Home About

VPN Users: New security changes affecting your access

****
0253 1432
RSA
SecurID
THE ROCKEFELLER UNIVERSITY
0253 1432
ENTER
PIN CODE
ON PHONE
GET
ONE-TIME
PASSCODE
LOG IN
TO VPN

The new, more secure way to log in to VPN: Instead of using your RUNet passphrase, you'll use a memorized PIN code and a one-time passcode you receive on your phone or on a hardware token (also called a key fob).

As part of the Rockefeller's new security initiatives, the way you access VPN is changing. Soon you will no longer be able to log in to VPN using your RUNet passphrase. The university is moving to a more secure login process called two-factor authentication. Instead of your RUNet passphrase, you will use two different login credentials to access VPN. The first credential is a 6- to 8-digit PIN number that you will need to memorize. The second credential is a dynamically generated passcode that is sent to you in one of two ways:

- via a smartphone app (your RSA software token)
- via a small device called a key fob (your RSA hardware token) that you can keep on your key ring or elsewhere on your person.

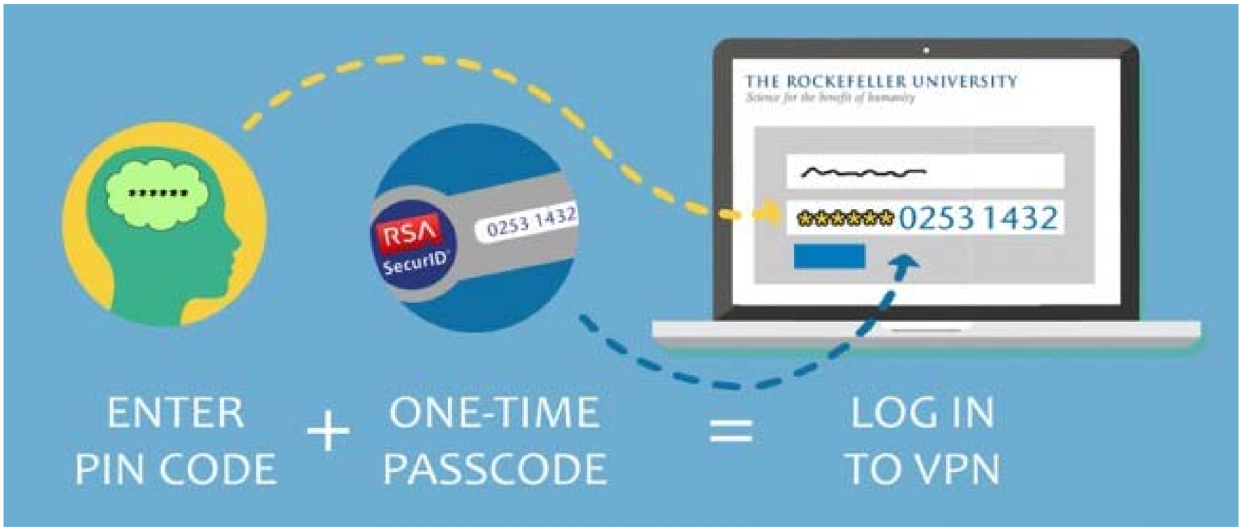
Rolling deadlines will be announced for users to request an RSA token or to opt out of VPN. Access to VPN will be disabled automatically for users who do not request a token by their scheduled deadline. If you use VPN regularly, you are encouraged to request your token now.

The RSA hardware token can be attached to your key ring.

To get your new login credentials for VPN:

STEP 1: Request your RSA software or hardware token
Log in to your RUNet account at http://runet.rockefeller.edu (click Manage Your RUNet Account).Select the '**Request RSA Token**' option and choose either a software or hardware token from the drop down menu.

STEP 2: Activate your token and set up your PIN
Instructions will be sent to you by e-mail as soon as your token is assigned. Once you receive the e-mail, your RUNet passphrase will no longer work with VPN. Activate your token and set up your PIN to log in to VPN.



When using a hardware token to log in, enter your PIN and passcode directly on the VPN login page.

About Two-factor Authentication

Two-factor authentication is the new “gold-standard” in password security. This method makes it nearly impossible for attackers to break in to your account because they must have both your PIN number and your phone or hardware token to do it. IT recommends you use two-factor authentication (also called two-step authentication or two-step verification) on all your personal accounts that offer this option.