



TIP SHEET

Vendor Web Status

Video Link - Overview of entire process -----

Steps for Vendor Web Status Access

- 1. IROC Access - Authenticate using eAuth or Login.gov ----- Page 1
 - Request an iNAP profile ----- Page 2
 - Link with existing iNAP profile ----- Page 4
- 2. IROC - Vendor Web Status Request - auto created ----- Page 6
 - IROC - Vendor Web Request - not auto created ----- Page 6
- 3. Stating Equipment ----- Page 8

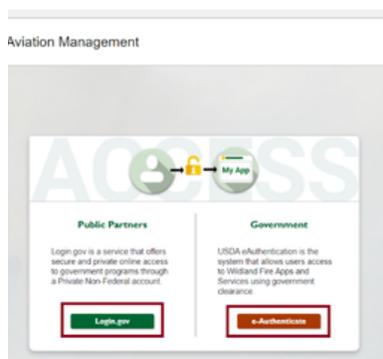
Troubleshooting

- o Helpdesk Information ----- Page 10
- o Helpful links ----- Page 10
- o If you have completed a step in the past or recently, please go to the next step or whichever step you are on. Many vendors got IROC access last year and you only need one account per user, per company.
- o Chrome is the preferred browser

1. IROC Access - Authenticate using eAuthenticate or Login.gov

From the FAMIT Dashboard (<https://famauth.wildfire.gov/>) Authenticate to the FAMIT Dashboard **using either eAuthentication (eAuth) or Login.gov** depending on which one you have. If you have both, use eAuth.

Note: If you do not have either of these types of accounts you will have to request a new one, which you can do by clicking on the links on the FAMIT dashboard, and then creating a new account. VIPR users will already have an e-authenticate account and can use that account for this process.



Login-Gov account creation

eAuth account creation

National Fire & Aviation Management is using Login.gov to allow you to sign in to your account safely and securely.



To sign up for IROC User Notices go to the following link:
<https://tinyurl.com/599tp6pf>

IIA Help Desk
 Toll-Free: (866)224-7677
 Local:
 (616)323-1667
<https://iiahelpdesk.nwgc.gov>



TIP SHEET

To access your Wildland Fire Application select one of the tiles below:

My Applications

View as: Logos Tiles



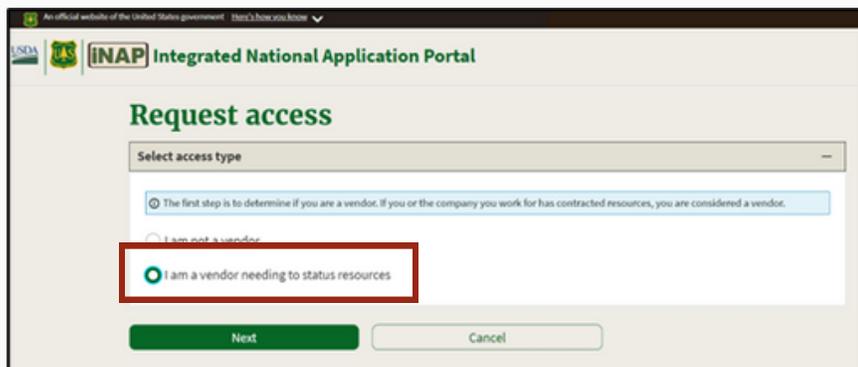
After logging in, you will be presented with a tile page of available applications. Click on the IROC tile to launch the application.

The first time you click on the IROC tile, you will be required to link your e-Authentication or Login.gov account to your iNAP profile. This will link the FAMAuth account to the iNAP profile. If you do not have an iNAP profile, you will need to request one at this point by choosing the **I do not have an iNAP profile yet** option. See Requesting an iNAP account below. Vendors that already have an iNAP profile may proceed to the "link account with existing iNAP profile" on page 4 of this document.

Requesting an iNAP profile



After choosing the **I do not have an iNAP profile yet** and clicking **next**, you will need to select if you are a vendor or not.





TIP SHEET

Clicking next will bring up the User Information window. Fill in the required information. Choose **Contractor/Vendor** for Primary affiliation. Please input your company **DUNS/UEI** number then click **Next**.

Once you click next, you will get the “Rules of Behavior” screen. Read these and select **Accept**.

On the Application Access portion choose IROC – Interagency Resource Ordering Capability and for the **Instance(s)** choose **PROD (Standard)** - **this may be already pre-selected**. Enter your **contracting officer’s** information for the Contacts name, Title, Phone Number, and email. Then click **Submit**.



TIP SHEET

Confirm additional access

Do you want to request access to another application?

If so, select Yes to return to the request form and use the + button to request additional application(s).

Yes

No, submit my request

Click **No, submit my request**.

Note: You will see the below page display. You have successfully requested a new iNAP profile that will be connected to your new Login.gov or eAuth account.

Leaving iNAP

Please return to FAMAuth to continue.

For increased security, please close your browser window.

You have now requested your iNAP profile and will need to wait for it to be approved. Please note, this can take up to 3 business days to occur. Also, if you do not have an active contract in IROC, your request will not be approved until you have a contract. **Once approved you will receive 3 emails from donotreply@nwcg.gov**. After you receive the emails, you will be able to proceed.

Emails from donotreply@nwcg.gov:

- o iNAP User Account Information (Username) keep this one
- o iNAP User Account Information (Temporary Password) - you will receive this if you request a reset of your password.
- o Application Access for IROC-PROD Approved

Login to <https://famauth.wildfire.gov> again and click on the IROC tile.

Link profile with existing iNAP profile

Once your new iNAP profile is approved or if you have an iNAP profile already, choose the **I have an iNAP profile already** button.

Link with iNAP

As a final step in verifying your access to OIS-PROD, FAM-IM Security requires that your eAuthentication or your Login.gov account (or both) be linked to your iNAP profile.

I do not have an iNAP profile yet

I have an iNAP profile already

Next



TIP SHEET

Enter your iNAP Primary email address, and select Submit.

Note: iNAP will email your PIN to the email address provided. The email will come from donotreply@nwcg.gov

Find my iNAP profile

My iNAP e-mail address

Submit Cancel

Enter your PIN that was emailed to you and select **Submit**.

Enter your PIN

A temporary PIN has been sent to julie.johnson@bylighthouse.com.

PIN

Submit Get another PIN Cancel

Review your profile for accuracy, and select **Save**

Note: If logged in via Login.gov then under “Linked accounts” it shows you have linked your Login.gov account with your iNAP profile. If logged in via eAuth then under “Linked accounts” it shows you have linked your eAuth account with your iNAP profile.

Linked accounts

eAuthentication (not-linked)	Login.gov (linked)
E-mail	E-mail
Identity provider ID	Identity provider ID

Rules of behavior

Current type: Non-Forest Service Standard

Recent acceptance history

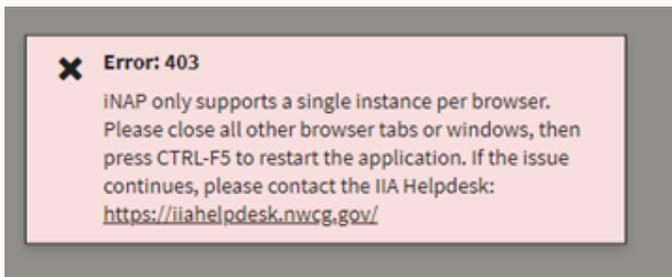
Rules of behavior type	Acceptance date
Non-Forest Service Standard	11/29/2021
Non-Forest Service Standard	11/18/2020
Contractor	10/08/2020

Save Cancel



TIP SHEET

Note: A known error message pops up if you still have another tab with iNAP open while trying to link your iNAP to your Login.gov or e-Auth account. Close the other tab that has iNAP open and you will be able to proceed, however you may need to refresh the browser.



2. IROC - Vendor Web Status Request

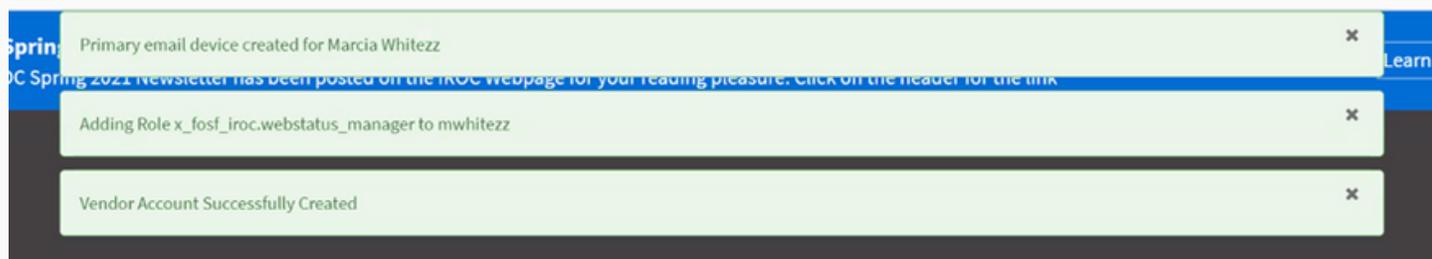
You will need to have completed step 1 and logged into the FAMIT dashboard (<https://famauth.wildfire.gov/index.html>) using either your eAuth account or your login.gov account and have linked your account through iNAP to complete the steps below.

There are two different ways to get a Vendor Web Status account in IROC.

- Your account will be auto-created if you entered a UEI when submitting your iNAP request and you have an active contract and resources.
- If you did not enter a UEI, or if you have no active contract or resources, your account will not be auto-created and you will need to submit a new access request in IROC.

IROC Vendor Web Status access was auto created - Proceed to Step 3.

If your account was auto-created you will see similar messages the first time you log into IROC.

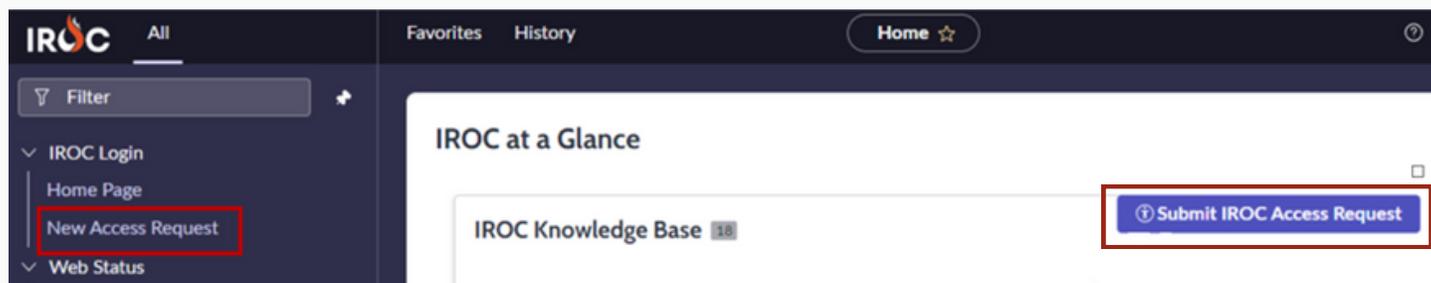


IROC Vendor Web Status access was NOT auto created -

Once you have clicked on the IROC tile Access link, the below page will appear. You will need to enter a **New Access Request**. You can use either of the options below.



TIP SHEET



A new screen will appear - see below. Under “Which type of access you’re requesting?” choose **Vendor Web Status** from the dropdown.

Under the “Please select your vendor organization.”, you can either start typing your company name or you can click on the magnifying glass and look for your company that way. Note: The spacing, punctuation and spelling are all specific, so use the name on your contract.

You can put in comments if you would like, but that is not required.

Click the **Submit** button when your information has been entered.

Submit a request to grant access to IROC.

Submit a request to grant access to IROC.
Please fill out the form and select the appropriate access type you're requesting for.
NOTE: A Dispatch Manager access also includes a "Dispatcher" access. You don't need to submit a separate request for each type.

Requested For
Elise Hawes

* Which type of access you're requesting?
More information
Vendor Web Status

* Please select your vendor organization.
A & A PORTABLES, INC.

Comments

Submit

Your request will have to be approved by an IROC Application Representative, not your local dispatch center, to ensure the request is correct and that it isn't a duplicate. This process can take up to 3 business days. You will get an email when your access request has been approved.

Proceed to Step 3.



TIP SHEET

3. Statusing Equipment

Once your Vendor Web Status Access request has been approved, login into IROC through the FAMIT Dashboard <https://famauth.wildfire.gov/> with your Login.gov or e-Authenticate account.

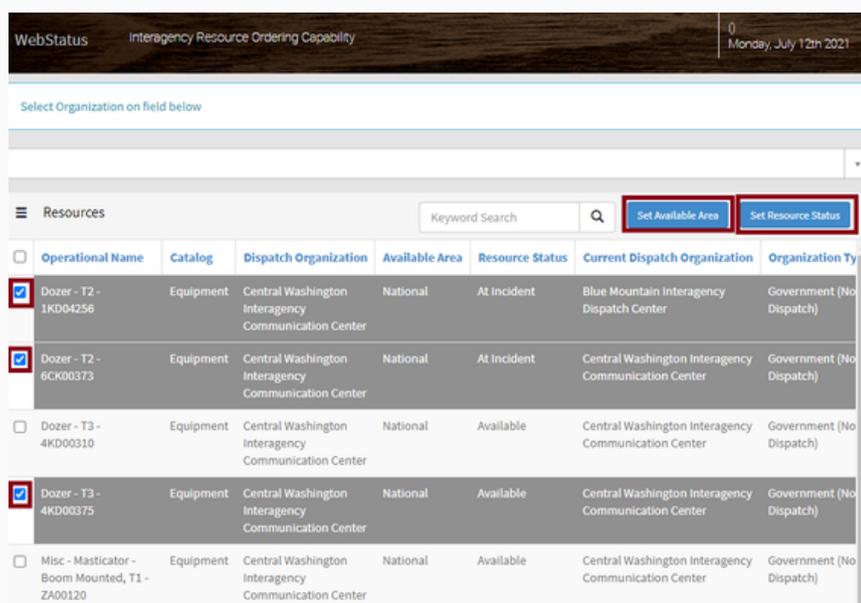
When you log into IROC there is a box on the right side of the screen labeled Web Status Resource Manager that will take you directly to your resources or you can click on the all button at the top of the screen and type in the word “**Web**” in the filter box which will bring up the Web Status Resource Manager option.

There are useful documents for assisting in the web statusing process on this screen under IROC Knowledge Base.



Once you click on **Web Status Resource Manager**, a new window will pop-up. This is the window that will allow you to status your resources.

You can multi-select your resources using the check boxes on the left side of the screen. Then choose either the **Set Available Area** button or the **Set Resource Status** button.



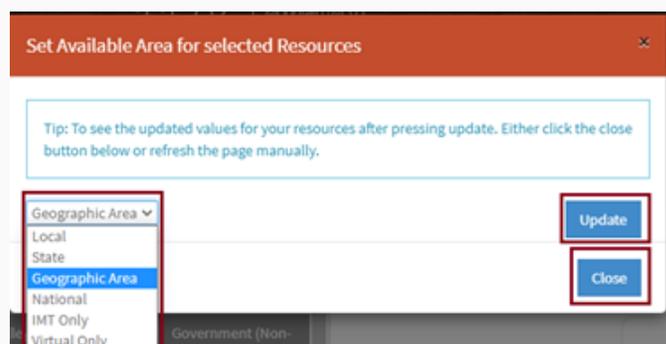


TIP SHEET

Set Available Area

In the pop-up box, choose Local, State, National, or GACC from the drop-down. Then click Update, and then click close.

- Local - Resource is available to the dispatch area that your resource is contracted under.
- State - Resource is available to the state your resource is contracted in.
- Geographic - Resource is available to the Geographic area your resource is contracted in. Picture of geographic areas to the right.
- National - Resource is available to anywhere in the Nation.
- IMT Only and Virtual Only apply to Overhead resources only.



Set Resource Status

In the pop-up box, choose either Available or Unavailable. Then click Update and then Click close.

Note: If your resource is at an incident, mob enroute, demob enroute, etc. it will show that way in resource status and you will not be able to update its availability. If your resource is showing "returned form assignment" it will be unavailable until you change its status.

Note: Some pieces of equipment have more than one contract and can be different types of resources. If that is the case, they will not show up individually, the primary qualification will show in the list of resources but if you highlight the resource and look on the right side of the screen and click the qualifications tab, it will show what that resource is contracted as.



TIP SHEET

Q Set Available Area Set Resource Status

Central Washington Interagency Communication Center	Government (No Dispatch)
Central Washington Interagency Communication Center	Government (No Dispatch)
Central Washington Interagency Communication Center	Government (No Dispatch)
Central Washington Interagency Communication Center	Government (No Dispatch)
Central Oregon Interagency Dispatch Center	Government (No Dispatch)
Central Washington Interagency Communication Center	Government (No Dispatch)
Central Washington Interagency Communication Center	Government (No Dispatch)
Central Washington Interagency Communication Center	Government (No Dispatch)

Dozer Type 3 - Duke, Andrew - 4KD00375 - D5HTSKCAT2 - (WA-CWC)

Dispatch Organization: Central Washington Interagency Communication Center

Available Area: National

* Home Unit Organization: Duke, Andrew

Home Location:

* Resource Status: Available

Record Manager Contact: VIPR Resource

Related Lists: DPL Agreements 1 Resource Assignments 1 Resource Unavailables Qualification 2 Contacts 4

Resource Qualifications

Catalog - Category - Item	Primary	Qualification Type	Dispatch Level	Incident Type Endorsement
Equipment - Misc - Pumper Cat, T2	false	Qualified	NWCG Qualified	Wildland Fire
Equipment - Dozer - T3	true	Qualified	NWCG Qualified	Wildland Fire

Troubleshooting and Links

Helpdesk Information

Webpage: <https://iiahelpdesk.nwcg.gov/>

Toll-Free: 866-224-7677

Helpful Links

iNAP: <https://nap.nwcg.gov/NAP/>

FAMIT Dashboard: <https://iwfirp.nwcg.gov/index.html>

Login.gov: https://secure.login.gov/?request_id=1168e209-5984-4102-83df-c1a61a1954f2



TIP SHEET

Dispatch - Rejecting wrong type of access requests

In DMT, people with Dispatch Manager Access can approve most types of access requests. Sometimes users put in for the wrong type of access. The IROC SME's approve all vendor requests, so if you get a different type of an access request for a vendor, please reject the request, and ask them to put in for Vendor Web Status. The most common request we have been seeing is, self-status.

In DMT go to the **My Organization Approvals**. This screen will have access requests that have come in for resources in your center. You will want to look at the ones that have a Status of **New**.

Dispatch Manager User is Cheryl Dickson .or. Dispatch Organization IROC Organization is Cody Interagency Dispatch Cent
> Status = New

Number	Requested For	Access Type	Status	Dispatch Organization
IRQ0011311		Dispatcher	New	Cody Interagency Dispatch Center
IRQ0011271	IROC Dispatcher	Self-Status	New	Cody Interagency Dispatch Center
IRQ0011138		Dispatcher	New	Cody Interagency Dispatch Center
IRQ0011312		Self-Status	New	Cody Interagency Dispatch Center

Click on the information icon of the request to manage the request. If a user has requested the correct access you can click the approve button. If they have not requested the correct access use the **Additional Comments** section to let them know why you are rejecting the request and then click the **Reject Request** button.

Example for Vendors that request the wrong access to IROC:

It appears you are a vendor, so this request has been rejected. Please submit a new request for Vendor Web Status.

Request - IRQ0014346

IROC Admins can override approvals.

Number: IRQ0014346 | Status: New

Requested For: Joshua O'Connor | Access Type: Self-Status

Dispatch Organization: Columbia Cascade Communication Center | Approved/Rejected By: [Empty]

Dispatch Manager: Scott Eubank | Active:

Additional Comments: It appears you are a vendor, so this request has been rejected. Please put in a new request for Vendor Web Status

Buttons: Update, Approve Self-Status, Reject Access



TIP SHEET

Magnifying glass is grayed out

If you've noticed that the magnifying glass on some DMT pages is grayed out, here is the reason why.

The screenshot shows the MemorialCare Health System DMT interface. The top navigation bar includes the MemorialCare logo and the text "Excellence in Health Care". Below the navigation bar, there is a search bar with the text "my groups" and a magnifying glass icon that is grayed out. To the right of the search bar, there are buttons for "Tasks", "New", "Go to", and "Updated". Below the search bar, there is a filter section with a magnifying glass icon and the text "All > Assignment group = (MHS ServiceN...". Below the filter section, there is a table with columns for "Number" and "Priority". The table contains four rows of task data:

Number	Priority
TASK0056822	3 - Medium
ENHC0010033	4 - Low
ENHC0010032	4 - Low
ENHC0010031	4 - Low

The screenshot shows the MemorialCare Health System DMT interface. The top navigation bar includes the MemorialCare logo and the text "Excellence in Health Care". Below the navigation bar, there is a search bar with the text "Number" and a magnifying glass icon that is grayed out. To the right of the search bar, there is a button for "New" and a "Go to" dropdown menu. Below the search bar, there is a filter section with a magnifying glass icon and the text "All > Task type = Incident .or. Task type = Problem". Below the filter section, there is a table with columns for "Number", "Priority", and "Sta".

To sign up for IROC User Notices go to the following link:
<https://tinyurl.com/599tp6pf>

IIA Help Desk
 Toll-Free: (866)224-7677
 Local:
 (616)323-1667
<https://iiahelppdesk.nwcg.gov>



TIP SHEET

IROC/ICBS INTERFACE TIPS & FAQs

- **What are ICBS and this interface all about?**
 - The “Interagency Cache Business System” is an inventory management system used by NFES National Interagency Support Caches. The system interfaces with IROC. The interface goes both ways. Requests created in IROC can be placed to a Cache and requests created in ICBS can be sent to IROC. In addition, when requests are processed by an ICBS user (whether it was created in IROC or in ICBS), ICBS will communicate the actions taken to ROSS.
- **Why would a cache create a request to send to ROSS?**
 - The cache may receive a request from an incident that is ordering direct to the cache. While the cache would fill the order, they can send the request to IROC for record keeping purposes.
- **I sent a request to the cache but they don't see it. Why?**
 - Before ICBS can accept a request from ROSS, the incident host and unit ID must be entered in ICBS. Most hosts ID's have been entered, but occasionally one is missing. This causes a failure in ICBS and the ICBS data base administrator must enter the organization before ICBS will see the request.
- **Why can't I make a request using the 100,000 numbers?**
 - IROC now automatically creates a user-issued request number block for supplies on each incident. This block encompasses requests S-100,000 through S-199,999. This request block will be used in Phase 2 to prevent ICBS from creating duplicate request numbers in ROSS. Incidents will use these numbers when they have been authorized to communicate requests directly to the cache. ICBS will also use this block when processing approved replacement requests. This block is not displayed on the New Request screen and may not be changed or deleted by the ROSS user.”
 - A block of supply numbers (100,000 - 199,999) is automatically set aside on all incidents for incident to cache direct ordering. This block is available to the cache for use when an incident is ordering directly to the cache. Those incidents will maintain control of the request numbers and direct the cache on which number to assign to a request. The cache is not assigning the requests numbers but does the data entry as directed by the incident. The dispatch office will not see these numbers unless entered by the cache and attached to an incident in ROSS. Incidents using ROSS will proceed as normal when placing requests to a cache.