


SAFE CONNECT INSTALLATION FOR WINDOWS USERS

Students

Before you begin you will need the data encryption key code. Call the Computer Service Center at 936-261-9330 to obtain the key code. You will also need to remove any unlicensed sharing and downloading software from your computer. (example: Bearshare)

****READ INSTRUCTIONS ALL THE WAY THROUGH****

Connecting to the PVAMU Wireless Network

1. Connect your computer to the network through a wired network connection or a WiFi connection a PVAMU campus
2. Click on the Wireless networks icon located on your task bar next to your volume control 



3. Click **Pvmobilenet**
4. Check the **Connect automatically** button
5. Click the **Connect** button
6. Type the network security key you obtained from the PVAMU Helpdesk (936-261-2525) or the ITS Computer Service Center at 936-261-9330



7. Wait a few minutes for the network connection to establish then open a web browser and attempt to navigate to any web page. You should be greeted with the following login page:

PRairie View A&M UNIVERSITY

Welcome to the PVAMU Network
To access network resources, please sign in.

Sign In

Network Username

Password

I accept the Acceptable Use Policy

Sign In

8. Login using your **PantherNetID** username and password. This will be the same as the username and password you use to access PVPlace.
9. Check **I accept the acceptable use policy**
10. You can click the link to read the acceptable use policy (see below)



Acceptable Use Policy

All computers attached to the network must have appropriate software running on their machine to ensure a secure environment for all users. Monitoring software will be provided to ensure compliance with this policy. The software will assist users in maintaining their computer in the manner prescribed by the network. Software needed to ensure a secure environment will include:

1. Organization approved anti-virus software
 2. The most current security patch software for your operating system(s).
 3. Monitoring software to ensure that copyrighted files are not freely shared over the Internet.
 4. Other software as periodically deemed appropriate by the organization to ensure a safe and secure Internet and Intranet for all users.
 5. In addition, bandwidth consumption is monitored to prevent inappropriate use of network resources (for example, setting up a public web site). Excessive or sustained bandwidth consumption may burden the network and such usage may be restricted.
 6. The use of the network is a privilege that may be revoked at any time for inappropriate behavior. Such behavior would include, but not be limited to, the use of obscene, abusive, or otherwise objectionable language and/or materials in either public or private messages.
 7. The primary purpose of the network is to support organizational goals. In support of these goals, the following activities are prohibited without the express written consent of the organization. Participating in these activities may result in revocation of network access without refund and possible judicial action and/or criminal charges:
 - Setting up a router and building a private subnet.
 - Setting up any type of information server such as a web, gopher, e-mail, game, etc.
 - Propagating e-mail chain letters.
 - Forging mail.
 - Allowing unauthorized persons access to the network.
 - Using the network for personal financial gain.
 - Copying organization-owned or licensed information to another computer without prior written approval.
 - Sharing copyrighted files and software over the network.
 - Modifying or attempting to modify organization-owned or licensed information including software and data.
 - Attempting to damage or disrupt networking services.
 - Using the network or related resources in the commission of a crime.
 - Using traffic intensive applications that may cause problems within the network or diluting the level of service to other users. No print servers, mail servers, FTP servers, etc. are allowed. The network sharing of any computer-related device or materials that may cause excessive network traffic is forbidden.
 8. The user will abide by all policies and statutes included in the Computer Crimes Act. Crimes against this Act will result in judicial action and/or investigation by law enforcement for criminal offense. The Act includes offenses against intellectual property; offenses against computer equipment and supplies; and offenses against computer access.
11. Click the **Sign In** button when you are ready to continue. After you sign in if you do not already have the policy key you will be taken to the policy key download page.

Download the Policy Key

In order to ensure a safe environment for all users of the network, we require that certain devices install the Policy Key.

The Policy Key validates that your system meets the organization's standards per the [Acceptable Use Policy](#).

[See the FAQ](#) for more information about the Policy Key.

Download Now

Click Download Now to install the Policy Key.

12. Click download now to install the policy key.

INTERNET EXPLORER USERS:

When asked if you wish to Run or Save the software, choose **Run**. When the download completes, the installer should start automatically. If it does not, you can click the download link provided and save the software to the Desktop. Once the download is complete, run the installer by double-clicking it on the Desktop.

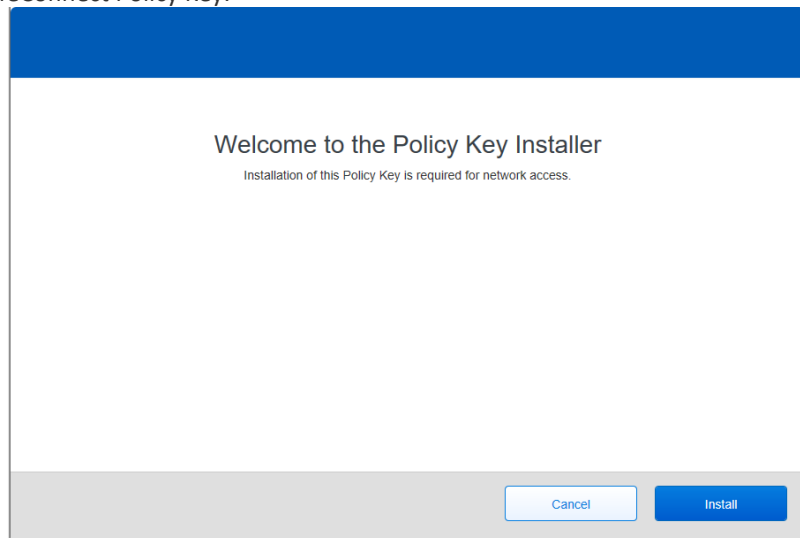
FIREFOX, OPERA, SAFARI AND OTHER WEB BROWSER USERS:

When asked if you wish to Open or Save the software, choose **Save** and select the Desktop as the save location. Once the download is complete, run the installer by double-clicking it on the Desktop.

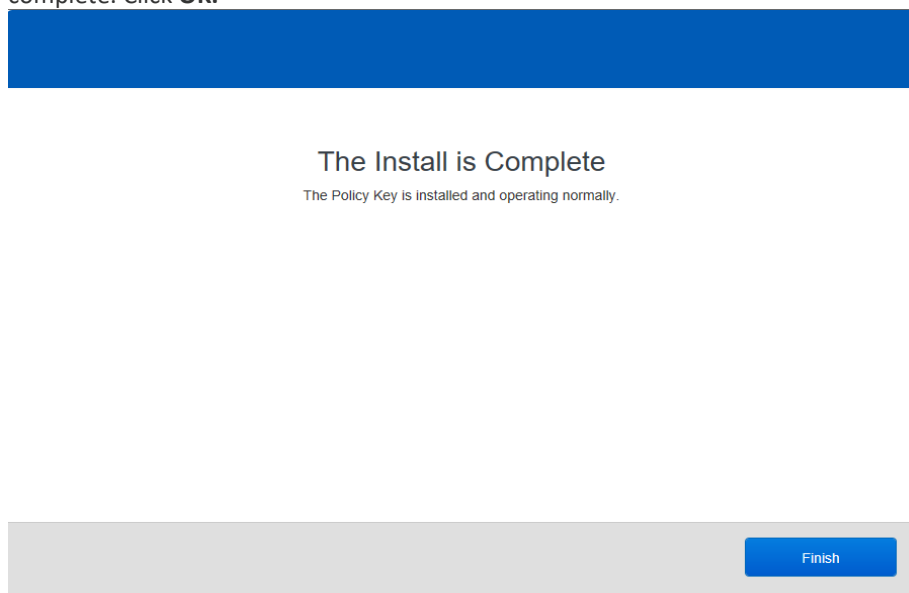
WINDOWS VISTA AND WINDOWS 7 USERS:

A **User Access Control** dialog box will come up when the installer is run. Click **Continue** or **Allow** in the dialog box to continue the installation.

- When the installer is run, you will be presented with the following window. Click **Install** to install the SafeConnect Policy Key.



- The install should be very quick. It will present you with the following dialog box when successfully complete. Click **OK**.



13. Click on the link I'm done installing

Install Policy Key

In order to ensure a safe environment for all users of the network, we require that certain devices install the Policy Key. The Policy Key validates that your system meets the network's security standards as per the school's Acceptable Use Policy. See the [FAQ](#) for more information about the Policy Key.

Follow the instructions below to complete the installation.

- 1 Save the file to your preferred directory.
- 2 After the download is complete, navigate to the file and run it.
- 3 Follow the instructions on the installer.
- 4 Click "I'm done installing" below.

[I'm done installing](#)

14. The PVAMU web site should appear, happy safe computing!

Secure | <https://www.pvamu.edu>

PRAIRIE VIEW A&M UNIVERSITY

STUDENTS FACULTY AND STAFF PARENTS AND FAMILY ALUMNI

ABOUT PVAMU ACADEMICS ADMISSIONS ATHLETICS CAMPUS LIFE RESEARCH [GIVE NOW](#)

SWAC 2018 CHAMPIONSHIP OUTDOOR TRACK & FIELD

PVAMU 2018 SWAC OUTDOOR TRACK & FIELD CHAMPIONS

[Learn more](#)

2018 SWAC MEN'S TRACK & FIELD CHAMPIONS

IGNITE your passion...EXPERIENCE PVAMU [APPLY NOW](#)