Cryptocard FAQ's

Why do we need cryptocard?

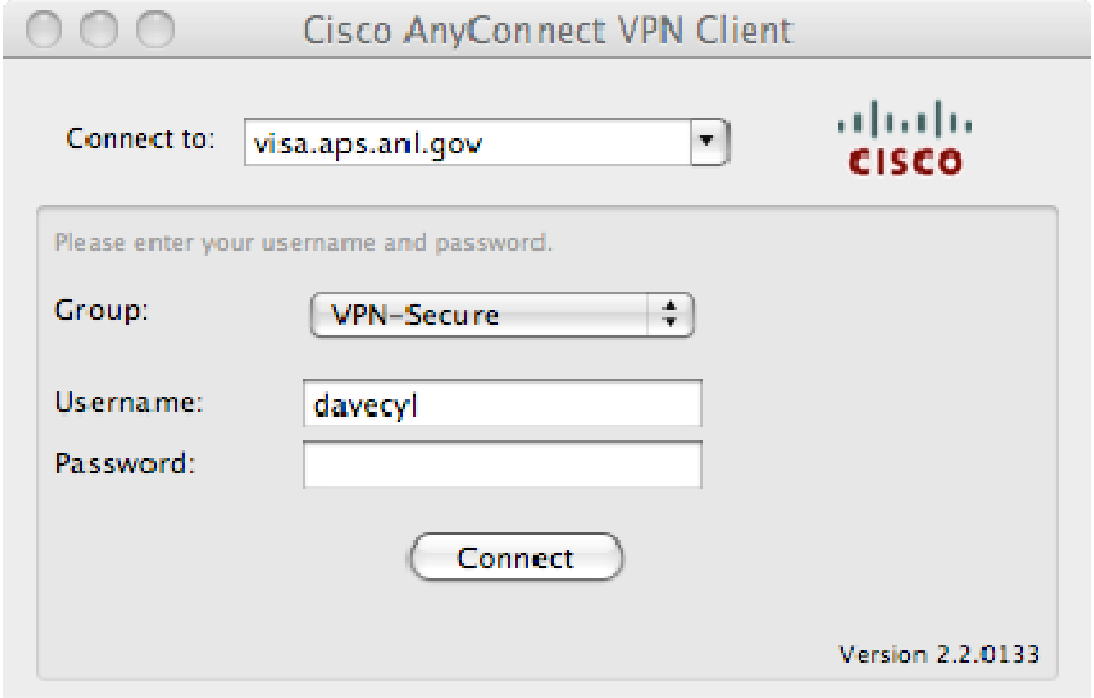
Using cryptocard will address one of the most common targets of a security attack, the use of static passwords. Cryptocard is an example of 2 factor authentication the two factors being 1) the token you have and 2) the PIN which only you know. The one time password together with the lack of static files on the system will create a difficult cracking condition.

What services is this for?

External access to the APS network using either VPN or SSH will require a cryptocard. The services you can access via your account will be dictated by your original account privileges. Having a cryptocard does not imply your account will have both VPN and SSH.

How do I use cryptocard with VPN?

You will need to use the AnyConnect VPN client in secure mode. This is a pull-down option which looks like this.



In the password field you will now enter your cryptocard PIN plus the key generated password. The password format is

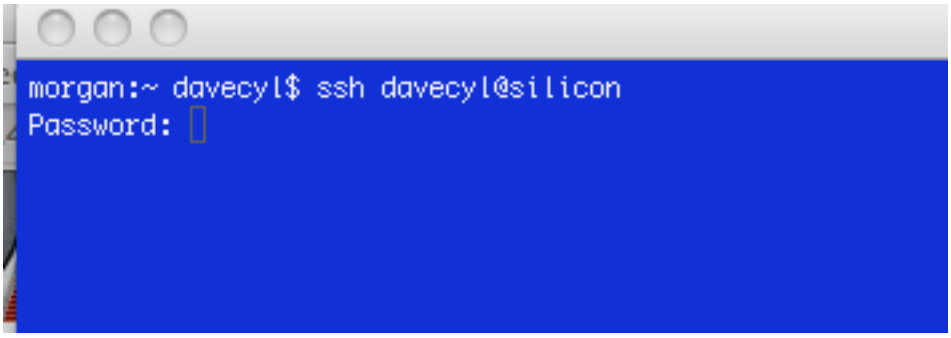
PINkey

e.g. if my PIN was 2321 and the key generated was jLx84*1*

I would type 2321jLx84*1* in the password field.

How do I ssh in with cryptocard?

Open a terminal of choice and ssh to the machine using your regular username.



At the password prompt type in your cryptocard PIN plus your key generated password of type PINkey.

What are the rules for my new PIN?

There is a sanity check on the PIN number which will not allow for any sequence greater than 2 e.g. 2376 is valid but 2346 will fail or abc5 will fail but abd5 will be valid. As per normal practices, this failed condition in not broadcast back to the user to eliminate the feedback of true/false scenarios to unauthorized users. The only signal to the user that this PIN in invalid is a request for a correct password again. Therefore if a PIN is tried and a login does not occur but is followed immediately by a request for a password it is likely to be caused by a bad PIN.

Is there a limit on the number of unsuccessful attempts?

Yes, you can try 7 times to login before your key will be disabled. This disabled state will not time-out and requires an administrator to re-enable. Any successful attempt within the 7 tries will reset the attempt count back to 0.

Is there any limit on the number of times I can press the button on the key?

The present mode of action on a press is to show the keycode for 1 min. If you press the button within this 1 min. window, the keycode will stay on the display for an extra minute. After the minute the key will shut off and subsequent button press will generate a new keycode. There is a limit of 15 unacknowledged keycodes that can be generated by the key device after which it will be put in a “LOCKED” state which is displayed on the LCD. A unacknowledged keycode is one in which the user did not attempt to login and was left to time-out. This locked state will require the key device to be re-initialized and a new PIN assigned.

What should I do if I lose my key.

Report all lost or stolen keys to the APS IT dept. During the day use the normal IT-help number to request assistance in replacing a key. For emergency off-hours requests use the IT-oncall numbers.

After I am logged in using cryptocard will I need this to access my other machines on the APS network.

No, the key is to get to the gateway machine (e.g. Apollo) from that point onward you will use your normal credentials to access the other machines.

Will I need the cryptokey if I am at the APS on the wireless visitor network?

The recommended method of connecting to the internal network while on the visitor network is to join using 802.1X thereby eliminating the need for cryptocard access . Refer to the following link for information on setting up the 802.1X

http://www.aps.anl.gov/APS_Engineering_Support_Division/Information_Technology/General_Support/Remote_Access/8021x/

If, for some reason, this option is not available to you then a VPN-Secure connection using cryptocard will be necessary.