What is Safe•Connect and why is it being used?

Safe•Connect is part of TAMUK's effort to help keep computers on its network as free as possible from viruses, spyware, and operating system security holes. Machines protected in this way generally perform much better and require much less downtime due to damage caused by malicious software. Also, the Safe•Connect Policy Key can help to ensure that the average user has the fastest possible browsing experience while connected to the TAMUK network. It does this by ensuring that communication from malicious software does not flood TAMUK's internet connection, resulting in slower connections for legitimate users or by restricting certain applications that would otherwise consume an unfairly large share of the total available bandwidth, again resulting in a slower connection for the majority of users.

Safe•Connect will require users to authenticate with a username and password before allowing them to access the Texas A&M University Kingsville wireless network. When you authenticate, the system records which network address you were assigned and how long you used it. Your username and password are your keys to the network; don't share them with anyone. You are responsible for all acts performed using your account, including copyright violations. If you are concerned that someone may be able to use your account, change your password immediately.

What do I need to do?

First and foremost, you must know your TAMUK userid (such as "KUABC000") and password. Your password should be kept secret. Do not write it down and do not share it with anyone.
Secondly, if your device is running a Microsoft Windows or Macintosh OS X operating system you will also need to:

- have an updated anti-virus application,
- have updated system patches for Microsoft Operating Systems
- have the Safe•Connect policy key installed and running

It is critical that you have only one anti-virus program installed on your computer. Having multiple antivirus programs installed may result in false readings and prevent you from accessing network services.

How do I get and install the Safe•Connect Policy Key?

If your computer is NOT running Microsoft Windows or Macintosh OS X then you do NOT need to download and install the policy key application.

On Microsoft Windows

- Open a web browser. You will be prompted to download the policy key application.
- If you are NOT prompted to download the policy key application then type a website you don't normally go to – such as IBM.com. This should get you where you need to be.
- When prompted to either run or save the file, click the "Run" button.
- After the installer downloads it will run.
- Follow the prompts presented by the installer to proceed through the installation process. You can expect to click an "Install" button to start the installation process and a "Finish" button when the installation has completed successfully.
- The PolicyKey.exe application will be running as a background process and will start automatically each time you start up your computer.

On Macintosh OS X (10.6 & above)

- Open a web browser. You will be prompted to download the application.
- Save the Policy Key software to the desktop.
- If the install process does not begin automatically, double click the ZIP file that was downloaded and the installer should be placed on the desktop.
- Double click the installer PKG file to begin the installation process.
- Click "Continue" to advance.
- On the next screen of the installer, click "Install" to continue. You may be asked to provide your Mac OS X administrator username and password to continue.
- Once the installation is complete you should get the following "Install Succeeded" message. Click "Close" to finish the installation.

On Linux and Other WiFi Compatible Devices

Linux machines, iPhones, and iPod Touches do not yet have a Safe•Connect policy key, but will still be required to authenticate. Nintendo Wii, Microsoft XBox, and Sony PS3 systems should be automatically recognized by Safe•Connect and will not be required to authenticate. If your device can connect to WiFi and you are still having difficulty connecting, please contact the iTech Help Desk (x4357) for assistance.

Do I have to use the Safe•Connect Policy Key?

Yes. All Microsoft Windows PCs and Macintosh computers are required to use the Safe•Connect Policy Key to help ensure a safe computing environment for all users.

You can uninstall Safe•Connect Policy Key at any time; however within minutes you will then be unable to access the Internet through the campus network. You will be required to reinstall the Policy Key as if you are a new user to gain Internet access.

How do I authenticate and how often do I have to authenticate?

The authentication screen for Safe•Connect should pop up when you try to surf the web. If it does not then then type in a website you don’t normally go to – such as IBM.com and press enter. This should get you where you need to be. Authentication is required once every 7 days or when the IP address on your computer changes, whichever comes first.

Are guests required to install the Safe•Connect Policy Key?

No, an internet only guest network has been created for campus visitors. Look for javNET – Guest in your available WiFi connections. You will need to have a personal email account (not a TAMUK.edu account) in order to connect. Note that Guest Network access is good for 12 hours at a time. Please do not try and connect to Guest Wireless if you are a current Student, Faculty or Staff member.

How do I know the Safe•Connect Policy Key is running?

On Windows machines, you can right-click any blank space on the task bar at the bottom of your screen and select the option “Task Manager”. When the Windows Task Manager appears, click the “Processes” tab and then click on the "Show processes from all users" button in the lower left. Look for the processes “SCClient.exe” and "SCManager.sys," as both should be present.

Mac OS users can open the Activity Monitor located in the Utilities folder. From the Activity Monitor, look for the processes "SafeConnect" and "SCManagerD," both should be present. If you have only recently installed the Macintosh Policy Key, both processes may be called SafeConnect.
If these small applications are uninstalled or disabled, the system will disallow network access until the end user re-authenticates and reinstalls SafeConnect.

What are the things Safe•Connect checks for?

The Safe•Connect Policy Key continuously validates that your system meets minimum security requirements as per the University's acceptable use policy.

- **Authentication:** Required once every 7 days or whenever the IP address on your computer or mobile device changes.
- **Policy Key:** If using Windows or Mac and you do not have policy key installed, you will not be able to access the wireless network.
- **Windows Operating System – Current:** Windows XP is no longer supported as Microsoft has stop supporting XP. Also note the Windows 7 will no longer be supported as of January 2020.
- **Windows Operating System - Updates:** Windows update patches are required and you are advised to set the automatic updates to "ON" for your Windows based devices.
- **Anti-Virus Software Installed and Running:** If anti-virus software is not detected as being installed, then you will be quarantined until you install an AV package.
- **Anti-Virus Definitions Up-to-Date:** If anti-virus software is out-of-date, then you will be quarantined until you update the virus definitions for your AV Software.
- **Peer-to-Peer Software:** If P2P software is detected as running on your device, you will be quarantined until you remove the P2P Software from your device.
- **Unsanctioned Wireless Device:** The use of personally owned routers, switches, hubs and other network gear is prohibited on the TAMUK Network. You will not be able to connect if one of these devices is detected.

Texas A&M Kingsville provides students and faculty with a free version of McAfee Antivirus software for use on personally owned PCs.
McAfee Antivirus can be downloaded here:

http://www.tamuk.edu/finance/itech/services/software.html

Which anti-virus software can I use?

Safe•Connect recognizes most anti-virus programs including:

- Authentium
- Avast AV
- AVG
- AVG for MAC
- AVGuard
- Avira for MAC
- BitDefender
- ClamXAV for MAC
- Comodo

- Comodo for MAC
- EZ Antivirus
- ESET for MAC
- Faronics
- F-Secure
- Fortinet
- GData
- iAntivirus for MAC
- Immunet
- Intego VirusBarrier
- Kaspersky
- LanDesk
- LightSpeed
- LoLo
- MacKeeper for MAC
- McAfee
- McAfee 45
- McAfee NA
- Microsoft OneCare
- Microsoft Security Essentials
- NOD32
- Norton for Macintosh
- Panda
- Panda for MAC
- PC Tools
- Secure IT
- Sophos
- Sophos for MAC
- SpySweeper AV
- Symantec Personal
- Symantec Enterprise
- TrendMicro
- TrendMicro for MAC
- Vipre Antivirus
- Webroot
- ZoneAlarm AV

What if my system is not up-to-date?

If your system has been determined not to be up-to-date, a web browser will open and you will be warned of non-compliance. If you require assistance in updating your computer, please call the Help Desk at x4357 or take your device to iTech Help Desk in the Library Commons where you will be assisted.

What about my privacy?

Your privacy is very important to us. The Safe•Connect Policy Key checks only for the following:

- DNS Server settings

- DHCP Settings
- MAC and IP Address of default gateway
- IP Address
- Windows Update settings
- Whether or not a valid anti-virus solution is installed
- Whether or not anti-virus definitions are up-to-date
- Whether or not an anti-virus program is running
- Whether or not a P2P file sharing application is running

The Safe Connect Policy can easily be removed at any time and is non-intrusive. It is unable to look at any content on a user's computer and its only purpose is to check for the processes we have configured to help ensure a secure connection to the internet.

How do I uninstall the Safe•Connect Policy Key?

- **On Macintosh**
  - Open the Applications folder and locate "SafeConnect.app". Right-click (or Control-Click) on the SafeConnect.app and select "Show Package Contents." Open up the Contents folder, and you'll see the "SCUninstall.app". Run this uninstaller.
- **On Windows 7**
  - Open the Control Panel and choose Add and Remove Programs. Find SafeConnect in the list and choose Uninstall.
- **On Windows 10**
  - Open the Control Panel and choose Add and Remove Programs. Find SafeConnect in the list and choose Uninstall.

Why are P2P file sharing applications not allowed?

Texas A&M is required to ensure compliance with various federal and state laws in regard to downloads and uploads of copyrighted material. Therefore, computers connected to the Texas A&M University networks are continuously monitored to see whether P2P file sharing applications are installed and/or running.

I am unable to install the Policy Key on Mac OS X 10.3.9

The Safe•Connect Policy Key cannot be installed on computers running OS X 10.5.8 or below as this platform is no longer supported by Apple.

I am unable to install the Policy Key on Windows XP

The Safe•Connect Policy Key cannot be installed on computers running Win XP as this platform is no longer supported by Microsoft.

I can browse for some time and then I am asked to authenticate later.

Safe•Connect may not catch your computer or mobile device immediately after turning it on. Rather, it may catch your computer or device and ask for authentication after some traffic has passed across the network. If you find yourself unable to continue browsing or using other web services on your mobile device, simply open a browser and authenticate.

Additionally, in most cases where Safe Connect has determined that your PC does meet the minimum requirements it will grant you a “grace” period in order to remediate the issue. If you have not resolved the issue within the “grace” period – you will be disconnected from the internet.

Also note, the date and time **MUST** be correct on your computer. Many issues can be resolved by making sure that both are correct and stay correct.

Windows 7 Problems

On Windows 7, User Account Control (UAC) may have prevented the Policy Key from installing correctly. Either or both of these steps may be necessary to install the Policy Key with elevated privileges:

- Uninstall and Reinstall as Administrator o Open the folder "C:\Program Files\SafeConnect" or "C:\Program
  Files(x86)\Safeconnect." o Right-click on "uninstall.exe" and choose "Run as Administrator."
  - Then right-click on the Policy Key installer, "ServiceInstaller.exe", and choose "Run as Administrator." o If this doesn't work, try the steps below.
- Uninstall and Reinstall with UAC turned off.
  - Turn off UAC
    1. Click the Start button.
    2. Type "UAC" in the search box and hit [Enter].
    3. Move the slider all the way to the bottom.
    4. Reboot the computer.
  - Uninstall and reinstall the Policy Key in the usual way. o Re-enable UAC as above, moving the slider back to the previous position.

The UAC control panel can also be found by going to Control Panels > User Accounts > Change User Account Control Settings. The Default setting is one notch lower than Always Notify.

Typical issues that may occur and troubleshooting

I cannot connect to the internet on my Apple Computer or Phone

The legacy WiFi (javNET) is unable to support Apple devices. Both of the other javNET platforms (javNET2 and javNET3) DO support Apple devices. The campus is continually updating campus Wifi to phase out these legacy platforms but there are still a few areas where javNET is still installed.

Is the Policy Key running?

- Press Control-Alt-Delete and start the Task Manager
- Click on the "Processes" tab.
- Check the box "Show processes from all users" at the bottom left.
- Click on the "Image Name" column heading to sort.
- Look for "SCClient.exe" and "scManager.sys" - Both should be present.

A personal firewall is blocking the Policy Key

If the policy key is running (see above), a personal firewall may be interfering with it. You may have a firewall installed as part of your antivirus application, particularly likely if it's a "Total Internet Security Suite," or you may have the built-in Windows firewall enabled. Some firewalls will block the Policy Key without notifying you. If you are notified, choose "Allow" for both "SCClient.exe" and "scManager.sys."

We do not recommend you disable the firewall.

Instead, add the Policy Key to the firewall's *exception list.* Both "SCClient.exe" and "scManager.sys" should be allowed to communicate on all ports.

Some firewall programs may also require that the IP addresses 198.31.193.211 and 127.0.0.1 be added as *trusted hosts.*

Here are instructions for the built-in Windows Firewall. Other firewalls will have different steps, but the idea is the same.

Open the Windows Firewall Control Panel.

- Click on "Allow a program or feature through Windows Firewall"
- If one or both of the Policy Key files above are missing from the list, click on the "Change Settings" button.
- Next click on the "Allow another program..." button.
    - Again, if the Policy Key files don't appear in the list, click the "Browse" button.
    - Navigate to either the "C:\Program Files\SafeConnect" or "C:\Program Files(x86)|SafeConnect" folders, as appropriate.
    - Select the "SCClient.exe" file and click "Open." o Click the Add button.
- Repeat the "Allow another program" procedure for "scManager.sys"
- Click the Public checkboxes for each of these programs, too (Home/Work should already be checked).
- Click OK to save your changes.

Once you've done the above steps, restart your computer.

This typically will only come up when the Policy Key is first installed. But the Policy Key periodically updates itself to a newer version, and sometimes a firewall will block the Policy Key again. It's worth checking your firewall settings if you continue being prompted to reinstall the Policy Key.

If no personal firewall is found, or if the above steps do not work, it's possible that remnants of a formerly installed security suite are still running, but hidden from view. If your computer has ever had a Symantec (Norton), Trend Micro, or McAfee product installed on it, there is a chance some bits are left behind, even if it no longer shows up in Add and Remove Programs. For assistance in removing these remnants and installing the Policy Key, please contact the iTech Help Desk (x4357).

An Antivirus application is blocking the Policy Key

Have you installed more than one antivirus application?

Multiple antivirus programs compete for system resources, slowing your system down, and interfering with each other. We highly recommend you remove all but one antivirus application from your computer.

Use the Add and Remove Programs control panel to see what applications may be removed. Look for those from McAfee, Symantec or Norton, or Trend Micro. Sometimes Symantec or another antivirus application can be installed *on a trial basis* when installing the Acrobat Reader, or Java, and it's easy to miss that "extra gift" when you're updating applications.

Check your remaining antivirus program's Quarantine folder for Policy Key files, or the Policy Key installer. Look for "scManager.sys," "SCClient.exe," scManager.dll," "SCClient.dll," "SCUpdate.sys," or "ServiceInstaller.exe." If any of these are found in your quarantine, add them to the antivirus allow list and restart your computer.

The Policy Key isn't set to run at startup

Press Control-Alt-Delete and open the Windows Task Manager. Click on the Processes tab. If you don't see SCClient.exe listed in the running processes, it may not be starting up with Windows.

Click on "Start > All Programs > Startup" and look for SafeConnect, with a red, white, and black shield icon. If you don't see it, here's how you add it:

Click on “start > All Programs”. Right-click on Startup, and choose “Open All Users”. If this option is not available, choose “Open”.

Open the Policy Key’s install folder. On most Windows machines, look for “\Program Files\SafeConnect”. On 64-bit Operating Systems, look for “\Program Files (x86)\SafeConnect”. Right-click on SCClient.exe and choose “Create Shortcut”.

Drag the new file “Shortcut to SCClient.exe” to the Startup folder you just opened. Then close the Startup folder.

You can test the new configuration by logging off of Windows and logging in again. After you log in, look for SCClient.exe in the Task Manager.

How can the Policy Key get left out of the Startup folder? It's possible that an anti-spyware application may have removed the shortcut after the Policy Key was first installed. If so, the next time you run an anti-spyware scan, you should be able to choose not to have the SCClient shortcut removed.

Issue - Mac OS X is Repeatedly Asking for Policy Key Installation

You need a local password to properly install the Policy Key

You won't be able to install the Policy Key on a Mac without administrator privileges. When launching the Safe•Connect installer, you will be prompted for the username and password of an administrator's account. Even this account can fail to install the Policy Key if it has *no* password. Set a password for the account and try installing the Policy Key again.

Intego VirusBarrier interfering with Safe•Connect?

VirusBarrier is an incredibly comprehensive security application for the Macintosh. Unfortunately, that also makes it a bit complex. We've identified two ways in which VirusBarrier can interfere with Safe•Connect

You must configure VirusBarrier after you install it.

You need to tell VirusBarrier that Safe•Connect is a *trusted host.*

When VirusBarrier is downloaded and first installed, you've only done half the task. Click on the "castle" icon on the menu bar over by the clock. Slide your mouse down over "VirusBarrier X6" and a menu will appear. Select "Open VirusBarrier X6" at the bottom of this menu. Once VirusBarrier opens up, it will ask you several questions on how you want the program to operate on your computer.

Follow this process through to the end, and VirusBarrier will be configured and ready to run. We suggest at least one additional step:

While you have VirusBarrier open, click on the "Antivandal" button.

Click on the "Blocked Addresses" tab and look for 132.162.199.162 or 198.31.193.211 in the 'Intruder' list. If you find either of these addresses, right-click on that address and choose "Switch to Trusted Addresses" list instead. These addresses are used by the SafeConnect system, and if you block them, you can't authenticate.

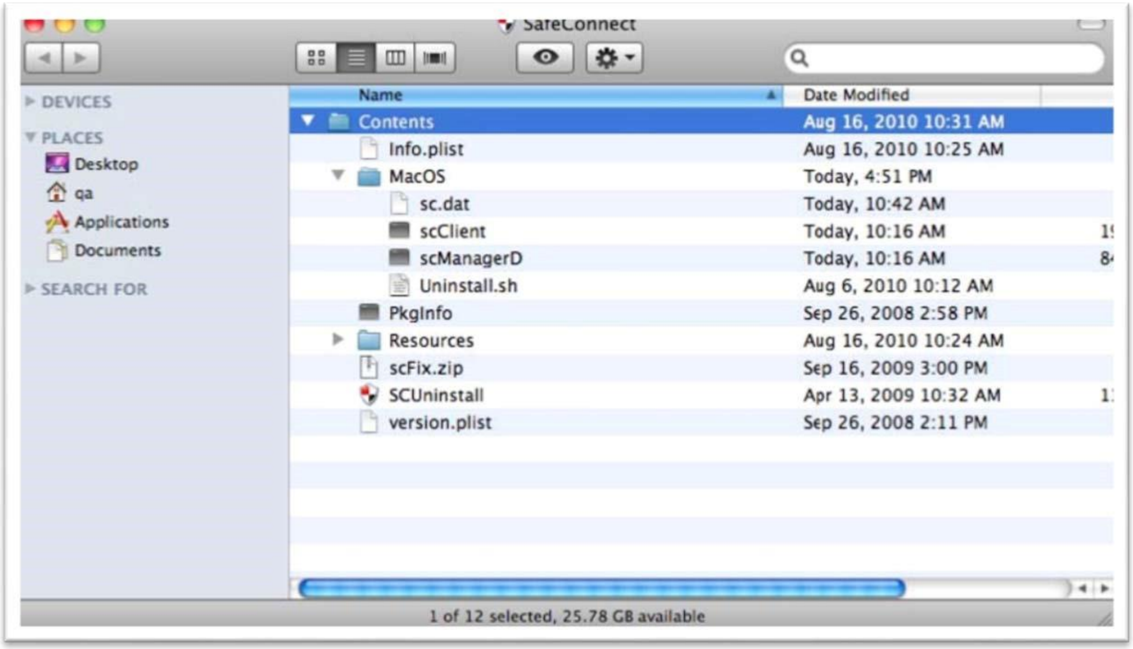
Then, let's make sure both these addresses are in the Trusted Hosts list.

- Click on the "Trusted Addresses" tab.
- click on the plus sign in the lower left.
    - In the Trusted Addresses Editor box that appears, o Enter the address 198.31.193.211 in the Host: box o Duration will default to 'infinity' and Permanent, which is good.
    - Add a note that this is the SafeConnect box.
    - Click OK.
- Do the same for 132.162.199.162, if you haven't done so already.

Are all the pieces of the Policy Key installed correctly?

From the Finder, open Applications, and look for SafeConnect. If SafeConnect is missing, look for PolicyKey.If SafeConnect is present, right-click (or Control-click) on it and choose "Show Package Contents." Then open the Contents and MacOS folders. Inside MacOS, please note which of the following files are present:

- sc.dat
- scClient
- scManagerD
- uninstall.sh

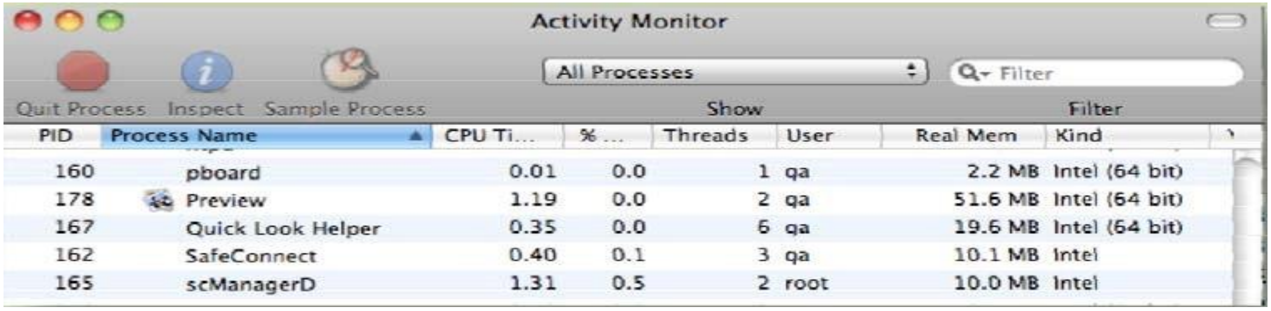


Name	Date Modified
▼ Contents	Aug 16, 2010 10:31 AM
Info.plist	Aug 16, 2010 10:25 AM
▼ MacOS	Today, 4:51 PM
sc.dat	Today, 10:42 AM
scClient	Today, 10:16 AM
scManagerD	Today, 10:16 AM
Uninstall.sh	Aug 6, 2010 10:12 AM
PkgInfo	Sep 26, 2008 2:58 PM
▶ Resources	Aug 16, 2010 10:24 AM
scFix.zip	Sep 16, 2009 3:00 PM
SCUninstall	Apr 13, 2009 10:32 AM
version.plist	Sep 26, 2008 2:11 PM

1 of 12 selected, 25.78 GB available

Is the Policy Key running?

Next, open Finder > Applications > Utilities > *Activity Monitor* and choose "Show All Processes" at the top right. You should see two processes named *SafeConnect* and *scManagerD.*

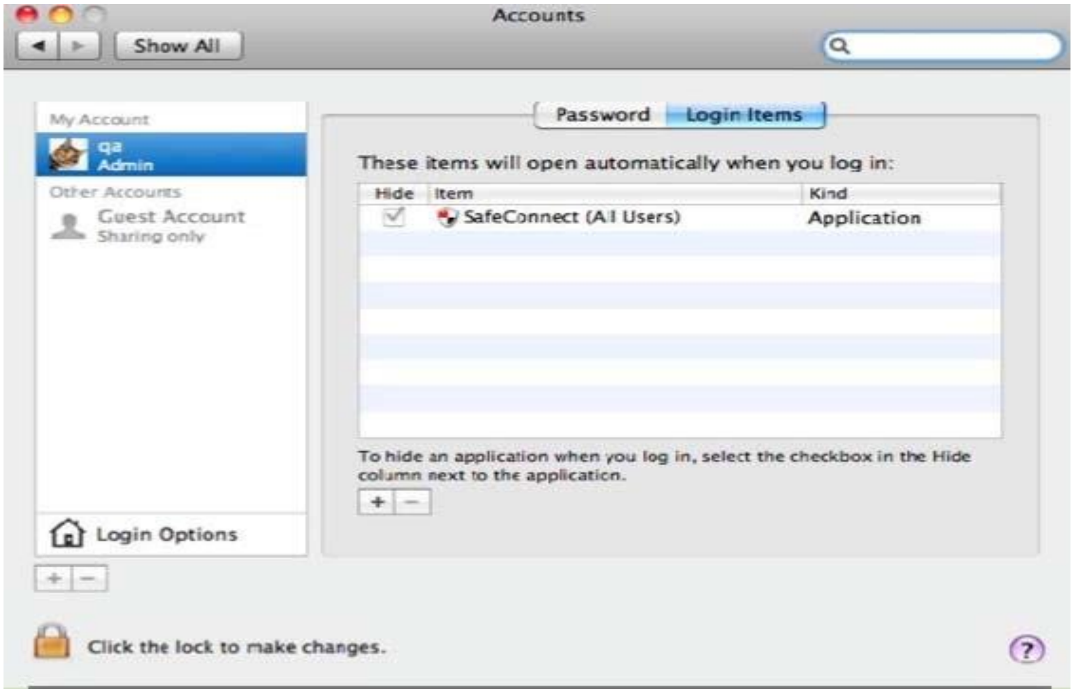


PID	Process Name	CPU Ti...	% ...	Threads	User	Real Mem	Kind
160	pboard	0.01	0.0	1	qa	2.2 MB	Intel (64 bit)
178	Preview	1.19	0.0	2	qa	51.6 MB	Intel (64 bit)
167	Quick Look Helper	0.35	0.0	6	qa	19.6 MB	Intel (64 bit)
162	SafeConnect	0.40	0.1	3	qa	10.1 MB	Intel
165	scManagerD	1.31	0.5	2	root	10.0 MB	Intel

If SafeConnect is not present in the Activity Monitor, see below. If scManagerD is not present, continue with "Is the scManagerD daemon registered? below.

Is the Policy Key set to run at startup?

- Click on the Apple Menu and choose System Preferences
- In the System Preferences panel, under "System", click on "Accounts"
- In the Accounts panel, click on your username to select it, then choose "Login Items" Under "Login Items," "SafeConnect (All Users)" should be present.



These items will open automatically when you log in:

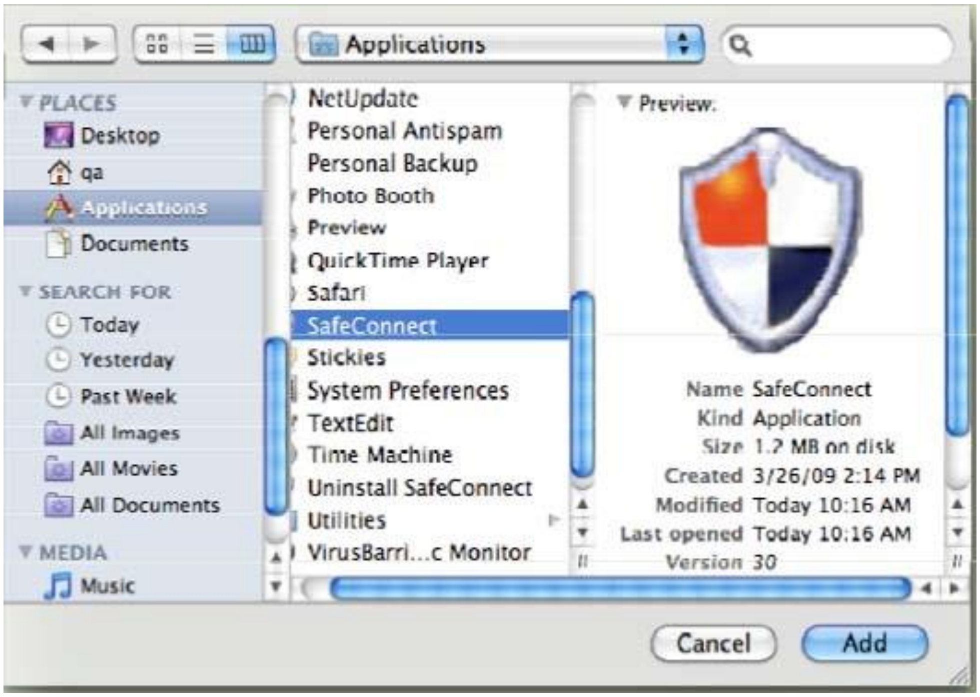
Hide	Item	Kind
✓	SafeConnect (All Users)	Application

To hide an application when you log in, select the checkbox in the Hide column next to the application.

If it is not present,

- Click on the Lock to make changes

- Click on the plus button below the Login Items (not the one below the user list). This will open the file browser.
- Choose "Application"s from the left panel, and then click on "SafeConnect" in the middle panel.
- Click on the Add button from the bottom to add.



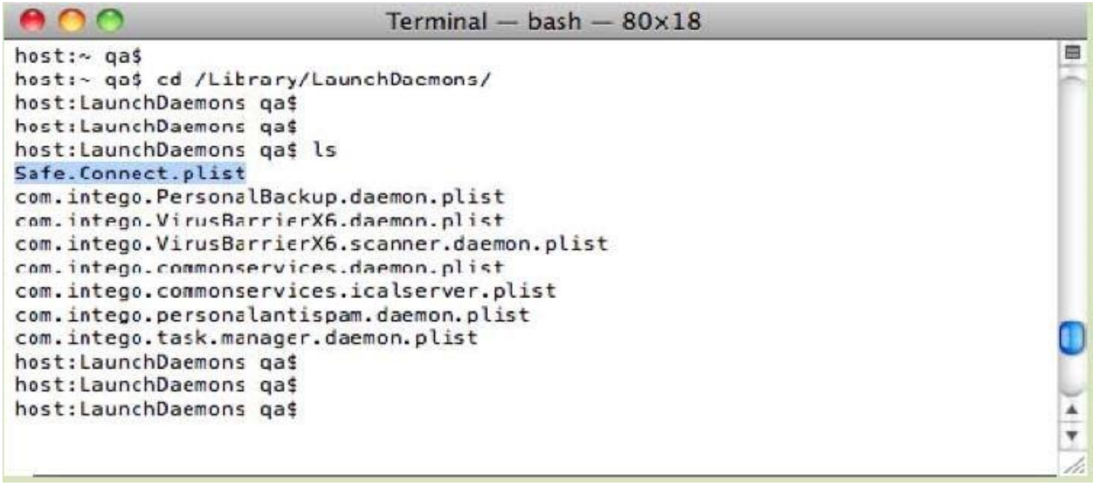
Name SafeConnect
Kind Application
Size 1.2 MB on disk
Created 3/26/09 2:14 PM
Modified Today 10:16 AM
Last opened Today 10:16 AM
Version 30

- this will bring you back to "Login Items" to verify that SafeConnect is listed. Check the box labeled "Hide" next to "SafeConnect (All Users)."

Is the scManagerD daemon registered?

Open up a Terminal session and type the

following: **ls/Library/LaunchDaemons/**



```
host:~ qa$
host:~ qa$ cd /Library/LaunchDaemons/
host:LaunchDaemons qa$
host:LaunchDaemons qa$
host:LaunchDaemons qa$ ls
Safe.Connect.plist
com.intego.PersonalBackup.daemon.plist
com.intego.VirusBarrierX6.daemon.plist
com.intego.VirusBarrierX6.scanner.daemon.plist
com.intego.commonservices.daemon.plist
com.intego.commonservices.icalserver.plist
com.intego.personalantispam.daemon.plist
com.intego.task.manager.daemon.plist
host:LaunchDaemons qa$
host:LaunchDaemons qa$
host:LaunchDaemons qa$
```

This will display the contents of that folder. Look for a file titled "Safe.Connect.plist." If this file is not present, the "scManagerD" daemon will not run at startup. Try uninstalling and reinstalling the Policy Key once again. If you have further difficulties with the Policy Key, or you feel you need help with these steps, please take your device to the iTech Help Desk in the Jernigan Library Commons for assistance or you can call the iTech Help Desk at (361) 593-4357.