Under construction Fix Me!

New Users and RSA re-activation

PLEASE CHECK BACK OFTEN FOR UPDATES DURING THE TRANSITION PERIOD.

Updated 11/03/16

Introduction

Currently all RDHPCS users are required to have an activated RSA token, even if they are required to do intitial login via CAC. This will be changing as we transition from RSA to CAC over the next several months so stay alert for update and notifications.

RSA activation

Prerequisites You have a newly issued RSA token from the RDHPCS account management group. This could be because you are a new user, or we are replacing an expired, defective, or lost token.

Process

1) Send an email message to rdhpcs.aim.help@noaa.gov with the subject, “Enable RSA Token”.

If this is a replacement token, when you have received confirmation that your token has been enabled, you should be able to login and resume work.

If you are a new user, continue with the following steps.

2) Using ssh, login to the system to which you have been granted access. Your username is your

```
  noaa.gov email address name and is listed above in the “User” field. The
systems and their hostnames
  are listed here:
```

System Hostname Alternate Hostname Jet jet-rsa.boulder.rdhpcs.noaa.gov jet-rsa.princeton.rdhpcs.noaa.gov Theia theia-rsa.boulder..rdhpcs.noaa.gov theia-rsa.princeton.rdhpcs.noaa.gov Gaea gaea-rsa.boulder..rdhpcs.noaa.gov gaea-rsa.princeton.rdhpcs.noaa.gov

Ex: SSH John.Doe@jet.rdhpcs.noaa.gov If you are geographically located on the East Coast of the US, you may want to use the alternate hostname listed. This will provide better routing and may improve interactive performance for you. The RSA token is used to provide two-factor authentication access to the RDHPCS systems. When you are asked for a password, this will be your personal PIN number plus

the code on the RSA token. You will set your PIN number the first time you try to login. When you login to the system, you will see the prompt: Access is via First.Last username only. Enter RSA PASSCODE:

When there at least 3 bars shown on the right side of your token display, enter the 6 digit code on the screen. If there are less than 3 bars, wait until the code changes. The system will then ask you to define a 5-8 character alpha-numeric PIN number. Select a PIN number and enter it, then re-enter it to confirm your PIN when asked. To complete this process, the system will prompt you to enter your RSA passcode.

Enter RSA PASSCODE: At this time, enter your PIN+RSA code. If the code on the RSA token is the same you used to initially login, you must wait for the code to change before completing this step. All future logins will require that you enter your PIN+RSA code to authenticate.

3) Creating an Authentication Certificate After you have successfully authenticated with your PIN+RSA code, you will be asked to create an authentication certificate. This certificate is used across the RDHPCS program and is used for internal system authentication as well as data transfer for some transfer tools between RDHPCS sites. Follow the instructions provided on the screen to complete this process. The passphrase must be at least 3 words (for now, DO NOT USE ANY SPECIAL CHARACTERS e.g. ‘”*#, etc.), each word separated by a space. It would be good to use a phrase that is complex, but easy to remember. The passphrase is only needed in two cases. First, if you do not login every 30 days, you will be asked for your passphrase. Second, every 12 months, your master certificate needs to be regenerated and you will need your passphrase to do this.

4) Confirming success If you get to the point where the login process is trying to actually log you into the system then the preceding steps have been successful. However, since your certificate will not have been validated, this is as far as you can go. Wait for an email that tells you that your certificate has been signed. When you have reached this point, you will be prompted for a password. The certificate needs to be validated by an administrator which can take up to 1 business day. If you haven’t received an email after one business day, please try to continue with Step 5 and if the process still requests a password send an email help request.

5) After receiving your confirmation that your certificate has been signed (or waiting a business day), you can now login using the hostnames listed above. When you have successfully logged in and your certificate is activated, you will message similar to: You will now be connected to NOAA RDHPCS: Jet system Hit ^C within 5 seconds to select another host. After a few seconds, you will be at the system prompt. If you have any problems with this process please email rdhpcs.aim.help@noaa.gov. If you have any questions about the system or other RDHPCS issues, please email rdhpcs.help@noaa.gov. Documentation for the systems can be found at https://wiki.rdhpcs.noaa.gov. To access the RHPCS wiki, use your email credentials to login and authentication (NEMS name and password).

From:
https://rdhpcs-common-docs.rdhpcs.noaa.gov/wikis/rdhpcs-common-docs/ - **RDHPCS-Common-Docs**

Permanent link:
https://rdhpcs-common-docs.rdhpcs.noaa.gov/wikis/rdhpcs-common-docs/doku.php?id=new_user_activation&rev=1478192344

Last update: **2016/11/03 16:59**