Carnegie Mellon University
School of Computer Science
Computing Facilities

Introduction to SCS Computing

SCS Computing Facilities
School of Computer Science
Carnegie Mellon University
Gates Hillman Complex 4201
Monday—Friday 9am to 5pm
(412) 268-4231
help@cs.cmu.edu
https://www.computing.cs.cmu.edu
Visit our website for current availability.

Welcome

Welcome to the School of Computer Science at Carnegie Mellon University!

This guide offers an overview of the SCS computing environment for new users at the School of Computer Science. This is not intended to be a comprehensive set of instructions, but a good place to get started and gain familiarity with our computing environment.

Throughout this guide we will provide relevant links to our website which contains more complete and expansive information on any of the topics covered in this guide. For updated service hours or availability, please visit our website at https://computing.cs.cmu.edu, as these may change as the university's COVID-19 response evolves.

What We Do

End User Support

- Help Desk
- User Consulting
- Research
- Documentation
- Technical Procurement
- Account Management
- Operations
- Loaner Equipment
- Resource Management

Computing Support

- Hardware Maintenance, Upgrades & Repair
- Software Installation, Maintenance & Upgrades
- Requirements Consulting
- Product Research
- Software Licensing
- Virtual Machines

Infrastructure Support

- Authentication
- Calendaring Services
- Printing Services
- Archive Backup Services
- Data Protection Service
- Web Services
- High Performance Computing

What We Can Help With

While we are unable to assist directly with problems, requests, or concerns relating to other computing environments on campus (Andrew, ECE, etc.), we are happy to act as liaisons to help address any issues you may have that involve computing outside of SCS.

The SCS Help Desk

The SCS Help Desk is the place to go for support; you are welcome to send us an email, give us a call, or drop by in person with any and all of your questions and requests.

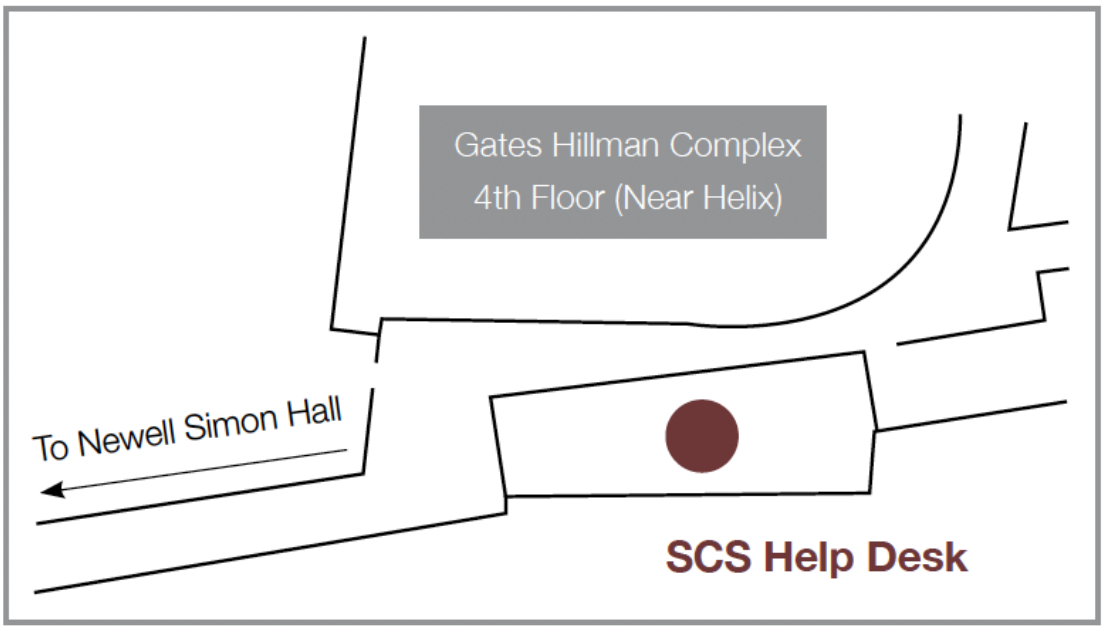
SCS Help Desk Hours

COVID-19 Special Remote Support Schedule

9:00 am to 5:00 pm

Monday through Friday

SCS Help Desk Location



Gates Hillman Complex

Room 4201

Gates Hillman Complex, 4th Floor

Near Helix

We are prepared to support you as CMU's pandemic response evolves.

Our technical teams are now structured to provide remote support as well as on-site support on an as-needed basis.

For all technical support, you can:

- Submit a request through our website via https://computing.cs.cmu.edu/gethelp.
- Contact our help desk at 412-268-4231, Monday through Friday, 9:00 am to 5:00 pm.
- Email our help desk at help@cs.cmu.edu.
- Contact SCS Operations, who provide after-hours support for critical issues and infrastructure. They can be reached by phone at 412-268-2608.

Please note: For updated service hours or availability, please visit our website as these may change as the university's COVID-19 response evolves.

The Computing Website

The SCS Computing website, or our "Help Pages" as they are commonly known, are our online resource for documentation, tools, solutions to common SCS computing problems, and news about computing at SCS.

You can consider our site the central place to learn more about the computing environment, manage your passwords and account preferences, and keep up to date with current events that affect the facility.

Visit our website, at https://computing.cs.cmu.edu.

Some popular support topics include:

- **Change your Kerberos password using our Instance Manager**
    - https://computing.cs.cmu.edu/help-support/instance-manager.html
- **Publish a Web Page**
    - https://computing.cs.cmu.edu/help-support/web-publishing.html
- **Register Computer Equipment for Support (hardware, software, backup, network access and more)**
    - https://computing.cs.cmu.edu/help-support/equip-registration
- **Recommended Hardware Configurations**
    - https://computing.cs.cmu.edu/desktop/supported-hardware.html

Getting to Know the School of Computer Science

The SCS community follows the Reasonable Person Principle.

It holds that reasonable people strike a suitable balance between their own immediate desires and the good of the community at large.

- Everyone will be reasonable.
- Everyone expects everyone else to be reasonable.
- No one is special.
- Do not be offended if someone suggests you are not being reasonable.

The SCS community has also developed a set of rules and customs for behavior that is generally considered acceptable by others in the Department. These rules suggest ways to conserve and share public resources, as well as how to best be a reasonable and responsible member of the SCS community. Here are some guidelines to help you get off to a good start.

Shared Computing Resources

Help keep our computing environment safe and working well:

- Keep your account and its password private. You are responsible for anything done from your account.
- Notify SCS Computing Facilities in advance and review our website's section on network policy.
- Policy before connecting any computer or other networked device to our network.
- If you need to make multiple copies of a document, use a photocopier.
- Print large documents at off-peak hours.
- Respect others' privacy.
- Do not read someone else's files unless you know you have permission: if in doubt, always
  ask for permission, even if that person has not employed any file protection mechanisms.
- Consider printer output private.
- Make sure that all of your computers have been kept up to date with all of the current
  patches.
- Do not use government-sponsored equipment and resources to post messages outside of SCS for commercial gain.

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.

Locating People

There are several online directories that can easily be used to get information about members of the University community.

SCS Directory

The School of Computer Science maintains an online directory of all current faculty, staff, and graduate students who are part of the SCS community. The directory can be accessed at the following website:
https://www.cs.cmu.edu/directory/

Campus Directory

Carnegie Mellon maintains an online directory of all current faculty, staff, and students affiliated with the university community. The directory can be accessed at the following website:
https://directory.andrew.cmu.edu/

The SCS Environment

End-User Resources

Most departments in the School of Computer Science will provide incoming faculty, PhD students, and staff with a desktop or a laptop computer that has been configured by SCS Computing Facilities. For more information about end-user computing, visit the desktop computing section of our website at https://computing.cs.cmu.edu/desktop/.

Personal Resources

You are welcome to use personally owned computers, mobile devices, and other equipment within the SCS environment. Personal equipment that causes problems on the SCS network may be blocked from network access as a result. For more information, visit the networking section of our website at https://computing.cs.cmu.edu/desktop/network.

For more about connecting personally owned computers, mobile devices, and other equipment to the wireless network, please visit the campus Computing Services website at https://www.cmu.edu/computing/services/endpoint/network-access/wireless/.

Support for personally owned equipment is limited; we can only provide best-effort support, and support for personally owned equipment is not given priority. Personally owned equipment is ineligible to enroll in hardware or software support from SCS Computing Facilities staff. Some personal devices are permitted to use the Crashplan data protection client.

Shared Resources

We provide remote access to Linux services through a general-purpose Linux system.

Accessing The General-Purpose Linux Services

The Linux General Purpose (GP) services may be accessed via any SSH client. Use an SSH client to connect to the following hostname:

`linux.gp.cs.cmu.edu`

You can log in with your SCS username and Kerberos password. The Linux GP Services can be used for access to command-line or SFTP clients.

For more information about using the Linux GP Services, please see: https://computing.cs.cmu.edu/desktop/os-linuxgp.html.

Passwords

Within the SCS Computing environment, you will have several different passwords. Below is an overview of the most frequently used passwords and their purposes.

Types of Passwords

Type of Password	Description
Kerberos	This is your main username/password combination in SCS. This password is used to log in to any web site or service protected by SCS Web Authentication. This password is also used to log in to Linux machines in the SCS Environment. This username and password are assigned to you when you first join the SCS community. You will need to change this password; please see Changing a Kerberos Instance Password on page 7.
Andrew	This password is used primarily to authenticate to Windows-based machines, but is used for other services, such as: • Access to Resource Scheduler • Printing to SCS printers • Cluster authentication

Password Security

It is important when setting your passwords to choose a strong password. A common or weak password is a means by which any account can be broken into by an attacker. A strong password is one that is at least eight characters, and includes a combination of letters, numbers, and symbols. Your password should be easy for you to remember, but difficult for others to guess. It should not be a word that is found in the dictionary.

Please Note: It is very important that you use a unique password for each system. You should never re-use old passwords or a password used for any other purpose. Below is a link to ISO's guidance on password management:
https://www.cmu.edu/iso/governance/guidelines/passwordmanagement.html

Password Managers

For this purpose, you may choose to use a password manager to maintain your list of strong, unique passwords (or to generate random passwords for you, though these are harder to remember if you don't have access to your password manager).
Here is information about password managers (including vetted managers) by CMU Information Security Office:
https://www.cmu.edu/iso/governance/guidance/passwordmanagers.html

Changing Passwords

If you suspect that your account has been compromised, it is critical that you change your password immediately!

If you are unable to change your passwords through self-service tools available, or require assistance for any reason, we're happy to help. Our help desk can assist with SCS Kerberos password changes. For Andrew account password changes, you can contact the Andrew Computing Services Help Center. For more information on their services, visit https://www.cmu.edu/computing/support/index.html.

Due to the COVID-19 Pandemic response and our adjusted service offerings, we may need to schedule a virtual appointment to assist you with your password change, as our help desk is not open for in-person visits yet. We always require you to provide your CMU ID for verification.

For more information about our password policy, please visit https://computing.cs.cmu.edu/security/security-password.

Managing Kerberos Instances

To create, remove, or update your Kerberos instances, please go to the SCS Kerberos Instance Manager in any web browser:
https://computing.cs.cmu.edu/help-support/instancemanager.html
To use the SCS Kerberos Instance Manager, you will need to authenticate via WebISO (see Figure 1)

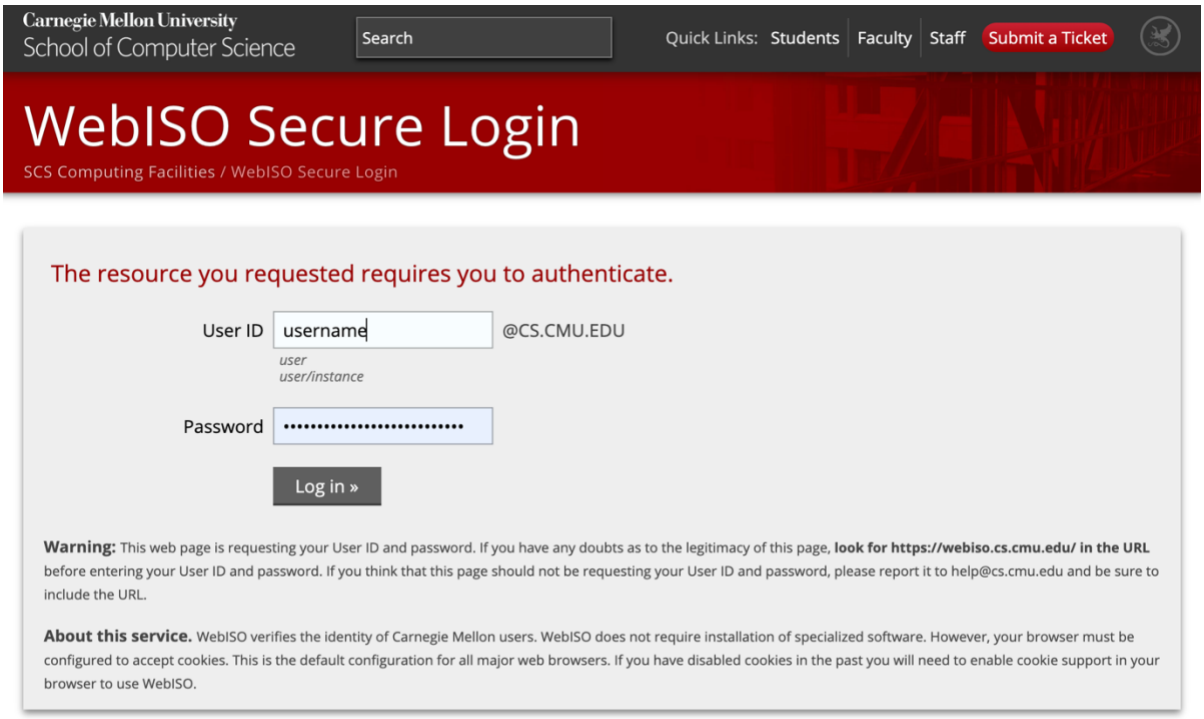


Figure 1: authenticating with SCS WebISO

Once authenticated, you can use the SCS Kerberos Instance Manager to create new instances and change instance passwords.

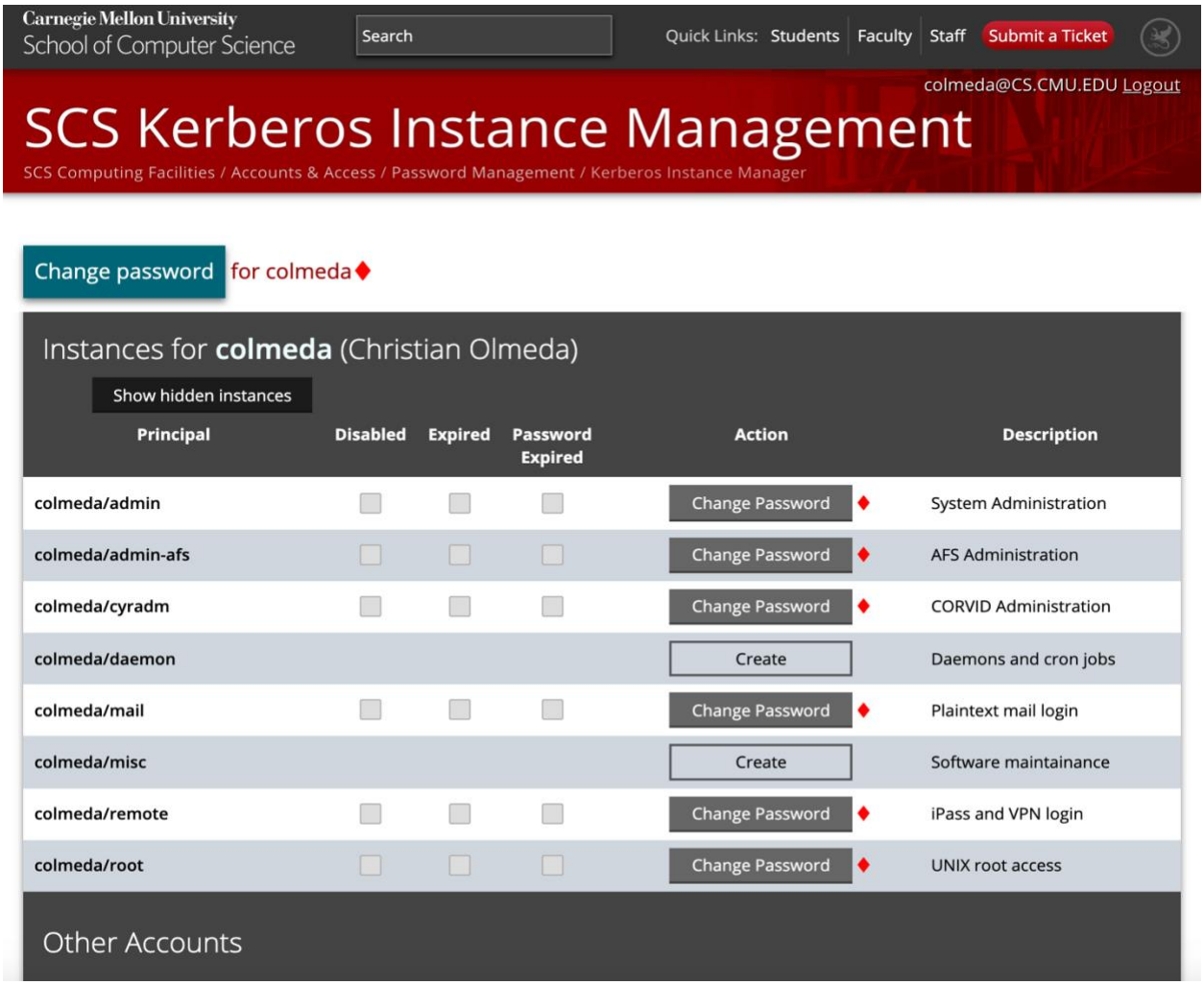


Figure 2: instance manager and instances available for password changes (or first-time creation)

Please Note: you may see Password Instances that do not apply to you; you may ignore them.

Changing a Kerberos Instance Password

If a Kerberos instance already exists, but you need to change the password for that instance, you can use the SCS Kerberos Instance manager to reset that password.

To change the password of an existing instance with the Instance Manager:

1. Click 'Change Password' next to the appropriate instance.
2. Enter and verify the new password.
3. Click Change Password to set the new password.

Forgotten Passwords

If you have forgotten your Kerberos password, our help desk can schedule a remote password reset appointment using video chat to confirm your identity and reset your password. Supported video chat clients are: Zoom, Google, Hangouts, Apple FaceTime, and Skype.

Valid Photo ID (CMU ID or government issued ID) is required for any password changes (remote or in-person).

Please Note: The SCS Help Desk cannot reset /admin or /root passwords. Additionally, we unable to reset your Andrew account password, visit Computing Services's Andrew Password Management page for more information.

Logging On

Your access is comprised of two credentials: your SCS Kerberos account and your Andrew account:

- Your SCS Kerberos account allows you to log in to SCS-provisioned Linux computers or VM's in addition to select web resources.
- Your Andrew account allows you to log in to Windows computers and VM's as well as provides access to most CMU and SCS websites and resources.

Logging on to Windows

- On a Windows-based computer, you will be prompted to click any button to log in.
- Once you click a button, you will see a login window with the Username and Password fields.
- Ensure that "Sign in to:" is set to "Andrew".
- You will use your Andrew username and password to log in.

Logging on to Linux

To log in to an SCS Linux computer or VM, you need both an SCS Kerberos account and a local account on the computer (or vm) you wish to log in to. You can submit a ticket to request a local account on the computer. You will need to provide the hostname and be the owner or a contact on the computer in question. If you have received a graduate student machine from your department, you will have an account on the computer assigned to you.

If you are not a contact on the computer, the owner of the Linux computer will be contacted to approve the request. Once this local account has been created, simply use your Kerberos username and password to log in to the computer.

Logging on to macOS

To log in to a SCS Mac computer running macOS, you will need a local user account (not centrally managed but locally created on each Mac). Local user accounts on Mac computers are added when the system is initially configured by SCS Computing Facilities. If you have a Mac, your initial account password will be provided to you.
To log in to your SCS Mac computer, use your SCS username and local password.

Electronic Mail

Delivery Options

Delivery to your Andrew Mailbox

The university provides you with a mailbox associated with your @andrew.cmu.edu and @cs.cmu.edu email addresses. This mailbox can be accessed through the webmail portal at https://email.cmu.edu.

We support a variety of clients to access your Andrew email on supported desktop operating systems, as well as mobile devices. Instructions for using a client to access your email can be found here at https://computing.cs.cmu.edu/comm-collab/email-clients.

Supported Standalone Clients

We support a wide range of clients to check your Andrew mail. Please not that for IMAP email clients, the mailbox must have IMAP functionality enabled.

Windows

- Thunderbird
- Outlook

macOS

- Thunderbird
- Outlook

Linux

- Thunderbird

Configuration instructions for supported email clients can be found at the following URL https://computing.cs.cmu.edu/comm-collab/email-clients.html.

Email Security

Computer viruses, trojans, and other malware often try to infect your computer via email. Bad actors may also try to use email to lure you into providing sensitive information. It is important to exercise caution when dealing with email that appears suspicious or is sent from an untrusted source.

Neither SCS Computing Facilities nor CMU Computing Services staff will ever ask you for your password.

If you have any questions or suspicions about a particular message, contact us.

Attachments and Trojans

To reduce the likelihood of being infected by a virus or a Trojan via an email message, use the following guidelines.

Do not run or open email attachments unless:

- You know the sender
- You expect an attachment from that person
- The subject line of the mail and type of attachment fit with what you're expecting from the sender

Do not run programs from untrusted sources. Spam mailers and email viruses have the ability to forge messages to make it appear as if the email is coming from someone you know. If you have suspicions about where an email message came from, contact us.

Phishing

Phishing is the tactic of convincing someone to reveal sensitive information, such as:

- Passwords
- Credit card numbers
- Banking details

- Other similar information through misdirection, deception, or other subterfuge.

Phishing often takes the form of email messages. Phishing messages often request or demand personal information, usually with some sense of urgency or threat that a service or opportunity is about to expire. If you receive a notice of loss of access or an impending fine that looks legitimate, treat the message with caution and verify the contents of the message through other means (via phone, etc.) before following the instructions in the message.

Phishing attempts via email often have clickable links embedded in the message, which can misrepresent themselves as links to the websites of well-known companies or services. If you are at all suspicious of a message containing clickable links, always manually check the link before clicking on it.

Please Note: SCS Computing Facilities staff will never ask you for your password.

If you encounter a message that demands personal details, always check to make very sure the message is legitimate. You can report phishing attempts to the CMU Information Security Office through the PhishAlarm button in Google Mail and Exchange or email (isoir@andrew.cmu.edu). If you have any questions about a suspicious email, or would like assistance with verification, contact us.

Displaying Remote Images

Most modern email clients can display images embedded in an email message. Sometimes, these embedded images are not included in the message itself but are served off a remote webserver.

These remote images can pose a privacy risk. If the sender is monitoring the webserver that is serving the images in your mail, when you read the message and load the remote images, the sender will be able to verify your email address and note when the email was read.

Most modern mail clients will allow you to turn off automatic loading of remote images. If the option is available, we recommend that you set your client to only load remote images on demand, and then only load remote images from trusted sources.

Spam and Virus Detection and Filtering

Server-Side Tagging and Filtering

All incoming email is scanned for spam content and viruses. We use the Pure Message filtering service offered by Sophos to score messages for spam and flag messages with malicious attachments.

Pure Message works by applying a set of rules and checks to each piece of email. If Pure Message discovers suspicious patterns in the email, the service will tag the piece of email as spam. By default, email that has been tagged as spam will be automatically filed into your SPAM folder; you may also set your preferences to discard spam entirely.

Please Note: By policy, email that has been tagged as spam will not be forwarded to an account outside of Carnegie Mellon University.

If Pure Message discovers a virus in an attachment, the message will be delivered with the attachment removed and [PMX-Virus] prepended to the Subject header.

Client-Side Spam Filtering

Many email clients also offer built-in SPAM filtering. Client-side SPAM filters usually work by training. You can teach the filter what to treat as SPAM, and the filter will adapt to your incoming mail as it learns to discern good mail from unwanted mail.
Because client-side SPAM filters can sometimes treat legitimate mail as SPAM, we recommend using client-side filters only when necessary.

Printing

SCS Computing Facilities provides support for a range of public printers distributed within SCS designated spaces, along with infrastructure that allows printing from Windows, Mac, and Linux hosts.

Printing Etiquette

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

- Only print large jobs at night or off-hours
- Use SCS printers only for SCS-related work
- Preview your output before printing

Getting Help

If you have a problem with a printer, contact the SCS Help Desk to report printing problems during normal business hours (Monday-Friday, 9am-5pm).

SCS Operations also provides after hours printer support for many printer problems, such as being out of toner, routine paper jams, etc. SCS Operations may be reached by calling (412) 268-2608.

More severe printer problems will need to be handled during normal business hours. Print jobs can be released from any of our public printers without having to resubmit the job.

List of Printers

To review the full list of all available public printers and their locations, please refer to https://computing.cs.cmu.edu/desktop/printer-list.

Networking

The SCS network is one of three network entities on campus. In addition to the SCS network, the other two networks are the ECE Department network managed by ECE Facilities, and the Computing Services-managed network.

The Computing Services network provides local network connectivity for everyone on campus except for wired connections in SCS offices. Computing Services also provides the campus with connectivity to both the commodity Internet and research networks. The CMU Computing Services networking group manages the CMU-DEVICE, CMU-GUEST, and CMU-SECURE campus wireless networks.

SCS Network Use Policies

- The SCS network is vital to the school's research and educational activities.
- Use only IP addresses that have been assigned to your host.
- Configure your machine to use DHCP.
- Use only authorized DHCP servers.
- Do not use unpatched or compromised hosts.
- Contact the SCS Help Desk before performing any network-related experiments which may adversely affect network performance.
- Do not install or use unauthorized wireless access points.
- DHCP addresses are persistent and will not change unexpectedly in the SCS environment.

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 University computing policy and provide some SCS-specific additions to that policy.

SCS Computing Facilities reserves the right to disconnect or otherwise remove hosts and equipment from the network without notice if they:

- Cause technical issues that impede other users
- Violate network usage policies
- Use an unassigned or unauthorized network resources
- Show signs that they have been compromised

SCS Computing Facilities reserves the right to monitor network traffic 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.

Connecting Hosts to the Network

You must register any host or network device that you would like to connect to the SCS network with SCS Computing Facilities. To register a device to use the SCS network, you must provide all the following information about the device before putting it on the SCS network:

- device type
- asset tag number
- serial number
- location
- hardware address
- contact information

Please Note: When registering personally owned equipment for a network connection, you do not need to provide an asset tag number.

You must notify us if any of the above information changes for any network connected device. It is especially important that SCS Computing Facilities is notified when a

computer is moved. Moving a computer may require an IP address change 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 the campus network and is managed on our behalf by campus Computing Services. For more about the wireless network at Carnegie Mellon, please visit the Computing Services website:
https://www.cmu.edu/computing/services/endpoint/network-access/wireless/

Use the Equipment Registration form found at the following URL for all new registrations and updates of SCS network-connected devices:
https://computing.cs.cmu.edu/help-support/equip-registration

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

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.

Outlets are not automatically activated. If you are moving your computer to an unused outlet, you will need to request the activation of that outlet. To request an activation either send a picture of the outlet or make a note of the outlet number beginning with an R, which will be visible on a label attached to the network port and follow this form:

R00A00-000-00

Please send any activation request, including the appropriate outlet number, to help@cs.cmu.edu.

Host Naming Conventions

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.
- Project subdomains will only be assigned for groups of machines relating to the project.
- SCS Computing Facilities tries to avoid having multiple hosts that have the same hostnames.
- All personally owned machines will be assigned a name in the .pc.cs.cmu.edu namespace without exception.
- SCS Computing Facilities reserves the right to reject inappropriate hostnames.

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,
- you notify SCS Computing Facilities prior to engaging in the activity,
- and 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 you must first notify SCS Computing Facilities as well as obtain permission before beginning any activity that could affect the network.

Network monitoring for research purposes or debugging network problems is allowed. Please contact SCS Help Desk 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 email, 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 email, 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.

Computing Services Bandwidth Restrictions

CMU Computing Services monitors university data network and Internet bandwidth consumption to ensure that this shared resource is not abused. There is no bandwidth quota for research network traffic. For more information on CMU Computing Services usage guidelines see:
https://www.cmu.edu/computing/services/endpoint/network-access/guidelines/bandwidth.html

If you need to use more bandwidth than is allowed by campus policy, you can request an exemption from the bandwidth limit. For information about how to request a bandwidth exemption, please see:
https://www.cmu.edu/computing/services/endpoint/network-access/guidelines/bandwidth.html

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.

Hosting Domains

If your project is using a vanity domain, we may be able to host that domain. We can host domains for both website and email traffic under certain conditions.

Domain Hosting

You can use equipment on the CMU 128.2.*.* and 128.237.*.* 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 non-profit activities.

SCS Computing Facilities does not delegate DNS for SCS or sub-domains of SCS projects.

A special address space has been set aside for non-commercial domains with a top-level domain other than .org. Domains hosted in this address space must be related to the School of Computer Science and/or Carnegie Mellon University. Please contact the SCS Help Desk if you have a domain that requires this special IP address space.

Email for Hosted Domains

We can provide the following email services for hosted domains:

- mail aliases
- mailing lists
- mail forwarding

Please Note: Email services for hosted domains are only available for domains associated with CMU sponsored research.

VPN

The Cisco AnyConnect VPN (Virtual Private Networking) software allows a computer on another network to appear that it has an CMU 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, Mac OS X, and Linux.

Download the VPN client for Windows, Mac and Linux systems from:
https://www.cmu.edu/computing/software/all/cisco-anyconnect/

For a description of how to use the VPN, please see:
http://www.cmu.edu/computing/services/endpoint/network-access/vpn/index.html

Wireless Networking

The campus wireless network is administered and maintained by campus Computing Services.

While SCS Computing Facilities is not responsible for the campus wireless, we can help verify configuration settings. We can also work with Computing Services to report and track outages in the campus wireless networks. If you experience wireless issues, please contact the SCS Help Desk.

Computing Services Wireless in SCS

Many users in the SCS community use the campus wireless networking service. However, there are some things to consider when using these wireless networks:

- A wireless connection is not as fast or reliable as a wired connection
- You must use the CMU VPN to access the following services:
    - Windows domain services (with some exceptions)
    - Any other SCS service restricted by IP or hardware address.

Wireless is not meant to be a substitute for wired Ethernet for tasks that require large amounts of bandwidth. For example, we cannot create archival backups of hosts over the wireless network. If you have any questions about Computing Services wireless service, contact the SCS Help Desk.

Computing Services Secure Wireless

Campus offers an encrypted wireless network that requires authentication to join. This secure wireless network is named **CMU-SECURE**.

You do not need to register your device to use the **CMU-SECURE** wireless network. To use this network, connect your device to the network named **CMU-SECURE**. You will be prompted for a Username and password. Use your Andrew Username and password

to connect to the CMU-SECURE network. In some cases, you may be asked to verify the connection.

Computing Services Open Wireless

Campus offers a wireless network that requires registration to join. This open wireless network is named **CMU-DEVICE**.

Traffic on the **CMU-DEVICE** wireless network is unencrypted. If you have concerns about transmitting sensitive data over a clear network, we recommend either using a VPN client, or using the **CMU-SECURE** wireless network.

Using the **CMU-DEVICE** wireless network requires registration. To register your wireless device to work with the campus open wireless network, follow the instructions at https://www.cmu.edu/computing/services/endpoint/network-access/wireless/how-to/cmudevice.html.

Once registration is complete, you will be directed to a web page confirming that your device now has access to the campus CMU open wireless network.

Until you have properly registered your device for use with the CMU wireless network, all network connections except to the Computing Services authorization website will fail. Please register your device before attempting to use the CMU wireless network for reaching mail servers, filesharing servers, or other types of connections.

Computing Services Guest Wireless

Campus offers an encrypted wireless network for temporary use by guests of the University. This secure wireless network is named **CMU-GUEST**. This network should not be used by current students, faculty, or staff.

This network requires an access code to join. Faculty and staff can use the Computing Services' Event Manager to create access codes for guests to connect to the **CMU-GUEST** network.

For more information about the Computing Services Event Manager, please visit https://www.cmu.edu/computing/services/endpoint/network-access/wireless/how-to/guest.html.

AFS

AFS is a distributed file system providing a client and server architecture that offers:

- File sharing within a single name space
- Security
- Scalability
- Transparent data migration

For hosts running macOS Mojave or Windows 10, users should not use OpenAFS. You can use another client such as Auristor or a SFTP client (i.e. FileZilla). AFS is used to share and store data for classes, projects, and users. Your SCS user or project website is likely served from AFS.

To access your AFS volume, you may connect to `linux.gp.cs.cmu.edu` using your SCS username and SCS Kerberos password.

Authentication

Authentication is automatic on Linux workstations when you login with your Kerberos password.

Kerberos credentials automatically expire after 24 hours and must be refreshed, even if you remain logged in. You can refresh your Kerberos credentials by using the kinit command from a shell window. This will prompt you for your Kerberos password.

Checking Authentication

Use of the `klist` command from a Linux shell window to display your current login credentials:

```
example@linux:~$ klist

Credentials cache: FILE:/tmp/krb5cc_14871_f31544

Principal: example@CS.CMU.EDU

Issued Expires Principal

Jun 5 12:31:17 Jun 6 12:31:17 krbtgt/CS.CMU.EDU@CS.CMU.EDU

Jun 5 12:31:17 Jun 6 12:31:17 afs@CS.CMU.EDU

example@linux:~$
```

Access Control

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

AFS Permissions

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

File		
Read	r	Allows for file reads and directory statistics.
Write	w	Allows for writing changes to files.
Lock	k	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.

Displaying an Access Control List

The command line interface of a Linux shell may be used to list the membership and authorizations of a given directory with the fs la command:

```
example@linux:~$ fs la .

Access list for . is

Normal rights:

system:anyuser l

example rlidwka

example@linux:~$
```

Managing Access Control Lists

Owners or users with administrative permissions may edit or add additional entries to the directory's ACL. The Linux shell command `fs sa` may be used to manage directory ACLs.

In the following session, our example user:

1. Displays the access list on their home directory using the `fs la` command
2. Sees that the user bovik has read access
3. Removes specific access rights for the user bovik using the `fs sa` command (note: this command is non-recursive)
4. Checks to make sure that access is revoked:

```
example@linux:~$ fs la .

Access list for . is

Normal rights:

system:anyuser l

bovik rl

example rlidwka

example@linux:~$ fs sa . bovik none

example@linux:~$ fs la .

Access list for . is
```

```
Normal rights:

system:anyuser l

example rlidwka

example@linux:~$
```

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 from many ACLs across multiple directories.

For example, you may choose to 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.

AFS has several special group definitions already in place. For more information, please visit https://computing.cs.cmu.edu/help-support/afs-groups.html.

Making a New PTS Group

Our example user would like to have a PTS group to manage who has read access to his home directory.

The first step is to create the group, using the `pts creategroup` command:

```
example@linux:~$ pts creategroup example:readers

group example:readers has id -4928
```

```
example@linux:~$
```

Next, our example user must grant the appropriate access to the group with the fs sa command (along with the fs la command to make sure the Access Control List was properly modified):

```
example@linux:~$ fs sa . example:readers read

example@linux:~$ fs la .

Access list for . is

Normal rights:

example:readers rl

system:anyuser l

example rlidwka

example@linux:~$
```

Our example user needs to add other users to the group using the `pts adduser` command:

```
example@linux:~$ pts adduser -user bovik -group example:readers

example@linux:~$
```

The command `pts membership` can be used to check who is on in PTS group:

```
example@linux:~$ pts membership example:readers

Members of example:readers (id: -4928) are:

bovik

example@linux:~$
```

The command `pts removeuser` can be used to remove a user from a PTS group:

```
example@linux:~$ pts removeuser -user bovik -group example:readers

example@linux:~$
```

The command `pts` membership will verify the removal:

```
example@linux:~$ pts membership example:readers

Members of example:readers (id: -4928) are:

example@linux:~$
```

Updating Web Pages

Modest websites may be hosted within AFS directories. Security measures restrict the use of PHP, CGI, or other dynamic content generation; however, server-side includes which do not rely on exbjb may be used.

Web content should be in an exclusive subdirectory of a volume. The permissions on this directory should be configured to provide the necessary AFS access list privileges on for the website to be served by SCS web servers.

Setting Permissions for the Website Directory

Make a web subdirectory within the AFS volume and set the appropriate AFS ACL and permissions. The top-level directory of the volume will have different permissions than its web subdirectories.

If necessary, set the permissions on your AFS home directory so that the web servers can access your www directory:

```
example@linux:~$ fs sa . wwwsrv:http-ftp l

example@linux:~$
```

Then, set the permissions on your www directory so that the web servers can access your content:

```
example@linux:~$ fs sa www wwwsrv:http-ftp rl

example@linux:~$
```

Subdirectories created within the www directory will automatically inherit the required access list and privileges.

Adding Content

Content for the site may be created using any tools available on the workstation or uploaded to it. We recommend the use of SSH copy (scp) or secure FTP (sftp) for uploading your web content.

You may use any SCS Linux host where you have an account to upload content; a common choice is to use the general purpose Linux server:

```
linux.gp.cs.cmu.edu
```

If you would like to have a personal web page served by the SCS web servers, you will need to place the files that make up your website into the `www` directory of your AFS home directory.

Privacy and Access Restrictions

Websites served from AFS will honor .htaccess file restrictions. However, we do not recommend any sensitive data such as SSNs, credit card numbers, passwords, etc. to ever be stored on websites.

Linking Your Content to the Web Servers

If your content does not appear at `http://www.cs.cmu.edu/~[your username]` your content directory may need to be linked to the Web Servers. To link your content to the web servers, please submit a ticket.

AFS 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, available via the Linux path:

```
/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 machine in the computing environment where AFS is installed and enabled.

Requesting Volumes and Quotas

Project names must consist of 11 characters or fewer (academic volume names are pre-determined to match the SCS designated course number and year - section numbers are also available, if they are required).

- Project sponsor or course instructor, and one additional individual to be granted full administrative rights within the volume.
- The initial quota request; please limit it to meet your current requirements (it may be resized to meet your future requirements as they change).

Classes may request classwork submission student directories; please include a class roster of only the student usernames, and designate TA usernames to be added for administration of volume contents when requesting a classwork submission folder.

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.

Types of AFS Volumes

Volume Type	Description	Default Quota	Max Quota
User	Home directory. Moderate data requirements. /afs/cs.cmu.edu/user/username	1 GB	10 GB
Academic	Class directories for sharing common documents. Student dropoff directories available upon request. /afs/cs.cmu.edu/academic/class/classno-termYear	1 GB	25 GB
Project	SCS Affiliated projects may request space for collaboration purposes. /afs/cs.cmu.edu/project/projectname	1 GB	25 GB
Backup	Backups for existing volumes made nightly. /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. `/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 using the `fs lq` command:

```
example@linux:~$ fs lq

Volume Name Quota Used %Used Partition

user.example 1000000 25 0% 0%

example@linux:~$
```

If you require additional quota, please submit a ticket.

Backups and 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
/afs/cs.cmu.edu/user/username	/afs/cs.cmu.edu/.BACKUP/user/username
/afs/cs.cmu.edu/project/projectname	/afs/cs.cmu.edu/.BACKUP/project/projectname

/afs/cs.cmu.edu/academic/class/classnum-termYear	/afs/cs.cmu.edu/.BACKUP/academic/class/classnum-termYear

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 make restore requests as soon as possible.

End-User Computing

General Support

SCS Computing Facilities can provide support for CMU owned end user equipment. Some CMU-provided equipment (such as PhD machines) is under full hardware and software support by default, but departments may opt to support machines themselves.

Hardware Support

Warranty processing and hosts covered by hardware support are entitled to the following:

- Hardware, troubleshooting, & diagnostics
- Out-of-warranty component replacement of failed hardware (cost of hardware not covered)
- Uninterruptible Power Supply (UPS) for use if there is ever a power-loss event (not available for GPU machines)

We can service laptop batteries on supported machines after diagnostic testing has identified that the battery needs to be replaced. Battery replacement due to normal wear and tear is not covered, but should a battery experience an early failure, its replacement will be covered if the machine is under warranty.

Moving Equipment

If you need to move supported hardware, we are happy to assist. Contact the SCS Help Desk to schedule a technician to move your equipment to a new location.
You may choose to move your equipment yourself. If you are moving equipment that connects to the wired network, you may need to request an outlet activation at the new location.

Please make sure to notify us of any equipment you have moved; list the old location, the new location, and the asset number of the equipment by submitting a ticket via https://computing.cs.cmu.edu/gethelp or sending an email to help@cs.cmu.edu.

Unsupported Equipment

We are unable to support personally owned equipment. You should contact your computer manufacturer directly for all problems, diagnostics, and repairs of personally owned computer equipment.

We can help with connecting personally owned equipment with the SCS Computing Environment. For personally owned equipment, we support connecting to printing, wireless, and other computing services on a best-effort basis.

Backups

The data that you create is the lifeblood of your work, therefore it is critical that it is protected from accidental loss either caused by system failure, inadvertent deletion, viruses, or theft of your device. Since different users have different data protection needs, CMU/SCS Computing Facilities provides several different data protection methods:

Standard Data Protection

Recommended for mobile and desktop systems. This system features real-time backup of your data, multiple restore points for data that has changed, and immediate restore of data to any device. This is currently free for SCS users. This service allows for self-service data restores.

Archival Data Protection

Recommended for servers and some desktop systems. This system features nightly backups of your system, archival to tape for long-term, off-site storage, and operator-assisted restores of your data. There is a fee for this service.

AFS File Servers

All CMU/SCS Computing Facilities supported AFS servers are backed up every night to a tape archival data protection system.

Why would you pick one data protection method over another?
These examples might help:

- If you have a laptop that is frequently not on the SCS Wired Network, you should choose Standard Data Protection.
- If you have a desktop that is used for normal office functions (word processing, email, etc.), you should probably choose Standard Data Protection.
- If you have a desktop that has multiple users, or that has SCS business critical data, you should choose Archival Data Protection.
- If you have a server machine, especially one in one of the SCS machine rooms, you should choose Archival Data Protection.

If you have questions about which service to choose, please contact SCS Computing Facilities.

To have backup services installed, a host must be running an SCS Computing Facilities-supported operating system. There is a monthly charge for archival backups.

Important Note: Hosts are not subscribed to either the Standard or Archival Data Protection systems by default. These services must be specifically requested.

Restrictions on Backups

- We may not be able to provide backups for hosts with unusual software or hardware configurations, extremely large disks, or that have large amounts of data that change on a daily basis.
- If your system is connected via wireless or home network connection, only the Standard Data Protection system is supported.

- We do not back up databases, virtual OS images, or specific file types.
- On all platforms, the backup system is not able to back up open files. Therefore, it is important to close long-running programs (e-mail, calendar programs, etc.) before backups run in order to make sure that data files get backed up successfully.

Restores

In order to request a file restore for systems using archival backups, complete your request at https://computing.cs.cmu.edu/backup/forms/restore-request or email help@cs.cmu.edu with the following information:

- The name of the workstation or personal computer.
- 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.
- Insufficient information may delay the restore process.

Before requesting a restore on an AFS volume please check the `OldFiles` directory in your AFS space:

```
/afs/cs.cmu.edu/user/username/OldFiles
```

If the OldFiles directory is not available, please contact the SCS Help Desk for further assistance.

Crashplan data restores can be initiated using the self-service application.

Desktop VM Support

We offer support for a wide range of virtual hosting solutions across all supported platforms. Virtual hosting is available for machines that are subscribed to software support.

VMs are not backed up unless backups have been enabled for that VM. The backup client must be installed on the VM guest and an additional backup support fee will apply. VMs must have a dedicated IP address, and run on machines with a wired ethernet connection to be eligible for archival backups. Crashplan backups can use wireless connections.

For all virtual machine operating systems, SCS Computing Facilities uses the VirtualBox hypervisor client.

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) for SCS owned machines.

SCS Computing Facilities supports most modern versions and configurations of the Microsoft Windows operating system. For more information about Windows support, please visit https://computing.cs.cmu.edu/desktop/support-windows.html.

Software Support

Windows machines built by SCS Computing Facilities are configured with pre-installed software. The baseline software collection is available for distribution from the Andrew Windows software distribution host called Software Center, which is pre-installed on Windows hosts.

For more information about obtaining windows software, please see:
https://www.cmu.edu/computing/software/index.html

Additional software is available from SCS and CMU Windows software distribution servers.

Recommended Hardware

Our recommended hardware configurations for new computer purchases can be found at:
https://computing.cs.cmu.edu/desktop/recom-configs.html

Purchasing

To purchase through SCS Computing Facilities, please use the purchase request form:
https://computing.cs.cmu.edu/business/purchasing.html

Printing

Detailed instructions for printer setup under Windows can be found in our SCS Help Pages:
https://computing.cs.cmu.edu/desktop/printing-windows-public.html

Backups and Restores

Archive backups are available upon request. To have archive backups added to your machine, please send your request to help@cs.cmu.edu asking for backups to be added and include the name of your machine.

For data protection service options please visit https://computing.cs.cmu.edu/backup/.

Ubuntu Linux Support

SCS Computing Facilities software support for Linux hosts involves installing an SCS specific Linux environment that provides the means for remote administration, software distribution, network backups, and other services.

Support for Ubuntu Linux PCs includes network backups (if explicitly requested), and hardware and software support. Users incur a monthly charge for this support. Software support is unavailable for laptops running Linux.

Software Support

The SCS Computing Facilities supported Linux environment is based on the most recent Long Term Support release of the Ubuntu operating system. In general, all Ubuntu packages found in a standard install are present.

The system command `apt-get` can be used to install any needed software that is not currently installed on your computer. We offer some popular software as packages that are tailored for use with the SCS environment:

- Mathematica
- Matlab

These packages are available for installation via the apt-get package management tool. Home directories are located on local disk by default. Local home directories should be placed in /usr0/home or some other partition which is backed up on a regular basis.

If the computer is under backup support, only `/etc` and directories of the form `/usrN` are usually backed up. Directories in other places, such as `/var/mysql`, are not backed up by default.

Recommended Hardware

Our recommended hardware configurations for new computer purchases can be found at:
https://computing.cs.cmu.edu/desktop/recom-configs.html

Purchasing

To purchase, please use the purchase request form:
https://computing.cs.cmu.edu/business/purchasing.html

Printing

Detailed instructions for printer setup under Linux can be found in our SCS Help Pages:
https://computing.cs.cmu.edu/desktop/printing-linux.html

Backups and Restores

Archive backups are available upon request. To have archive backups added to your machine, please send your request to help@cs.cmu.edu asking for backups to be added and include the name of your machine. For data protection service options please visit https://computing.cs.cmu.edu/backup.

Apple Mac Support

SCS Computing Facilities is an authorized Self Service provider for Apple, Inc. Our trained technicians are Apple certified and can perform on-site service repairs for all Apple computer hardware, both in and out of warranty.

Support for Mac computers 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.

Centralized and Self Service Support

As part of the Mac environment, SCS Computing Facilities offers enrollment in a service that allows us to centrally support Mac computers in the SCS Environment. This service is supported by the Casper Suite software from JAMF.

Casper Suite is a centralized maintenance system that makes it simpler to manage software, install printers, and easily perform troubleshooting steps. SCS Mac users can perform these tasks themselves or rely on SCS Computing Facilities Staff to maintain their machines remotely. Casper Suite also makes it easy to run repair and diagnostic tools for both the user and administrators.

For more information about how Casper Suite can be used in the SCS environment, please see https://computing.cs.cmu.edu/desktop/support-mac.html.

Software Support

Mac computers built by SCS Computing Facilities are shipped with preinstalled software. The baseline software collection and additional software packages are available through the Self Service application.

For more information about obtaining Mac software, please see https://computing.cs.cmu.edu/desktop/support-mac.html.

Recommended Hardware

Our recommended Apple product hardware configurations can be found at: https://computing.cs.cmu.edu/desktop/recom-configs.html

Purchasing

To purchase, please use the purchase request form: https://computing.cs.cmu.edu/business/purchasing.html

Printing

SCS Mac computers use the Self Service application to manage printers. The Self Service application is installed as part of the Casper Suite of management software. For more information about Self Service and macOS support, please visit our macOS support page at https://computing.cs.cmu.edu/desktop/support-mac.

Detailed instructions for printer setup for macOS systems can be found on our website at https://computing.cs.cmu.edu/desktop/printing-mac.html.

Backups and Restores

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

Network & Email Security

Network Security

The SCS Network

Due to the nature of research done on our network, there is no firewall between the SCS network and the Internet. Hosts on our network are therefore constantly scanned for security vulnerabilities by would-be intruders, and there are numerous break-ins to SCS hosts each year. Almost all these break-ins are preventable, and most are due to either weak passwords (often cracked via brute-force SSH attacks) or poorly configured or unpatched web applications (Wikis, phpMyAdmin, etc).

To Protect Yourself and Your Computers

- Always use strong passwords, including for temporary accounts and accounts you've created in the process of installing a software package. This can't be emphasized enough.
- Securely configure any software you install. This includes using strong passwords for services exposed to the network and restricting access to sensitive services, such as a web application's administrative console. If you are installing a network-aware software package, you should never trust its default configuration to be secure.
- Keep software you install, particularly software exposed to the network, up to date with patches. If you do not keep your software up to date, there is a good chance that the host running the software on will eventually be compromised.
- Do not send sensitive data, such as passwords, unencrypted over the network.
- Do not reuse passwords.

If you believe your computer has been compromised, contact the SCS Help Desk as soon as possible by submitting a ticket via https://computing.cs.cmu.edu/gethelp or sending an email to help@cs.cmu.edu. Even if your computer is not supported by SCS Computing Facilities, report any intrusion.

Conclusion

Thank you for taking the time to read our introduction to SCS Computing.

While we hope that this document has provided a brief but helpful introduction to computing at the School of Computer Science, we also understand that we have a large and complicated computing environment, and a condensed guide will not cover every single aspect of our environment.

If you have any questions about services or information contained in this document, please let us know; your feedback helps us ensure that all the material presented here is complete and easy to understand. For a deeper dive into any of the topics covered in our introduction guide, news, critical alerts, knowledge articles, helpful links, and request forms, we encourage you to visit our website at https://computing.cs.cmu.edu.

Welcome to the School of Computer Science at Carnegie Mellon University!