

Safe•Connect | Policy Key Troubleshooting Guide

This document is designed to give support personnel tools to resolve the most common issues that may result in the need to reinstall the Safe•Connect Policy Key.



Impulse Point
6810 New Tampa Highway
Lakeland, FL 33815
863-802-3738
www.impulse.com

February 2012

Contents

Repeated Prompts to Reinstall the Policy Key.....	3
Is the Policy Key running?	17
Restarting the Policy Key	17
Policy Key Logging	18
Policy Key Troubleshooting Checklist	19

Repeated Prompts to Reinstall the Policy Key

PC / Mac

Possible Cause	The endpoint may have an incorrect system time and/or date .
Problem Determination	Check the time and date on the endpoint.
Resolution	Update the system time and/or date to current and log out and back in to the machine.

PC / Mac

Possible Cause	The endpoint may have a malware infection.
Problem Determination	If any of the steps below don't work, and particularly if the machine has shown signs of other problems, especially network issues, unrelated to Safe•Connect, this may indicate an infection of some sort.
Resolution	The endpoint may need to be treated with a dedicated malware removal tool. Safe•Connect customers have had good results with Malware Bytes and Spybot. It is advisable to boot the machine into Safe Mode before attempting to remove any infections.

PC / Mac

Possible Cause	The endpoint may have pending updates .
Problem Determination	If there are pending updates on the endpoint, it can put the Policy Key in a suspended state.
Resolution	The endpoint will need to have updates applied and be rebooted.

PC

Possible Cause	This is typically a sign that the Policy Key is either unable to install correctly , or that, after installation, it is unable to communicate .
Problem Determination	Either way, the steps here are a good place to start. For more detailed steps, and in-depth troubleshooting, please see the pages that follow.
Resolution	<ul style="list-style-type: none">• On Vista and newer, turn off UAC, then uninstall/reinstall the Policy Key with UAC turned off. See page 2 below for details.• On Windows XP, there is a rare issue that can cause a corrupt installation. The fix is simply to completely uninstall and then reinstall the Policy Key.• On all versions of Windows, add an exemption to any Antivirus or 3rd party firewalls for the entire Policy Key install folder, and for the Policy Key installer.<ul style="list-style-type: none">○ Policy Key install folder: "Program Files(x86)\SafeConnect"○ Policy Key installer: ServiceInstaller.exe• Some AVs (most notably McAfee) also aggressively monitor the Temporary Internet Files folder, which can prevent ServiceInstaller.exe from running. However adding an AV exemption for ServiceInstaller.exe should resolve that.• Please see below for more details and further troubleshooting steps.

PC

Possible Cause	On Windows Vista and newer, User Account Control (UAC) may have prevented the Policy Key from installing correctly.
Problem Determination	This is often a good 1 st step on Windows Vista, 7 and 8 machines.
Resolution	<p>Uninstall and reinstall the Policy Key with elevated privileges, or with UAC turned off:</p> <ul style="list-style-type: none">• Uninstall/Reinstall as Administrator<ul style="list-style-type: none">• Open "Program Files\SafeConnect" or "Program Files(x86)\SafeConnect".• 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".• If this doesn't work, try the steps below.• Uninstall/Reinstall with UAC turned off<ul style="list-style-type: none">• Turn off UAC<ol style="list-style-type: none">1. Press the Start Menu2. Type "UAC" in the search box and hit <Enter>3. Move the slider all the way to the bottom.4. Reboot the machine.• Uninstall/Reinstall the Policy Key in the usual way.• If desired, re-enable UAC.

PC

Possible Cause	A personal firewall is blocking the Policy Key.
Problem Determination	<p>Make sure the Policy Key is running. (Please see “Is the Policy Key running?” at the end of this document.</p> <p>If the Policy Key is running, look for a personal firewall installed on the host machine.</p> <p>McAfee and Norton/Symantec products often have very aggressive, built in firewalls, which account for the majority of this type of issue.</p>
Resolution	<p>It is not recommended that you disable the host’s personal firewall.</p> <p>Instead, add the Policy Key to its exception list. Both SCClient.exe and scManager.sys should be allowed to communicate on all ports.</p> <p>Some firewall programs may also require that the IPs 198.31.193.211 and 127.0.0.1 be added as trusted hosts.</p> <p>There have been cases, with the TrendMicro firewall in particular, where even though the exceptions are added, the firewall will not unblock the Policy Key. Some users have found it necessary to uninstall and reinstall the Policy Key.</p> <p>Once the above steps are done, restart the computer.</p> <p>If your organization uses a centrally managed antivirus solution, the exceptions listed here should be pushed out to all managed hosts.</p> <p>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 the host you are working on has ever had a Symantec, Trend Micro, or McAfee product installed on it, there is a chance that remnants of that program may still remain, even if there is no entry in Add/Remove Programs.</p> <p>In a number of cases, previously uninstalled versions of these products have been found to block the Policy Key from communicating. This is true no matter how long ago the program was removed. The only way to rule this out with any confidence is to run the solution's removal tool. Following are links to each vendor's removal tools:</p> <p>Symantec/Norton: ftp://ftp.symantec.com/public/english_us_canada/removal_tools/Norton_Removal_Tool.exe</p> <p>Trend: http://www.support.antivirus.co.uk/trendmicro/kbresolution.jsp?hmid=2530&serviceId=1</p> <p>McAfee: http://download.mcafee.com/products/licensed/cust_support_patches/MCPR.exe</p> <p>Once the removal tool has run, restart the computer.</p>

NOTES

1. Some of the more aggressive personal firewalls will block the Policy Key without notifying the end user. Most will provide a popup notice asking to allow or block. As long as users choose **allow**, the Policy Key should be able to communicate normally.
2. This issue will typically only come up when the Policy Key is first installed. However, the Policy Key will periodically updates itself to a newer version. In rare cases, such an update will cause a personal firewall to block the Policy Key again.

So even if the Policy Key has been running fine for an extended period, it's always a good idea to recheck the firewall settings if an end user is unexpectedly prompted to reinstall.

PC

Possible Cause	The SCCM 2012 client was recently deployed
Problem Determination	After deploying the SCCM 2012 client, the endpoint was not rebooted and the Policy Key was stopped by the SCCM client installation.
Resolution	<p>When deploying the SCCM 2012 client, use the /forcereboot hook. This will force a reboot and will allow the Policy Key to start up. The only caveat is that the end user is NOT prompted of the reboot, so this should be scheduled.</p> <p>/forcereboot</p> <p>Specifies that CCMSSetup should force the client computer to restart if this is necessary to complete the client installation. If this option is not specified, CCMSSetup exits when a restart is necessary, and then continues after the next manual restart.</p> <p>Example: CCMSSetup.exe /forcereboot</p>

PC

Possible Cause	The Policy Key is quarantined by an Antivirus program.
Problem Determination	<p>If you've already checked for the presence of a personal firewall, try to restart the Policy Key. (Please see "Restarting the Policy Key" at the end of this document.)</p> <p>If this fails, the Policy Key may have been quarantined.</p> <p>Symantec/Norton products are by far the most likely quarantine the Policy Key. Less frequently, Sophos, McAfee and even TrendMicro have been known to do so.</p>
Resolution	<p>First, check to see exactly which antivirus programs are installed. If multiple AVs are found, please see the first NOTES section on this page for further discussion.</p> <p>Check each remaining antivirus program's Quarantine section, for Policy Key files. These could be any files from the "\Program Files\SafeConnect\" directory, but especially scManager.sys and SCClient.exe.</p> <p>If you find any Policy Key files, (i.e. scManager.sys, SCClient.exe, scManager.dll, SCClient.dll, or SCUpdate.sys) add them to the AV program's allow list and reboot the computer. You may also need to add the Policy Key installer, ServiceInstaller.exe to the allow list.</p> <p>If you don't find that any Policy Key files have been quarantined, OR if the Policy Key download page comes up again after reboot, you will need to run the Norton Removal Tool. Please see the 2nd NOTES section on this page for further discussion.</p> <p>If you are still prompted to reinstall the Policy Key after running the Norton Removal Tool, please contact your Safe•Connect Support Representative.</p>

NOTES

1. It is highly recommended to uninstall duplicate Antivirus programs until only one remains.

Multiple Antivirus programs can compete for system resources, potentially causing dramatic performance decreases and other more serious problems.
2. If the host you are working on has **ever** had a Norton or Symantec product installed on it, there is a chance that remnants of that program may still remain.

In a number of cases, previously uninstalled versions of these products have been found to quarantine the Policy Key. This is true no matter how long ago the program was removed.

The only way to rule this out with any confidence is to run the [Norton Removal Tool](#), designed by Symantec to remove all traces of any Symantec or Norton products.

For further details, please see [Symantec's website](#).

PC

Possible Cause	The Policy Key's client application, SCClient.exe is not configured to launch when Windows starts up.
Problem Determination	<p>Open the Windows Task Manager and click on the Processes tab. Click on the Image Name column heading to sort. If you don't find SCClient.exe, it may not be starting up with Windows.</p> <p>Click on "start > All Programs > Startup" and look for SafeConnect, with a red, white and black shield icon. If you don't see it, SCClient.exe is not starting up when Windows loads.</p>
Resolution	<p>Click on "start > All Programs". Right-click on Startup, and choose "Open All Users". If this option is not available, choose "Open".</p> <p>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".</p> <p>Drag the new file "Shortcut to SCClient.exe" to the Startup folder you just opened. Then close the Startup folder.</p> <p>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, as in the Problem Determination section, above.</p>

NOTES

1. The Policy Key installer places this shortcut in your Startup folder automatically when you first install the Policy Key. It's possible that an **Anti-Spyware** application may have removed the shortcut at a later date.

If so, the next time you run an Anti-Spyware scan, you should be able to choose not to have the shortcut removed.

Depending on your program, you may also be able to instruct it to ignore that shortcut in future scans.

PC

Possible Cause	The Policy Key cannot communicate because it is waiting for the endpoint's DNS Client service to respond.
Problem Determination	<p>The Policy Key is installed and running (see “Is the Policy Key running?” below). Attempted reinstalls fail because the Safe•Connect Manager service cannot be stopped.</p> <p>As part of its normal operations, the Policy Key sometimes needs to restart the DNS Client service. In some cases, if the DNS Client service does not restart in a timely fashion, the Policy Key will be unable to communicate.</p> <p>Manually restarting the DNS Client service may allow the Policy Key to communicate:</p> <ul style="list-style-type: none">• Click “start > Run” and type “services.msc” to open the Services control panel.• Look for the service titled “DNS Client” or “DNS Cache”.• Right-click on the service and choose “Restart”. <p>If the Policy Key was in fact waiting on the DNS Client service, the end user should now be able to browse freely without being prompted to install the Policy Key.</p>
Resolution	Please inform Safe•Connect support of the above steps. They should be able to make an adjustment to resolve the issue.

PC

Possible Cause	On a Domain machine , Group Policy will not allow the Policy Key to run under all privileges.
Problem Determination	<p>The Policy Key runs as expected for users with Administrator privileges, for example. Default users of the same machine are prompted to reinstall the Policy Key within minutes of logging in.</p> <p>Try the following, both as an Admin and as a default user. Open the Windows Task Manager and select “Show processes from all users”. Look for both scManager.sys and SCClient.exe.</p> <p>If those processes are present for the administrator, but not for the default user, you may be looking at a Group Policy configuration problem.</p>
Resolution	Ask that your Domain Administrator add scManager.sys and SCClient.exe to the list of programs allowed to run under default privileges.

NOTES

1. Lab machines, public kiosks, and other tightly controlled endpoints are the most likely candidates for issues such as these.

MAC

Possible Cause	The local user password is not known, causing the user to be unable to elevate privileges when running the Safe•Connect Mac Installer.
Problem Determination	Download the installer (SafeConnectMacInstaller.zip) and double-click to run it. When it prompts for a username and password, the end user cannot provide one.
Resolution	Reset the local user's password. Please see Apple's website for instructions: http://support.apple.com/kb/HT1274 .

MAC

Possible Cause	The local user password account does not have a password. Even though the Safe•Connect Mac Installer appears to run successfully, it cannot elevate privileges and the installation fails.
Problem Determination	<ol style="list-style-type: none">1. Open the terminal (Finder > Applications > Utilities > Terminal).2. Type "sudo su" and press "enter". You should be prompted for the local user's password.3. Press "enter". If the local user account has a password, you will be prompted to enter it again. If the local user account doesn't have a password, you will be brought back to a command prompt.4. Type "whoami" and press "enter". If you entered a password, this should return the administrator's username (typically root).5. If Step 4 returns the local user's login name, this machine is unable to elevate privileges.
Resolution	<p>Reset the local user's password. Please see Apple's website for instructions: http://support.apple.com/kb/HT1274.</p> <p>Next, redo the steps under Problem Determination, above.</p> <p>Finally, if the "whoami" command returns the administrator's username (typically root), download and double-click on SafeConnectMacInstaller.zip to re-run the Macintosh Policy Key installer.</p>

MAC

Possible Cause

After verifying that the local user is able to elevate privileges, the installer runs, but the Macintosh Policy Key still does not operate properly.

Most issues that prevent the Macintosh Policy Key from running will need to be addressed with Impulse Support. Below are some things to verify before contacting Impulse.

Problem Determination

Please verify the information below. Call Support for assistance as noted and needed.

There are four items to check:

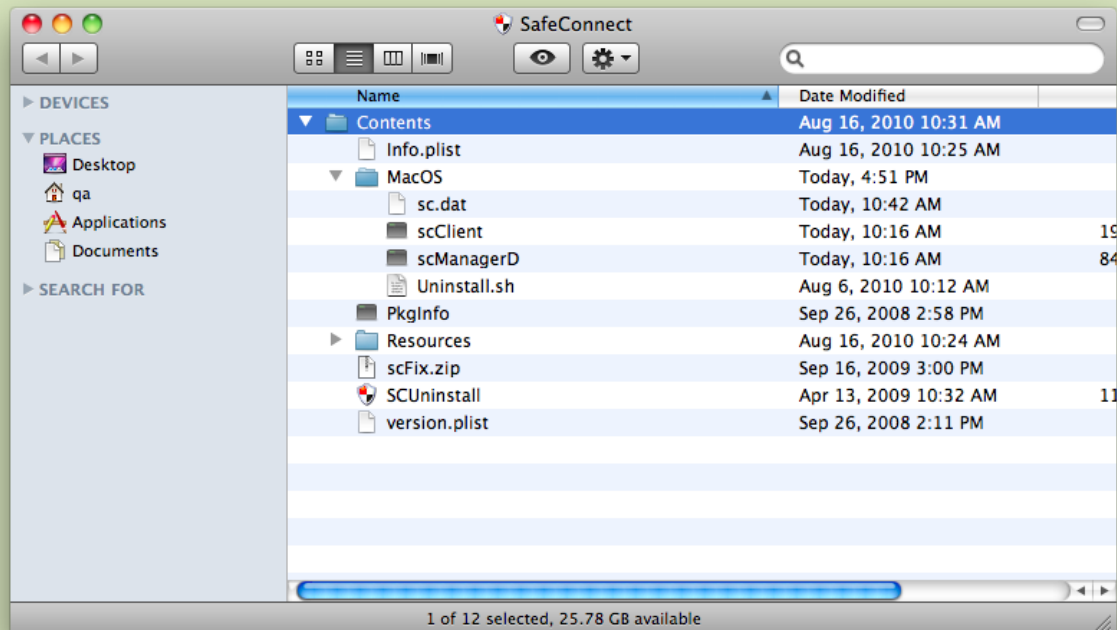
And Resolution

A). Determining if the Safe•Connect Policy Key is installed:

From the **Finder**, open **Applications**, and look for **SafeConnect**. If **SafeConnect** is missing, look for **PolicyKey**.

If **SafeConnect** is present, **ctrl-click** on it and choose “**Show Package Contents**”. Then open the **Contents** and **MacOS** folders. Inside **MacOS**, please note which of the following files is present:

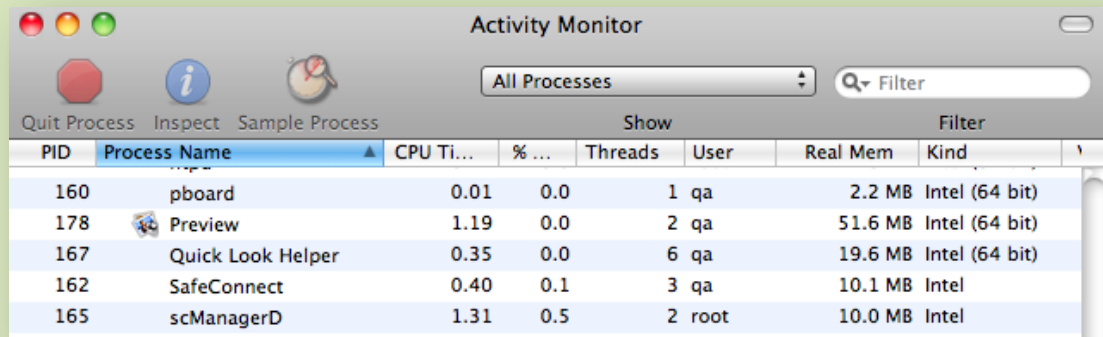
sc.dat
scClient
scManagerD
uninstall.sh



Cont'd next page...

B). Determining if the Safe•Connect Policy Key is running:

Next, open **Activity Monitor** (Finder > Applications > Utilities > Activity Monitor), and choose “**Show All Processes**” at the top right. You should see processes named **SafeConnect** and **scManagerD**. (If the Policy Key has just been installed, you may see 2 processes called **SafeConnect**. In this case, please reboot.) After a reboot, please note whether **SafeConnect** or **SCManagerD** is missing.

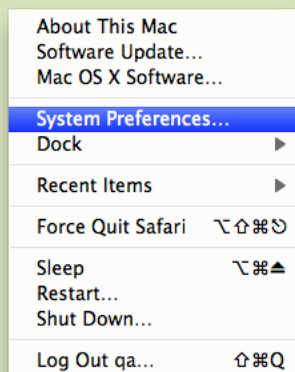


PID	Process Name	CPU Ti...	% ...	Threads	User	Real Mem	Kind
160	pboard	0.01	0.0	1	qa	2.2 MB	Intel (64 bit)
178	Preview	1.19	0.0	2	qa	51.6 MB	Intel (64 bit)
167	Quick Look Helper	0.35	0.0	6	qa	19.6 MB	Intel (64 bit)
162	SafeConnect	0.40	0.1	3	qa	10.1 MB	Intel
165	scManagerD	1.31	0.5	2	root	10.0 MB	Intel

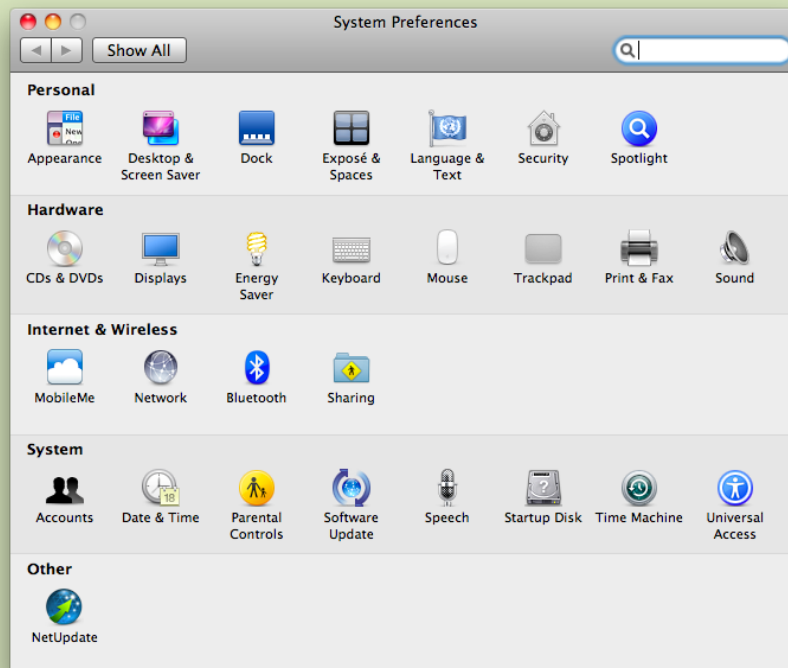
If “SafeConnect” is not present in “Activity Monitor” continue on to step “C” below. If “scManagerD” is not present, continue on to step “D” below.

C). Determining if the Safe•Connect Policy Key is configured to run at startup

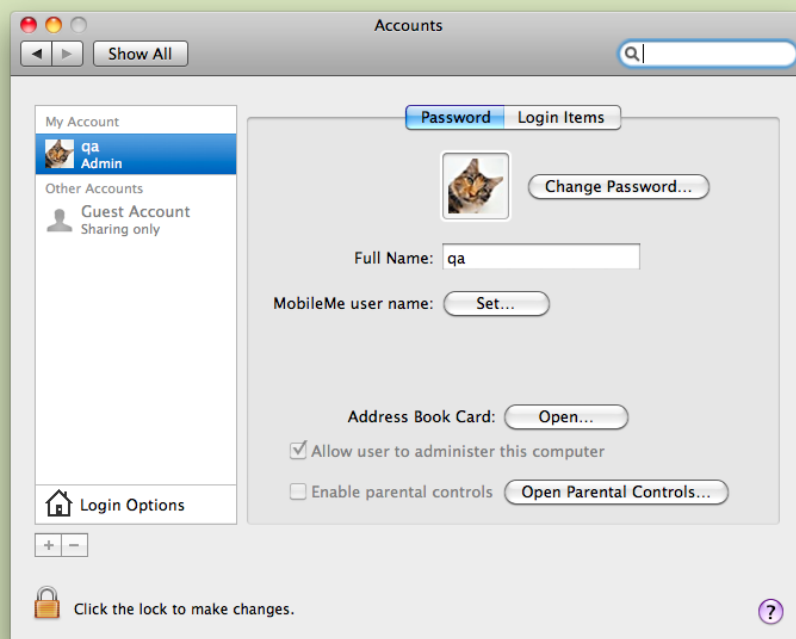
Click on the Apple Icon and choose System Preferences



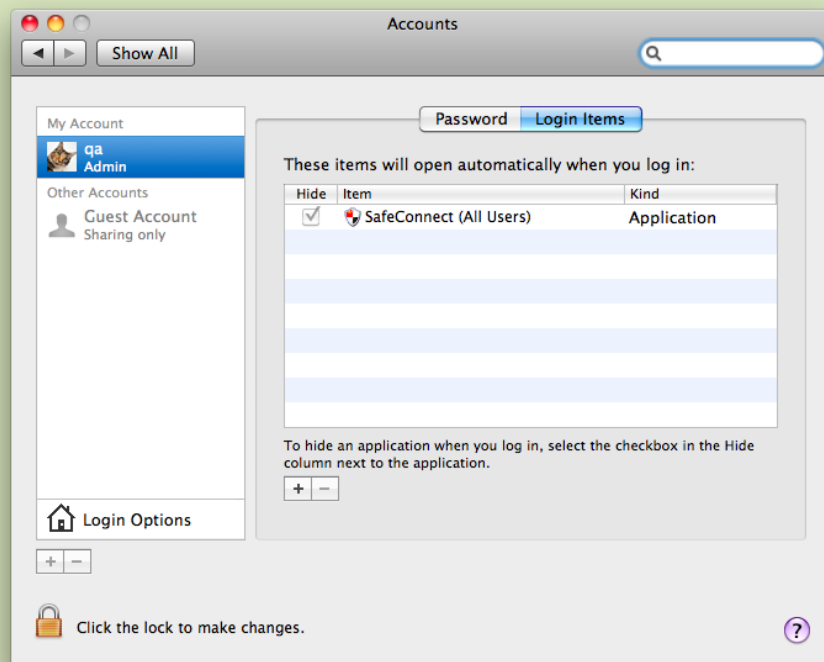
In the “System Preferences” panel, under “System”, find and click the “Accounts” option.



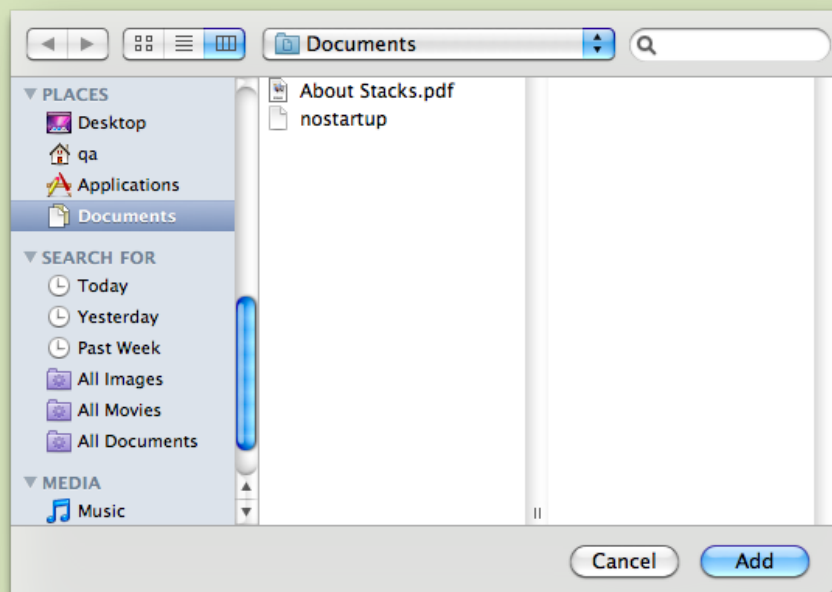
In the “Accounts” panel, find the current user in the left side and select it. Then choose “Login Items” on top right. You will need to click the lock icon in the lower left of the screen and put in the local user’s credentials.



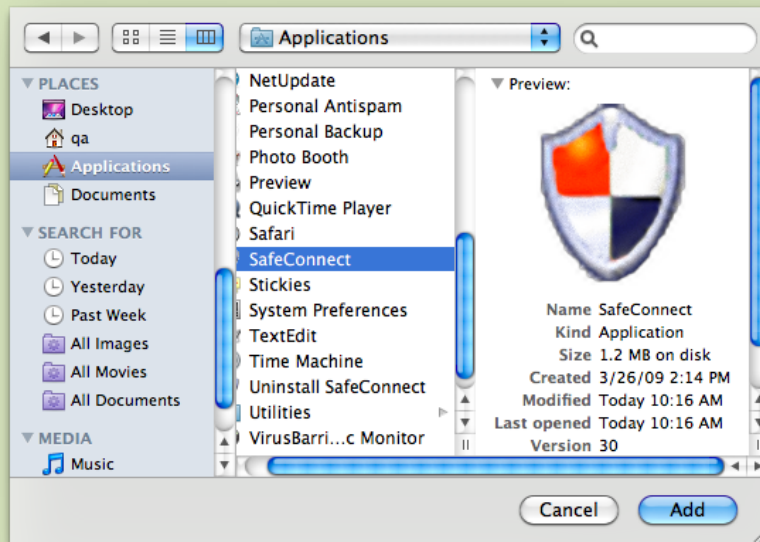
Under “Login items,” “SafeConnect(All Users)” should be present.



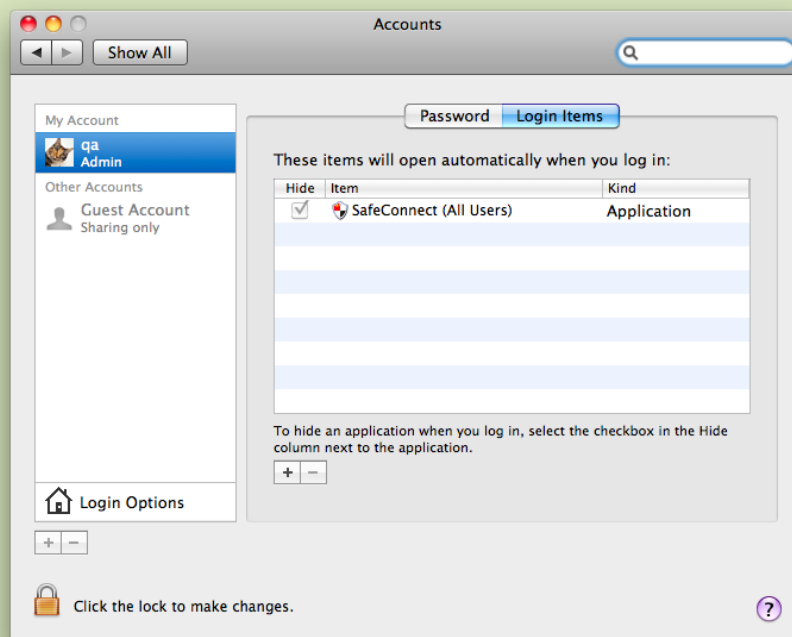
If SafeConnect is not present, click on plus (+) button on the bottom left of the Login Items table. This will open the file browser



Choose “Applications” from the left hand panel, and then click on “SafeConnect” in the middle panel. Click the “Add” button from the bottom to add



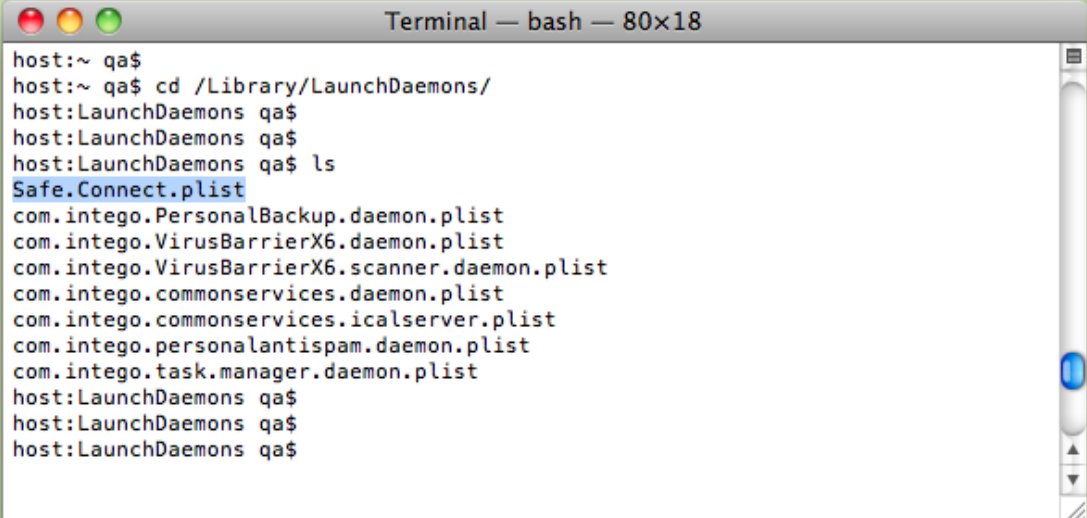
This will bring you back to “Login Items” to verify that SafeConnect is listed. Check the box labeled “Hide” next to “SafeConnect (All Users)”.



D). Determining if the “scManagerD” is properly registered

Open up a terminal session and type the following:

```
cd /Library/LaunchDaemons/  
ls
```



```
Terminal — bash — 80x18  
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 change to that folder and list all the files.

Look for a file titled “Safe.Connect.plist”.

If that file is not present, the “scManagerD” daemon will not run at startup. Please contact support for assistance with this issue.

Resolution Please note the results of the above checks and contact Impulse support with your findings. They should be able to help you resolve the issue.

Is the Policy Key running?

PC

- Open the **Task Manager** to 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.

MAC

- Open **Activity Monitor** (Finder > Applications > Utilities > Activity Monitor).
- Choose "**Show All Processes**" at the top right.
- Click on the "**Process Name**" column heading to sort.
- Look for **SafeConnect** and **scManagerD**. Both should be present.
- If you have only recently installed the Macintosh Policy Key, both processes may be called **SafeConnect**.

Restarting the Policy Key

Windows

Open a command prompt. On Vista and newer, open it as Administrator. Paste the following:

```
net stop "Safeconnect Manager"
```

```
net start "Safeconnect Manager"
```

If the service cannot be stopped, you will need to task-kill **SCClient.exe**. When **SCClient.exe** has stopped, paste the above commands again to restart the **Safe•Connect Manager** service.

Once the **Safe•Connect Manager** service is started, restart **SCClient.exe**. You can do this by opening the **Policy Key install folder** (see the Logging instructions, above) and double-clicking on **SCClient.exe**.

Policy Key Logging

There are times when getting additional logging information directly from an endpoint can be beneficial to troubleshooting an issue. Information is the policy key log files should be forwarded to the impulse support team as soon as they are generated.

To enable Policy Key logging:

- Download config.xml
 - **Windows:** Download config.xml from <https://198.31.193.211:8443/html/> (or substitute your enforcer's internal IP) and place it in the "Program Files(x86)\SafeConnect" folder.
 - **Mac OS X:** Right-click (or ctrl-click) on the Safe•Connect application and choose "Show Package Contents". Navigate to the Contents/MacOS folder. Download config.xml from <https://198.31.193.211:8443/html/> (or substitute your enforcer's internal IP), and place it into the MacOS folder.
- Once this file is in the directory, 'logfile.txt' will appear. After the file appears, log out and log back into the machine. In most cases, 2 minutes of logging will be sufficient.
 - ***Note:** The log file has a maximum file size of 20MB. If the file grows to this size, older data will be removed to make room for new data. This allows for approximately 15 minutes of logging history.
- When finished, remove config.xml from the folder above to disable logging.

If you do not have a copy of **config.xml**, please contact your Network Administrator, or your Safe•Connect support representative.

Policy Key Troubleshooting Checklist

When using this document, this list can serve as a guide for what has been checked.

IP Address

Is the date correct?

Yes ☐ No ☐

Is the time correct?

Yes ☐ No ☐

Has the endpoint been scanned for malware?

Yes ☐ No ☐

Which malware scanner was used?

Was malware found?

Yes ☐ No ☐

Was all malware removed?

Yes ☐ No ☐

Is the Policy Key exempted in the firewall?

Yes ☐ No ☐

Is the Policy Key exempted in the anti-virus?

Yes ☐ No ☐

Has the Policy Key been reinstalled with UAC disabled?

Yes ☐ No ☐

Navigate to <https://auth.impulse.com:8443/html/dl.htm>

Do you get a certificate error?

Yes ☐ No ☐

Do you see the Policy Key download page?

Yes ☐ No ☐