



e-Services WSA

CAPNHQ Electronic Services e-Services
Web Security Administration (WSA)
California Wing
Basic Procedures

Maj Howard N LaPierre
MIMS Coordinator CAWG
hlapierre@cawg.cap.gov
951-658-7304

1-0 Table of Contents

	Paragraph	Page
Preface	1-1	3
Web Security Administration (WSA) Defined	2-0	4
What is a WSA?	2-1	4
e-Services Restricted Applications access	2-2	4
Definition of Terms	2-3	4
Who assigns what authority to whom?	2-4	5
Assigning e-Services access	2-5	5
WSA Access Procedures	3-0	6
Signing on to the CAQNHQ Home page	3-1	6
Signing on to the CAPNHQ e-Services home page	3-2	6
First time user	3-3	7
Lost Password procedure	3-4	7
WEB Security Administration Procedures	4-0	8
Select WSA Module	4-1	8
Delete Permissions	4-2	8
Duplicate Permissions	4-3	8
Quick Add Permissions/Edit Expiration	4-4	9
View Permissions	4-5	9
Print a Restricted Application listing	4-5.1	9
Web Security Administration	4-6	9
Web Security Administration Applications	5-0	11
WSA Restricted applications	5-1	11
Recommended applications for a Unit Commander (WSA)	5-2	12
Default 'Cap Utilities' applications for all Members	5-3	12
Possible Additional Restricted Applications For A Member	5-4	13

Changes:
Major re-write.

If you discover any errors, please contact the author and they will be corrected

1-1 Preface

The intent of these procedures is to help anyone understand the CAP National Headquarters e-Services, Web Security Administration (WSA) procedure

WSA is a control system. The WSA application replaces WMU "Permissions" for the control of how a member relates to the CAPNHQ applications.

WSA defines which CAP NHQ "Restricted" online applications a member can use. There are numerous applications that any member can access on the CAPNHQ Web site, but there are numerous others that require that the member be authorized to use them. In order to use these restricted applications, you must have "Permission" to use them.

WSA is the system that allows a member, generally a Group or Unit Commander with WSA authority, to assign certain levels of access to these programs, for members within his organization. i.e. "permission". The WSA delegates access authority downward, Wing to Group, Group to Unit, Unit to members.

A Wing level WSA can assign any access authority to any member in the Wing. This authority defines what programs a member can access and also what he/she can do within that application.

The things that are controlled by the WSA are the programs that can be accessed and whether the member can enter data (Data Entry) or just read it (Read Only). It also defines the functional areas that can be accessed, CADET Programs, OPS-CAPPilot or OPS-Emergency Services. It controls the organization a member can access, usually just his own assigned Unit and the level of access (Scope), Group, Unit of Member.

WSA may be somewhat intimidating to the first time user.

The first time you try to accomplish any given task, simply follow each procedural step *exactly*. You will find that after you have done a particular procedure a few times, rather than read every word in the procedure, simply note the **BOLD** words and they will act as reminders, as to what to **Enter or Click**. It's like a cook book, and like a cook book, failure to follow the procedure exactly, may result in something other than what you desired. .

The procedures included, cover most of the tasks that the WSA will have to accomplish. Once the WSA has assigned all of his subordinates whatever WSA authority is required, no further action must be taken, unless the members or organization changes. **Care must be taken to remember to remove any permissions for members who transfer out of your organization, as whatever permissions they may have now, are probably not applicable in their new Unit.**

Effective 6 Sept 2005, major improvements have been made in the WSA application to give the user much more flexibility in assigning members permissions and controlling what members can or cannot do with restricted applications.

No guarantees are included with these procedures, as e-Services and WSA are changing all the time, with little or no notification from the authors at CAPNHQ.

If you find that a given procedure does not work, please advise the author and the procedure will be corrected.

2-0 Web Security Administration (WSA) Defined

2-1 What Is A WSA?

A “Web Security Administrator” (WSA) has the authority to assign a member, the capability to access various “Restricted Applications” in the CAP National Web Site. These are the applications that are listed on the right side of the e-Services Home page. (These are called “Permissions”.)

2-2 e-Services Restricted Application Access

“Restricted Applications Access” defines the user’s ability to access any of these restricted applications within e-Services. It is assigned by the WSA in the next higher level of Command. When assigning a member the ability to access an application, some applications are further divided into the following

1. Application i.e. MIMS(FMS) or Personnel Information Change, etc.
2. Module i.e. ES SQTR Quick Entry or Validate Achievements or Tasks, etc.
3. Process i.e. Data Entry or Read Only
4. Functional Area i.e. Cadet Programs or OPS-Emergency Services, etc.
5. Scope i.e. GROUP, UNIT or MEMBER
6. Org Level i.e. Region-Wing-Unit e.g. Your Unit

2-3 Definition Of Terms

APPLICATION

An Application is a computer program, which allows a user to process or look at information.

MODULE

Most Applications such as “CAPWATCH Download” or “Interactive Personal Information” only have one module. Others such as MIMS (FMS) have several. A Module is a sub-division of an Application.

The MIMS (FMS) Application is divided into several modules:

1. CAPF101 by CAPID
2. ES Multi-Person Specialty Entry (Achievement Level)
3. ES SQTR Quick Entry
4. ES Single-Person Specialty Entry (Achievement Level)
5. FMS Currency
6. FMS Reports
7. General ES & Pilot Task Data Entry (Task Level)
8. Multi-Pilot Entry
9. SQTR by CAPID
10. Validate Achievements or Tasks

PROCESS

A Process is a data related capability that can be assigned to any Application/Module:

1. Read Only. Only allows the user to LOOK at information, not enter or change it.
2. Data Entry. Allows the user to enter, look at or change data

FUNCTIONAL AREA

Some Applications/Modules are broken down into Functional Areas

1. Cadet Programs
2. OPS-CAPPilot
3. OPS-Emergency Services
4. OPS-CounterDrug

Some applications only operate within a single area, such as Personnel.

If a member is only involved with Cadet Programs, it is only necessary to authorize his access to applications that deal with Cadet Programs. If a member is not a pilot, it is usually only necessary to authorize him to access OPS-Emergency Services applications

REGION-WING-UNIT or ORG LEVEL

Region-Wing-Unit defines the Unit[s] that the member can access. e.g. A member can be given access to CAPWATCH Download for his Unit and also be given access to other Units as well.

This would normally be used in cases where the member is assigned to one Unit, but also assigned other duties in another Unit (IAOD) i.e. Group and has a need to look at or update data in both Units.

SCOPE

Scope refers to the ability of an individual to access information at different levels.

1. **“Wing” scope** allows a member to access data for all members in the Wing.
2. **“Group” scope** allows a member to access data for any member in all Units within the Group
3. **“Unit” scope** allows a member to access data for any member of his Unit.
4. **“Member” scope** only allows a member to access his own data.

2-4 Who Assigns What Authority To Whom?

The Wing WSA assigns WSA Authority and Application access to the Group WSA, usually the Group Commander

The Group WSA assigns WSA Authority and Application access to the Unit (Squadron) Commander

The Unit (Squadron) WSA assigns Application access to the members of the Unit

2-5 Assigning E-Services Access

Each WSA can authorize access to any of the restricted applications that he/she has to anyone under his Command authority, any application, process and scope of access, up to, but not higher than, his own authority. For example, a Group WSA can assign anyone under his Command any Scope, Member, Unit or Group, but not Wing scope. i.e. A WSA can delegate his authority to anyone in his organization.

In addition, most of the applications can be accessed either of two (2) ways, “Read Only” or “Data Entry” (Read/Write). If a member is authorized Data Entry access to an application, he has both capabilities. With Data Entry, it would be redundant to authorize Read Only. (Also, in some applications, “read/only” may lock out data entry capability.)

Data Entry capability is used to allow a person to enter data in such applications as FMS Currency, Multi-Pilot entry or Personnel Information Changes.

All CAP members have been given authority to enter their own data (Data Entry) under these applications. There are a number of other applications under the e-Services Utilities that a member can access, without any authorization from any WSA. These are listed under "Default 'Cap Utilities' Applications.

The Unit Commander (WSA) can assign any member Data Entry authority for ES SQTR Quick Entry, General ES & Pilot Task Data Entry, Multi-Pilot entry or Personnel Information Changes, if he wants to allow that member to enter data for other members. These would be Restricted Applications for that member. This can be very useful, as some members do not have or use computers.

Any member can also be given Read Only authority for the Validate Achievements or Tasks.

The Data Entry capability for Validate Achievements or Tasks and the Approval Module, is used to Validate/Approve Achievements or Tasks, as required in CAPR 60-4. The only people who should be given Data Entry authority for Validate Achievements or Tasks would be the Unit Commander or his designee.

The Approval Module is used to approve only the completed Achievements. Authority to use the Approval Module is not assigned by the WSA, but it is automatically given to any member defined as Unit Commander, Vice Commander or ES Officer for the Unit. These assignments are defined by using the Duty Administration application

A list of recommended applications is listed in this document.

3-0 WSA Access Procedures

Each Web Security Administrator (WSA) should assign certain WSA permissions to each WSA under his Command: (He has been assigned this authority, by the next higher level of Command)

3-1 Signing On To CAPNHQ Home Page

- a. Sign on to the INTERNET
- b. **Open <www.cap.gov>**. This gets you to the CAPNHQ Home page. It is suggested that you save this page in your "Favorites"

3-2 Signing On To The CAPNHQ E-Services Home Page

- a.. **Click "e-Services"** button under "Members" on the CAPNHQ Home page to get into the e-Services Home page. The "Welcome to e-Services" page will appear.
- b. Enter your **CAPID** and **Password** and click "**Log On**". The "e-Services Home page" will appear.

Remember, password is one of the few "case" sensitive items in e-Services.

3-3 First Time User

- a. If you are a first time user, Click on “First time users **“Click here”**. The “New User Registration” page will appear.
- b. Enter your **Social Security Number** and your **E-Mail address** and Click **“Submit”**.
- c. You will be asked one of several questions such as “What was your Mother’s maiden name?” for future use by the system. **Remember how you entered this**, as if you ever need to go back into the “Lost Password” procedure, you will need to remember how you entered this item.
- d. A computer generated “Password” will be sent to the E-Mail address you just entered. Once you have received that password, you can log on to e-Services as described above.
- e. It is suggested that you use the **“Change Password”** procedure to change the password to something you can remember and record somewhere.

3-4 Lost Password Recovery Procedure

If you cannot remember your password:

- a. Click on **“Password Assistance”**. A screen will appear requesting more information.
- b. Enter your **CAPID**.
- c. Click on **“Submit”**. A new screen will appear, requesting the following information: You will have to answer three questions. Such as, What was your mother’s maiden name? It might be, What was your first dog’s name? This will be whatever you entered the first time you logged on to e-Services.
- d. Enter that question. **“Answer to the question”**
What are the last four digits of you SSN?
- e. Enter that **“number”**
What is your date of birth?
- f. Enter that **“date”**
- g. Click on **“Submit”**
A message will appear: “Check your e-mail for your password”

4-0 WEB SECURITY ADMINISTRATION Procedures

4-1 Select WSA Module

- a. From the e-Services home page, Click on “**Web Security Admin**”. The “Web Security Administration Main” page will appear.

There are five modules within the Web Security Administration application:

1. Delete Permissions
2. Duplicate Permissions
3. Quick Add Permissions/Edit Expiration
4. View Permissions
5. Web Security Administration

- b. **Click on any of these five modules desired.** The Member Selection fields for that module will appear.

4-2 Delete Permissions

To delete any or all permissions for a member:

- a. If you know the member’s **CAPID**, enter it into the CAPID box.
- b. If you don’t know the member’s CAPID, enter the **member’s last name [and first name]** in the appropriate boxes.
- c. Click on “**Click to Search by Name**” If there are more than one member who matched the search criteria, a list of these members will be displayed.
- d. Click on the **CAPID** of the member desired. The member’s CAPID, first and last name will be entered into the boxes and the data page for the module selected will appear.
- e. Click on the “**check box**” for any permission you wish to delete or click on the “**Select All**” check box.
- f. Click on “**Delete**”. All selected permissions will be deleted

4-3 Duplicate Permissions

To duplicate all of a member’s permissions from one member to another: This is particularly useful when a member assumes a Command position and needs to have a large number of permissions to do his/her job.

Enter the **FROM** member:

- a. Enter the **CAPID** of the member and press the **TAB** key. This will fill in the First and Last name of the member.

Or

- b. Enter the **Last Name [First Name]** of the member and click on “**Click to Search by Name**”. This will fill in the CAPID of the “From” member desired. If there are more than one member who matched the search criteria, a list of these members will be displayed.
- c. Click on the **CAPID** of the member desired. The member’s CAPID, first and last name will be entered into the boxes and list of this member’s permissions will appear.

Enter the **TO** Member:

- d. Enter the **CAPID** of the member and press the **TAB** key. This will fill in the First and Last name of the member.

Or

- e. Enter the **Last Name [First Name]** of the member and click on “**Click to Search by Name**”. This will fill in the CAPID of the “To” member desired. If there are more than

one member who matched the search criteria, a list of these members will be displayed.

- f. Click on the **CAPID** of the member desired. The member's CAPID, first and last name will be entered into the boxes.
- g. Click on "**Duplicate Permissions**" All permissions of the FROM member will be copied to the TO member.

4-4 Quick Add Permissions/Edit Expiration

This module can be used to enter a number of permissions for a member at one time.

- a. If you know the member's **CAPID**, enter it into the CAPID box.
- b. If you don't know the member's CAPID, enter the **member's last name [and first name]** in the appropriate boxes.
- c. Click on "**Click to Search by Name**". If there are more than one member who matched the search criteria, a list of these members will be displayed.
- d. Click on the **CAPID** of the member desired. The member's CAPID, first and last name will be entered into the boxes and the data page for the module selected will appear.
- e. Select the "**Scope**" desired.
- f. Select the "**Org Level**" desired, Region-Wing-Unit. Normally the member's Unit.
- g. If desired, click Add Expiration Date "**Yes**" or "**No**"
- h. If "Yes", Enter **expiration date**.
- i. Check the "**Add**" check boxes for each permission desired.
- j. Click "**Submit**". All checked permissions will be added to the member's permission list.

4-5 View Permissions

To review the applications and scopes just entered:

- a. If you know the member's **CAPID**, enter it into the CAPID box.
- b. If you don't know the member's CAPID, enter the **member's last name [and first name]** in the appropriate boxes.
- c. Click on "**Click to Search by Name**". If there are more than one member who matched the search criteria, a list of these members will be displayed.
- d. Click on the **CAPID** of the member desired. The member's CAPID, first and last name will be entered into the boxes and a list is displayed showing all of the Restricted applications entered for this member his/her scope of authority.

4-5.1 Print a Restricted Application listing

If you want to prepare a printed report for this member,

- a. Select "**Landscape Mode**" for your printer.
- b. Click the **Print** button

4-6 Web Security Administration

This module is to be used to enter a single permission at a time for a member

- a. If you know the member's **CAPID**, enter it into the CAPID box.
- b. If you don't know the member's CAPID, enter the **member's last name [and first name]** in the appropriate boxes.
- c. Click on "**Click to Search by Name**". If there are more than one member who matched the search criteria, a list of these members will be displayed.
- d. Click on the **CAPID** of the member desired. The member's CAPID, first and last name will be entered into the boxes and the initial page for the module selected will appear.
- e. Entries on this page are made in nine (9) steps:

1. Select the **Application** desired. i.e. MIMS (FMS)
2. Select the **Module** desired i.e. ES SQTR Quick Entry.
3. Select the **Process** desired i.e. Data entry or Read only (Some only have Data Entry)
- 4.. Select the **Functional Area** desired i.e. OPS-Emergency Services
5. Select the **Scope** desired i.e. UNIT
6. Select the **Region-Wing-Unit** desired i.e. Your unit
7. If desired, Click "**Add Expiration Date**"
8. If "Yes", enter the **Expiration Date**
9. Click **Submit**. The screen will refresh and you can select the next application.

The screen now shows a list of all of the permissions the member has.

Repeat steps 1 - 9 for each application or module you wish to authorize. The recommended applications are listed below.

5-0 Web Security Administration Applications

5-1 WSA Restricted Applications

There are several restricted applications that may be assigned access for each WSA or member.

- | | |
|---------------------------------------|--|
| a. CAP Image Upload for Commanders | Transmit pictures to MIMS |
| b. CAPWATCH Download. | Download the National Database |
| c. Duty Assignment | Assign Duty positions for your Unit i.e. A PA |
| d. Interactive Personnel system | Look at Personnel information |
| e. MIMS (FMS) Applications. | These are divided into nine modules |
| 1. CAPF101 by CAPID | Print a CAPF 101 ES card |
| 2. SQTR by CAPID | Print a SQTR card (CAPF 101T) |
| 3. FMS Currency | Member pilot currency data |
| 4. FMS Reports | Numerous reports. |
| 5. ES SQTR Quick Entry | Entry of information about completion of Qualifications or Tasks required in CAPR 60-4. i.e. CAPF 101T xxx data. |
| 6. Multi-Pilot Entry | Entry of information about completion of Pilot ratings etc. |
| 7. General ES & Pilot Task Data Entry | Enter information about completion of Qualifications or Tasks required in CAPR 60-4. i.e. CAPF 101T xxx data. |
| 8. ES Single-Person Specialty Entry | Enter or delete Achievements or enter a Specialty Renewal date for a member. |
| 9. ES Multi-Person Specialty Entry | Enter or delete Achievements or enter a Specialty Renewal date for multiple members. |
| 10. Validate of Achievements or Tasks | Verification of an Achievement or Task by the approving authority, initially the Unit Commander. |
| f. Organizational Contacts | Access to information about Units |
| g. Personnel Information Change | Change personnel Information. |
| h. Validate CAP Picture | Verify that pictures are valid |
| i. Vehicles (Form 73) | Transmit vehicle to National |
| j. Web Security Admin | Assign access to e-Services applications. |

5-2 Recommended Applications For A Group/Unit Commander (WSA)

	Application	Module	Process	Functional Area	Scope *
a.	CAPWATCH	Download	Read Only		Group/Unit
b.	Duty Assignment		Data Entry	Personnel	Group/Unit
c.	Image Upload for Commanders		Data Entry	Personnel	Group/Unit
d.	Interactive Personnel System		Read Only	Personnel	Wing
e.	MIMS (FMS)	CAPF101 by CAPID	Read Only	OPS-Emergency Services	Group/Unit
f.	MIMS (FMS)	SQTR by CAPID	Read Only	OPS-Emergency Services	Group/Unit
g.	MIMS (FMS)	FMS Currency	Data Entry	OPS-CAPPilot	Group/Unit
h.	MIMS (FMS)	FMS Reports	Read Only	Cadet Programs	Group/Unit
i.	MIMS (FMS)	FMS Reports	Read Only	OPS-CAPPilot	Group/Unit
j.	MIMS (FMS)	FMS Reports	Read Only	OPS-Emergency Services	Group/Unit
k.	MIMS (FMS)	ES SQTR Quick Entry	Data Entry	OPS-Emergency Services	Group/Unit
l.	MIMS (FMS)	Multi-Pilot Entry	Data Entry	OPS-CAPPilot	Group/Unit
m.	MIMS (FMS)	GES & Pilot Task Entry	Data Entry	Cadet Programs	Group/Unit
n.	MIMS (FMS)	GES & Pilot Task Entry	Data Entry	OPS-CAPPilot	Group/Unit
o.	MIMS (FMS)	GES & Pilot Task Entry	Data Entry	OPS-Emergency Services	Group/Unit
p.	MIMS (FMS)	Validate A/T	Data Entry	Cadet Programs	Group/Unit
q.	MIMS (FMS)	Validate A/T	Data Entry	OPS-CAPPilot	Group/Unit
r.	MIMS (FMS)	Validate A/T	Data Entry	OPS-Emergency Services	Group/Unit
s.	MIMS (FMS)	ES Single-Person Specialty Entry	Data Entry	OPS-Emergency Services	Group/Unit
t.	MIMS (FMS)	ES Multi-Person Specialty Entry	Data Entry	OPS-Emergency Services	Group/Unit
u.	Personnel Information Change		Data Entry	Personnel	Group/Unit
v.	Validate CAP Picture		Data Entry	Personnel	Group/Unit
w.	Web Security Admin		Data Entry	Mission Support	Group/Unit

(A/T = Achievements or Tasks)

Note: The **Organization** for each of the above Applications, would usually be the Member's assigned Unit

* Assign either Group or Unit Scope, depending on level of Command.

These applications allow each Commander (WSA) to look at or change, the data for all members in his Unit and use the various applications to enter Achievements or Tasks completed and other data for himself or any member of his organization. These are the *TASKS* that are required by CAPR 60-4 Volume II, CAPF 101T's, to qualify for Emergency Services Specialties.

5-3 Default "Cap Utilities" Applications For All Members

	Application	Module	Process	Functional Area	Scope
a.	CAPWATCH	Download	Read Only	General	Unit
b.	Interactive Personnel System		Read Only	Personnel	Unit
c.	MIMS (FMS)	Personal Currency	Data Entry	OPS-CAPPilot	Member
d.	Personal GES & Pilot Task	Data Entry	Data Entry	Cadet Programs	Member
e.	Personal GES & Pilot Task	Data Entry	Data Entry	OPS-CAPPilot	Member
f.	Personal GES & Pilot Task	Data Entry	Data Entry	OPS-Emergency Services	Member
g.	Member Qual Info		Read Only	OPS-Emergency Services	All CAP
h.	My Member Info		Data Entry	Personnel	Member
i.	Personal CAPF 101		Read Only	All	Member
j.	Personal SQTR		Read Only	All	Member
k.	Personal ES SQTR Quick Entry		Data Entry	OPS-Emergency Services	Member
l.	Personal Multi-Pilot Entry		Data Entry	OPS-CAPPilot	Member
m.	Upload CAP Picture(within CAPF101)		Data Entry	Personnel	Member

These applications allow each member to look at his/her own data and use the "Qual/Cert" and other applications to enter Achievements or Tasks completed for him/herself.

These are the *TASKS* that are required by CAPR 60-4 Volume II, CAPF 101T's, to qualify for any Emergency Services Specialty.

In the future, there may be additional applications added that are not listed in this document.

Each Unit Commander has the option of delegating any of the MIMS (FMS) applications authority to any member of his/her Unit up to the "Scope" level that he/she holds.

5-4 Possible Additional Restricted Applications For A Member

Each Unit Commander has the option of delegating any of the MIMS (FMS) applications authority to any member of his/her Unit up to the "Scope" level that he/she holds.

	Application	Module	Process	Functional Area	Scope
a.	Interactive Personnel System		Read Only	Personnel	Group
b.	MIMS (FMS)	FMS Currency	Data Entry	OPS-CAPPilot	Unit
c.	MIMS (FMS)	FMS Reports	Read Only	Cadet Programs	Unit
d.	MIMS (FMS)	FMS Reports	Read Only	OPS-CAPPilot	Unit
e.	MIMS (FMS)	FMS Reports	Read Only	OPS-Emergency Services	Unit
f.	MIMS (FMS)	ES SQTR Quick Entry	Data Entry	OPS-Emergency Services	Unit
g.	MIMS (FMS)	Multi-Pilot Entry	Data Entry	OPS-CAPPilot	Unit
h.	MIMS (FMS)	GES & Pilot Task Entry	Data Entry	Cadet Programs	Unit
i.	MIMS (FMS)	GES & Pilot Task Entry	Data Entry	OPS-CAPPilot	Unit
j.	MIMS (FMS)	GES & Pilot Task Entry	Data Entry	OPS-Emergency Services	Unit
k.	MIMS (FMS)	Validate A/T	Read Only	Cadet Programs	Unit
l.	MIMS (FMS)	Validate A/T	Read Only	OPS-CAPPilot	Unit
m.	MIMS (FMS)	Validate A/T	Read Only	OPS-Emergency Services	Unit
n.	Personnel Information Change		Data Entry	Personnel	Unit

(A/T = Achievements or Tasks)

*Note: The **Organization** for each of the above Applications, would usually be the Member's assigned Unit.*

Only assign these capabilities for a member who has a "NEED" for such authority.

Other applications are occasionally added to MIMS and may not be referenced in this document.

These applications allow each member to look at data and use these applications to enter Achievements or Tasks completed for himself and any other member of his/her Unit. These are the *TASKS* that are required by CAPR 60-4 Volume II, CAPF 101T's, to qualify for any Emergency Services Specialty

The "Validate Achievements or Tasks" procedures with Data Entry capability at the Unit or higher level allow for the Approval of Achievements or Tasks.

The assignment of these WSA permissions should be used with great discretion. Also, any time a member transfers from the Unit, these restricted applications should be removed.