Carnegie Mellon University
School of Computer Science
Computing Facilities

Introduction to SCS Computing

Gates Hillman Complex 4203
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/.

Table of Contents

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

We support SCS-affiliated persons and SCS-owned computing equipment, and we are happy to act as liaisons to help address any issues you may have that involve computing outside of SCS.

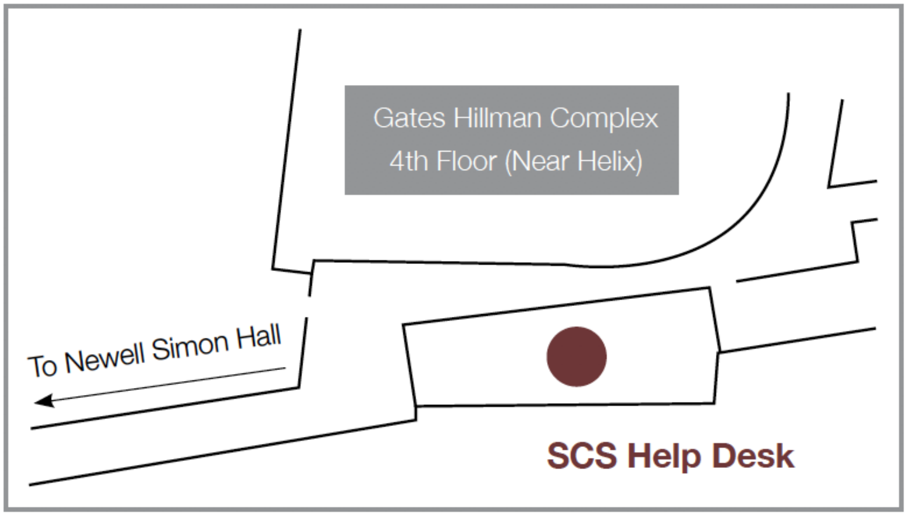
The SCS Help Desk

The SCS Help Desk is the first place to go for support; you are welcome to send us an email, give us a call, or schedule an in-person appointment.

Help Desk Hours

9:00 am to 5:00 pm
Monday through Friday

SCS Help Desk Location



Gates Hillman Complex
Room 4203
Gates Hillman Complex, 4th Floor
Near Helix

We strongly encourage you to contact us to schedule your visit to our help desk.

For Technical Support

- Submit a request through our website via https://computing.cs.cmu.edu/gethelp.
- Contact our help desk at 412-268-4231.
- 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.

The Computing Website

The SCS Computing website is 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 SCS password using our Instance Manager
- Publish a web page
- Sign up for support (hardware, software, backup, network access and more)
- Recommended Hardware Configurations

Shared Computing Resources

Help keep our computing environment safe and working well:

- Use SCS equipment for SCS/CMU work.
- Keep your account and its password private and respect the privacy of others.
- Make sure that your computer is secure by applying updates and security patches.
- Notify SCS Computing Facilities in advance and review our website's section on network 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.
- Consider printer output private.

To learn more about security and best practices, visit the Information Security Office website.

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

SCS Computing 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 is supported by SCS Computing Facilities. For more information about end-user computing, visit the desktop computing section of our website.

Privately-Owned Computer Resources

You are welcome to use privately-owned (non-CMU) computers, mobile devices, and other equipment within the SCS environment. Private 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.

For more about connecting privately owned computers, mobile devices, and other equipment to the wireless network, please visit the campus Computing Services website.

We offer limited support for privately-owned computers. Although not all services are available for private computing equipment, some private devices are permitted to use the SCS network and benefit from backup services such as Crashplan data protection.

Shared Resources

Our community has access to campus-wide computing, storage and productivity resources, such as:

- Email
- Google Apps, including Google Drive storage
- Box
- Virtual Andrew
- Microsoft Office 365

We also have SCS-specific computing resources, such our remotely accessible general purpose Linux environment.

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 website 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 the section called, "Changing a Kerberos Instance Password".
Andrew	This password is used for SSO across CMU websites and primarily to authenticate to Windows systems, but is used for a number of other services including: • Workday • Zoom • VPN • Gmail • Resource reservations

	• Printing to SCS printers • Computer labs

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 resource or system. You should never re-use passwords. To learn more about password management, visit ISO's website.

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). To learn more, visit the ISO website.

Changing Passwords

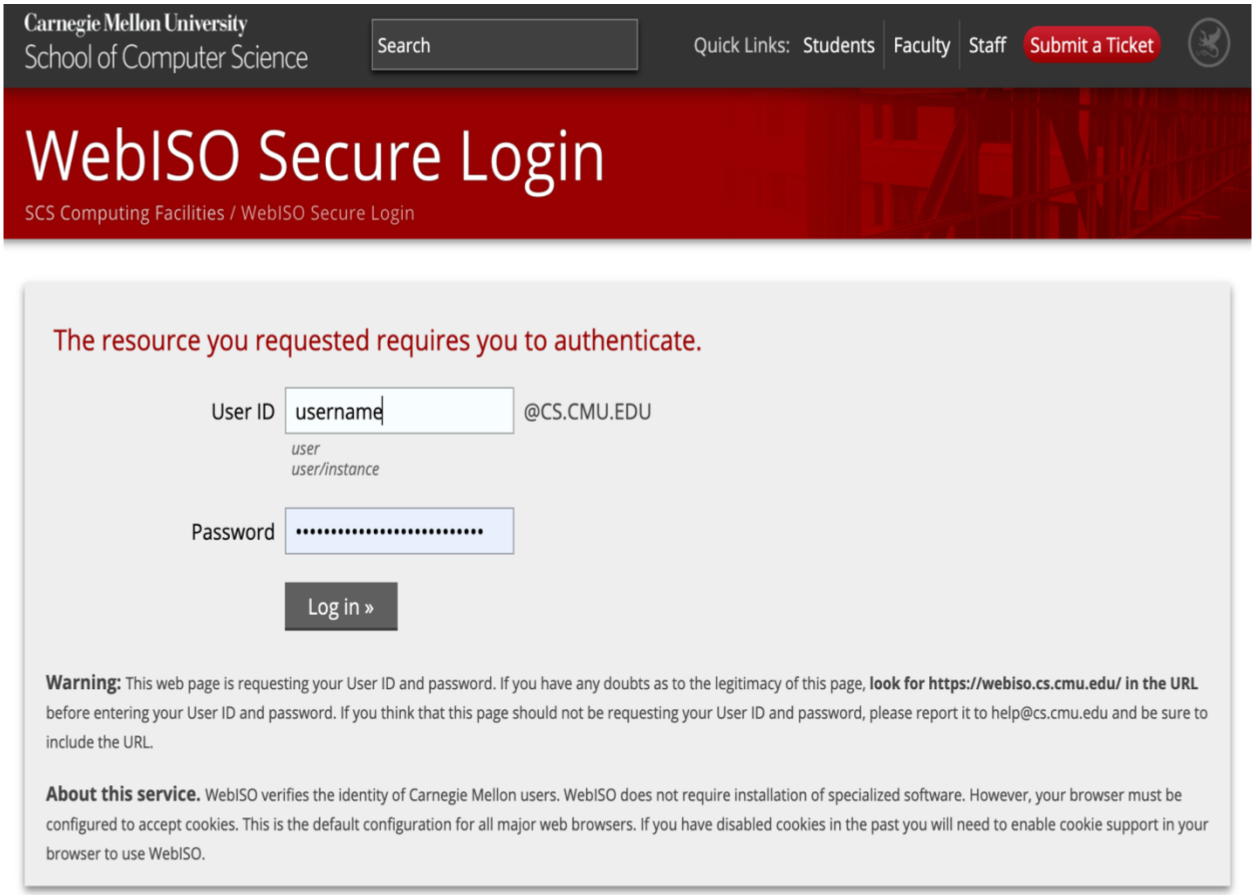
If you suspect that your account has been compromised, it is critical that you change your password immediately!

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/instance-manager

To use the SCS Kerberos Instance Manager, you will need to authenticate via WebISO (see Figure 1):


Carnegie Mellon University
School of Computer Science
Search
Quick Links: Students | Faculty | Staff
Submit a Ticket
WebISO Secure Login
SCS Computing Facilities / WebISO Secure Login
Log in »

The resource you requested requires you to authenticate.

User ID: username @CS.CMU.EDU

user
user/instance

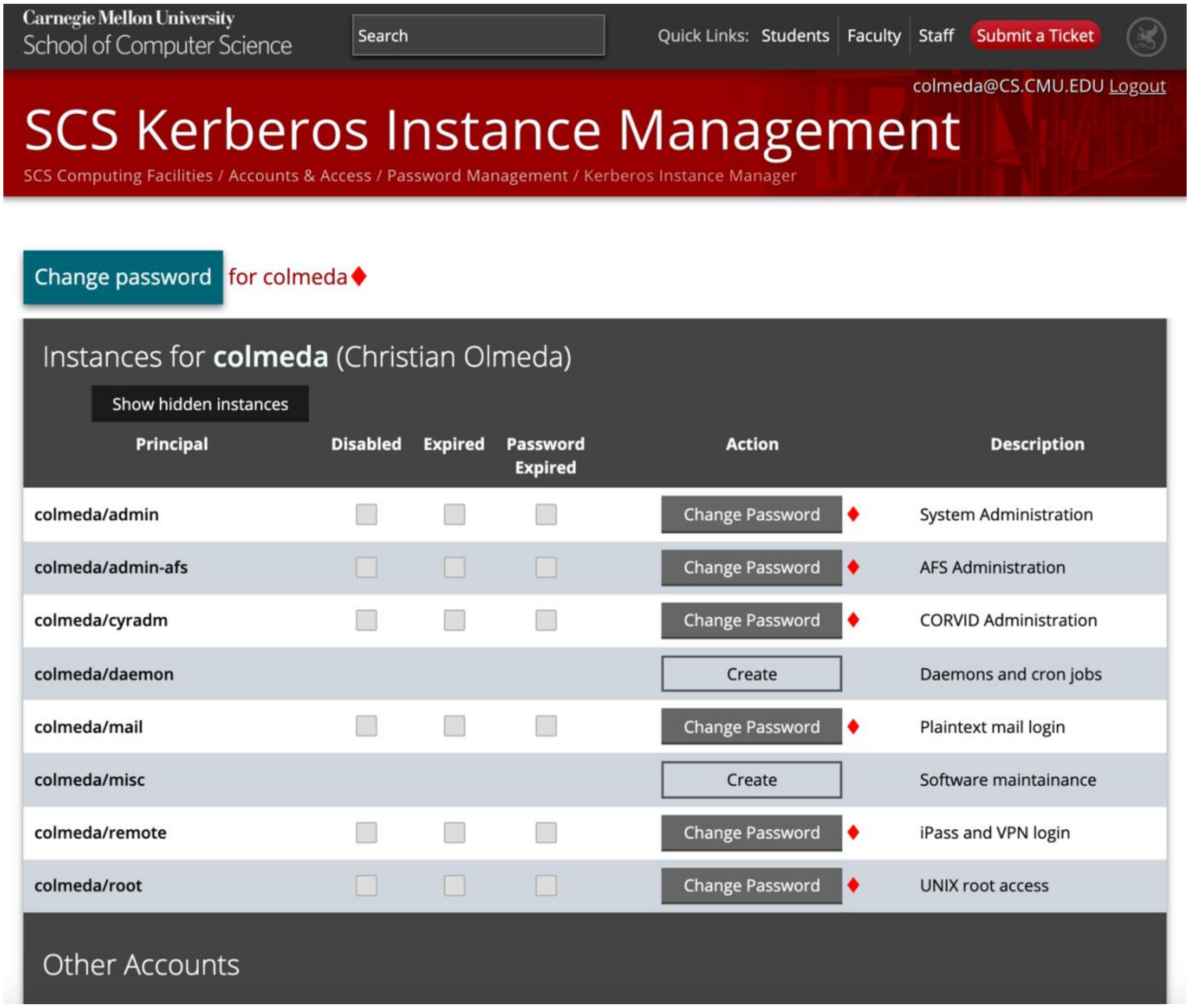
Password: ••••••••••••••••••••••••••

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 and be sure to include the URL.

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.

Figure 1: Authenticating with SCS WebISO

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


Carnegie Mellon University
School of Computer Science
Search
Quick Links: Students
Faculty
Staff
Submit a Ticket
colmeda@CS.CMU.EDU Logout

SCS Kerberos Instance Management

SCS Computing Facilities / Accounts & Access / Password Management / Kerberos Instance Manager

Change password for colmeda ♦

Instances for **colmeda** (Christian Olmeda)

Show hidden instances

Principal	Disabled	Expired	Password Expired	Action	Description
colmeda/admin	□	□	□	Change Password ♦	System Administration
colmeda/admin-afs	□	□	□	Change Password ♦	AFS Administration
colmeda/cyradm	□	□	□	Change Password ♦	CORVID Administration
colmeda/daemon				Create	Daemons and cron jobs
colmeda/mail	□	□	□	Change Password ♦	Plaintext mail login
colmeda/misc				Create	Software maintainance
colmeda/remote	□	□	□	Change Password ♦	iPass and VPN login
colmeda/root	□	□	□	Change Password ♦	UNIX root access

Other Accounts

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

Please Note: You may see Password Instances that you do not currently use, it is safe to ignore these.

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.

If you are having trouble changing or have forgotten your password, 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.

We always require you to provide valid ID (in person or via remote video meeting), such as CMU ID, valid state ID, driver’s license, or valid passport for verification.

Please Note: The SCS Help Desk cannot reset /admin or /root passwords but can assist with coordinating a password reset for these accounts. Contact us to schedule an appointment with a senior engineer to reset these kinds of passwords.

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 managed Linux systems or VM's in addition to select resources such as the SCS AFS cell.
- 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

In order to log in to an SCS Linux computer or VM, your SCS account must be added to the computer or VM. You can submit a ticket to request access to the computer. You will need to provide the hostname or asset number of the computer. If you have received a graduate student machine from your department, you should already have an account on the computer.

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

Logging on to macOS

To log in to an SCS managed computer running macOS, you will need a local user account (not centrally managed). Local user accounts on Mac computers are added when the system is initially configured by SCS Computing Facilities. Your initial account password will be provided to you.

Newly deployed macs will provide the user with a first-time setup where a password can be set. In other scenarios, your account may already be provisioned for you and an initial password provided.

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 by logging into mail.google.com.

Supported Standalone Clients

We support a wide range of clients to check your Andrew mail. Please note that for IMAP email clients, the mailbox must have IMAP functionality enabled.

Windows

- Thunderbird
- Outlook

macOS

- Thunderbird
- Outlook
- mail.app

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.

Attachments and Trojans

To reduce the likelihood of being infected by a virus or a Trojan via an email message, do not open an attachment unless you are expecting the attachment from the sender.

Do not run or open email attachments unless:

- 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 often 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 CMU ISO.

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 normally takes the form of email messages that demand personal information. They create a sense of urgency by threatening that a service or opportunity is about to expire. If you receive an alert threatening fines or loss of access, we recommend reaching out to the service provider through normal channels as listed on their website. Do not rely on any contact information or link contained in the suspicious email to contact them.

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.

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

You can report phishing attempts to the CMU Information Security Office through the PhishAlarm button in Google Mail or email (iso-ir@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 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.

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.

Spam and Virus Detection and Filtering

Server-Side Tagging and Filtering

All incoming email is scanned for spam content and viruses. 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.

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.

Printing

SCS Computing Facilities provides access to high-capacity public printers in most SCS buildings on campus. Off campus printing support is limited to self-maintained desktop and private printers. We support 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 problems with public printers, 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.

Please note: 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.

Network

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

- Only use IP addresses that have been assigned to your host.
- On the SCS wired network, DHCP addresses are persistent and will not change unexpectedly in the SCS environment.
- Do not run unauthorized DHCP servers on public network segments that are managed by the university.
- 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.

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 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. 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 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.

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. You can also visit Computing Services' network status monitoring page at https://cmu.service-now.com/status?id=cmu_service_status&service=fee0bd0c135cea00f4fe7b104244b0db.

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.

Eduroam

The Eduroam service provides free wireless access at education and research institutions world-wide. Using your Carnegie Mellon Andrew email address and password you can connect to the wireless network at a participating institution. Those visiting Carnegie Mellon from a member institution can access our wireless Eduroam network using their university email address and password. Eduroam uses secure encryption and authentication standards, which make it significantly safer than commercial Wi-Fi hotspots. For more information, visit https://www.cmu.edu/computing/services/endpoint/network-access/wireless/how-to/eduroam.html.

Computing Services Open Wireless

Campus offers a wireless network that requires registration to join. This open wireless network is named CMU-DEVICE. CMU-DEVICE is a dedicated wireless network for smart devices that typically do not support web browsers or log in (authentication) capabilities. This network is not for smartphones, tablets, laptop, or desktop computers.

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 visit the Computing Services Event Manager page..

Note: People who are returning to campus after a long absence may need to have their computing devices "forget" the CMU-secure wireless network and then re-join it to restore network access.

Connecting Hosts to the SCS Network

To successfully connect to the SCS wired network, you must register your device ahead of time. You will need to provide the following information to complete the registration process:

- **Device type**
- **Asset tag number**
- **Serial number**
- **Location**
- **Hardware address**
- **Contact Information**

Note: When registering privately-owned equipment which does not belong to CMU for a network connection, you do not need to provide an asset tag number.

Use the Equipment Registration form for all new registrations and updates of SCS network-connected devices.

In special cases may we give out an IP address without knowing the host's hardware address.

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 syntax/identifying convention:

R00A00-000-00

You can submit your request via our website at https://computing.cs.cmu.edu/gethelp or follow the instructions to activate the port via CANDO.

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 privately-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 or reserved 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, review the CMU Computing Services usage guidelines.

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.

VPN

The Cisco AnyConnect VPN (Virtual Private Networking) software allows a computer on another network to appear that it has a 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.

VPN users will be prompted to approve their login through Two Factor Authentication (2FA) when using the Campus or Full VPN service options. CMU uses DUO for 2FA.

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.

Network & Email Security

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 Information Security Office via iso-ir@andrew.cmu.edu or visit their website for more information on compromised computers.

AFS

AFS is a distributed file system providing a client and server architecture. AFS is used to share and store data for classes, projects, and users. Your SCS user or project website is likely served from AFS. AFS offers:

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

Note: The OpenAFS client software is no longer supported on macOS or Windows. We recommend you access AFS using an SFTP/SCP client instead. SCS Computing Facilities is not authorized to distribute or support the Auristor AFS client.

You can read more about AFS on Windows at https://computing.cs.cmu.edu/help-support/afs-windows and macOS https://computing.cs.cmu.edu/help-support/afs-macos.

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

AFS 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. Web content should be located in an exclusive subdirectory of a volume. The permissions on this directory should be configured to provide the necessary AFS access list privileges 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. You can find more information on ISO's guidelines for data classification.

Linking Your Content to the Web Servers

If your content does not appear at the following URL: 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 contact the SCS Help Desk.

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

Computers covered by hardware support are entitled to the following:

- Hardware, troubleshooting, & diagnostics
- Out-of-warranty component replacement of failed hardware (cost of parts 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. If you are moving equipment to a different building, please inform us so we can assign your computer's new IP address on the appropriate building subnet. Failure to do so may result in a temporary loss of network connectivity.

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 updating information in the CASE portal, 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 privately owned equipment that does not belong to CMU. You should contact your computer manufacturer directly for all problems, diagnostics, and repairs of privately owned computer equipment.

We can help with connecting privately owned equipment with the SCS Computing Environment. We also support connecting to printing, wireless, and other computing resources 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

Our standard data protection tool is Crashplan. This cloud backup solution is recommended for mobile and desktop systems being used by a single individual. 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

For archival backups, we use TiBS. This backup service is 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 monthly 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 single user desktop that is used for normal office functions (word processing, email, etc.), you should 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 us.

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 Archival 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.
- 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 private (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 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

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 may 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 and do not incur additional fees.

Recommended Hardware

You can find our updated computer hardware recommendations on our website. You can also purchase your computing equipment through SCS Computing Facilities technical procurement services.

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.

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.

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.

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/

Conclusion

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

If you have any questions about services or information contained in this document, please let us know; your feedback helps us ensure that all of 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!