Once you hit ctrl-alt-del, you will see a login window with two fields: Username and Password. Below the password field it should read "Log on to: SCS". This indicates that you are logging onto the SCS Windows domain. Use the Windows username and password that was sent to you in the email mentioned above. If you have not received this email, you most likely do not have a Windows domain account and will not be able to log in to any Facilitized Windows machines. In this case, you should contact the SCS Help Desk at x8-4231 or send email to [help@cs.cmu.edu](mailto:help@cs.cmu.edu) and ask them to create a Windows domain account for you.



## Logging on to Linux

In order to log in to a Facilitized Linux (or other Facilitized UNIX-based) machine you need not only an SCS Kerberos account (that is, your main SCS account) but also a local account on the particular machine to which you wish to log in to. Contact the SCS Help Desk (x8-4231) and ask them to create this local account once your main SCS user account has been created and you have a specific UNIX-based machine that you wish to use. If you have received a graduate student machine from your department you will have an account on the machine assigned to you. Once this local account has been created, simply use your Kerberos username and password to log in to the machine.

# Password Overview

Here in SCS, you will have several types of passwords. Below is an overview of these passwords and their purposes.

**Note:** You should not have any other password be the same as your main SCS Kerberos password. As a new student you should have received your login ID and temporary password, if you have not please contact your advisor.

## Kerberos Passwords

Type of Password	Instance
<b>Kerberos</b>	<p>This is your "Main" username/password combination in SCS. Use this password to authenticate to: AFS services on a Windows machine (using Leash, for example), UNIX-based machines and services.</p> <p>This username and password are assigned to you when you first join the SCS community. See Changing Password section to change this password</p>
<b>/mail</b> (Kerberos instance)	<p>This password is used exclusively with your SCS email. This password is assigned to you when your email account is created.</p>
<b>/root</b> (Kerberos instance)	<p>This is a special Kerberos instance for people who need to do advanced system administration on UNIX-based machines.</p> <p>This password is NOT created for you initially. If you need root access to a Facilitized SCS host, contact the SCS Help Desk.</p>
<b>/remote</b> (Kerberos instance)	<p>Use this password to authenticate to remote services such as: VPN and iPass. This password is NOT created for you initially.</p> <p>If you require the use of iPass or VPN, use the instance creation page to create this Kerberos instance or contact the SCS Help Desk.</p> <p>Refer also to Changing Your Kerberos Password</p>

**Table 1-1**

## Other Passwords

Type of Password	Instance
<b>Oracle Calendar</b> (Non-Kerberos)	This password is used exclusively with Oracle Calendar in SCS. This password is assigned to you when your Corporate Time account is created.
<b>Windows Domain</b>	This password is used to authenticate to Windows-based machines and services, such as: Logging in to Windows machines, printing from Windows to SCS printers, mapping network drives to other Windows machines in the SCS domain, including Monolith.

Table 1-2

## Changing Passwords

It is important when setting your passwords to choose a strong password. A strong password is one that is at least eight characters, includes a combination of letters, numbers, and symbols and is easy for you to remember, but difficult for others to guess.

It should not be a word that is found in the dictionary.

The easiest way to create a strong password that you won't have to write down is to come up with a pass phrase. A pass phrase is a sentence that you can remember, like "My son Aiden is three years older than my daughter Anna." You can make a strong password by using the first letter of each word of the sentence, for example, msaityotmda. However, you can make this password even stronger by using a combination of upper and lowercase letters, numbers, and special characters that look like letters. For example, using the same memorable sentence and a few tricks, your password is now M\$8ni3y0tmd@.

**Note:** Never use/reuse a password that has been published as an example for your actual account password. It is also a good idea to change your password on a regular basis. It should be changed when the time changes in the spring and the fall.

## Changing Your Kerberos Password

When your SCS Kerberos user ID was created along with your Kerberos instance a temporary password was generated by our system. To change your Kerberos password(s) please go to our password instance page at:

<https://webiso.cs.cmu.edu/instance>

Create new Kerberos instances in the form *username/instance*. Multiple Kerberos instances allow different passwords for different situations. You can create the multiple instances including your /mail and /remote instances.

Please refer to the tables 1-1 on page 8 and 1-2 on page 9 for an explanation of the various Kerberos instances

You will see the following page:

WebISO Secure Login - School of Computer Science - Carnegie Mellon University - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://webiso.cs.cmu.edu/

**WebISO Secure Login** School of Computer Science Carnegie Mellon

The resource you requested requires you to authenticate.

User ID:  Instance:

Password:   None  /mail

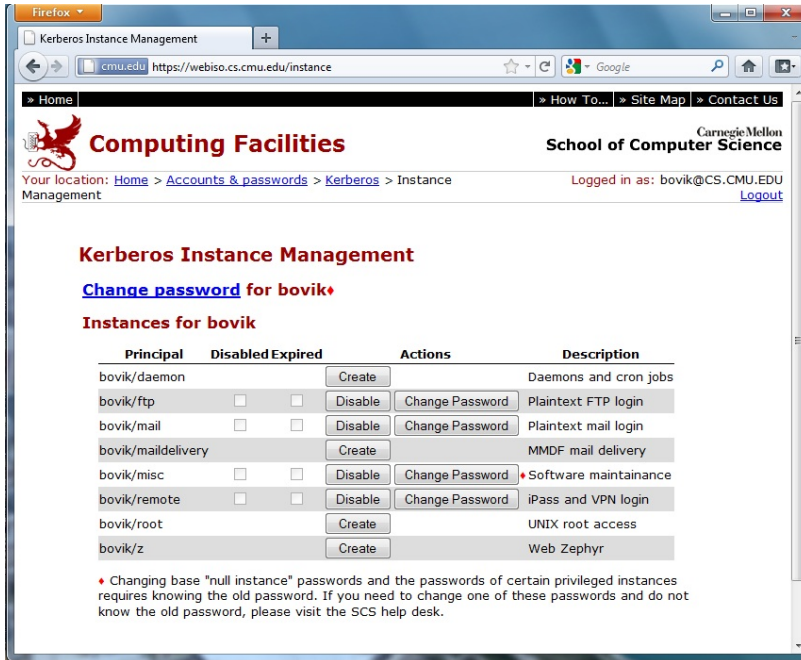
**Warning:** This web page is requesting your User ID and password. If you have any doubts as to the legitimacy of this page, look for <https://webiso.cs.cmu.edu/> in the URL before entering your User ID and password. If you think that this page should not be requesting your User ID and password, please report it to [help@cs.cmu.edu](mailto:help@cs.cmu.edu) and be sure to include the URL.

**Carnegie Mellon Certificates:** Many of the services that use WebISO also use the Carnegie Mellon Certificates. If you haven't already done so, [install the Carnegie Mellon CA Root Certificates in your browser.](#)

**About this service.** WebISO verifies the identity of Carnegie Mellon users. WebISO does not require installation of specialized software. However, your browser must be configured to accept cookies. This is the default configuration for all major web browsers. If you have disabled cookies in the past you will need to enable cookie support in your browser to use WebISO.

This site is maintained by SCS Computing Facilities; send comments to [help@cs.cmu.edu](mailto:help@cs.cmu.edu).  
Version: 3.3.2d-002 © Carnegie Mellon University

To access the tool use your main CS Kerberos ID and password, you will see all of your available instances.



## How to Use the SCS webISO instance tool to Create New Kerberos Instances

Create new Kerberos instances in the form *username/instance*. Multiple Kerberos instances allow different passwords for different situations. You can create the multiple instances including your /mail and /remote instances.

Please refer to the tables 1-1 on page 8 and 1-2 page 9 for an explanation of the various Kerberos instances

Before creating any other instances you should change your initial Kerberos password. Login to a Facilitized Linux based machine and follow the command listed below:

At the command line or in your terminal window type  
`/usr/local/bin/k5passwd`

You should see the following line:

Changing Kerberos password for [username@CS.CMU.EDU](mailto:username@CS.CMU.EDU)

Type in your old password and hit return.  
 Type the new password and hit return.  
 Re-type the new password and hit return.  
 Your password is now changed.

If you do not remember your SCS Kerberos password go to the SCS Help Desk in GHC 4203. Bring a photo ID with you and the Help Desk will assist you with the password change.

## Windows Passwords

A common or weak password is a means by which Windows hosts can be broken into by an attacker. In particular, the following accounts are often the target of break-ins:

- SCS Windows domain accounts
- The local Administrator account on your PC

You should make sure that your Windows domain password is a strong password.

In addition, if you are installing a networked service such as MS SQL server, you should make sure that any passwords for that service are reset to a strong password that is something other than the default (this is especially true of the *sa* account on SQL server). Please insure that all necessary patches have been installed.

## How to Change Your SCS Domain Password

- Press **ctl-alt-delete** after you have logged in to your PC
- Select **Change Password** on the dialogue box
- Fill in the given fields on the change password dialogue box. Make sure that the pull-down menu labeled "Log on to:" or "Domain" says "SCS"

**Note:** The computer must be connected to the SCS wired network and it must be a member of the SCS Windows domain.

## Using Jeeves to Administer Your Accounts

You can connect to Jeeves by using a terminal program such as *putty* to connect to *linux.gp.cs.cmu.edu*. On a Windows PC use *putty* to login to *linux.gp.cs.cmu.edu*. Connect to *jeeves.srv.cs.cmu.edu*. On a Facilitized Linux host use the standard *telnet* client to connect to *jeeves.srv.cs.cmu.edu*.

Once you are connected, you will be presented with a menu-based interface where you will be able to do the following; change your AFS quota, change mail forwarding, and create Kerberos instances such as */root*, or */mail*, without having to ask the SCS Computing Facilities staff for help

Please refer to table 1-1 on page 8 for an explanation of the various Kerberos instances.

To access Jeeves, make a Kerberos-encrypted telnet connection to the host *jeeves.srv.cs.cmu.edu* (you should just be able to use *jeeves* as the name of the host). For example, on a Facilitized Linux system:

```
%telnet-ax jeeves.srv.cs.cmu.edu
Trying 128.2.191.155...Connected to SERVICEBERRY.SRV.CS.CMU.EDU.
Escape character is '^]'.
[ Kerberos V4 accepts you ]
[ Kerberos V4 challenge successful ]

Welcome to Jeeves...
```

The telnet connection places you in the main menu, as follows:

1. Perform AFS related operation (afs)
2. Perform kerberos related operation (kerberos)
3. Perform electronic mail related operation (mail)
4. Perform WWW related operation (www)
5. Perform CorporateTime calendar server related operation (corptime)
6. Disconnect from Jeeves (quit)

To select a function, type either:

1.the number at the left

**Enter selection: 2**

- or a unique abbreviation of the key word found in parentheses

**Enter selection: kerberos**

This will take you into a submenu, for example:

- ```
Kerberos related operations

1. Create a Kerberos principal
   Syntax: create <new principal> <new principal's password>
   Example: create bovik.mail
2. Create/re-key a Kerberos principal with a random key
   Syntax: key <principal>
   Example: key rcmd.deneb.fac.cs.cmu.edu
3. Examine a Kerberos principal
   Syntax: examine <principal>
4. Change a Kerberos principal password Syntax: password
   <principal name> <current password> <new password
   Example: password bovik <current password for bovik> <new password
   for bovik>
   Example: password bovik.ftp <current password for bovik> <new
   password for bovik.ftp>
5. Return to the main menu (back)
6. Disconnect from Jeeves (quit)
```

The same selection convention works in the sub menus. Type “?” in any menu to reprint its contents.

To cancel a function selection, use the interrupt character ^C followed by a RETURN.

**Note:** Once a command has been entered and you have hit return, the command cannot be cancelled. If you need assistance please call the SCS Computing Facilities Help Desk at x8-4231 or send mail to [help@cs.cmu.edu](mailto:help@cs.cmu.edu).

## How to use Jeeves to Change AFS Quotas

- Type "afs" to go to the AFS-related operations sub-menu.
- Type "quota" to go to the AFS quota operations sub-menu.
- Type "change" to change your AFS quota.
- You will be asked for the name for the volume. Type *user.userID*, for example "user.bovik" if your username is "bovik".
- You will be asked for a new quota. Type the amount of quota in kilobytes that you want. For example, "2000000" if you want to change your quota to 2 GB.
- The maximum SCS Computing Facilities-provided quota for AFS user volumes is 10GB.

**Note:** The default AFS quota for a CS user is 1 Gigabyte of space.

## How to Use World Wide Web Functions in Jeeves

### Managing your public web space in SCS <http://www.cs.cmu.edu/~username>

The SCS HTTP servers support abbreviation mechanisms which allow home pages to be referenced by a short URL of the form "[http://www.cs.cmu.edu/~username/...](http://www.cs.cmu.edu/~username/)" by translating this URL into a reference to "[/afs/cs.cmu.edu/Web/People/username/...](/afs/cs.cmu.edu/Web/People/username/)"

- **change:** Create or alter a symbolic link in  
</afs/cs.cmu.edu/Web/People/~username>
- **delete:** Delete link.
- **examine:** Find out more about the link.

The link must point to a directory within the CS.CMU.EDU AFS cell, and that directory should contain an **index.html** file which is either your home page or a link to it.

When you make changes to your personal web space, changes to your link will not become active immediately on the SCS HTTP servers. Jeeves will initiate a replicate request for this volume soon after making the change. Your change should become active within 2-3 hours.

## How to Use Jeeves to Create an Oracle Calendar Server Account

**Note:** Oracle Calendar was previously known as Corporate Time and is still referred to as Corporate Time in Jeeves

You must have an Oracle Calendar server account before you can access the server. You can create an account for yourself by using Jeeves.

- **Choose menu option 5 (Perform Oracle Calendar server related operation) from the main Jeeves menu,**
- **Select option 1 (Create a Corporate Time account) from the Corporate Time menu.**

**Note:** Oracle Calendar account passwords are transmitted to the server over the network "in the clear" and are exposed to possible eavesdropping by password sniffers. You must use a different password for your Oracle Calendar server account than your normal Kerberos password.

## Creating the Oracle Calendar Client Account in Jeeves

There are Oracle Calendar clients for Windows, Mac and UNIX based machines.

You must type your full name (not your login name) exactly as reported back by Jeeves when your Oracle Calendar account was created. If you aren't sure what form of your name to use, do the following:

- Click the magnifying-glass icon, fill in your last name in the box and click Search.
- Select your name from the scrolling list.

The SCS Oracle Calendar server host name is: **CALENDAR.SRV.CS.CMU.EDU**.

Once you have logged-in, the Oracle Calendar client has extensive on-line help. See the Oracle Calendar Reference Manual & User's Guide available in PDF format (readable and printable using Adobe Acrobat Reader) for additional information. This guide can be found at:

<http://www.cmu.edu/computing/doc/software/calendar/index.html>

## SCS Email

SCS Computing Facilities provides a full range of email services to faculty, students, and staff in the SCS community via the Corvid email system. These services include:

- Ability to add or remove Email Addresses to your account
- Server-side spam tagging and virus scanning
- Mailing list creation and management

You have the options of either:

- Having your email stored on our local IMAP server, Or
- Having your email delivered to an external account, like gmail.com you may request space on the SCS IMAP server

You may request space on the IMAP server. If you store your email on our local IMAP server, you have these features available:

- Customized mail-handling scripts
- A 2 GB initial limit that can be increased as needed
- A webmail interface
- Support for both IMAP and POP mail protocols

## Managing Your Email Addresses

There are several email Addresses and settings for your account that you can administer:

- Email Forwarding Address
- Email Local Addresses
- Preferred Email Address
- Full Grey Listing Setting
- Discard Spam Setting

Each of these are covered below. You can view and adjust these settings for your account at:

<https://www.fac.cs.cmu.edu/corvid/lookup>

You can also use this page to view information about other users account settings.

You will be redirected to the CMU WebISO page, where you must enter your SCS username (in the CS.CMU.EDU realm) and password to continue to the Email Address Lookup page.

Once you've reached the lookup page, you'll see five search fields:

## Corvid - Email Attribute Search

Corvid is the email system that is in place in the School of Computer Science. This page will allow only CMU SCS members to search the information stored about email addresses, users, and accounts.

[User ID](#)   
[Full Name](#)   
[Preferred Email Address](#)   
[Email Forwarding Address](#) \*   
[Email Local Address](#) \*

*\*The wild card character \* will not work with these fields.*

From here, you can view and adjust your own email configuration information, or view the email configuration of another user.

By default, the Email Address Lookup tool will automatically display all of the above settings associated with your account, and a link for changes to these settings in a column on the right:

### Directory Search Results: (User ID = "bovik")

|                                          |                                                                                                                                                                                                                                                                                                            |                                                  |
|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------|
| <a href="#">User ID</a>                  | bovik                                                                                                                                                                                                                                                                                                      |                                                  |
| <a href="#">Full Name</a>                | Harry Bovik                                                                                                                                                                                                                                                                                                |                                                  |
| <a href="#">Preferred Email Address</a>  | bovik+@cs.cmu.edu                                                                                                                                                                                                                                                                                          | <a href="#">Modify Preferred Email Address</a>   |
| <a href="#">Email Forwarding Address</a> | bovik+@imap.srv.cs.cmu.edu                                                                                                                                                                                                                                                                                 | <a href="#">Modify Email Forwarding Address</a>  |
| <a href="#">Email Local Address</a>      | bovik<br>bovik+<br>bovik+@cs.cmu.edu<br>Harry.Bovik@cs.cmu.edu<br>Harry_Bovik@cs.cmu.edu<br>Harry.Bovik@ri.cmu.edu<br>Harry_Bovik@ri.cmu.edu<br>Harry.Bovik@scs.cmu.edu<br>Harry_Bovik@scs.cmu.edu<br>bovik+@ri.cmu.edu<br>bovik+@scs.cmu.edu<br>bovik@cs.cmu.edu<br>bovik@scs.cmu.edu<br>bovik@ri.cmu.edu | <a href="#">Modify Email Local Address</a>       |
| <a href="#">Full Grey Listing</a>        | TRUE                                                                                                                                                                                                                                                                                                       | <a href="#">Modify Full Grey Listing Setting</a> |
| <a href="#">Discard Spam</a>             |                                                                                                                                                                                                                                                                                                            | <a href="#">Modify Discard Spam Setting</a>      |

## Managing Your Email Forwarding Address

All users in SCS have the ability to control where their mail is forwarded. The user has the option to forward all mail at their CS account to an account of their choice.

The email forwarding address is a single email address that your email will be directed.

Your Email Forwarding Address can be set to any one of the following:

- the SCS IMAP server (userid@imap.srv.cs.cmu.edu)
- your Andrew mail account (userid+@andrew.cmu.edu)
- any other valid local or remote email address where you accept mail (username@gmail.com, for example)

To add or remove Mail Local addresses, please click on the **Modify Email Forwarding Address** link on <https://www.fac.cs.cmu.edu/corvid/lookup>.

**Note:** Please make sure that you have an account on the SCS IMAP server before selecting it as a final destination. If you are uncertain if your SCS IMAP account has been set up, please contact the SCS Help Desk at x8-4231 or send mail to help@cs.cmu.edu.

If you do forward your email to our local email server, please avoid publishing your [userid@imap.srv.cs.cmu.edu](mailto:userid@imap.srv.cs.cmu.edu) address. Think of that address as being an internal routing address. Instead try to use your [userid@cs.cmu.edu](mailto:userid@cs.cmu.edu) or other **Email Local Address** instead.

**Note:** If you choose to have your mail forwarded to an off-site account, SCS Computing Facilities will be very limited in the assistance we can provide to resolve email problems.

## Modifying Your Email Local Addresses

Each Corvid mail account is associated with a list of Email Local Addresses. These are email addresses at which Corvid will accept mail for delivery on your behalf. There are several email addresses associated with your account by default.

A few of the default addresses are required for historical and practical purposes:

- userid
- userid+
- userid+@cs.cmu.edu

Additionally, your list of Email Local Addresses would also include common combinations of first and last name at common CMU domains.

To add or remove Mail Local addresses, please click on the **Modify Email Local Address** link on <https://www.fac.cs.cmu.edu/corvid/lookup>.

Some examples of acceptable local addresses are:

- FirstName.LastName@cs.cmu.edu
- FirstName\_LastName@ri.cmu.edu
- Nickname@scs.cmu.edu

There are restrictions on additional Email Local Address requests:

- Do not request large numbers of additional Email Local Addresses; keep your list manageable
- Do not request Email Local Addresses that are possibly offensive or inappropriate
- Limit your Email Local Addresses to schools or departments with which you are associated
- Do not include domains that are not local to our facility (for example, domains such as gmail.com or an andrew.cmu.edu are not local)

Your request will be sent to the help desk. You will be notified when the changes have taken effect.

**Note:** SCS Computing Facilities reserves the right to reject any request that is not in compliance with University Computing policies and guidelines. In addition, the requested Email Local Address may not be available. You will be notified by the SCS Computing Facilities Help Desk if this situation arises.

## Modifying Your SCS Preferred Email Address

Your **Preferred Email Address** is the email address most commonly associated with your account, and is published in local email directories. Typically, your Preferred Email Address should be set to one of:

- one of your Email Local Addresses, as above
- an external email address where you receive mail (username@gmail.com, for example)

To change the value of the **Preferred Email Address** attribute, please click on the **Modify Preferred Email Address** link on <https://www.fac.cs.cmu.edu/corvid/lookup> . Your request will automatically be sent to the Help Desk; you will be notified when the change has taken effect.

## Grey Listing

*Grey Listing* is a mechanism for reducing spam, and works as a supplement to the existing Sophos anti-spam service. In conjunction with Sophos, greylisting has been shown to very effective for reducing the amount of spam that reaches both a user's INBOX and SPAM folder. Greylisting is turned on by default.

SCS Computing Facilities greylists only email from outside the university. Email from within the university is not subject to this mechanism. By default, all new accounts have this attribute set to **TRUE**. We **STRONGLY** recommend that you do not change this setting. For more information about greylisting in the SCS Computing environment please refer to our Help pages at:

[http://www.cs.cmu.edu/~help/mail\\_news/corvid/greylisting.html](http://www.cs.cmu.edu/~help/mail_news/corvid/greylisting.html)

To change the value of the **Full Grey Listing** attribute, please click on the **Modify Full Grey Listing Setting** link on <https://www.fac.cs.cmu.edu/corvid/lookup> .

## Discard Spam

As Email is received it is examined for evidence of spam. This is done this with a commercial software product called Sophos. If the email is spam, it is tagged with the addition of the email header **X-Spam-Warning**.

The **Discard Spam** attribute will determine whether email that we believe is spam is delivered to your **Email Forwarding Address** or rejected or discarded as early as possible.

This Discard Spam attribute can have one of three values

- **TRUE** - If it is spam, we reject or discard it as soon as possible
- **FALSE** - Always try to deliver email, even if it is spam
- **Blank or Not Set** – The same as False

If you forward your email offsite our servers will avoid forwarding spam, regardless of the setting of this attribute. Some remote sites don't like it if our servers forward spam. If they see spam coming from @cs.cmu.edu, they refuse all email from our servers.

To change the value of the **Discard Spam** attribute, please click on the **Modify Discard Spam Setting** link on the <https://www.fac.cs.cmu.edu/corvid/lookup> page.

## Mailing Lists

Mailing lists in the SCS environment are managed by the Mailman mailing list system. Some of its many features include

- A web based interface
- The ability for subscribers to control their subscription status and delivery options
- The ability for list administrators to use their Kerberos passwords for authentication to access administrative functionality
- Moderated list posting
- Some spam control

Mailman gives the administrator the ability to do the following:

- Accessing the list's administrator page
- Setting the administrator password
- Making a list visible to the public
- Include sub lists
- Configuring member posting policy
- Adding members
- Setting the moderator password
- Assigning moderators
- Configuring white lists and blacklists
- Blocking messages that have been tagged as spam

For more information about Mailman mailing lists please see:

[http://www.cs.cmu.edu/~help/mail\\_news/mailman/mailman\\_brief\\_intro.html](http://www.cs.cmu.edu/~help/mail_news/mailman/mailman_brief_intro.html)

## Email Etiquette

When sending Email to mailing lists please be considerate of the following:

- Keep messages short
- Keep attachments small
- Avoid sending spam

## SCS IMAP Email Store

If you choose to have your email stored on our IMAP server, you can access your SCS email using any of the supported email clients. These clients are listed per platform and are listed below.

### Windows

- Outlook
- Thunderbird

### Mac

- Apple Mail.app
- Entourage
- Thunderbird

### Linux

- Alpine
- Thunderbird

### Web

- Webmail

Configuration instructions for the email clients can be found at:

[http://www.cs.cmu.edu/~help/mail\\_news/index.html#clients](http://www.cs.cmu.edu/~help/mail_news/index.html#clients)

## Webmail

Webmail offers convenient and secure access to your email from any web browser. To check your email using our webmail interface, simply go to:

<https://webmail.cs.cmu.edu> this will redirect you to the webiso authentication server.

WebISO Secure Login - School of Computer Science - Carnegie Mellon University - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://webiso.cs.cmu.edu/

 **WebISO Secure Login** School of Computer Science Carnegie Mellon

The resource you requested requires you to authenticate.

User ID:  Instance **@CS.CMU.EDU**

Password:   None  /mail

**Warning:** This web page is requesting your User ID and password. If you have any doubts as to the legitimacy of this page, **look for <https://webiso.cs.cmu.edu/> in the URL** before entering your User ID and password. If you think that this page should not be requesting your User ID and password, please report it to [help@cs.cmu.edu](mailto:help@cs.cmu.edu) and be sure to include the URL.

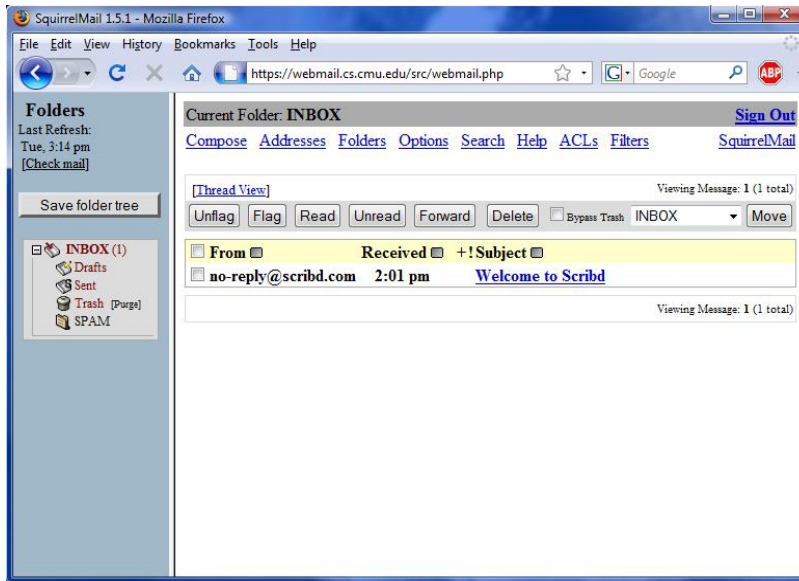
**Carnegie Mellon Certificates:** Many of the services that use WebISO also use the Carnegie Mellon Certificates. If you haven't already done so, [install the Carnegie Mellon CA Root Certificates in your browser](#).

**About this service.** WebISO verifies the identity of Carnegie Mellon users. WebISO does not require installation of specialized software. However, your browser must be configured to accept cookies. This is the default configuration for all major web browsers. If you have disabled cookies in the past you will need to enable cookie support in your browser to use WebISO.

This site is maintained by SCS Computing Facilities; send comments to [help@cs.cmu.edu](mailto:help@cs.cmu.edu).  
Version: 3.3.2d-002 © Carnegie Mellon University

And enter your SCS Kerberos ID and **/mail** password.

You are now logged into the SCS Webmail client. You should see the following screen:



## Message Auto-Expiration

The IMAP server now offers users the ability to configure individual mailboxes to remove messages automatically after a specified period. Messages in each mailbox with an expiration setting will be deleted when their age exceeds the expiration limit. The SCS Webmail system includes an interface for managing these settings.

### **Caveats:**

Even unread messages will be deleted once they are older than the expiration date. Do not set expirations on infrequently-checked mailboxes that are likely to contain unread messages for extended periods.

The server uses the "Date:" header to determine message age. Messages with a "Date:" header in the future will not be deleted until after the bogus date *plus the expiration time* passes. Conversely, messages with an incorrect "Date:" header in the past may be deleted sooner than expected. Since most messages with wildly incorrect "Date:" headers tend to be spam, this mechanism should not cause a problem for most users.

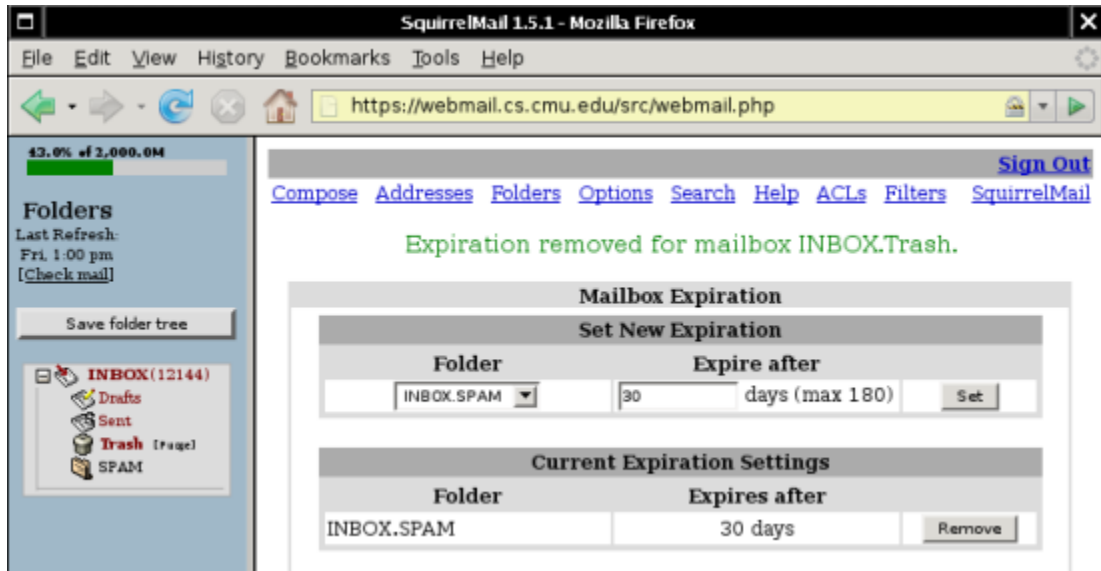
The interface deliberately prevents you from setting an expiration period on your "INBOX." If you have a specific need for that arrangement (for example, you regularly file all mail into to subfolders and your "INBOX" contains only unimportant or unwanted mail), please contact the SCS Help Desk, [help+@cs.cmu.edu](mailto:help+@cs.cmu.edu) or x8-4231. We will enable it at your request.



The expiration options interface is available via the [Webmail](#) menu bar's "Options" link. From there, choose the "Message Expiration Options" item.

The lower "Current Expiration Settings" window lists mail folders for which you currently have expirations set. The default is no expiration, so this window will initially be empty. To set or reset an expiration, select the mailbox folder from the dropdown menu in the upper "Set New Expiration" window, enter a value (default 30 days) in the "Expire after" field, and click "Set."

A status message will confirm that the expiration has been set on the mailbox.



To remove expiration from a mailbox, click the "Remove" button in the lower table next to the expiration setting you wish to remove.

Again, a status message will confirm that the expiration setting has been removed.

## Sieve Scripting Information

### Sieve Scripts

Our server implements the "Sieve" scripting language which allows users to define operations such as vacation messages, refiling of mail messages based on header comparisons (anti-spam refiling, for example) and forwarding mail to alternative addresses.

Sieve scripts are simple text files that are uploaded to, and run on, the IMAP server. In our environment, there are two options for placing Sieve scripts onto our IMAP server:

- Through the Web sieve interface
- Command line interface run from an SCS UNIX machine

## How to Create and Activate a Sieve Script Using the Web Sieve Interface:

The Web Sieve interface offers both a basic and advanced method of manipulating Sieve scripts on the server:

<http://webmail.cs.cmu.edu/websieve>

The basic interface is useful for simple operations, such as:

- Enabling and disabling the default spam filter and
- Enabling and disabling automatic vacation notices.

Web sieve also offers an advanced interface that allows for direct manipulation and editing of scripts on the server.

For more information, please see:

[http://www.cs.cmu.edu/~help/mail\\_news/intro.sieve.html](http://www.cs.cmu.edu/~help/mail_news/intro.sieve.html)

## Setting up an “Out of Office” Message with the Web Sieve Interface:

- Log into the Web Sieve editor and select “vacation options”.
- Fill in the web form with the appropriate subject and body of the reply message.
- Select “enable vacation script”. Click “Update” to enable the vacation message.

When you return,

- Uncheck “Enable Vacation Script” from the front page of the Web Sieve interface.
- Verify that SPAM filtering is still checked.

# Printing

SCS Computing Facilities provides support for over 150 printers within the SCS, along with infrastructure that allows printing from Linux, Windows, and Mac hosts.

## Printing Etiquette

The public printers in the School of Computer Science are a shared resource. For that reason, people should:

- Only print large jobs at night or off-hours
- Promptly pick up your printer output (and *only* your output)
- File output that you see
- Use the copier, not the printer, for multiple copies
- Use color printers only when necessary (as color copying is more expensive than black and white)
- Use SCS printers only for SCS-related work
- Preview your output before printing

To preview your output, you can use a Postscript viewer such as Ghostview (gv on Linux hosts), a DVI previewer such as xdvi for TeX output, or whatever print previewing facility comes with the application you are using (such as the Microsoft Word Print Preview ability).

## Getting Help

If you have a problem with a printer, you can call SCS Help Desk at x8-4231, contact the SCS Help Desk at x8-4231 or by email at [help@cs.cmu.edu](mailto:help@cs.cmu.edu) to report printing problems.

SCS Operations also provides 24x7 help with many printer problems, such as being out of toner, routine paper jams, etc. More severe printer problems will need to be handled during normal business hours.

## Lists of Printers

To review the full list of all available printers and their locations please refer to

<http://www.cs.cmu.edu/~help/printing/index.html>

# Networking in SCS

The SCS network is one of three network entities on campus. The other two networks are the ECE Department network and the Computing Services network managed by CMU Computing Services. The Computing Services network provides local network connectivity for everyone on campus except for users in SCS and ECE and also provides the campus with connectivity to the commodity Internet and Internet2. The CMU Computing Services group also manages the campus wireless network.

CMU Computing Services enforces a quota of ten gigabytes (10GB) of bandwidth per day inbound or outbound over the commodity Internet connection. There is no bandwidth quota for Internet2 traffic. For more information on CMU Computing Services usage Guidelines see:

<http://www.cmu.edu/computing/guideline/bandwidth.html>

## Network Use Policies

### Introduction

The SCS network is vital to the School's research and educational activities. Hosts or other equipment that are improperly configured, malfunctioning, have been broken into, or are using excessive resources, may cause major problems for network operation and for other hosts on the network. We ask that you adhere to the following practices:

- Use only IP addresses that have been assigned to your host.
- Use only authorized DHCP servers
- Do not run routing software on user systems
- Do not use unpatched hosts that have been compromised and are conducting denial of service attacks against other sites
- Do not conduct unannounced network-related experiments that adversely affect network performance for all of SCS
- Do not install or use unauthorized wireless access points throughout the campus

To help prevent network problems and assist SCS Computing Facilities in fixing problems when they occur, people using the SCS network must abide by the network use policies given below. These policies are meant to supplement the official Carnegie Mellon computing policy and provide some SCS-specific additions to that policy.

### Connecting Hosts to the Network

You must register any host or network device, including printers and wireless access points, with SCS Computing Facilities, giving machine type, location, hardware address, and contact information, before putting it on the network. You must notify us if any of the above information changes. It is especially important that SCS Computing Facilities is notified when a machine is moved. Moving a machine may require an IP address change to the machine and network connectivity may be inconsistent at best without the IP address change.

The wired network in SCS buildings belongs to the SCS network infrastructure. The wireless network is part of campus Computing Services

All network registrations and updates are done using the following URL:

<http://www.cs.cmu.edu/~help/networking/netregister.html>

Hosts, equipment, and cables/wiring should not be connected to the SCS network, moved to different network outlets, or reconfigured in any way that might affect network performance or functionality, without prior notification and approval of SCS Computing Facilities.

Only in special cases will we give out an IP address without knowing the host's hardware address.

SCS Computing Facilities reserves the right to disconnect or otherwise remove hosts and equipment from the network without notice if they are causing problems, violating network usage policies, or showing signs that they have been compromised.

SCS Computing Facilities reserves the right to monitor network traffic in order to detect or debug network problems and to detect unauthorized use of the network or activity that violates network usage policies. We reserve the right to scan any host or equipment connected to the SCS network for open ports, possible security holes, or any other information that may be gained by scanning. By using the SCS network, or connecting hosts or equipment to the SCS network, you consent to such monitoring and scanning.

## Naming Policy

The machine naming convention here in SCS is (*hostname.project.department.cmu.edu*)

- The project component of a hostname must somehow be related to SCS or CMU
- SCS Computing Facilities tries to avoid having multiple hosts that have the same first component of their hostnames
- All personally owned machines will receive a ".pc.cs.cmu.edu" extension
- SCS Computing Facilities reserves the right to reject inappropriate hostnames
- SCS Computing Facilities will not rename the graduate student machines i.e. gs##.sp.cs.cmu.edu
- Personal machines can have only network support

## Domains and Virtual Hosting

### Domain hosting

- You can use equipment on the CMU 128.2.\*.\* IP address space to host a domain as long as it is non-profit and the domain is .org
- SCS Computing Facilities will provide name service for a domain if the domain is related to SCS or CMU research/educational activities
- SCS Computing Facilities does not delegate DNS for SCS or sub domains of SCS projects

**Note:** A Special non 128.2.\*.\* address space has been setup for non-commercial or domains other than .org that are related to the School of Computer Science / Carnegie Mellon University. Please contact the SCS Help Desk at x8-4231 or by email at [help@cs.cmu.edu](mailto:help@cs.cmu.edu) if you have a domain that requires this special IP address space.

## Virtual Web Hosting on the SCS Web server

SCS will provide virtual web hosting services on an SCS maintained web server if:

- The request is for a project related to SCS or CMU, with a limit of one virtual web host per project
- The virtual host will be used for non-commercial, academic, purposes
- The virtual host is needed for research reasons or to provide a high-visibility (outside of CMU), high-traffic service

## Network Usage Restrictions

You may not use the SCS network or data gathered from the SCS network for purposes of gaining or attempting to gain unauthorized access to hosts, networked equipment or data. Any use of the SCS network to scan, break into, attempt to break into, or intentionally degrade the performance, functionality, or network connectivity of hosts or other networked equipment is prohibited, unless:

- You have the permission of the administrator(s) of said hosts and/or equipment, and
- You notify SCS Computing Facilities prior to engaging in the activity
- The activity will not cause service or performance problems for other hosts or equipment on the network

Some exceptions may be granted for non-obtrusive scanning, network measurement, or other activities, but SCS Computing Facilities must be notified and permission obtained from SCS Computing Facilities beforehand.

Network monitoring (tcpdump, etc.) for research purposes or debugging network problems is allowed. Please contact SCS Help for assistance. Monitoring is subject to relevant federal, state or other laws. It is expected that people collecting such data will respect the privacy of anyone whose traffic is incidentally collected by such activities. Network monitoring or packet sniffing for the purposes of intercepting e-mail, passwords, or other personal data without the consent of all parties is not permitted.

Any use of the SCS network that may possibly affect network performance, routing, connectivity, or possibly cause service or performance problems for other hosts or equipment must be approved by SCS Computing Facilities beforehand.

Using the SCS network for purposes of harassment, fraud, sending threatening communications, inappropriate sending of unsolicited bulk e-mail, or any violation of applicable federal, state or other laws, or university policy, is prohibited.

Any use of the SCS network or hosts for commercial purposes or personal gain, except in a purely incidental manner, without advance authorization is prohibited.

## Running Network Services

If you install, enable, or administer any network-aware software on a host, including Web, FTP, SSH, file-sharing, and operating system services, you are responsible to make sure the software does not interfere with network operation, cause problems for other hosts on the network, provide unauthorized access to hosts or data, or otherwise violate network usage policies.

You are responsible for making sure that any network-aware software that you install or administer is kept up-to-date with respect to security patches, and for taking appropriate steps to prevent unauthorized access or use of such software. Hosts or other networked equipment running software or services that are known to be insecure, or that are configured in an insecure manner, may be disconnected or otherwise removed from the network.

If a service generates a very large amount of network traffic, we will need a work-related justification and may ask you to find ways to reduce the amount of traffic.

Use of such services for illegal behavior, including illegal distribution of copyrighted materials without the consent of the copyright holder, is prohibited.

## Remote Access

You must use your username /remote instance when using SCS Remote Access Services.

Connecting via any remote site has the potential of exposing your username and password. If someone obtains your primary SCS Kerberos username/password they could gain full access to your data. If someone obtains your username/remote instance password they will only have the ability to access the SCS remote access services (VPN and iPass). Problems could occur if either account is compromised, however, the /remote instance does not provide attackers access to your data.

Instructions on creating a /remote instance can be found at:

[http://www.cs.cmu.edu/~help/accounts\\_passwords/create\\_instance.html](http://www.cs.cmu.edu/~help/accounts_passwords/create_instance.html)

## VPN

The SCS VPN (Virtual Private Networking) software allows a computer on another network to look like it has an SCS name and IP address. Using VPN, a remote host can access restricted network services that can only be accessed by SCS hosts. The VPN client is available for Windows, MacOSX, and Linux.

Download the VPN client for Windows, Mac and Linux systems from:

<https://www.cs.cmu.edu/~help/networking/downloads.html>

## iPass

iPass is the world's largest virtual network including dial-up in over 150 countries and, together with the T-Mobile HotSpot network, close to 60,000 Wi-Fi hotspot and Ethernet hotel broadband locations. The iPass service provides easy-to-use, reliable access to the Internet from virtually anywhere in the world.

Download the iPass client for Windows or Mac from:

<https://www.cs.cmu.edu/~help/networking/downloads.html>

### Running iPass:

To use iPass do the following:

- Double click installed icon or go to Start -> Programs -> iPass
  1. You will see ->iPassConnect
  2. Select country/state/city.
  3. Click find.
  4. Available iPass points of connection (modem, ISDN, wired broadband, wireless broadband) should appear in the lower window.
  5. Select the appropriate point of connection.
  6. Login with your /remote instance and password.
- In the US, select country and fill in area code. A list of available iPass points of connection should appear in the lower window for your location.

### To setup login info:

- Select Settings -> login information
- Enter username, i.e. username/remote
- Enter password for your username/remote instance

### iPass dialup:

You may need to add numbers to the dial string depending on your location i.e. (add a 9 to the front of the dial string to get an outside line).

You may need to select a modem. Go to Settings -> connection settings. Select appropriate modem from pull down menu.

## iPass Tips

To find wireless hotspots online check:

<http://ipass.jwire.com>

You may find you need to "login manually" to an iPass point of connection. Linux users will need to do this. Windows and Mac users may also need to manually login to an iPass providers web page in order to gain network connectivity. If so, the username needs the format:

[IPASS/cs.cmu/user/remote@cs.cmu.edu](mailto:IPASS/cs.cmu/user/remote@cs.cmu.edu)

And the password needs to be the password for your *user/remote* instance.

**Note:** Be sure to try out the iPass service before leaving on your trip.

Check with your hotel before using iPass. Users are responsible for any local toll charges and hotel fees incurred while using the iPass client

**Usage Restrictions:** Please do not use the iPass service from the Pittsburgh area. The iPass service is intended for use by SCS users while traveling and iPass charges are billed to SCS Computing Facilities on a per minute basis.

## Wireless Networking (CMU Computing Services)

### Computing Services Wireless Network

To use the wireless network (administered by Computing Services) establish a wireless connection to the network (network name: CMU) and open a web page with your preferred browser. If your machine is not already registered to use the wireless network, you will automatically be redirected to Computing Services Authbridge service, where you will be prompted to enter your Computing Services user ID and password. From there, you should have an active and open connection to the Internet.

The link for Computing Services wireless registration is:

<http://netreg.net.cmu.edu/>

For more information about the Computing Services wireless network please refer to:

<http://www.cmu.edu/computing/about/history/wireless/>

SCS Computing Facilities is **not** responsible for the campus wireless. If you experience wireless issues please contact the SCS Help Desk.

### Computing Services Wireless in SCS

Computing Services has placed wireless access points throughout the School of Computer Science and many in the SCS community use this service. However, there are some things to consider when using the Computing Services wireless network.

- A wireless connection is not as fast or reliable as a wired connection
- You must use SCS VPN to access the following SCS services:
  - Windows domain services (such as mapped drives to SCS machines)
  - Any other SCS service restricted by IP or hardware address.
- Traffic over the wireless is in **not** encrypted

Because Computing Services wireless communications are sent in the clear we strongly recommend using the SCS VPN service in conjunction with the Computing Services wireless network.

If you have any questions about Computing Services wireless service, contact the SCS Help Desk at x8-4231 or by email at [help@cs.cmu.edu](mailto:help@cs.cmu.edu).

When you register your host, you should register it in the *WV.CS.CMU.EDU* domain in order to access SCS-specific services.

### Restrictions on Using Wireless Connections

Computing Services states that no individual service or system running on the wireless network should use more than a total of **10 gigabytes (10GB) of bandwidth per day**, regardless of whether it is inbound or outbound. Please refer to the Computing Services Network Bandwidth Usage Guideline for the wired/wireless network at:

<http://www.cmu.edu/computing/guideline/bandwidth.html>

**Note:** Wireless is not meant to be a substitute for "wired" networking. In particular, we **cannot back up** hosts over the wireless network, and you should not run high-bandwidth connections over wireless.

# AFS

AFS is a distributed file system product providing client and server architecture that offers file sharing within a single namespace, security, scalability, replicated read-only content distribution, and transparent data migration.

The OpenAFS client software is installed and preconfigured on each facilitated machine to allow secure, and transparent access within the SCS computing environment. Environmental system configurations and updates, and data for classes, projects, users and corresponding websites are made available through AFS.

## Authentication

AFS may be accessed through the command line shell on Linux, or the Windows Explorer. Both authentication and the appropriate authorization are required for accessing AFS.

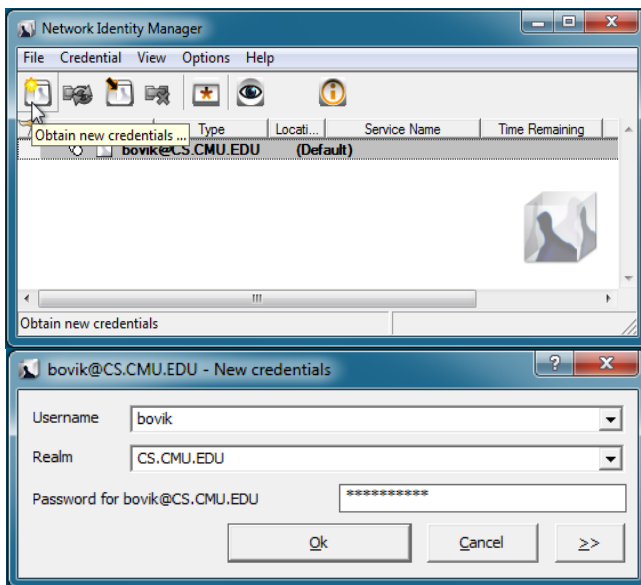
Authentication is automatic on Linux workstations when you login with your Kerberos password, and is obtained in Windows by supplying your Kerberos password to the Network Identity Manager.

## Windows

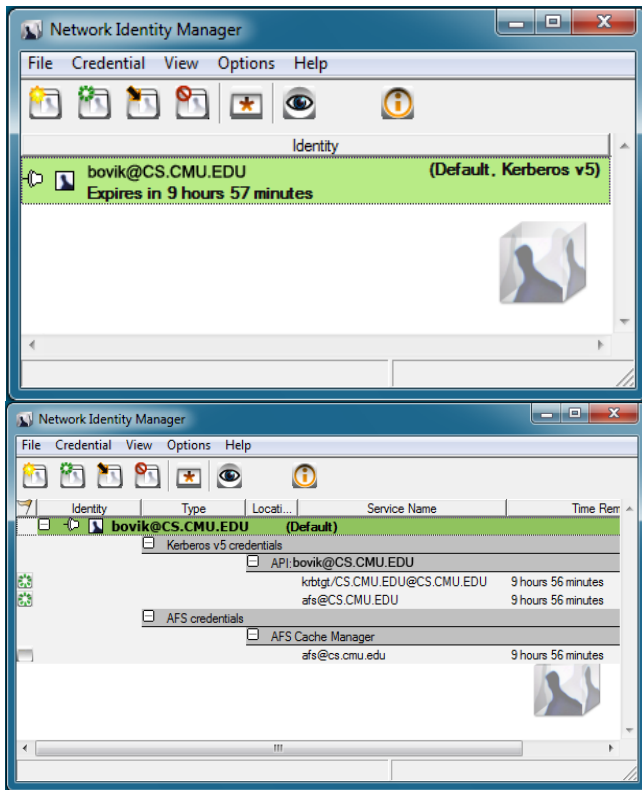
The Network Identity Manager is responsible for obtaining and managing credentials on Windows workstation and is accessible from the Start menu, or from the *Quicklaunch* toolbar.



Left-clicking on the toolbar icon will show the main NIM dialog window. Clicking on the first application icon in the upper right, "Obtain new credentials..." will prompt for your Kerberos password.



Once credentials have been obtained the NIM dialog will show the time remaining in your authenticated session. An "Advanced view" is available from the application window's "View" menu or by typing F7.



## Linux

All the appropriate credentials for access to AFS are obtained at a graphical or console login on Linux workstations.

Use of the “klist” command from a shell window will display your login credentials.

```
[bovik@hostname]# klist
Credentials cache: FILE:/tkt/1234-1a2bdd21-Nyggp0
Principal: bovik@CS.CMU.EDU

Issued      Expires    Principal
Jun 1 13:32:26 Jun 2 13:32:26 krbtgt/CS.CMU.EDU@CS.CMU.EDU
Jun 1 13:32:26 Jun 2 13:32:26 afs@CS.CMU.EDU

V4-ticket file: /tkt/1234-1a2bdd21-896fun
Principal: bovik@CS.CMU.EDU

Issued      Expires    Principal
Jun 1 13:32:26 Jun 2 14:58:47 krbtgt.CS.CMU.EDU@CS.CMU.EDU
```

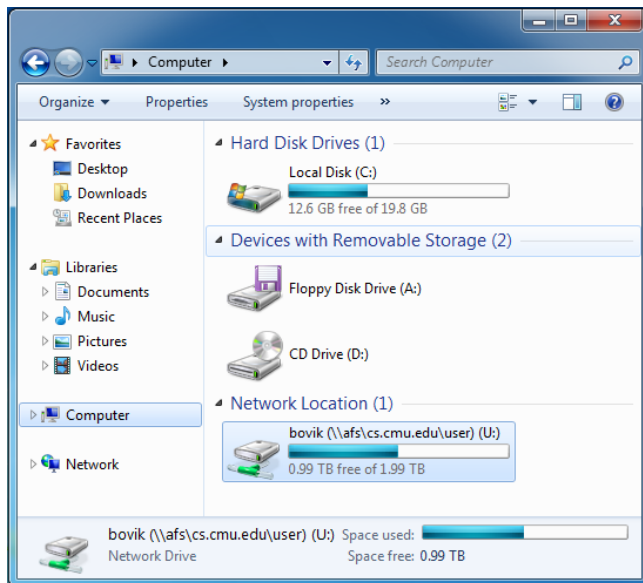
## Volumes

Units of storage in AFS are referred to as volumes, and are comprised of related directories. The most common example is your home directory's volume, available via the Linux path `/afs/cs.cmu.edu/user/username`, or the Windows UNC path of `\\afs\cs.cmu.edu\user\username`.

This unified namespace is one of the advantages of AFS. You may access AFS volumes from the same path from any facilitated machine in the computing environment.

```
[bovik@hostname~]$ pwd
/afs/cs.cmu.edu/user/bovik

[bovik@hostname~]$ dir
Mail  OldFiles  private  public  README.txt  www
```



## Requesting Volumes & Quotas

Requests for academic or project volumes may be sent to [help@cs.cmu.edu](mailto:help@cs.cmu.edu). Please include the following information:

- Project name consisting of 11 characters or less. Academic volume names are pre-determined to match the SCS designated course number and year.
- Project sponsor or course instructor, and one additional individual to be granted full administrative rights within the volume.

- State the initial quota request. Limit it to meet your current requirements. It may be resized to meet your future requirements as they change.
- Classes may request drop box student directories. Include a class roster of only the student usernames, and designate TA usernames to be added for administration of volume contents.

There are different classifications of volumes that may be found within the cs.cmu.edu cell hierarchy. The following summary provides a brief description of the types, their locations, and quota assignments.

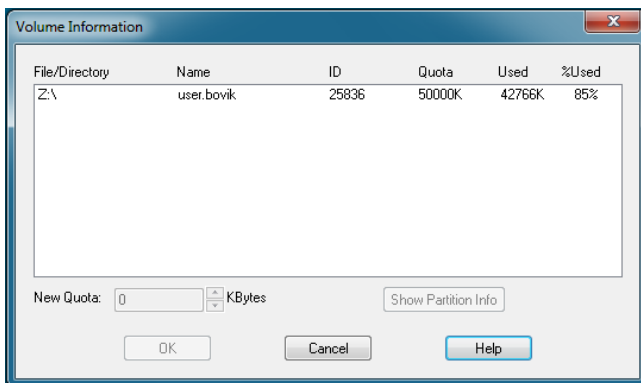
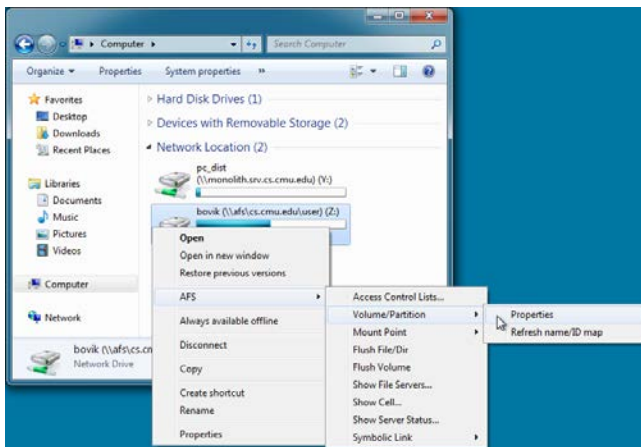
| Volume Type | Description                                                                                                                                                                         | Default Quota | Max Quota |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|-----------|
| User        | Home directory. Moderate data requirements.<br><br>/afs/cs.cmu.edu/user/username                                                                                                    | 1 GB          | 10 GB     |
| Academic    | Class directories for sharing common documents. Student dropoff directories available upon request.<br><br>/afs/cs.cmu.edu/academic/class/classno-termYear                          | 1 GB          | 100 GB    |
| Project     | SCS Affiliated projects may request space for collaboration purposes.<br><br>/afs/cs.cmu.edu/project/projectname                                                                    | 1 GB          | 100 GB    |
| Backup      | Backups for existing volumes made nightly.<br><br>/afs/cs.cmu.edu/.BACKUP/path-to-main-volume                                                                                       | -             | -         |
| Restored    | Volumes requested for restore. Making requests as soon as possible increase the likelihood of a specific date being available.<br><br>/afs/cs.cmu.edu/.RESTORED/path-to-main-volume | -             | -         |

Each volume has a flexible quota assigned to it. The quota may shift in size with the requirements of the volume without adversely affecting the content or availability of the volume.

Quota usage may be determined through the command line interface in a Linux shell, or through the Windows Explorer.

```
[bovik@hostname bovik]$ fs lq .
Volume Name      Quota    Used %Used  Partition
user.bovik       50000    42766  86%      43%

[bovik@hostname bovik]$
```



## Authorization

Permissions in AFS are granted per directory, rather than per file, and handled by *Access Control Lists* set on each directory. Variable levels of permission may be granted to users and user groups within a directory.

## Permissions & Access Control Lists

There are seven AFS permissions. Four permissions affect directories, and the remaining three effect file authorization.

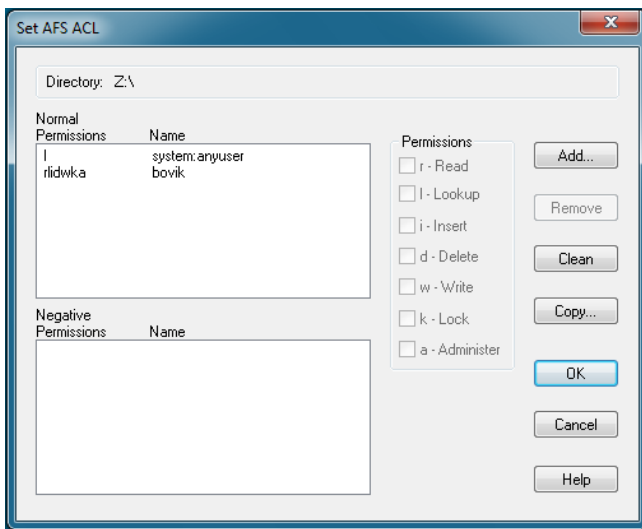
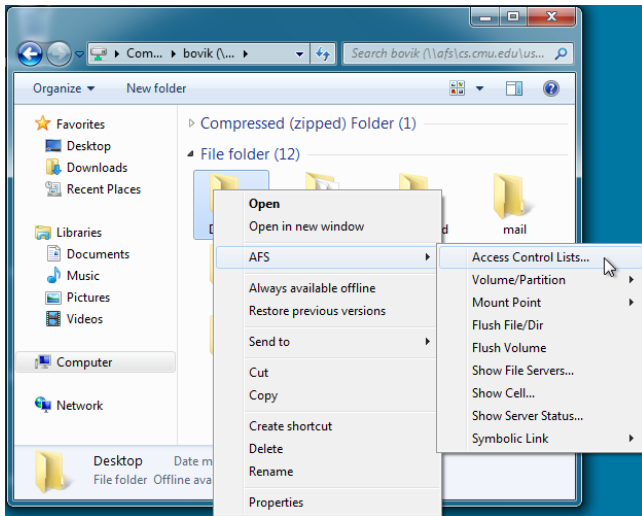
| Directory     | Permission | Description                                                                             |
|---------------|------------|-----------------------------------------------------------------------------------------|
| Lookup        | l          | Affords access to a directory to perform other operations, and list directory contents. |
| Insert        | i          | Allows file and directory creation or copying.                                          |
| Delete        | d          | Allows for removal of files or subdirectories.                                          |
| Administrator | a          | Allows for changing of the directory ACLs.                                              |
| <b>File</b>   |            |                                                                                         |
| Read          | r          | Allows for file reads and directory statistics (e.g., ls -l)                            |
| Write         | w          | Allows for writing changes to files.                                                    |
| Lock          | l          | May run applications that issue system calls to lock files within the directory.        |

AFS ignores any individual file permissions except for the owner's. Read, write, and execution file modes may be removed on a file. Denying owner permissions will remove the ability for anyone to access the file, including the owner. The Access Control List is comprised of all the users and groups, and their corresponding level of authorization within a directory.

### Show the ACL

The command line interface of a Linux shell, or Windows Explorer may be used to list the membership and authorizations of a given directory.

```
[bovik@hostname bovik]$ fs la .
Access list for . is
Normal rights:
bovik rldwka
system:anyuser l
```



## Add or Remove Users & Groups on ACLs

Owners or users with administrative permissions may edit or add additional entries to the directory's ACL. The appropriate Linux shell command or Windows Explorer interface may be used to manage directory ACLs.

```
[bovik@hostname ~]$ fs la .
Access list for . is
Normal rights:
  system:anyuser l
  bovik rlidwka

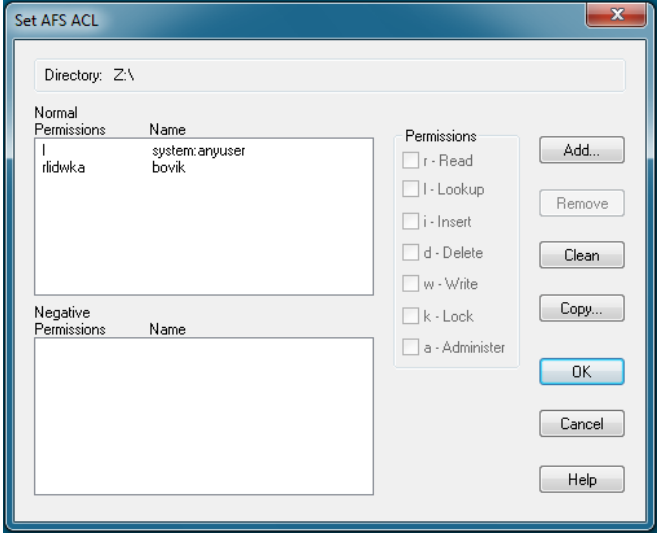
[bovik@hostname bovik]$ fs help sa
fs sa: set access control list (alias for setacl)
Usage: fs sa -dir <directory>+ -acl <access list entries>+ [-clear] [-negative]
[-id] [-if] [-help]
Where: -clear clear access list
       -negative apply to negative rights
       -id initial directory acl (DFS only)
       -if initial file acl (DFS only)

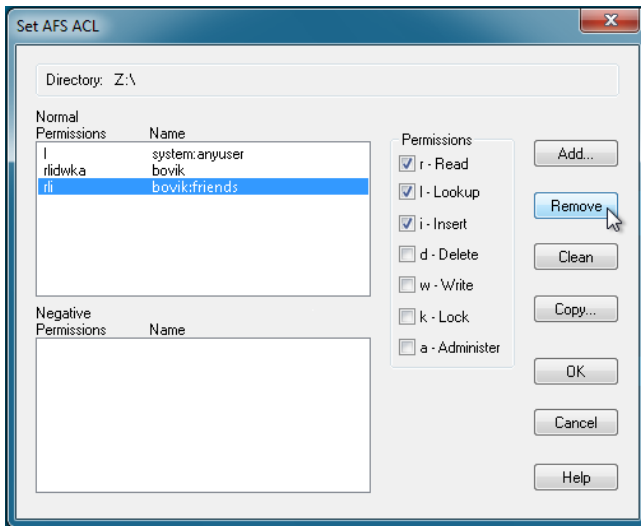
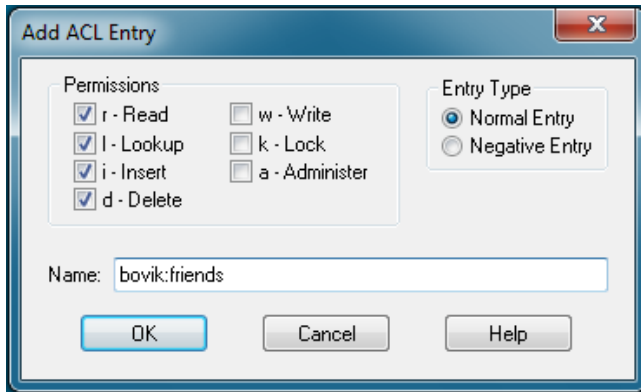
[bovik@hostname bovik]$ fs sa . username rliw
[bovik@hostname bovik]$
```

```
[bovik@hostname ~]$ fs la .
Access list for . is
Normal rights:
  system:anyuser l
  bovik rlidwka

[bovik@hostname bovik]$ fs help sa
fs sa: set access control list (alias for setacl)
Usage: fs sa -dir <directory>+ -acl <access list entries>+ [-clear] [-negative]
[-id] [-if] [-help]
Where: -clear clear access list
       -negative apply to negative rights
       -id initial directory acl (DFS only)
       -if initial file acl (DFS only)

[bovik@hostname bovik]$ fs sa . username none
[bovik@hostname bovik]$
```





## Managing PTS Group Memberships

Groups may contain multiple users, and allow for easy management of directories. Newly created subdirectories inherit the permissions of the parent directory, including any existing group entries. Managing similar levels of access through group memberships is easier than adding and removing individuals in countless, recursive directories.

Create a group as a subtext of your own username, *username:groupname*, and add that group to the appropriate directories as you would an individual user. Group creation and membership management must be done from the Linux shell with the use of PTS commands.

```
[bovik@hostname bovik]$ pts help creatgroup
pts creatgroup: create a new group
aliases: cg
Usage: pts creatgroup -name <group name>+ [-owner <owner of the group>] [-id <id
(negated) for the group>+] [-cell <cell name>] [-noauth] [-force] [-localauth]
[-auth] [-help]
Where: -noauth    run unauthenticated
        -force    Continue oper despite reasonable errors
        -localauth use local authentication
        -auth     use user's authentication (default)

[bovik@hostname bovik]$ pts creatregroup bovik:friends
group bovik:friends has id -1234

[bovik@hostname bovik]$
```

```
[bovik@hostname bovik]$ pts help adduser
pts adduser: add a user to a group
Usage: pts adduser -user <user name>+ -group <group name>+ [-cell <cell name>]
[-noauth] [-force] [-localauth] [-auth] [-help]
Where: -noauth    run unauthenticated
        -force    Continue oper despite reasonable errors
        -localauth use local authentication
        -auth     use user's authentication (default)

[bovik@hostname bovik]$ pts adduser -user hornbos -group bovik:friends

[bovik@hostname bovik]$ pts membership bovik:friends
Members of bovik:friends (id: -1234) are:
hornbos
```

```
[bovik@hostname bovik]$ pts membership bovik:friends
Members of bovik:friends (id: -1234) are:
hornbos
johnqp

[bovik@hostname bovik]$ pts help removeuser
pts removeuser: remove a user from a group
Usage: pts removeuser -user <user name>+ -group <group name>+ [-cell <cell name>]
[-noauth] [-force] [-localauth] [-auth] [-help]
Where: -noauth    run unauthenticated
        -force    Continue oper despite reasonable errors
        -localauth use local authentication
        -auth     use user's authentication (default)

[bovik@hostname bovik]$ pts removeuser-user johnqp-group bovik:friends

[bovik@hostname bovik]$ pts membership bovik:friends
Members of bovik:friends (id: -1234) are:
hornbos
```

## Negative Permissions

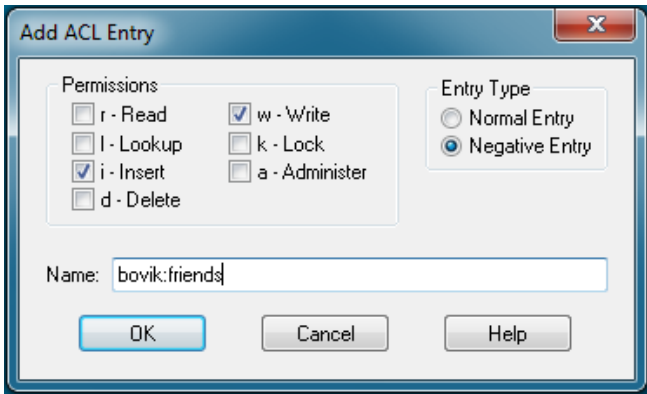
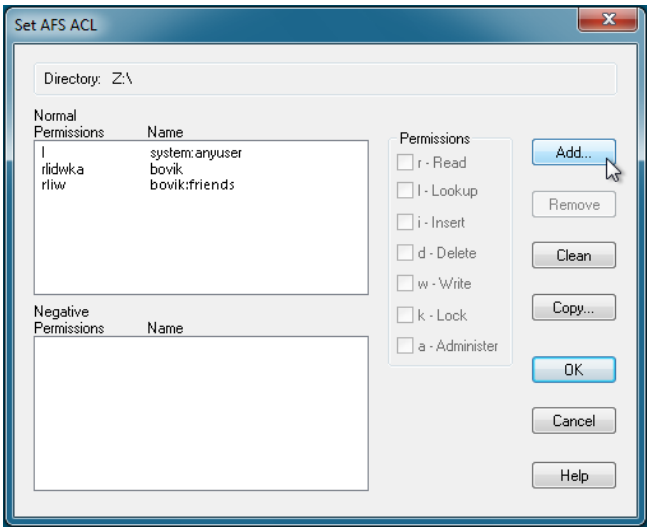
One or more individuals may be denied rights otherwise afforded from membership in a PTS group through the application of *negative* permissions.

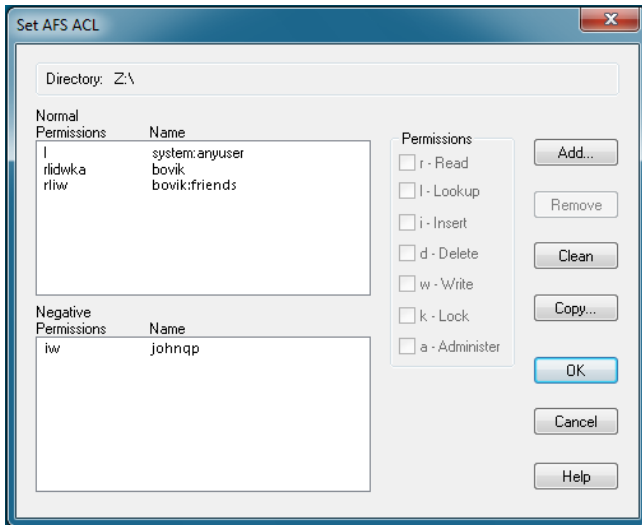
Negative permissions may be applied from the Linux command line or Windows Explorer interface.

```
[bovik@hostname bovik]$ fs la .
Access list for . is
Normal rights:
  system:anyuser l
  bovik rldwka
  bovik:friends rliw

[romeara@barsoom ~]$ fs sa . johnqp -negative iw

[romeara@barsoom ~]$ fs la .
Access list for . is
Normal rights:
  system:anyuser l
  bovik rldwka
  bovik:friends rliw
Negative rights:
  johnqp iw
```





## Backups & Restores

All AFS volumes receive nightly, incremental backups unless specified otherwise. User volume backups from the previous day may be accessed through the symbolic link *OldFiles* in home directories or within the corresponding backup hierarchy.

| AFS Location                                            | Backup Location                                                 |
|---------------------------------------------------------|-----------------------------------------------------------------|
| <i>/afs/cs.cmu.edu/user/username</i>                    | <i>/afs/cs.cmu.edu/.BACKUP/user/username</i>                    |
| <i>/afs/cs.cmu.edu/project/projectname</i>              | <i>/afs/cs.cmu.edu/.BACKUP/project/projectname</i>              |
| <i>/afs/cs.cmu.edu/academic/class/classnum-termYear</i> | <i>/afs/cs.cmu.edu/.BACKUP/academic/class/classnum-termYear</i> |

Volume restores for specific days are more readily available for dates within a week of the requested date, otherwise the nearest incremental backup will be used. Please check the previous day's backup location for a volume for missing data, and make restore requests as soon as possible.

# SCS Computing Facilities Support

Initially all graduate student machines are under full hardware and software support

## SCS Ubuntu Linux Support

SCS Computing Facilities provides support for Linux systems running Ubuntu 10.04 LTS. Depending on your needs, two different supported configurations are available:

For users who have self-installed Ubuntu 10.04LTS systems (or users who are comfortable performing day-to-day system administration tasks under Ubuntu), SCS Computing Facilities supports a set of packages that provide access to the following SCS services:

- Kerberos: for login authentication
- AFS: for file storage
- Printing: for printing to SCS printers

For users who desire full integration with the SCS Computing environment, a fully managed version of Ubuntu 10.04LTS is also available. This system provides the above core services plus full remote administration, SCS specific software (installed in /usr/cs), and local patch management.

Both environments allow users to install any software supported by the Ubuntu project. User home directories are located on the local disk (although it may be located under AFS if desired).

Under the fully managed environment, hard drive space is divided up to improve the efficiency and speed of the backup process. If the computer is under backup support, ONLY directories of the form /usrN are usually backed up. Directories in other places, such as /home are not backed up by default. We also back up the contents of /usr/BACKUP and do not back up /etc/srvtab (since backup traffic is not encrypted).

Backups are available upon request. To have backups added to your machine, please send your request to [help@cs.cmu.edu](mailto:help@cs.cmu.edu) asking for backups to be added and include the name of your machine.

## Microsoft Windows Support

SCS Computing Facilities support for Windows-based hosts includes: hardware support, installation and support of a baseline software environment, and network backups (if explicitly requested.) Users incur a monthly charge for this support. SCS Computing Facilities supports hosts running the following Windows operating systems:

### **Windows 7 Enterprise Edition** (64 bit default)

- **Note:** Although our baseline software has been tested and is compatible with Windows 7 64bit, users may experience problems with 3rd party software that is not compatible. If you rely on legacy software, it is highly recommended that you check the vendor specifications regarding compatibility with Windows 7.
- Windows 7 32 bit is available upon request

### **Windows Vista Enterprise Edition** (supported but no longer being deployed)

### **Windows XP Service Pack 3**

Other Versions of Windows:

**Windows 2000:** Support for Windows 2000 was officially discontinued in August of 2008. Any remaining Windows 2000 hosts are subject to removal from SCS software support.

Facilities support for Windows PCs includes: installation of a [baseline software environment](#), network backups (if explicitly requested), and hardware and software support. Users incur a [monthly charge](#) for this support.

## Hardware Support

Hosts covered by hardware support are entitled to the following:

- UPS: Uninterruptible power supply for use if there is ever a power-loss event.
- Warranty processing and component replacement of failed hardware typically by the next business day.
- Out-of-warranty component replacement of failed hardware.

### **Windows Disk Partitioning**

All facilitated Windows systems will be deployed with one large disk partition unless otherwise requested.

## Software Environment & Support

To request SCS Facilities staff to install or upgrade a PC operating system (Windows, Linux, or dual boot), use the [PC installation/upgrade request](#) form. Additional software is available from SCS and CMU Windows software [distribution servers](#).

The SCS Baseline Software Configuration includes the following:

- Microsoft Windows 7 Enterprise edition (64 bit Default) See **Note** above
- Adobe Acrobat Reader
- Ghostscript
- Ghostview
- MIT Kerberos for Windows
- Microsoft [Office 2010](#)
- Mozilla FireFox
- Mozilla Thunderbird
- Oracle Calendar
- PuTTY
- Symantec Endpoint Protection, including Antivirus and Antispyware
- WinSCP
- X-Win32
- iPass (remote network-access, mobile or off-site hosts only.)
- VPN (virtual-network client, mobile or off-site hosts only.)
- Nero 9 (CD\DVD burning software – **on request only**)
- Adobe Acrobat X Pro (**on request only**)
- Open AFS client (**on request only**)
- TiBs backup client (**on request only**)

## Backups

Backups of Windows hosts are not enabled by default. You must specifically request that SCS Computing Facilities backup your computer. Desktops and laptops use different backup systems, so consult our pages on [Windows backups](#) and [laptop backups](#) for details and limits on the service we can provide.

## Mac

Welcome to SCS Computing Facilities Mac support. We are an authorized Self-Service-Provider for Apple Computer. Our trained technicians are Apple certified and are able to perform on-site service repairs for all Apple computer hardware.

Warranty parts are ordered directly from Apple and in most cases we can complete hardware repairs in one business day with Apple's overnight shipping policy.

### What Apple Hardware and Software Do You Support?

To be eligible for Mac support services, your Mac must be CMU owned and covered under our SCS Computing Facilities monthly support charges.

Any Intel based Mac running OS X (ver. 10.5 and higher) can be supported. If you are using a supported Mac with an OS prior to OS X 10.5, we strongly recommend upgrading to a more current version. You can send email to [help@cs.cmu.edu](mailto:help@cs.cmu.edu) if you need help or have questions about upgrading.

We do not support personally owned equipment. You should contact Apple directly for all personally owned Apple computer problems.

### I Want to Upgrade My Mac to the Latest OS How Can I Do This?

One of our Apple certified technicians can do this for you. Simply email [help@cs.cmu.edu](mailto:help@cs.cmu.edu) with your request and someone will contact you within one business day or less. Be sure to include the CMU Asset number of the Mac you want to upgrade in your request.

### What Apple Computer Do You Recommend I Buy?

We can support any Intel based Apple computer. Our recommended Apple products are available at the CMU Computer Store:

<http://www.cmu.edu/stores/computer/Hardware/AppleProducts/index.html>

To purchase a new Mac email your request to [purchase@cs.cmu.edu](mailto:purchase@cs.cmu.edu) with a valid Oracle String and one of our purchasing consultants will contact you.

### Printing from a Mac

Detailed instructions for printer setup for Mac OS X can be found in our SCS Help Pages:

<http://www-2.cs.cmu.edu/~help/printing/index.html>

## What Software Do You Support for the Mac?

All facilitated Macs will be deployed with the following baseline software:

- Mac OS X Snow Leopard (10.6.x)
- Adobe Acrobat Reader
- Microsoft Office (Office 2011)
- iLife
- iWork
- Symantec Anti Virus software
- Fetch
- Oracle Calendar
- Firefox
- Adobe Acrobat Professional (**if requested**)
- Tibs backup client (**if requested**)
- iPass client (installed on laptops)
- VPN client (installed on laptops)

## What if I Want to Run Microsoft Windows on My Mac?

We support and recommend *Parallels* for desktop virtualization if you want to run Windows on your Mac

Users are responsible for purchasing the Parallels virtualization software. SCS Computing Facilities will provide the Windows operating system (Windows 7 by default) at no cost.

An additional software support charge will be applied for VM's. Backups for the VM are also available. The backup client must be installed on the VM host and an additional backup support fee will apply.

### Backups & Restores

See the Mac backup documentation for details on our Mac backup system and the limitations on what we can back up. Note that most Macs will not be put into the backup system (and thus will not receive backups) unless specifically requested:

[http://www.cs.cmu.edu/~help/backups\\_restores/mac\\_backups.html](http://www.cs.cmu.edu/~help/backups_restores/mac_backups.html)

## Mac

We recommend Mac OSX Snow Leopard 10.6 or later although we can support any Intel Mac.

### Mac Default Disk Partitioning

All Facilitized Mac hosts will have a maximum primary boot partition of approximately 50% of the total disk space. All remaining drive space will be created as one extended partition. All remaining drive space will be created as one extended partition.

Example: 500GB hard disk will be partitioned as follows:

Mac HD: 250GB (System)

Data Storage: 250GB (Data)

### SCS Baseline Configuration for Mac Hosts

SCS Computing Facilities-installed hosts within the SCS environment are delivered to the end user with a standard baseline configuration.

- Adobe Acrobat Reader
- Microsoft Office (Office 2008)
- Choice of Email client
  - Entourage
  - Apple MAIL (Mail.App)
  - Thunderbird
- Symantec Anti Virus software
- Stuffit Expander
- Oracle Calendar
- CMU Web Certificates
- FUGU
- VLC
- Firefox
- Tibs backup client (if requested)
- iPass client (installed on laptops)
- VPN client (installed on laptops)

## Hardware Support

SCS Computing Facilities provides repair and other services for hosts under SCS Computing Facilities hardware support. An Uninterruptable Power Supply (UPS) is provided for desktop hosts as part of that support. You should contact us if you have hardware problems with any host supported by SCS Computing Facilities. The contact is SCS Help Desk at x8-4231 or by email at [help@cs.cmu.edu](mailto:help@cs.cmu.edu) or call 8-4231 Monday-Friday 9:00AM-5:00PM. If the PC is intended to run both Windows and Linux, it is important that you either choose appropriate hardware from our list of recommended configurations or consult with us before purchasing. Our recommended configurations are found at:

[http://www.cs.cmu.edu/~help/purchasing/recommended\\_pcs.html](http://www.cs.cmu.edu/~help/purchasing/recommended_pcs.html)

## Backups

The host must be running a supported and properly configured client. To activate backups, you must send a specific email request to the SCS Help Desk at [help@cs.cmu.edu](mailto:help@cs.cmu.edu) for each machine that you want backed up. If you have a dual-boot machine, a separate request must be made for each OS. There is a monthly charge for machine backups. For dual boot systems only the OS that is running will be backed when the backup process runs.

For details on backups for individual platforms and the amount of data that can be backed up please see:

[http://www.cs.cmu.edu/~help/backups\\_restores/index.html](http://www.cs.cmu.edu/~help/backups_restores/index.html)

## Restores

In order to request a file restore, you must send the following information to the SCS Help Desk at [help@cs.cmu.edu](mailto:help@cs.cmu.edu). Insufficient information may delay the restore process:

- The name of the workstation or personal computer, including the administrative “domains” and/or other related aliases
- The name of the disk area, partition, and/or volume involved
- The cause of the file loss (accidental removal, disk failure, etc.)
- The current status of the affected disk area, partition, or volume
- The date at which you believe the file/volume/partition to have been damaged, or from which you would like to restore
- The complete file names of the lost files
- The time files were last modified (or created)
- The time files were lost or destroyed

Before requesting a restore on an AFS volume please check the OldFiles link. This link is located in `/afs/cs.cmu.edu/user/user ID/OldFiles`.

For example: `/afs/cs.cmu.edu/user/bovik/OldFiles`

## Locating People

There are several online applications that can be easily used to get information about people

- finger (More about this below)
- Campus Directory: [http://www.cmu.edu/ba/hr/camp\\_directory/directory\\_form.html](http://www.cmu.edu/ba/hr/camp_directory/directory_form.html)
- SCS Directory: <http://people.cs.cmu.edu/>
- Google and other Web Search Engines

## Finger

The finger program is available on the Windows and Linux command line. It is used to display information about local and remote accounts.

There are three basic ways to run finger.

- `finger` (with no arguments): display information about the local system and who is logged in
- `finger user` : display information about a user on the local system
- `finger user@host` : display information about a user on a remote host

**Note:** Although `user@host` looks like an email address, there are many cases where email to that string will not work. And there are many cases where typing a valid email address as an argument to the finger program will not display any useful information. This is especially true if the host portion is not on campus.

When finger displays information about an account it displays

- Information recorded about the account such as
  - The username or login name of the account
  - Full name of the owner
  - Home directory
  - Perhaps some login and/or logout times
- Information from the users `.plan` file

**Note:** As a courtesy to others, please consider creating a file named .plan in your home directory with some information about how to contact you. Routinely review it and keep it up to date. Others will use this information to contact you and help you.

For many accounts, your plan file will be

- /afs/cs.cmu.edu/user/\_yourusername\_/.plan

Some information you may want to put in your plan file

- Office Location
- Telephone numbers
- Vacation Status
- Job Title or Student Status
- Anything that tells a little bit about you

## Security

There is no firewall between the SCS network and the Internet. As a result, our network gets scanned several hundred times per day. Every year, there are reports of break-ins to SCS hosts. The vast majority of these break-ins happen because of the following, mostly preventable, causes:

- Using un-patched software, hosts that use un-patched software can be quickly (meaning within minutes/hours of being placed on the network) broken into
- The use of weak or poor passwords
- By sending passwords over the network unencrypted where they are easily sniffed
- Having undetected viruses/worms on Windows hosts
- Software that has not been securely configured i.e. having open shares on Windows hosts, unrestricted NFS exports, etc

## Windows and Mac Malware Protection

Running an up-to-date anti-virus program is recommended on all computers. Not only will such a utility protect you against the most common viruses, but it can also detect many (although not all) backdoor agents and Trojans an intruder might install on your system.

SCS Computing Facilities includes Symantec Endpoint Protection (SEP) as part of our baseline Windows and Mac software. SEP extends the Symantec AntiVirus (SAV) utility, previously deployed with the SCS baseline for many years, and now incorporates anti-spyware protection. If you are running Facilitized Windows or Mac, Symantec Endpoint Protection (SEP) is installed to protect you.

We encourage all Windows and Mac users to install SEP at their earliest convenience if not already installed on your computer. The installer is available on the server, MONOLITH:

**Windows** - "\\monolith.srv.cs.cmu.edu\pc\_dist\symantec\endpoint protection\"

**Mac** – "smb://monolith.srv.cs.cmu.edu/mac\_dist/Symantec/"

Running the SEP installer may take approximately 5-10 minutes. During the installation, it may appear that nothing is happening, but have patience: It *is* working (quietly). When the process completes, you will be prompted to restart your computer.

### Attachments & Trojans

Running anti-virus software is not a cure-all or a substitute for good security practices. There is always some time delay between the introduction of a virus and its incorporation into the anti-virus software's database. Backdoors and Trojans can also be designed to hide from virus detection programs. To reduce the likelihood of being infected by a virus/Trojan use the following common sense guidelines:

- **Do not** run or open e-mail attachments unless you know the sender, expect an attachment from that person, the subject line of the mail and type of attachment "make sense."
- **Do not** run programs from untrusted sources

**Note:** Microsoft never sends out patches via email and SCS Computing Facilities will **never** send you an email message with an attachment in it without prior notice.

Spam mailers and e-mail viruses have the ability to forge headers or messages making it seem like it is coming from someone you know, but it really is not. If you check the full headers of the e-mail message, you will see the actual origin of the message.

## Symantec Management Console

SCS Computing Facilities uses the Symantec Management Console (SMC). This central management allows for Symantec version control and logging in order to protect the security of our community. The SEP client is installed on all new SCS graduate machines running the Windows and Mac Operating System.

CMU has a [site license](#) for Symantec's anti-virus program [Symantec Endpoint Protection](#) (SEP). Our license agreement allows CMU (though not CERT nor SEI) staff, faculty, and students to install this software on both CMU-owned and personally-owned PCs. If you have a Windows or Mac host that you need to install SEP on, you can send an e-mail request to: [help@cs.cmu.edu](mailto:help@cs.cmu.edu) or obtain the software from the following location:

**Windows** - "\\monolith.srv.cs.cmu.edu\pc\_dist\symantec\endpoint protection\"

**Mac** – "smb://monolith.srv.cs.cmu.edu/mac\_dist/Symantec/"

## Keeping virus definitions up-to-date

All Windows and Mac hosts receive virus definitions directly from Symantec, typically on a daily basis.

To manually update your virus definitions:

### **Windows:**

1. Right-click the yellow shield on your taskbar or select the Symantec Endpoint Protection application from the Start\Programs menu.
2. Click on the "LiveUpdate" button

### **Mac:**

1. Click the yellow and black Symantec Endpoint Protection icon in the menu bar
2. Select LiveUpdate
3. Choose "Update virus definitions"

## Dealing with a malware infection

All Facilitized hosts within the SCS computing environment that have SEP installed are configured with auto-protect enabled which runs constantly providing real-time protection by monitoring activity. Auto-Protect looks for viruses and security risks when a file is executed or opened. It also looks for viruses and security risks when modifications to a file are made. Any file infected with a virus will prompt Symantec to issue a notice to the user. If you receive this notice on a host supported by SCS Computing Facilities, contact the SCS Help Desk at x8-4231 Monday – Friday 9:00AM-5:00PM or by e-mail at [help@cs.cmu.edu](mailto:help@cs.cmu.edu) for assistance in dealing with the infection. Symantec Endpoint Protection, by default, does not perform full scans. In addition, SEP will run an active scan when new virus definitions are loaded (typically daily). An active scan searches the most commonly infected areas.

SCS Computing Facilities does not enforce scheduled scans on users systems. The running of a full or scheduled scan is determined by the user as they see fit to their unique schedule. Such scheduled scanning is recommended.

If your machine is not supported by SCS Computing Facilities, or if you wish to attempt to fix it yourself, see the [Symantec virus database](#) for information on how to deal with the specific virus involved. Note that many viruses and worms create backdoors and/or make system changes that can require special cleanup procedures. If you do not fully clean-up after such an infection, it's possible that your machine may be compromised by backdoor that was created.

## Symantec Endpoint Protection FAQ

Here are some commonly-asked questions — and answers — about using Symantec Endpoint Protection (SEP) in the SCS environment. To submit your own question or to request one for this list, please send email to the SCS HelpDesk, [<help+@cs.cmu.edu>](mailto:help+@cs.cmu.edu).

---

### Contents

1. Where can I get the [SEP installer](#)?
  2. What types of scans are run on my machine?
  3. Can I [customize](#) automatic scans?
  4. How do I install SEP on my Facilities-supported [home computer](#)?
  5. How do I run LiveUpdate?
- 

### Frequently Asked Questions

#### 1. Where can I get the SEP installer?

The SEP installer is available on the SCS server: `monolith.srv.cs.cmu.edu`

**Windows** - `"\\monolith.srv.cs.cmu.edu\pc_dist\symantec\endpoint protection\"`

**Mac** – `"smb://monolith.srv.cs.cmu.edu/mac_dist/Symantec/"`

#### 2. What types of scans are run on my machine?

Symantec Endpoint Protection, by default, does not perform full scans. SEP does have Auto-Protect enabled, which runs constantly providing real-time protection by monitoring activity. Auto-Protect looks for viruses and security risks when a file is executed or opened. It also looks for viruses and security risks when modifications to a file are made. In addition, SEP will run an active scan when new virus definitions are loaded (typically daily). An active scan searches the most commonly infected areas.

SCS Computing Facilities does not enforce scheduled scans on users systems. The running of a full or scheduled scan is determined by the user as they see fit to their unique schedule. Such scheduled scanning is recommended by SCS Computing Facilities.

#### 3. Can I customize automatic scans?

Yes. After launching SEP, select "Scan for threats," this interface will allow you to create scans that run automatically at the day/time you choose.

4. **How do I install SEP on my Facilities-supported home computer?**

- a. Launch the VPN client and connect to monolith.srv.cs.cmu.edu
- b. Restart computer again when prompted

**Note:** Depending on your network-connection speed, the SEP installer may run 10 minutes or longer

5. **How do I run LiveUpdate?**

**Windows:**

1. Right-click the yellow shield on your taskbar or select the Symantec Endpoint Protection application from the Start\Programs menu.
2. Click on the "LiveUpdate" button

**Mac:**

1. Click the yellow and black Symantec Endpoint Protection icon in the menu bar
2. Select LiveUpdate
3. Choose "Update virus definitions"