ICBS-R Account Management Process

Updated 7/11/2013

The Basics

For a user to log into ICBS, a person needs password-protected access to both the "NESS Application Portal" (NAP) at NITC and to the ICBS application itself. To the user, it's a single sign-in, but it requires both a NAP account and an ICBS application account.

NAP user accounts are requested individually by each ICBS user via the NAP website https://nap.nwcg.gov/NAP/.

ICBS application accounts are created by a "Cache Account Administrator" (CAA) when new employees require ICBS access. The ICBS application account exactly matches the user's NAP account.

(Note: network accounts that enable a scan gun user to log onto a wireless local area network [WLAN] at a cache were created prior to the implementation of each cache, and are not addressed in this document)

Account Management Responsibilities

Management of ICBS application accounts (account creation and deactivation) are the responsibility of the Cache Account Administrators at each cache.

At least two CAAs are designated by a Cache Manager and receive specific training to perform their additional duties. CAAs manage individual accounts for *all* users at their cache regardless of whether they access the system via a PC (ICBS "console" users), a scan gun, or both. All CAAs must be "personal identity verified" (i.e. they must possess a government-issued ID).

For each user, a NAP account is created first; then the ICBS application account. The actual creation of new NAP accounts and account deactivation is performed by members of the FS Fire & Aviation Management IT group at NIFC, and by trained ICBS Helpdesk agents.

Pre-requisites for User Accounts

Before a user can access a government information system, the CAA at his or her cache needs to ensure that the users have completed a mandatory agency Security and Privacy course for the current fiscal year

It's the responsibility of the CAAs to ensure that each user (FS, other agency, or AD/EFF employee) provides a security/privacy course completion certificate *before* an ICBS application account is created. The online security/privacy courses are available through the FS and BLM for FS, BLM,

state agency and contractor personnel). Agency IRM specialists can provide online links for this training.
The CAA needs to keep hard copies of these training certificates on file for each user at their cache. These can be audited at any time by the FS Office of Chief Information Officer (CIO) or the Fire & Aviation Management Information System Security Officer (ISSO).

Rules of Behavior (ROB) agreements are verified by the user as part of their NAP account request process, so CAAs no longer have a role in maintaining this documentation.

Requesting New User Accounts
Instructions for requesting a new NAP account can be found at:
http://ross.nwcg.gov/quick_ref/How_to_request_a_NAP_User_Account.pdf

Here are a few additional tips:

- A unique email address is required for each ICBS user (e.g. agency email, personal email, or cell phone text email account such as [10-digit phone #]@vtext.com for Verizon cell phone users). This is where they'll receive information on their new NAP account and password.
- When prompted on the NAP site for their agency organization unit the user should enter their agency organization, *not* the name of their cache. For example:
    - Alaska Fire Service Resources (US-AK-AKD)
    - Billings Field Office (US-MT-BID)
    - Custer National Forest (US-MT-CNF)
    - Gila National Forest (US-NM-GNF)
    - Idaho Panhandle National Forest (US-ID-IPF)
    - Okanogan/Wenatchee National Forest (US-WA-OWF)
    - Daniel Boone National Forest (US-KY-DBF)
- When the new user is prompted on the NAP site for *"contact information for the manager or supervisor who will verify your request*," they should enter the info for a CAA at their cache.

Upon receipt of a new NAP account request, a NAP administrator will email the person entered as the CAA to confirm whether or not the requested NAP account should be created. Once created, the NAP account ID and password will be emailed to the user. At no time should the CAA know, or ask for, a user's password.

The user will provide their new NAP account ID to their CAA, who will create the ICBS application account for them. The CAA will also assign their specific user role(s). Now the user is ready to log-in.

The user logs in to the NAP site https://nap.nwcg.gov/NAP/ and changes their temporary password to a new one. For ICBS users, the asterisk (*) is the only special character recommended for passwords because it’s the easiest one to enter on a wireless scan gun. This ensures that the password will work regardless of which device a user is authorized to operate.

From here on, ICBS users log in to ICBS via the NAP log-in screen (https://nap.nwcg.gov/NAP/) so it’s suggested that they save or bookmark it in their Internet Explorer to make it easy to find.

Passwords

Password expiration for standard user accounts is set at 60 days (30 days for privileged accounts). When a user's password is within 10 days of expiring, they will begin receiving automated password reminder email messages from NAP.   These are sent to the address they provided when requesting their account. If a user receives a message saying their password is about to expire, they should log in to NAP to change it.

If a user happens to miss the notifications, they have until 30 days past the expiration date to go into the system and reset the password by typing their user name and clicking on the “**?**” icon next to the password box. The system will “ask” one of the user’s security questions. When the user answers it correctly, the system will automatically reset and email the user a new temporary password.

If, on the other hand, the user doesn’t reset their password within 30 days after it’s expired, he or she will need to contact the IIA Helpdesk and request a password reset. The Helpdesk can be reached at: helpdesk@dms.nwcg.gov or 1-866-224-7677.

CAA Accounts

ICBS Cache Account Administrator user accounts are considered privileged access accounts. The NAP accounts and ICBS accounts associated with these privileges are uniquely identified with an “ad.” prefix, and enable the user only to conduct account management tasks for their cache in ICBS.

Users with these privileges will typically have a CAA user account and another standard account to conduct all other cache business for which they are authorized (e.g. Cache System Administrator, Supply Tech, etc.).

Cache Account Administrator accounts are considered privileged user accounts. These accounts are required by policy to expire every 30 days.

NWCG-All Accounts

Another special ICBS application account type is the “NWCG-all” account. This account is used by just 1 or 2 people to make changes that affect the whole ICBS system across the enterprise (e.g. maintain the NFES catalog, add new caches, etc.). This requires a privileged NAP account as well.

If a person with an NWCG-all account in ICBS also has standard and privileged accounts for their cache-specific work, then they will have three NAP accounts:

1. Standard cache account
2. Privileged Cache Account Administrator account
3. Privileged NWCG-all account

NWCG-all accounts are also required by policy to expire every 30 days

Account Deletion or Deactivation

This process is essentially unchanged with NAP. Making sure that user accounts are deleted or deactivated when no longer needed is equally important as creating accounts. If it is suspected that a password has been lost or compromised, it will be treated as a security incident and addressed accordingly. Incident response and handling are outside of the scope of this document.

If an employee is terminated, released, or is reassigned to a position in which they will no longer require access to ICBS at a particular cache, the CAA must delete or deactivate their ICBS application account, and request through the IIA Helpdesk that their NAP account also be deactivated.

If the employee is *not* expected to require ICBS access in the future, their ICBS application account should be *deleted*. Here's how to *delete* an ICBS account:

- From the ICBS menu select Configuration > Launch Configurator
- Once in the Configurator, select Applications > Platform > Security > Users
- Search for the user by entering the user ID (or by querying all users for the cache)
- Select the user account by clicking on the user information in the Search Results panel, and click on the delete icon (red X)

If the employee *is* expected to require ICBS access sometime in the future, their ICBS application account may instead be *deactivated* (deactivating the account retains the user group assignments when the CAA reactivates the account sometime in the future). Here's how to *deactivate* an ICBS account:

- From the ICBS menu select Configuration > Launch Configurator
- Once in the Configurator, select Applications > Platform > Security > Users
- Search for the user by entering the user ID (or by querying all users for the cache)
- To deactivate a user account, double click on the user information in the Search Results panel and access the user details

- Uncheck the active box and click on SAVE

NAP accounts can't be deactivated, they can only be removed. When any employee is laid off at the end of their tour (e.g. AD/seasonal/term/ temporary/career part-time/WAE employee, etc.), their NAP account needs to be removed regardless of whether or not there's an expectation that they'll be rehired at a later date.

The CAA makes this "NAP account removal request" via an e-mail message to the IIA Helpdesk (helpdesk@dms.nwcg.gov). The following user information needs to be included in this request:

ACCOUNT (USER) ID
FIRST NAME
LAST NAME

To eliminate the potential for a person who no longer requires access from causing harm to system data or cache operations, **CAAs need to request removal of NAP accounts within 5 business days of the person's change of status.**

In the case of an involuntary separation of an employee, application accounts shall be deleted and NAP accounts shall be removed as the terminated employee is being notified of the termination or immediately thereafter. This is to ensure that the terminated employee can cause no harm to system data or cache operations.

Accounts for Users Assigned to another Cache

This process is essentially unchanged with NAP. Cache personnel often are assigned to a cache other than their own during increased incident activity or while on details. If they need to log in and perform ICBS work as a cache user at another cache, their home cache CAA needs to first delete their application account.

The CAA at the cache at which they're temporarily working then needs to create a new application account for them. The "temporary cache CAA" will also need to give them roles specific to the work they'll be doing by assigning them to the corresponding "user groups."

Their LDAP account does not change, so once their home application account is deleted and their temporary cache application account is created, they can log in as they normally do to work on the temporary cache's inventory.

Upon release to their home cache, the CAA at the temporary cache will delete their application account, and the home cache CAA will recreate their original home application account. A user cannot simultaneously have an application account at more than one cache.

Account Management Tracking

Cache Managers and Cache Account Administrators (CAAs) play an integral role in ensuring that ICBS is secure from unauthorized access. Cache Managers may be asked to provide specific account management information for users in their cache during annual security assessments, and during spot security audits conducted by the ISSO. In order to be able to provide accurate information, it's strongly suggested that each cache maintain a running log for all user accounts as shown below:

Cache ID	User First Name	User Last Name	User Account ID	Employee Type (FS, Other Agency, Seasonal/Temp or AD)	Date that Annual Agency Security/ Privacy Training was Completed	Date that New NAP Account was Requested by User	Date that New Application Account was Created	Application Account Created by (name)	Date of User Termination, Retirement or Transfer	Date that NAP Account Removal was Requested	Removal Requested by (name)	Date CAA was Notified that Account was Removed, if Known
RMK	John	Smith	jsmith	FS	6/30/2013	6/30/2013	7/1/2013	Jane Doe	9/1/2013	9/1/2013	Jane Doe	9/2/2013

Additional Resources for NAP Users:

Getting Started with NAP: http://ross.nwcg.gov/quick_ref/Getting%20started%20with%20NAP.pdf

Retrieving a Forgotten User ID and Resetting a Forgotten Password in NAP:
http://ross.nwcg.gov/quick_ref/Retrieve%20a%20user%20id%20or%20reset%20a%20password.pdf

Contact the IIA ("ICBS") Helpdesk: helpdesk@dms.nwcg.gov or 1-866-224-7677.