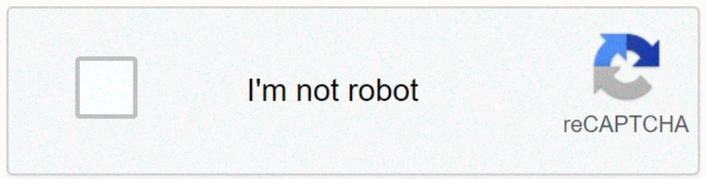

Continue

Pulse secure latest version free

Pulse Secure Installer for 64-bit Windows ps-pulse-win-5.2r7.0-b1025-64bit install.msi — Windows Installer Package, 16.64 MB (17453056 bytes) Sign in to Under Pulse Secure Center, click Licensing and Download Center. Select the account you want to use. On the Pulse Secure Licensing & Download Center page, select the Downloads tab. Under Browse software and documentation at the bottom of the screen, click Pulse Secure. Click On Pulse Connect Secure from product lines. This will download the latest Pulse Connect Secure software. After installingPulse Connect Secureandperformbasicsetup, you are able to install the firstStream Connect Secure software, license Pulse Connect Secure, confirm availability, and complete the configuration process: To install the latest Pulse Secure Connect software, license Pulse Connect Secure and create a test user to verify user availability, follow the task guide built into the Administrator Web Console. The PittNet VPN (Pulse Secure) service allows students, faculty, and staff to connect to limited university resources while off campus or use PittNet Wi-Fi. The service encrypts traffic between a user's computer and the university's network. These instructions explain how to use Pulse Secure Client with the PittNet VPN service. When you're off campus, Pulse Secure is the recommended method to establish a remote desktop connection to your office computer or to access department databases and servers that are behind network firewalls. To use Pulse Secure to access these resources, your Account Manager admin must have already created a PittNet VPN role for you. A PittNet VPN role (sometimes referred to as a Network Connect role) is a special set of permissions that gives you access to specific network resources. You must select your PittNet VPN role when using Pulse Secure. If you are using the University's PittNet VPN service, either through the recommended Pulse client or through the IPSec client, you must use multi-factor authentication for PittNet VPN connections. This requirement affects all students, teachers, and employees who use the PittNet VPN service. Download the Pulse Secure client Before downloading the Pulse Secure client, check to see if it is already installed. Windows users should look for the Pulse Secure client icon in the notification area, located in the lower-right corner of the screen. Macintosh users should look for the Pulse icon in the upper-right corner of the desktop (Finder). Note: The Pulse Secure client used to be marketed as Junos Pulse and contained a different logo (see below). If your system has an older version of Pulse installed, you should upgrade to the latest version of the Pulse Secure client. Download Pulse for Windows or Mac students, teachers, and staff can download the Pulse Secure client from download service. Heart rate Heart rate client software for Windows and Macintosh PCs is listed under the Pulse Secure provider as pulse VPN Desktop Client. Download Pulse for UPMC users, sponsored account holders, and other affiliates the Pulse Secure client is available for download at technology.pitt.edu/pulseclient for people who do not have access to the software download service. Download Pulse for mobile devices The Pulse Secure client is available for download in the Apple App Store (iOS), the Google Play Store (Android), and the Microsoft App Store (Windows Phone). Install Pulse Secure Client and Configure a Profile The following instructions explain how to install Pulse Secure on a laptop or desktop computer running Windows or macOS. For instructions on how to use Pulse with your mobile device, see our mobile instructions. Open Pulse Secure. For Windows systems, the program should be listed on the Start menu under Pulse Safe. Click the plus sign to create a profile. Note: On older versions of Junos Pulse, the plus sign is located in the lower-left corner of the Connections window. Enter email for sremote.pitt.edu. Leave the Type field on the default setting. Note: If you are an upmc user, type sremote.pitt.edu/upmc in the Server URL field. In the Name field,enter a name for your profile (for example, PittNet VPN Connection). Click Add to save the profile. Create a PittNet VPN session Note: You must have already registered a multi-factor authentication device before you can complete the following steps. Click the Connect button next to your profile. Note: In steps 2 through 4, you can save your settings with the Save settings check box. Saving your settings (which include saving your password in step 3) saves you time when you connect in the future, but it also poses a security risk if someone other than you also has access to your computer. A pre-logon notification shows the options for using multi-factor authentication. Click Continue. Enter your user name and password as usual and click Connect. A new window displays a secondary password field for multi-factor authentication. Enter multi-factor authentication credentials. You have several options: Type Push and click Connect. Accept the Push notification on your smartphone or tablet. Note that you must have the Duo Mobile app installed on your smartphone or tablet (if you haven't already installed the app, you can download it from your device's app store). Generate a password by tapping the key icon in the Duo Mobile app on your smartphone or tablet or using the hardware toxin. In the Secondary password field, type your password, and then click Connect. In the Secondary password field, type your phone and click Connect. This will call the default phone number you registered for multi-factor authentication. Answer the call and press 1. In the Secondary field, type sms and click Connect. The authentication attempt fails, but you will receive a on the registered device. In the Pulse window, in the Pulse window, type your password and click Reconnect. Note: You can also add a number at the end of these factor names if you have more than one entity registered. For example, Push2 will send a login request to the second phone, PHONE3 will call your third phone, and so on. Select the PittNet VPN role you want to use. Click Connect. Your connection will be established. The Pulse Secure tray icon appears with a green arrow that points up after you make a successful connection. When you're done, click disconnect next to your profile in the Pulse Secure client. You can also click the Heart rate icon in the notification area, select your profile, and click Disconnect. Tip: You can quickly open future Pulse Secure connections by clicking the Pulse icon in the notification area, selecting your profile, and clicking Connect. Advanced tips: Create separate heart rate profiles for multiple PittNet VPN roles Some people can use multiple roles with the PittNet VPN service. For example, you might have one role that you use to connect to your office computer from home, and another role that you use to connect to a department database from home. You can create individual Pulse Secure profiles for each of your roles. You can find this to be a faster and easier method to connect. To create a profile for a specific role, complete the steps: Click the plus sign icon to create a profile. Enter email for sremote.pitt.edu. Leave the Type field on the default setting. In the Name field, select a name similar to the PittNet VPN role you're going to use. Click Add. Click the Connect button next to your profile. Select Network Connection, and select the Save settings box. Click Connect. Enter your user name and password. Do not select Save settings if you are using a computer as other parts. Click Connect. A new window displays a secondary password field for multi-factor authentication. Enter multi-factor authentication credentials. You have several options: Type Push and click Connect. Accept the Push notification on your smartphone or tablet. Note that you must have the Duo Mobile app installed on your smartphone or tablet (if you haven't already installed the app, you can download it from your device's app store). Generate a password by tapping the key icon in the Duo Mobile app on your smartphone or tablet or using the hardware toxin. In the Secondary password field, type your password, and then click Connect. In the Secondary password field, type your phone and click Connect. This will call the default phone number you registered for multi-factor authentication. Answer the call and press 1. In the Secondary password field, type sms, and then click Connect. The authentication attempt fails, but you will receive a password on the registered device. In the Secondary field, type the password in the Pulse window with was invalid message and click Reconnect. Note: You can also add a number at the end of these factor names if you have more than one entity registered. For example, Push2 will send a login request to the second phone, PHONE3 will call your third phone, and so on. Select the PittNet VPN role you want to use and select the Save Settings box. Click Connect. You will be connected. The next time you open Pulse, you can quickly connect directly to this role. Role.