NAP Account Information

10/2016

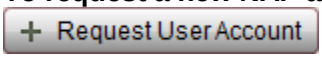
The NESS (National Enterprise Support Service) Application Portal (NAP) is used to manage user application log on account information. Once an account exists in NAP, it can be brought into Enterprise by an Account Manager. Roles will be assigned according to the duties the user is expected to perform.

Requesting New Accounts:

Users need to establish an account in NAP to log into e-ISuite Enterprise. A unique e-mail address is needed for the user plus contact information of the person to verify the account (i.e. Supervisor; local Incident Business person).

Click here to go to the NAP webpage: https://nap.nwcg.gov/NAP/

For step-by step instructions for requesting a new account, please see the Quick Reference Card NAP Account Request Instructions.

To request a new NAP account, on the upper right of the NAP log in screen, click the 

button.

For emergency account requests, Account Managers can contact the IIA Helpdesk at 866-224-7677.

After submitting an account request, the user will receive an e-mail with a temporary password and another e-mail with their user name.

The user should log on to NAP using the account information received through e-mail. As soon as the user logs on, they will be prompted to reset their temporary password. **NOTE:** The temporary password *must* be changed to a password the user establishes before the user account can be brought into Enterprise and roles assigned. The password rules follow:

NAP Password Requirements:

- Minimum Length = 12 characters.
- Maximum Length = 32 characters.
- Must contain at least one upper case alpha character (A-Z).
- Must contain at least one lower case alpha character (a-z).
- Must contain at least one digit (0 - 9).
- Must contain at least one special character **!@#$%^*** (Do not use< > or &)

NAP Password Policy:

- Twenty-four unique new passwords must be created before an old password may be reused.
- Standard Account Passwords expire after 90 days.
- Privileged Account Passwords expire after 30 days.
- "Password will expire in X days" warning is displayed for the 10, 5, 4, 3, 2, 1 day(s) prior to expiration.

Accounts are locked after 5 failed login attempts per session. There will be a 15 minute lockout before the user may attempt to log on again. In order to reset their passwords, users must establish security challenge questions - follow the steps below.

Users will need to contact the IIA Helpdesk to have their NAP passwords reset if the challenge questions are not established and their passwords expire

Security Challenge Questions:

Establishing security challenge questions in NAP will allow the user to reset a forgotten password. This is important to set up because an Account Manager cannot reset a NAP password. On the NAP Homepage, click on the person shaped icon  on the left of the screen. A window labeled Edit Standard (or Privileged) User Account will display.

- At the upper right of this screen is a button labeled **Challenge Questions.** Click on this button and the screen to Set Challenge Questions displays. Provide answers to three questions and then click on Save.
- Users may set or reset their security profile challenge questions any time they are logged into NAP.
- Click on Back to return to the Edit User Account screen, where the password can be changed.

After the challenge questions are established, to reset a forgotten password, click on the "Reset" button to the right of the Password field on the NAP Homepage. A temporary password will be sent to the e-mail account on record. Log in with the temporary password, select the Manage (person icon) button, and change the password on the Edit User Account screen.

Changing an Unexpired Password

To change a password that is about to expire (but is **not** expired), click on the link in the email advising that the password will expire in X days (or simply access the NAP webpage). Enter the current user name and password. Click on the Manage (person icon), and enter the current password, then enter a new password, verify the password, and click on Save. A message advising that the password has been changed will display.