Accounts

IMCOM Enterprise Web

Tutorial 5

Version 5.2 (January 2021)

Standard Operating Procedures

Contents and general instructions

Pages:

General instructions:

This tutorial contains guidance for setting up user accounts and sets out requirements for account maintenance. The topic integrates closely with Tutorial 6, "Permissions." This document takes you from user requirements to creating User Groups and Group Sets. Our permission system relies on this structure.

For each subpage, make groups to define the roles of the participants. Make a group set for the subpage, and also add the Admin group to the Page Manager group set and add the Contributors group to the Page Contributors group set.
Grant permissions to Group Sets whenever possible, and control access via group membership.

IMCOM Enterprise Web documentation can be found on IEW Pro Central, https://homeadmin.army.mil/imcom/index.php/contact/webmaster-1/pro-central
These tutorials also serve as SOP for IMCOM Enterprise Web.
NOTE: TWO-LETTER CODES in some examples are left over from a previous naming convention. They no longer need to be used.
See the last page for a list of tutorial/SOPs

IMCOM GUIDELINES:
The dark gray boxes are policy reminders.

Blue boxes offer helpful explanations

New or substantially changed pages

Important policy and version notes

IMCOM POLICY

When you set up a page contributor or manager account

- **Do not put expirations on the accounts themselves. Instead, rely on the expiration of the permission set (see Page 15 and Tutorial 6) to lock the account.**
- **No group/shared accounts are allowed. If more than one person in an office needs access to your web page, each person will have his/her own account.**
- **Do not delete any accounts. Disable them instead.**
- **Do not disable “admin,” “DBadmin,” “imcom” or “Neal.Administrator”**

Checklist: Setting up pages and accounts

Granting permission for programs or tenants to run their own subsites helps everybody share in the maintenance of the whole. The following checklist should help you start them successfully:

Checklist:

- ❑ Make the page (Tutorial 2)
- ❑ Create Page Manager, Page Contributor and Text Editor user groups (Page 15, Tutorial 8)
- ❑ Make a Page set (and Manager and Contributor sets if they don't exist)(Tutorial 8)
- ❑ Go into the new page and update permissions according to the recipe (Tutorial 8)
- ❑ Create a file folder to associate with the page and adjust the permissions for the folder (Tutorial 8)
- ❑ Make user accounts (if they don't exist) for the people who will edit the page (Page 8)
- ❑ Associate the accounts with the appropriate user groups (Page 15, Tutorial 8)

IEW Contributor roles

Role	Overview	Access to unreleased information	Authorized to create temporary accounts	Clear-ance	Training required	Assigns membership to these groups / accounts
CMS Administrator/ Manager	Access to application, limited access to data center. Manages the Concrete5 application and controls access for end users (Garrison and site Managers and contributors)	Yes	Authorized to create temporary accounts	Secret	OPSEC Level II	Garrison Manager, Site manager
Garrison Manager	Access to application (end user). Manages content, access and privileges within a garrison site. Granted additional permission on a case-by-case basis. *Typically garrison PAO or NEC*	Yes (within scope of responsibility)	Authorized to create temporary accounts on the garrison site	Secret	OPSEC Level II	Page Manager, Page Contributors, Text Editors
Site Manager	Access to application (end user). Manages content, access and privileges within a garrison site. *Typically garrison PAO*	Yes (within scope of responsibility)	Authorized to create temporary accounts on the garrison site	Secret	OPSEC Level II	Page Manager, Page Contributors, Text Editors
Page Manager	Access to application (end user). Manages content and occasionally access within a section of a garrison site. *Tenant PAOs, Directorates with publishing authority*	Yes (within scope of responsibility)		Secret	OPSEC Level II	
Page Contributor	Access to application (end user) Edits content within a garrison site without publishing priviliges. *Editors within a tenant or directorate.*	Yes (within scope of responsibility)		None	Webmaster OPSEC	
Text Contributor	Access to a page or editable area. No publishing privileges. Supervised by Page Manager or Site Manager. *Editors within a tenant or directorate. Special case for Operations staff.*	No	Authorized to add very specific content	None	Annual Cybersecurity	

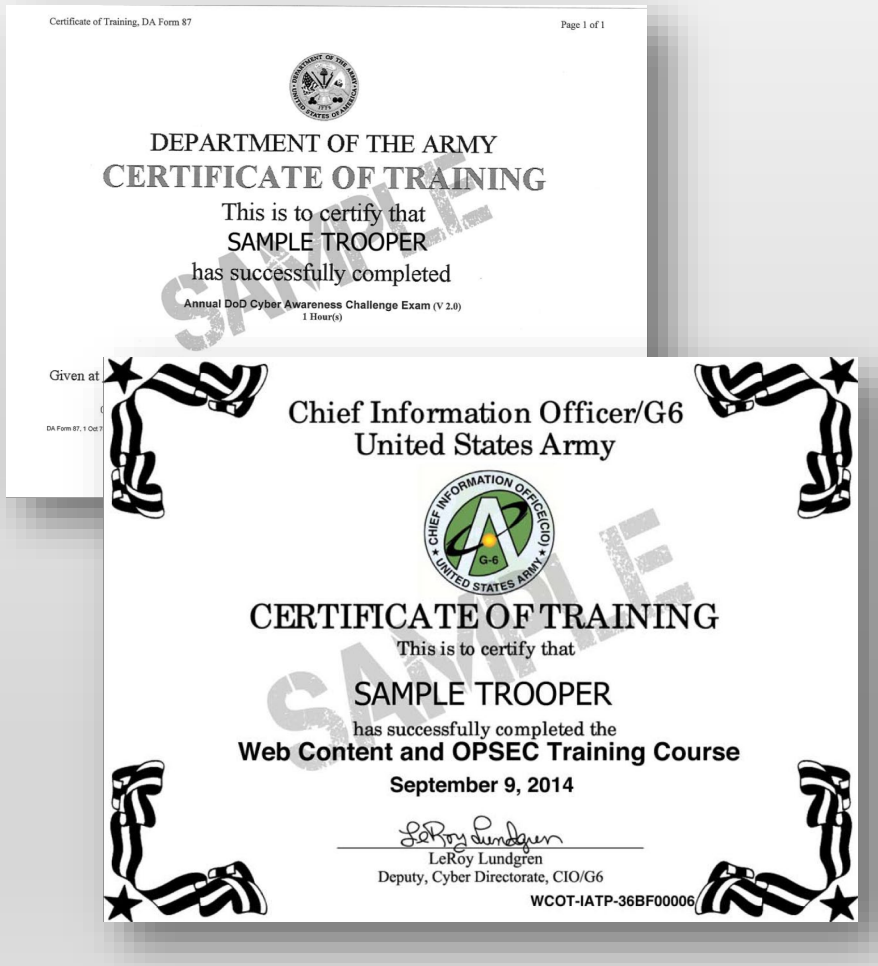
Minimum training requirements for contributors

IMCOM GUIDELINES:

To protect the operations security of the IMCOM Enterprise Web, every person allowed to log on must have at a minimum an up-to-date Cyber Awareness Challenge certificate. Page Contributors must also have a current certificate for the Web Content and OPSEC Traning Course. Those granted publishing rights ("Managers") must also have either OPSEC Level II certification or be CP-22/MOS 46A or Z.

Garrisons may add their own restrictions to these minimum guidelines.

Garrison PAOs will keep certifications on file for periodic review and send copies to the CMS Manger at IMCOM HQ PAO.



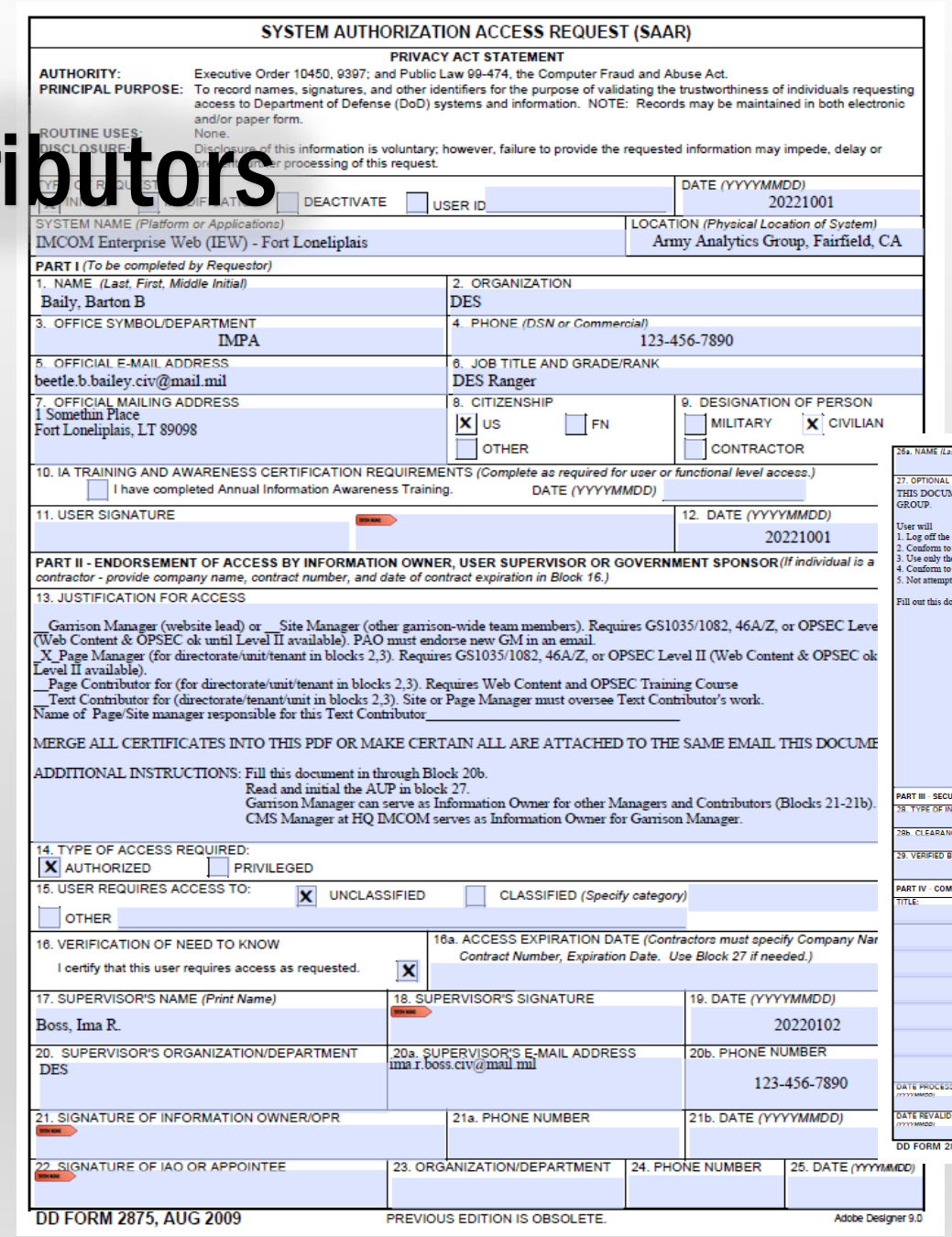
DoD Cyber Awareness Challenge Training (URL - https://ia.signal.army.mil/)
Complete Step 1: "DOD Cyber Awareness Challenge" then Step 2: Army Required Exam
1. Click Log in with CAC DoD-Approved Certificate Login
2. Update record
3. Select "DOD Cyber Awareness Challenge" to review the coursework.
3. Click Take Exam
4. Click Annual DoD Cyber Awareness Challenge Exam (must receive a 70 to receive certificate).

Web Content & OPSEC Training (URL- https://iatraining.us.army.mil/index.html)
The Web Content and OPSEC Certificatinon Training contains four lessons: a Web Content and OPSEC Intro Lesson, a DoD Web Guidance, a Web Content and OPSEC Lesson, and an Army Webmaster test. To receive the Certificate of Training for the Web Content and OPSEC Certification Training, students must take and pass two end-of-lesson tests and the final interactive Webmaster test (must receive a 70 to receive certificate).

Credentialing contributors

IMCOM standard:
Fill out and keep a 2875 for each person logged into the system. Use your local IA assets for blocks 22-25. Model forms are/will be downloadable from home.army.mil

- Fill in through Block 20
- Garrison Manager can be info owner (block 21)
- User should type initials below the AUP supplement in block 27 before signing
- Garrison may add requirements
- Send to CMS Manager with training certificates in a single email.



SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)

PRIVACY ACT STATEMENT

AUTHORITY: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.
PRINCIPAL PURPOSE: To record names, signatures, and other identifiers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form.
ROUTINE USES: None.
DISCLOSURE: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent processing of this request.

TYPE OF REQUEST: [X] INITIAL [ ] MODIFICATION [ ] DEACTIVATE [ ] USER ID
DATE (YYYYMMDD): 20221001

SYSTEM NAME (Platform or Applications): IMCOM Enterprise Web (IEW) - Fort Loneliplais
LOCATION (Physical Location of System): Army Analytics Group, Fairfield, CA

PART I (To be completed by Requestor)

1. NAME (Last, First, Middle Initial)	2. ORGANIZATION	
Baily, Barton B	DES	
3. OFFICE SYMBOL/DEPARTMENT: IMPA	4. PHONE (DSN or Commercial): 123-456-7890	
5. OFFICIAL E-MAIL ADDRESS: beetle.b.bailey.civ@mail.mil	6. JOB TITLE AND GRADE/RANK: DES Ranger	
7. OFFICIAL MAILING ADDRESS: 1 Somethin Place, Fort Loneliplais, LT 89098	8. CITIZENSHIP: [X] US [ ] FN [ ] OTHER	9. DESIGNATION OF PERSON: [ ] MILITARY [X] CIVILIAN [ ] CONTRACTOR

10. IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS (Complete as required for user or functional level access.)
[ ] I have completed Annual Information Awareness Training. DATE (YYYYMMDD):

11. USER SIGNATURE [SIGN HERE]
12. DATE (YYYYMMDD): 20221001

PART II - ENDORSEMENT OF ACCESS BY INFORMATION OWNER, USER SUPERVISOR OR GOVERNMENT SPONSOR (If individual is a contractor - provide company name, contract number, and date of contract expiration in Block 16.)

13. JUSTIFICATION FOR ACCESS

__Garrison Manager (website lead) or __Site Manager (other garrison-wide team members). Requires GS1035/1082, 46A/Z, or OPSEC Leve
(Web Content & OPSEC ok until Level II available). PAO must endorse new GM in an email.
_X_Page Manager (for directorate/unit/tenant in blocks 2,3). Requires GS1035/1082, 46A/Z, or OPSEC Level II (Web Content & OPSEC ok
Level II available).
__Page Contributor for (for directorate/unit/tenant in blocks 2,3). Requires Web Content and OPSEC Training Course
__Text Contributor for (directorate/tenant/unit in blocks 2,3). Site or Page Manager must oversee Text Contributor's work.
Name of Page/Site manager responsible for this Text Contributor_____

MERGE ALL CERTIFICATES INTO THIS PDF OR MAKE CERTAIN ALL ARE ATTACHED TO THE SAME EMAIL THIS DOCUME

ADDITIONAL INSTRUCTIONS: Fill this document in through Block 20b.
Read and initial the AUP in block 27.
Garrison Manager can serve as Information Owner for other Managers and Contributors (Blocks 21-21b).
CMS Manager at HQ IMCOM serves as Information Owner for Garrison Manager.

14. TYPE OF ACCESS REQUIRED: [X] AUTHORIZED [ ] PRIVILEGED

15. USER REQUIRES ACCESS TO: [X] UNCLASSIFIED [ ] CLASSIFIED (Specify category) [ ] OTHER

16. VERIFICATION OF NEED TO KNOW	16a. ACCESS EXPIRATION DATE (Contractors must specify Company Nar
I certify that this user requires access as requested. [X]	Contract Number, Expiration Date. Use Block 27 if needed.)

17. SUPERVISOR'S NAME (Print Name)	18. SUPERVISOR'S SIGNATURE	19. DATE (YYYYMMDD)
Boss, Ima R.	[SIGN HERE]	20220102
20. SUPERVISOR'S ORGANIZATION/DEPARTMENT: DES	20a. SUPERVISOR'S E-MAIL ADDRESS: ima.r.boss.civ@mail.mil	20b. PHONE NUMBER: 123-456-7890
21. SIGNATURE OF INFORMATION OWNER/OPR [SIGN HERE]	21a. PHONE NUMBER	21b. DATE (YYYYMMDD)
22. SIGNATURE OF IAO OR APPOINTEE [SIGN HERE]	23. ORGANIZATION/DEPARTMENT	24. PHONE NUMBER / 25. DATE (YYYYMMDD)

DD FORM 2875, AUG 2009 PREVIOUS EDITION IS OBSOLETE. Adobe Designer 9.0

26a. NAME (Last, First, Middle Initial) | 26b. SOCIAL SECURITY NUMBER

27. OPTIONAL INFORMATION (Additional information)
THIS DOCUMENT IS FOR STANDARD ACCESS ONLY. FOR PRIVILEGED ACCESS, APPLY TO ARMY ANALYTCS GROUP.

User will
1. Log off the system at the end of the session or work day.
2. Conform to IMCOM Enterprise Web processes and procedures outlined in published SOP/Tutorial documents.
3. Use only their own account to log into IEW back end.
4. Conform to any requirements set by the Garrison Web Manager.
5. Not attempt to reverse engineer, hack, break, or otherwise compromise the system.

Fill out this document through block 20b and turn it in to your installation Site Manager(s).

PART III - SECURITY MANAGER VALIDATES THE BACKGROUND INVESTIGATION OR CLEARANCE INFORMATION
28. TYPE OF INVESTIGATION | 28a. DATE OF INVESTIGATION (YYYYMMDD)
28b. CLEARANCE LEVEL | 28c. IT LEVEL DESIGNATION [ ] LEVEL I [ ] LEVEL II [ ] LEVEL III
29. VERIFIED BY (Print name) | 30. SECURITY MANAGER TELEPHONE NUMBER | 31. SECURITY MANAGER SIGNATURE | 32. DATE (YYYYMMDD)

PART IV - COMPLETION BY AUTHORIZED STAFF PREPARING ACCOUNT INFORMATION
TITLE: | SYSTEM: IMCOM Enterprise Web (IEW) -- (garrison) | ACCOUNT CODE
DOMAIN: n/a
SERVER: n/a
APPLICATION: IMCOM Enterprise Web
DIRECTORIES: n/a
FILES: n/a
DATASETS: n/a
DATE PROCESSED (YYYYMMDD) | PROCESSED BY (Print name and sign) | DATE (YYYYMMDD)
DATE REVALIDATED (YYYYMMDD) | REVALIDATED BY (Print name and sign) | DATE (YYYYMMDD)

DD FORM 2875 (BACK), MAY 2004 Reset

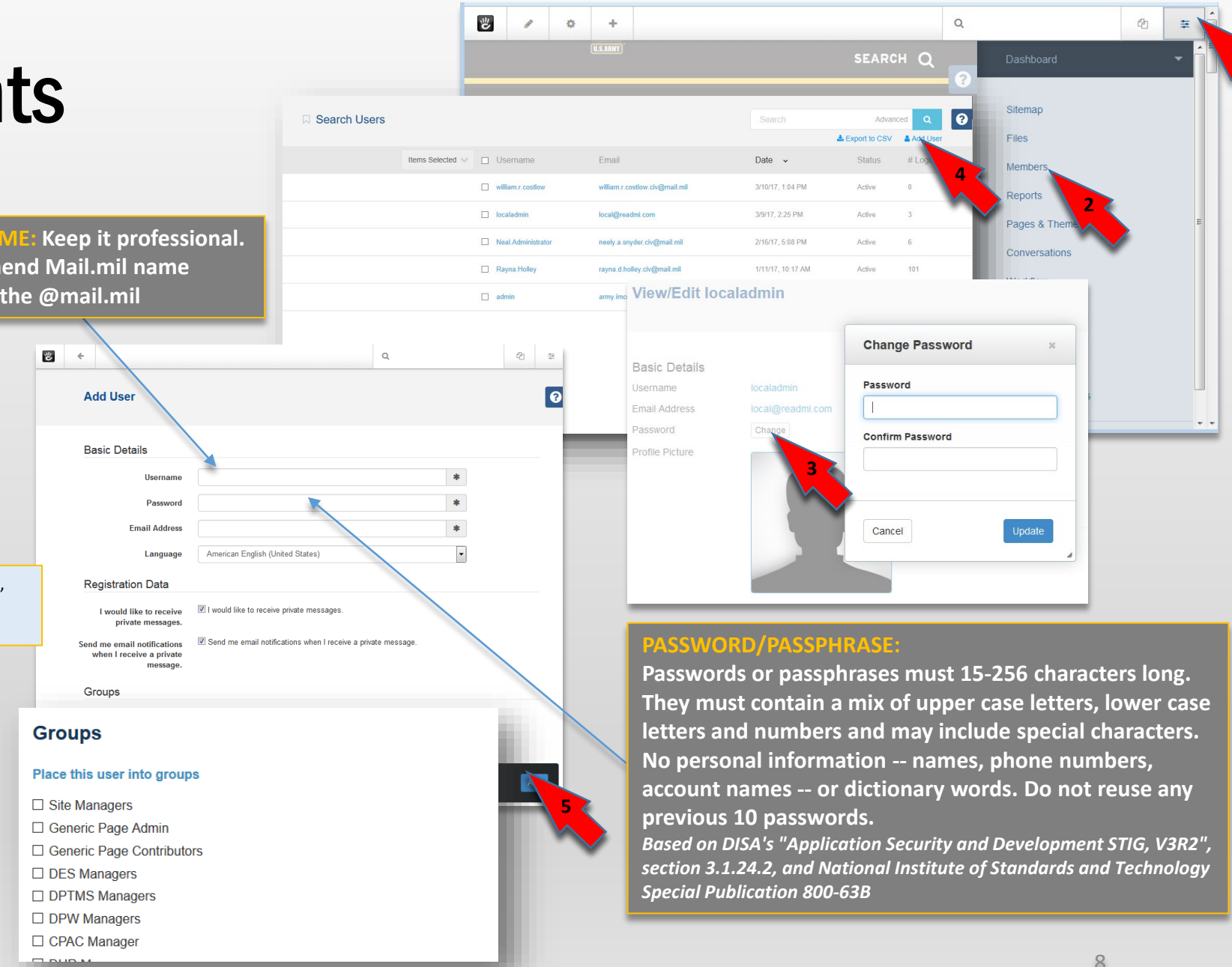
Creating Accounts

- Go to Dashboard (1) → Members (2)
- Click Add User (4)
- Fill in the form.
- PAOs on the Web team should be in the Site Managers* group
- ONE member should ALSO be in the Garrison Managers group
- **Do not delete any accounts. Disable them instead.**
- **Do not disable "admin," "imcom" or "Neal.Administrator"**

Accounts for contributors outside PAO should only be set up after you create their initial pages.

USERNAME: Keep it professional. Recommend Mail.mil name without the @mail.mil

*In older versions, "Site Manager" is "Administrator"



PASSWORD/PASSPHRASE:
Passwords or passphrases must 15-256 characters long. They must contain a mix of upper case letters, lower case letters and numbers and may include special characters. No personal information -- names, phone numbers, account names -- or dictionary words. Do not reuse any previous 10 passwords.
Based on DISA's "Application Security and Development STIG, V3R2", section 3.1.24.2, and National Institute of Standards and Technology Special Publication 800-63B

Creating Passwords /Pass Phrases

```
0pUn5esame?Rlly?!
^^^^^^^^^^^^^^^^^
```

^^^^^^^^^^^^^^^^^^^^
^^^^^^^^^^^^^^^^^^^^
^^^^^^^^^^^^^^^^^^^^
^^^^^^^^^^^^^^^^^^^^
^^^^^^^^^^^^^^^^^^^^
^^^^^^^^^^^^^^^^^^^^
^^^^^^^^^^^^^^^^^^^^
^^^^^^^^^^^^^^^^^^^^
^^^^^^^^^^^^^^^^^^^^
^^^^^^^^^^^^^^^^^^^^
^^^^^^^^^^^^^^^^^^^^
^^^^^^^^^^^^^^^^^^^^
^^^^^^^^^^^^^^^^^^^^

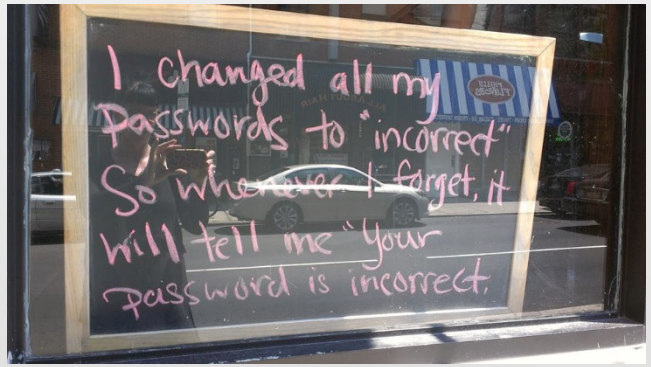
IMCOM GUIDELINES:

Passwords or passphrases must

- Be 15-256 characters long
- Contain at least two
  - upper case letters,
  - lower case letters
  - Numbers
  - special characters.
- Be free pf personal information -- names, phone numbers, account names –
- Not use dictionary words.
- Be at least 50 percent new
- Do not reuse any previous 10 passwords.
- Be changed every 60 days
- Not be changed more than once every 24 hours

Based on DISA's "Application Security and Development STIG, V3R2", section 3.1.24.2, and National Institute of Standards and Technology Special Publication 800-63B

IEW is protected by the NIPR-firewall. Using your CAC to log in to your computer protects IEW. The uneditable home.army.mil sites are available to the public, while the editable homeadmin.army.mil are not. This allows us to use passwords to log in from the NIPR. However, they must still be standards-compliant.



Monitoring accounts

IMCOM GUIDELINES:

Atypical Use

Atypical use could be a sign of an attempt to use your site for a malicious purpose. Keep an eye out for :

- **account activity occurring after hours or on weekends**
- **rapid logon/logoff**
- **multiple logons by same user**
- **failed access permissions**
- **elevated rights**

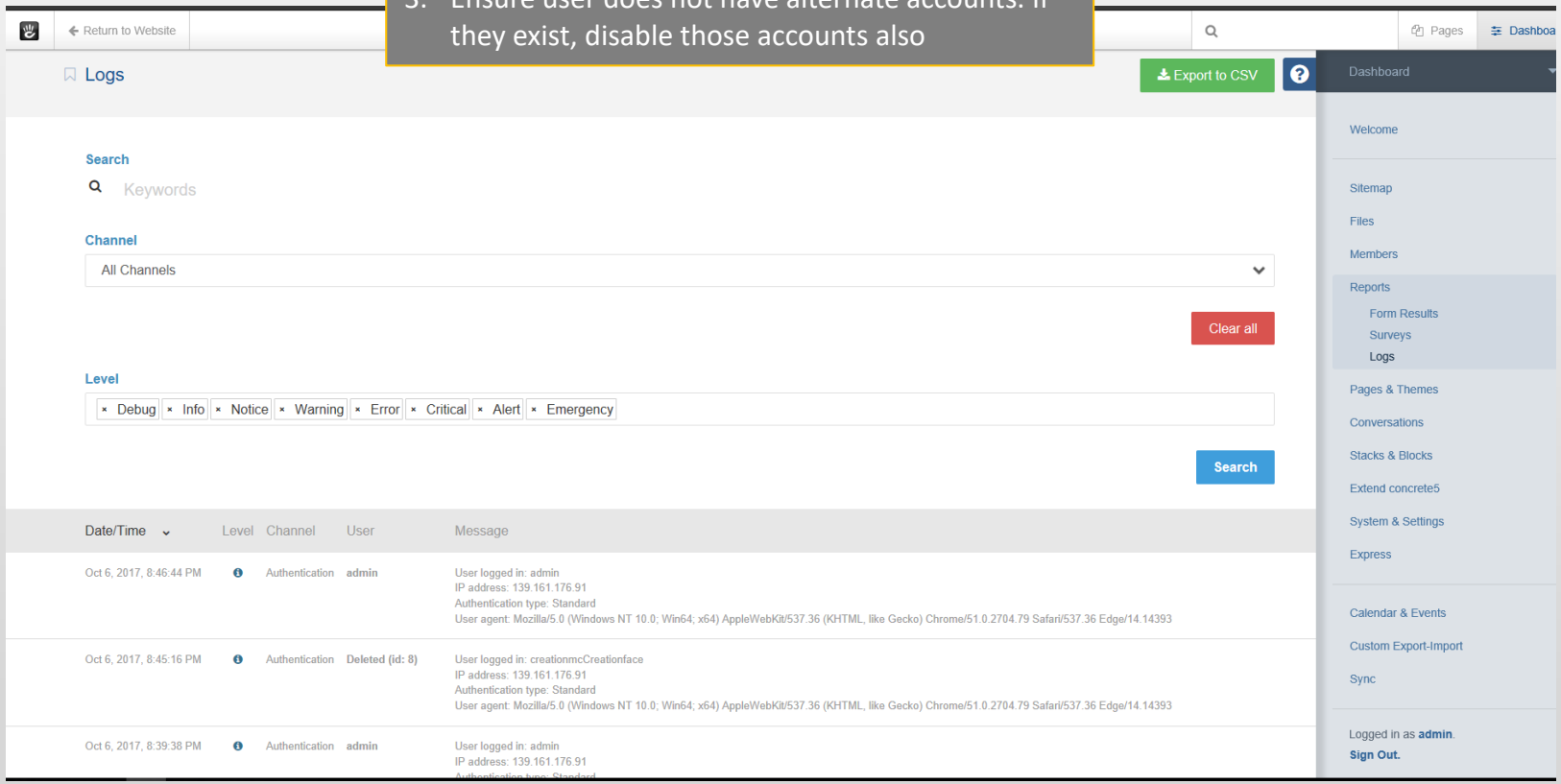
IEW logs account logins on the Dashboard → Reports → Logs page. If you notice atypical use, create a CSV file by clicking the Export to CSV button in the top right of the page. Email the resulting file to the ISSO and IMCOM PAO. All identified instances if atypical usage must be reported to the ISSO immediately [AC-2(12)]. Save a copy of all correspondence related to atypical use.

IMCOM GUIDELINES:

Significant Risk Accounts

When you identify users posing a significant ,take action. These types of users may have a history of inappropriate behavior.

1. Disable account within 30 minutes
2. Contact HQ PAO and the ISSO
3. Ensure user does not have alternate accounts. If they exist, disable those accounts also



Deleting contributors

- Disable the account
- Unless otherwise required (as in the case of an investigation), Send an email to the person and their supervisor with the date, time, and reason for disabling the account. It could be couched in a message such as “Congratulations on your retirement,” but explicitly state the account has been disabled.
- Send a copy of the message to IMCOM headquarters. If there is an investigation, please send an email with an explanation as soon as possible.
- IMCOM HQ will move the user to the deactivated list and send an acknowledgement.
- Maintain records for at least one year.

Snyder, Neely A CIV USARMY IMCOM HQ (USA)

From: Snyder, Neely A CIV USARMY IMCOM HQ (USA)
Sent: Friday, June 19, 2020 1:23 PM
To: Geistfeld, Patrecia F CIV USARMY IMCOM (USA)
Subject: RE: Fort Riley website account deactivation - DaWayne Krepel - FROC - page manager
Signed By: neely.a.snyder.civ@mail.mil

Perfect. Thanks.
(In fact, exemplary -- eMASS needs a sample of the process working.
VR

Neal Snyder, IMCOM PAO - IEW
Email: neely.a.snyder.civ@mail.mil
→Cell 210-238-5293 ←
Alt. 443-987-2153
Desk: 210-466-0116

-----Original Message-----
From: Geistfeld, Patrecia F CIV USARMY IMCOM (USA)
Sent: Friday, June 19, 2020 1:19 PM
To: Krepel, Dawayne L Jr CIV (USA) <dawayne.l.krepel.civ@mail.mil>
Cc: Pierce, Richard J (Rick) CIV USARMY IMCOM (USA)
<richard.j.pierce.civ@mail.mil>; Snyder, Neely A CIV USARMY IMCOM HQ (USA)
<neely.a.snyder.civ@mail.mil>
Subject: Fort Riley website account deactivation - DaWayne Krepel - FROC -
page manager

Good afternoon,

Thanks for the services you performed as an account holder while employed
with the Fort Riley Operations Center. This is to notify you that your
account has been deactivated.

Best wishes.

V/r

Patti Geistfeld
Public Affairs Specialist
Fort Riley Public Affairs
Building 500, Room 210
500 Huebner Ave
USAG Fort Riley, Kansas
785-239-3358 Commercial
312-856-3358 DSN

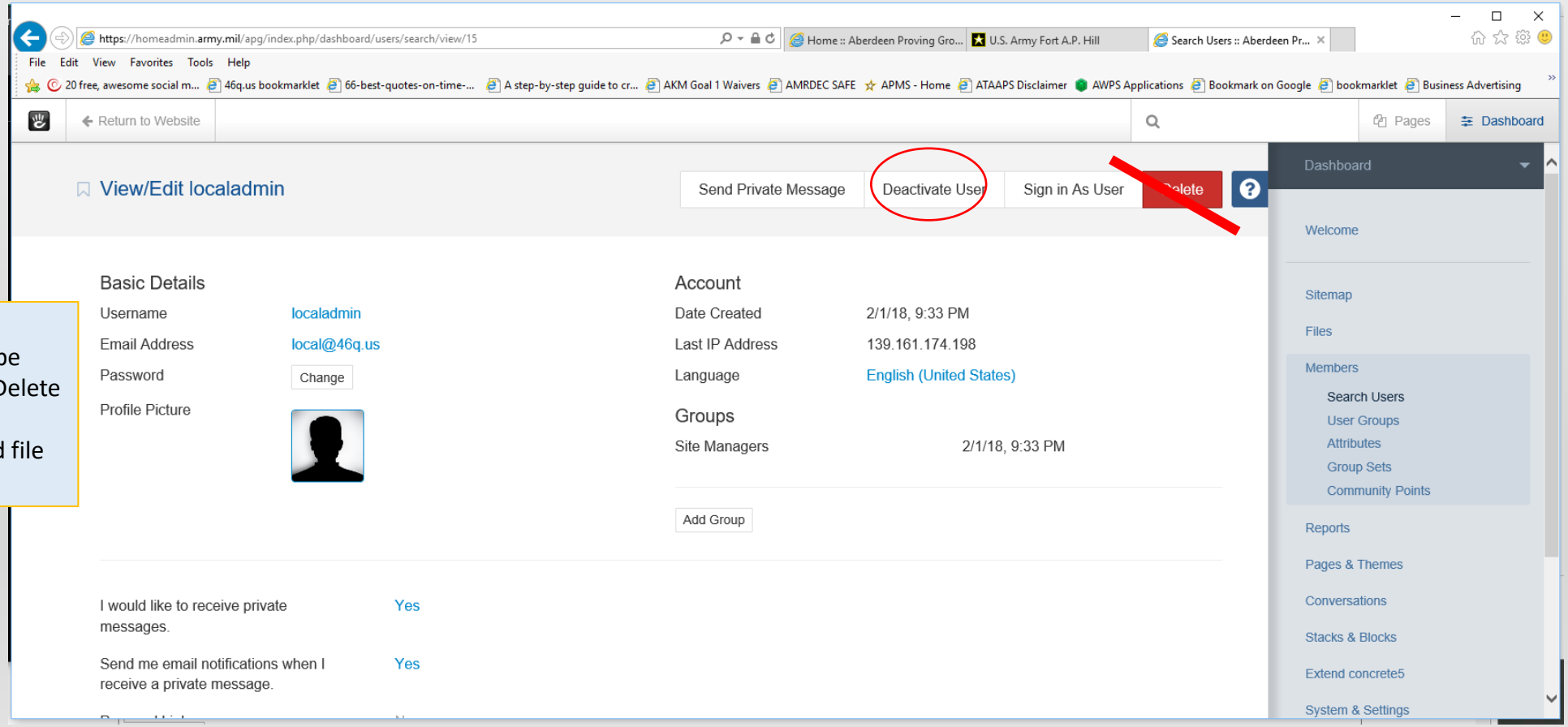
We Are The Army's Home-Serving The Rugged Professional
Learn more at https://home.army.mil/riley or https://home.army.mil/imcom.

1

Disabling accounts

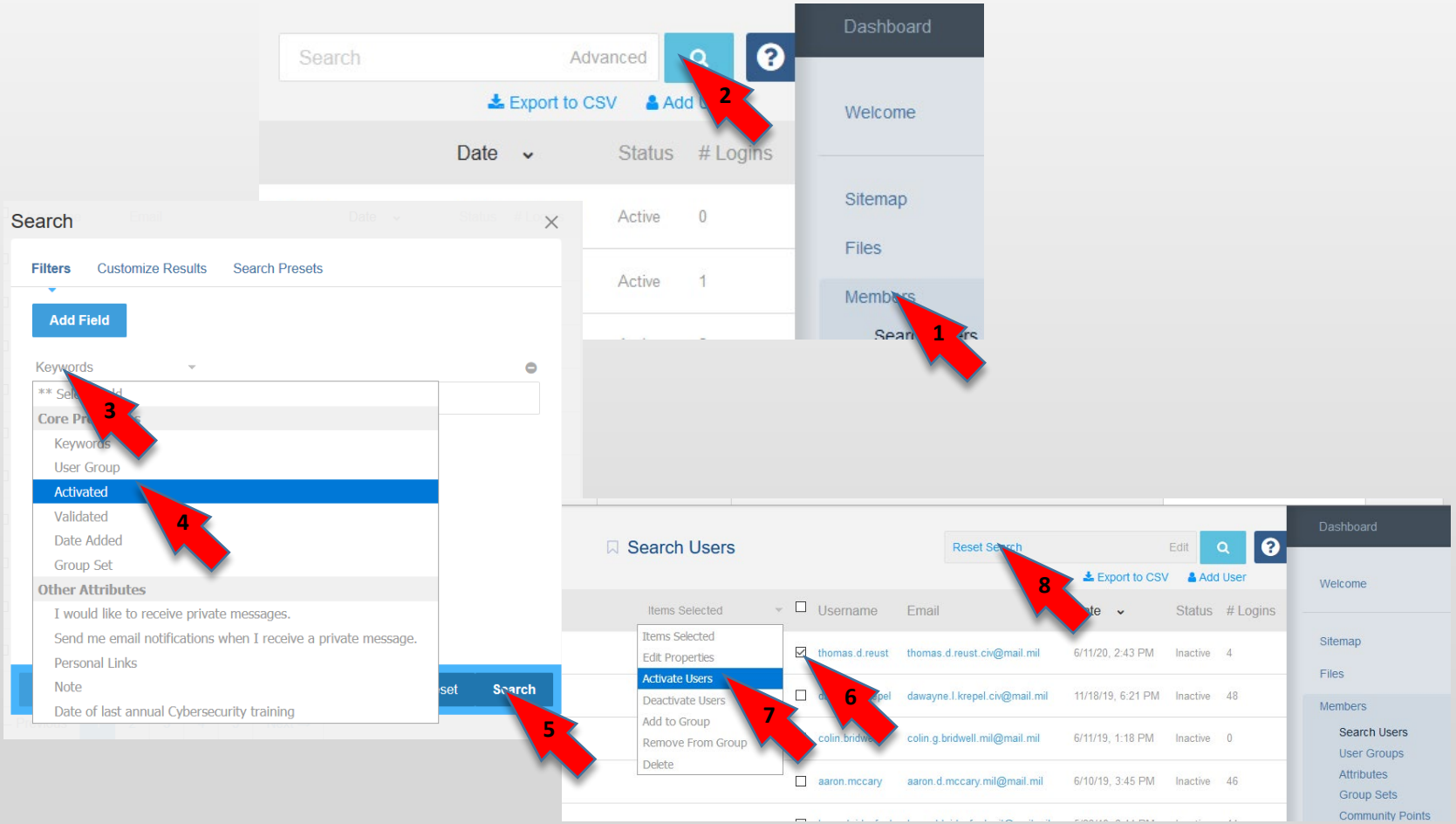
- **Do not delete** accounts even if you have the red “delete” button.
- Go to the account page and click “Deactivate”

Early in the deployment of IEW, we learned user accounts continue to be connected to the pages thy make. Delete the account and you risk the disappearance of your site map and file manager.



Finding and working with deactivated accounts

- Go to Dashboard→Members(1)
- In the Search box, click on Advanced(2)
- In the Search window, click on “Keywords” to activate the field selection dropdown
- Select “Activated.”(4) Inactive Users appears by default.
- Click Search.(5) The list will appear.
- Click the checkbox(6) next to the user name(s) you want to edit and use the dropdown menu (7) to make changes.
- Click Reset in the Search box(8) to exit this menu

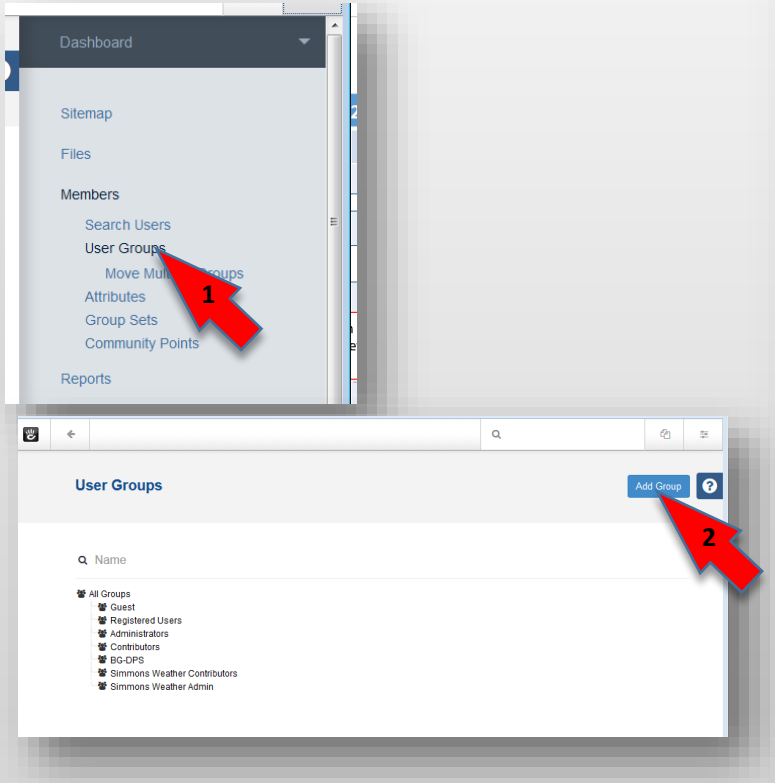


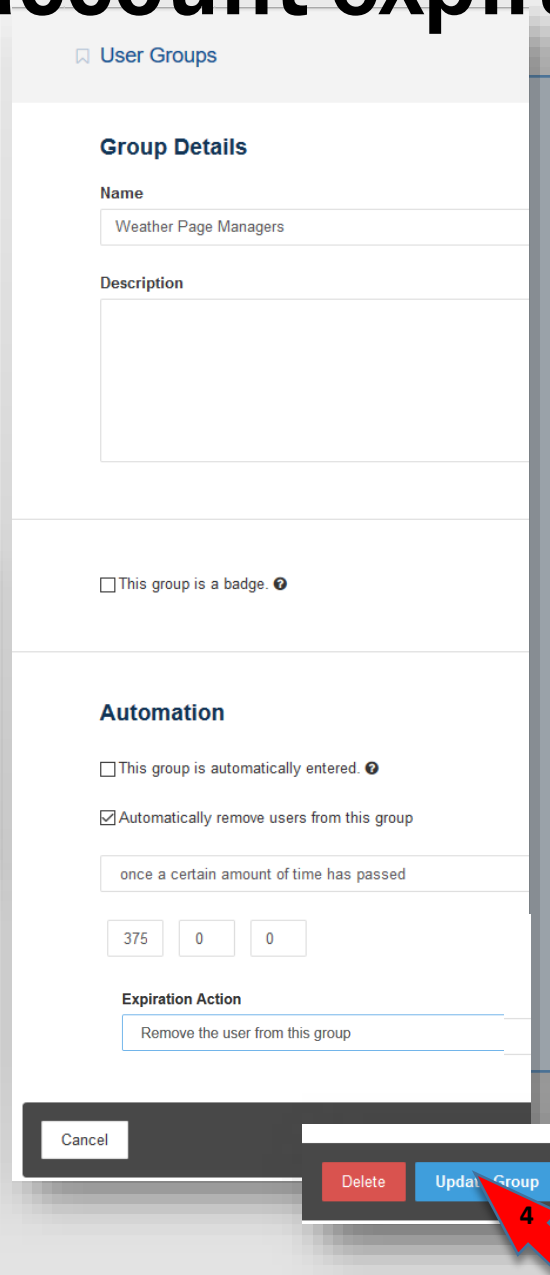
Training contributors

- Check out the resources at https://homeadmin.army.mil/imcom/index.php/contact/webmaster-1
- **In combination with the video https://www.youtube.com/watch?v=mLjvlHF_hjw, Tutorials 1 and 2 are designed to give page contributors the knowledge they need to make changes within the scope of their responsibility.**
- **Installations expecting large numbers of contributors may find it helpful to set up formal training.**
- **Groups of four or more can apply for training workshops led by IMCOM HQ staff.**

Creating User Groups, setting account expiration

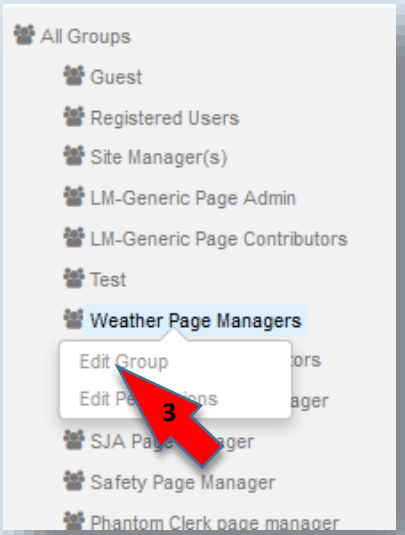
- Go to Dashboard → Members → User Groups (1) → Add Group (2)
- Enter the name and description. Check "Automatically remove users from this group," choose "Once a certain amount of time has passed," and give the user 375 days: one year, plus 10 days' grace period.
- Select "Remove the user from this group" for Expiration Action
- click "Add Group (4 – for new groups)."





Update Existing Groups:

- Click on the group name
- Click on "Edit Group"(3)
- Set expiration time
- Click "Update Group" (4).

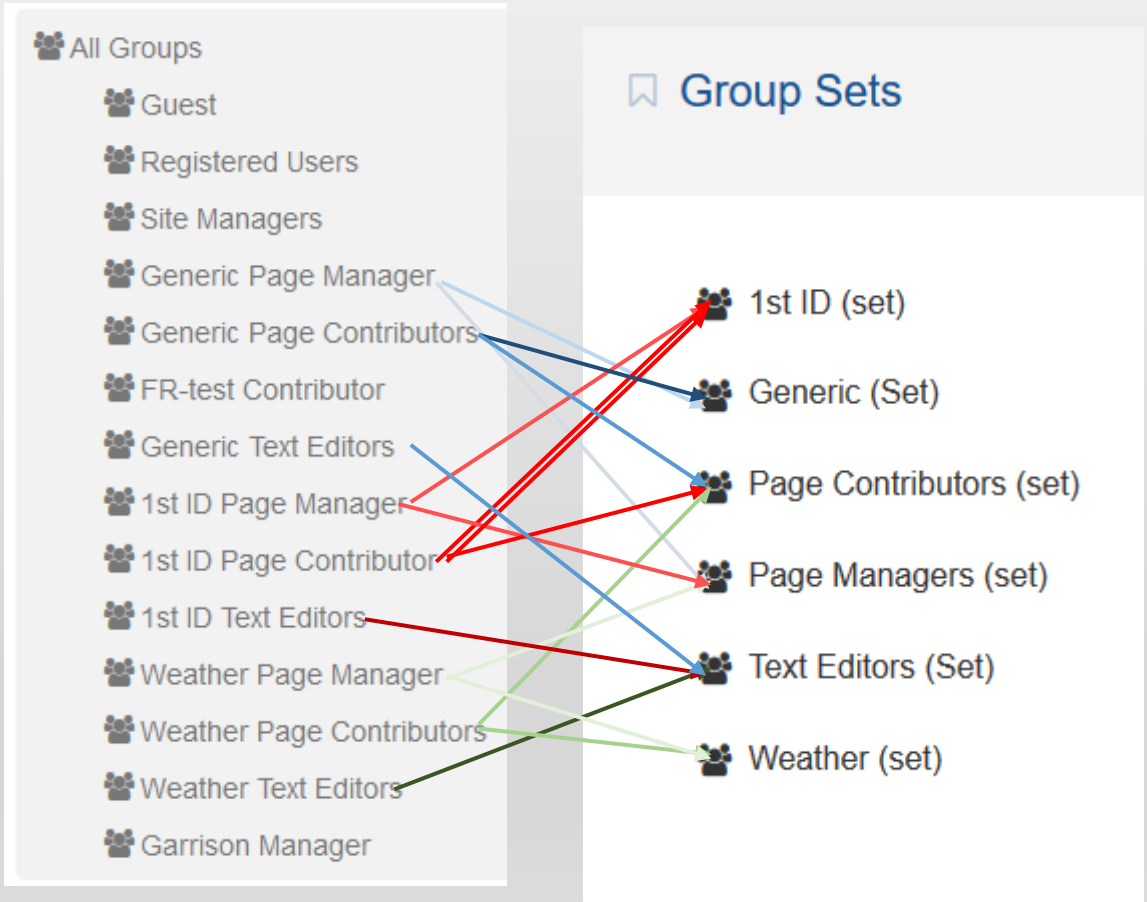


FEDERAL CYBERSECURITY GUIDELINES

All user accounts must be set to expire in no more than a year.

Making new permission sets

Giving a new office or unit its own page(s). [] = name of organization



- Make the site's page in its proper location in the site map. See Tutorial 2a.
- Create three User Groups for each office, directorate or tenant:
  1. "[ ] Page Manager,"
  2. "[ ] Page Contributors," and
  3. "[ ] Text Editors"
- – See the "Create Groups" page of this tutorial.
- Make one Group Set: "[ ] Set." See the "Make Group Sets" page.
- Put the Page Managers and Page Contributors user groups in the new group set. Do not include text editors.
- Open up the Page Managers group set and put the [ ] Page Manager in it. Put the [ ] Page Contributors in the Page Contributors set and the [ ] Line Editor in the Text Editors set.
- Follow the instructions in the pages "Apply Permissions to a Page and its Subpages" and "Select Permissions to Apply, " using the "Standard Permissions" page as your guide.

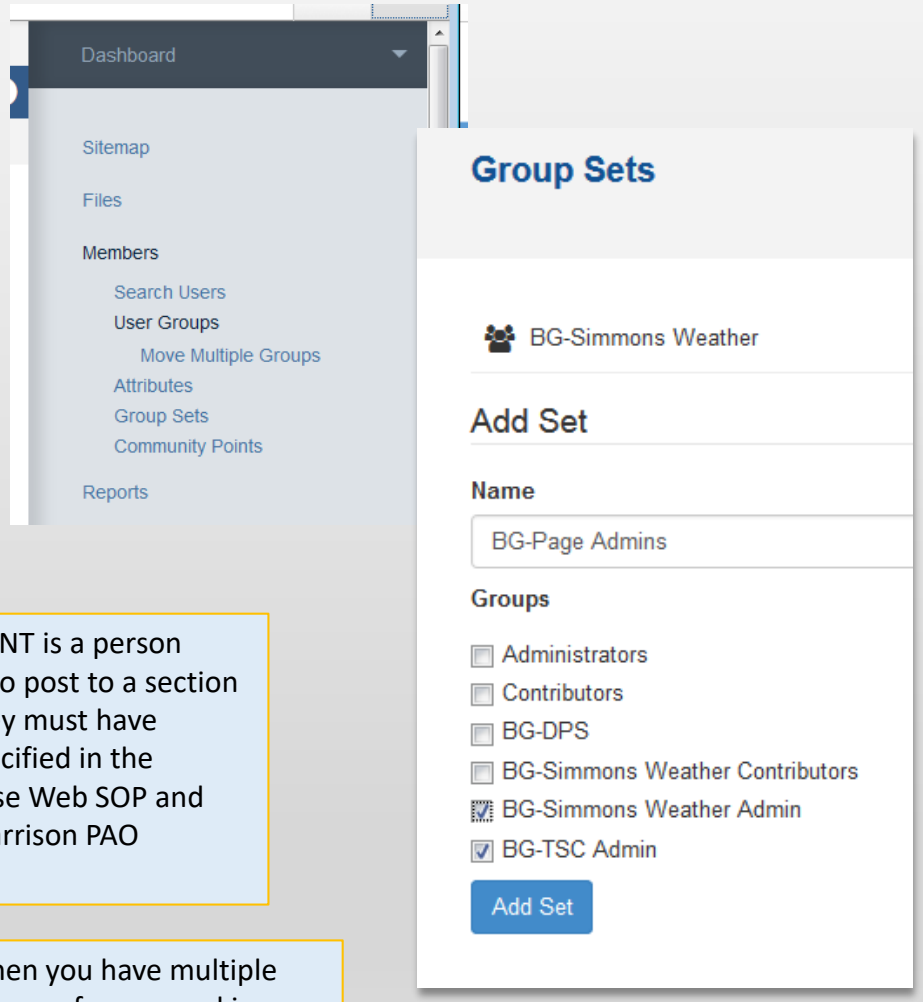
Changing User Group membership

- Go to Dashboard → Members
- Select member
- Find the list of groups in the lower right
- To remove a member from a group, hover over the group name until the trash can icon appears, and click it.
- To add the member to a group, click the Add User Group button.
- Select the group from the list and click it
- Membership applies immediately

Make Group Sets

- Go to Dashboard → Members → Group Sets
- Click Add Set
- Open the set
- Select the check boxes to associate the appropriate User Groups with the Group Set.

GROUP AND GROUP SETS REQUIREMENTS:
For each subsite (one or more pages to be edited by a certified agent), create User Groups for Page Managers (allowed to publish) Page Contributors (allowed to edit but not publish) and Text Editors. Make Group Sets for each subsite and for all Page Managers and Page Contributors. Put the Manager and Contributor – but not the Text Editor -- for each subsite in the Group Set for their page. Also, put all Page Managers in the Page Managers set and all Page Contributors in the Page Contributors set.



A CERTIFIED AGENT is a person allowed by PAO to post to a section of a website. They must have certifications specified in the IMCOM Enterprise Web SOP and operate under garrison PAO oversight.

When you have multiple groups of users working on a page, Group Sets speed things up.

-30-

IEW SOP/Tutorials:

1.Getting Started; Adding Text, Images and Links
2.Adding and working with pages
3.Adding and working with blocks
4.Working with files
5.Accounts
6.Permissions
7.Site management operations
8.Phonebook and special features
9.Advanced site management, design and standards
10.General policies