



## EAD Help File – V6.0

### JAP 100A-01 Engineering Authorizations Database Help File

#### Table of contents

Paragraph	Page
<b>1 General .....</b>	<b>2</b>
<b>2 EAD Manager .....</b>	<b>3</b>
2.1 Installation .....	3
2.2 Installation Errors .....	5
2.3 Activating the EAD .....	5
2.4 Setting up the Stn/Ship/Unit infrastructure .....	9
2.5 Adding a Sqn/Unit to the Stn/Ship/Unit .....	11
2.6 Adding authority level K and J's .....	12
2.7 Creating 'Local Authorizations' .....	14
2.8 Upgrading your EAD to Latest Version .....	16
<b>3 Sqn/Unit Manager .....</b>	<b>17</b>
3.1 Populating your Sqn/Unit .....	17
3.2 Adding personnel to the Sqn/Unit EAD .....	18
3.3 Awarding authorizations against Sqn/Unit personnel .....	18
3.4 Local authorizations .....	21
3.5 Printing of individuals Authorization Certificate (JAP and Local) .....	23
3.6 Flexibility of raising authorizations .....	24
3.7 Multiple personnel with same authorizations .....	25
<b>4 Things you may wish to do with the EAD .....</b>	<b>26</b>
<b>5 Printer problems.....</b>	<b>27</b>
<b>6 Your Comments.....</b>	<b>27</b>

#### List of tables

Table 1. Extract of JAP 100A-01 Chapter 0.7.....	19
--	----

#### List of figures

Figure 1. JAP 100A-01 Polestar Opening Screen. ....	3
Figure 2. EAD – File Download Screen. ....	4
Figure 3. Link Tables. ....	6
Figure 4. Selecting the Eng Auth Back End.....	7
Figure 5. Table Link Confirmation Message. ....	7
Figure 6. Stn/Ship/Unit. ....	7
Figure 7. Stn/Ship/Unit Initial Message.....	8
Figure 8. Stn/Ship/Unit Linked Correctly Confirmation Screen.....	8
Figure 9. EAD <a href="#">▶ Home Page ◀</a> .....	8
Figure 10. Setting up the Stn/Ship/Unit. ....	9
Figure 11. Change Stn/Ship/Unit & Move Person Button Appearance. ....	10
Figure 12. Change Stn/Ship/Unit Location Code.....	10
Figure 13. Adding a Sqn/Unit to your Stn/Ship/Unit EAD. ....	11
Figure 14. Adding Authority Level K. ....	12
Figure 15. Selecting Authorizations. ....	13
Figure 16. Empty Local Authorizations Screen.....	14
Figure 17. Partially filled In Local Authorizations List. ....	15
Figure 18. Local Authorization Source Reference Message. ....	15
Figure 19. Adding Source Details of Local Authorization. ....	16

Figure 20. Adding a Sqn/Unit Sub Section .....	18
Figure 21. Authorization Selection. ....	19
Figure 22. Authorization Details. ....	20
Figure 23. <i>Ineligible Authorization</i> . ....	21
Figure 24. <i>Local Authorizations Screen</i> . ....	22
Figure 25. Local Authorizations - Eligibility. ....	22
Figure 26. Preview (print) JAP Auths Message Screen. ....	23
Figure 27. Print Preview of 'Record of Engineering Authorizations'. ....	23
Figure 28. Preview (print) JAP Auths Message Screen. ....	24
Figure 29. Print Preview of 'Record of Local Engineering Authorizations'.....	24
Figure 30. <i>Flexibility of Authorizations</i> . ....	25
Figure 31. Copy and Paste Authorizations Message.....	25
Figure 32. <i>'Post' Profile Ready for Authorizations to be Pasted into to</i> . ....	26
Figure 33. Confirmation Message Following Pasting of Authorizations.....	26

## 1 General

There are two distinct functional areas/usage of the engineering authorities databases (EAD); the high level management (carried out by the EAD manager) and the day-to-day usage (carried out by the Sqn/Unit manager). The high level management should be carried out by a limited (it is suggested a maximum of 2 people) number of personnel, who will be required to:

- 1 Install, or arrange for the local IT specialists to install, the EAD.
- 2 Set up the initial structure of the EAD.
- 3 Assign passwords for the various sections that will use the EAD.
- 4 Add the Stn/Ship/Unit local authorizations.
- 5 Monitor and correct any database anomalies.
- 6 Update the EAD as and when amendments become available.

The day-to-day usage covers:

- 1 Loading the data of the individual sections.
- 2 Adding/deleting personnel authorizations.
- 3 Monitoring out-of-date authorizations.

Those units that are upgrading a standalone version should follow these instructions, but the role of EAD manager and Sqn/Unit Manager will be one and the same, as they will not have a network capability.

## 2 EAD Manager

### 2.1 Installation

The first step, prior to actual installation, is to confirm that you have the latest version of the Engineering Authorizations Database (EAD) by checking the details contained at <http://www.jap100a-01.dii.r.mil.uk/AuthDatabase/LatestEngAuthDatabase.htm>. You will also need a PC running Win NT, Win 9X or Win XP and a copy of MS Access 2000 (preferred option) or Access XP installed (An MS Access 97 version of the database is not currently available).

Having confirmed you have the correct version of the EAD, the next step is to identify where you wish the EAD to be stored – standalone PC or network. For either of these locations you will also need to ensure that you have administrator rights to enable you to load the EAD.

#### Note:

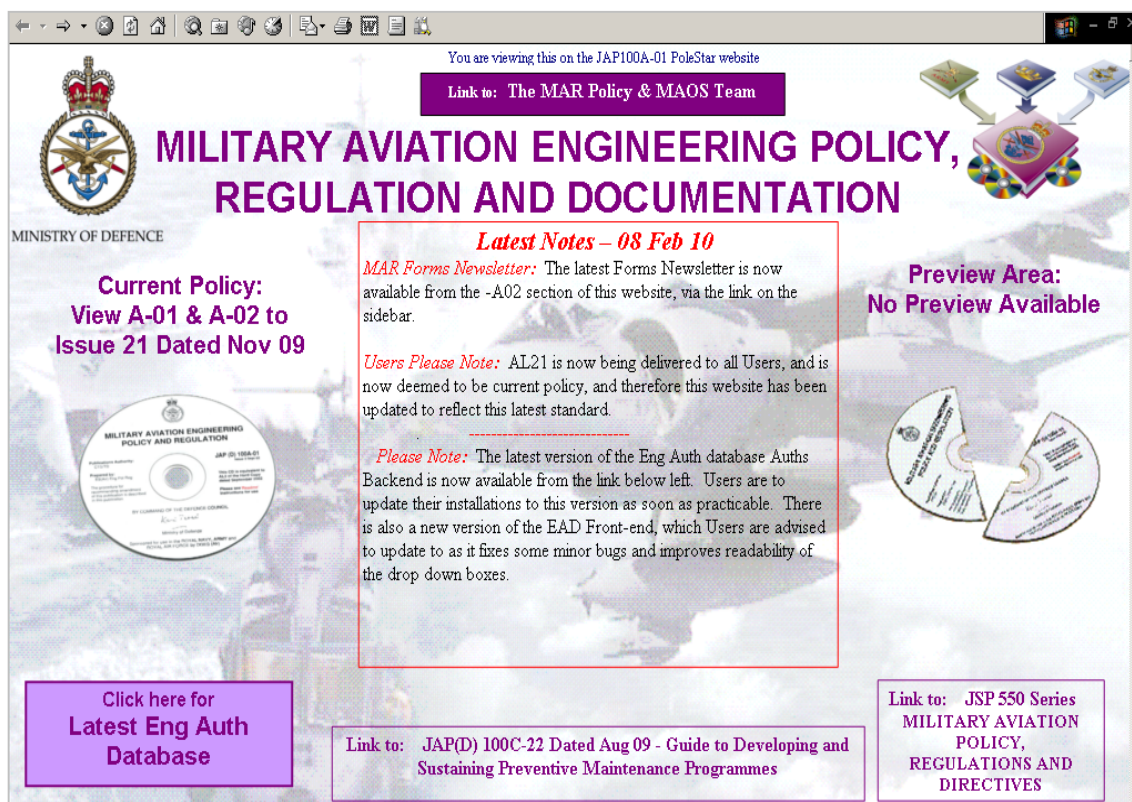
There are two methods of obtaining all files relating to the EAD; from <http://www.jap100a-01.dii.r.mil.uk/> or from the JAP 100A-01 CD ROM (dependant on relevant AL, hence the requirement to confirm the correct AL as described above).

For the purpose of this 'Help' document, it will be assumed that you will be using the <http://www.jap100a-01.dii.r.mil.uk/> to obtain the relevant files for installing your EAD.

#### 2.1.1 Downloading relevant Engineering Authorization Database files

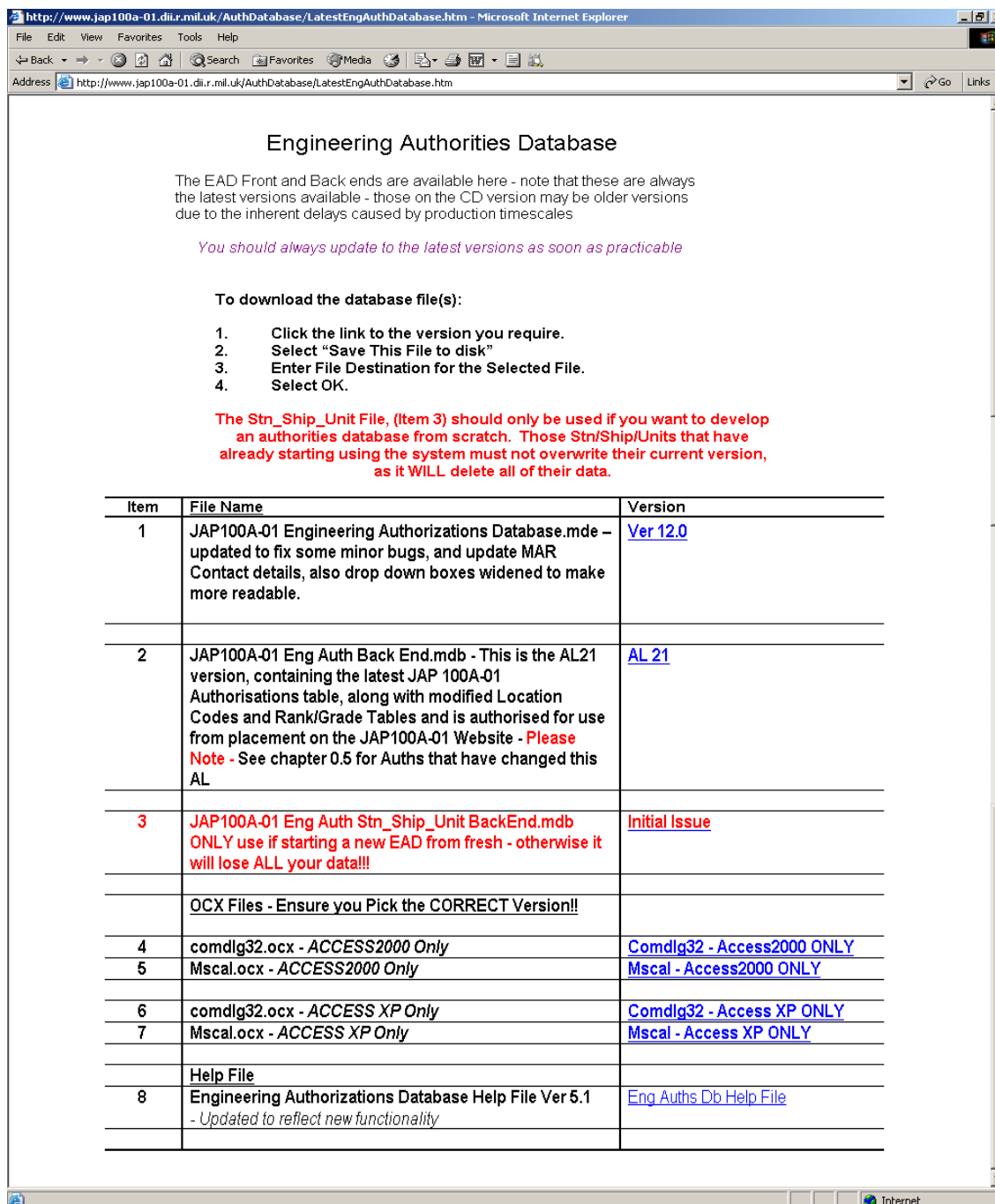
Click, or open Internet Explorer and type in <http://www.jap100a-01.dii.r.mil.uk/> and then press return, where you will be presented with the following screen (certain details will change dependant on actual AL state etc):

Figure 1. JAP 100A-01 Polestar Opening Screen.



Click on the 'Latest Eng Auth Database' link, where you will be presented with the following screen (note, the actual details will change depending on the current AL version of the EAD):

Figure 2. EAD – File Download Screen.



Follow the instructions displayed there and select the location where you intend to hold the EAD, as identified in paragraph 1, i.e. G:/RAF Waddington Engineering Authorizations Database/... or X:/RAF Brize Norton Engineering Authorizations Database/ .....If you intend more than one squadron to access the database then the path should be common to all i.e. choose a group drive that everybody has mapped as the same drive letter.

**Note:**

- 1 It is suggested you make a backup copy of these files following download.
- 2 At RNAS Yeovilton and Culdrose the front end and Stn/Ship/Unit information is held in the Squadron's own common area with a link to the one central version of the JAP 100A-01 Eng Auth Back End.mdb held in the public area.

## 2.2 Installation Errors

It is possible, during installation, that you will receive a number of errors, which are related to the build status of your version of Microsoft Access. If an error occurs stating that an object or control is not supported, or no message block is displayed when "Browse" is clicked when linking the Backend Tables, then:

- 1 Create a folder called "ActiveXControls" in the same directory as the JAP 100A-01 Eng Auth Stn\_Ship\_Unit BackEnd.mdb.
- 2 Download the two ActiveXControls for your version of Access from the JAP website and save them in the "ActiveXControls" folder you have just made (Care should be taken to ensure the correct versions are used or your Access Program will no longer function correctly!).
- 3 Start Microsoft Access from the "Start" menu and create a blank database. Call it tempdb.mdb and place it in the "ActiveXControls" folder.
- 4 Select "Tools", "Active X Controls", and from the buttons on the right select "Register".
- 5 Locate the two ActiveXControls - click on them and open. They will need to be registered one by one.
- 6 On completion of registration close down Microsoft access and activate your EAD.

## 2.3 Activating the EAD

Following installation of the following files:

- 1 JAP 100A-01 Engineering Authorizations Database.mde
- 2 JAP 100A-01 Eng Auth Back End.mdb
- 3 JAP 100A-01 Eng Auth Stn\_Ship\_Unit BackEnd.mdb

### Note:

1. The Stn\_Ship\_Unit File, (Item 3) should only be used if you want to develop an authority's database from scratch. Those Stn/Ship/Units that have already starting using the system must not overwrite their current version, as it will delete all of their data.
2. If copying the files from the CD version you will need to remove the "Read Only" attribute by right clicking on the file, select Properties and remove the tick by "Read Only". This can only be done once you have saved the file to the PC.

You will need to activate your EAD. This is carried out by double clicking the *JAP 100A-01 Engineering Authorizations Database.mde file*. On doing this you will be presented with the following screen:

Figure 3. Link Tables.

**Connect Data Tables**

Reset

**JAP100A-01 Eng Authority Level Back End**

If the connection to the JAP100A-01 Eng Authority Level Back End table has not been done automatically enter the path to it in the box below and click the connect table button.

Browse or enter path to data tables

Browse "Click" to Connect JAP100A-01 Eng Auth Back End Table

**JAP100A-01 Eng Auth Stn/Ship/Unit Back End**

If the connection to the JAP100A-01 Eng Auth Stn/Ship/Unit Back End table has not been done automatically enter the path to it in the box below and click the connect table button.

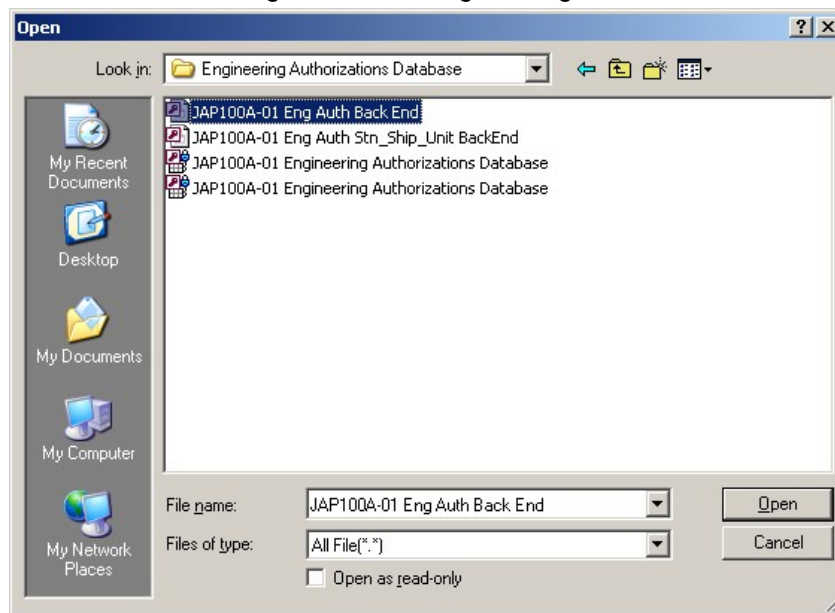
Browse or enter path to data tables

Browse "Click" to Connect JAP100A-01 Stn/Ship/Unit Tables

Go

Click 'Browse' to link the Eng Auth Back End Tables and if on a network choose to navigate via the Network Neighbourhood branch of Windows explorer to ensure the path is drive letter independent. Navigate to the following file (this is where you selected to download to):

Figure 4. Selecting the Eng Auth Back End.



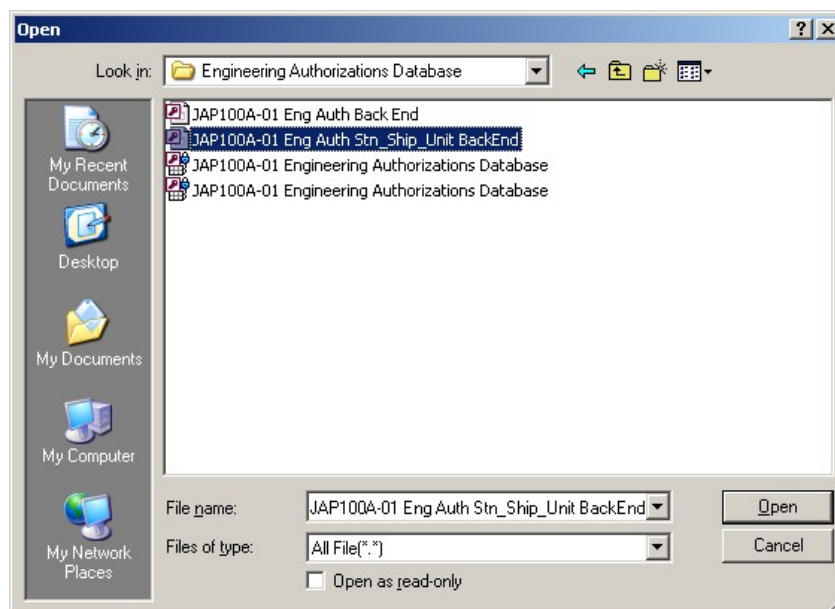
Click 'Click to connect JAP 100A-01.....' You will receive the following message:

Figure 5. Table Link Confirmation Message.



Repeat the process for linking the 'Stn/Ship/Unit' Back End Table:

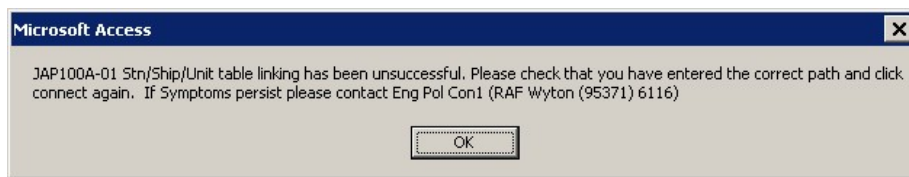
Figure 6. Stn/Ship/Unit.



You may get the following message:



Figure 7. Stn/Ship/Unit Initial Message.



This is probably because you are upgrading an existing Stn/Ship/Unit backend. Click connect again and you will get the following confirmation screen:

Figure 8. Stn/Ship/Unit Linked Correctly Confirmation Screen.

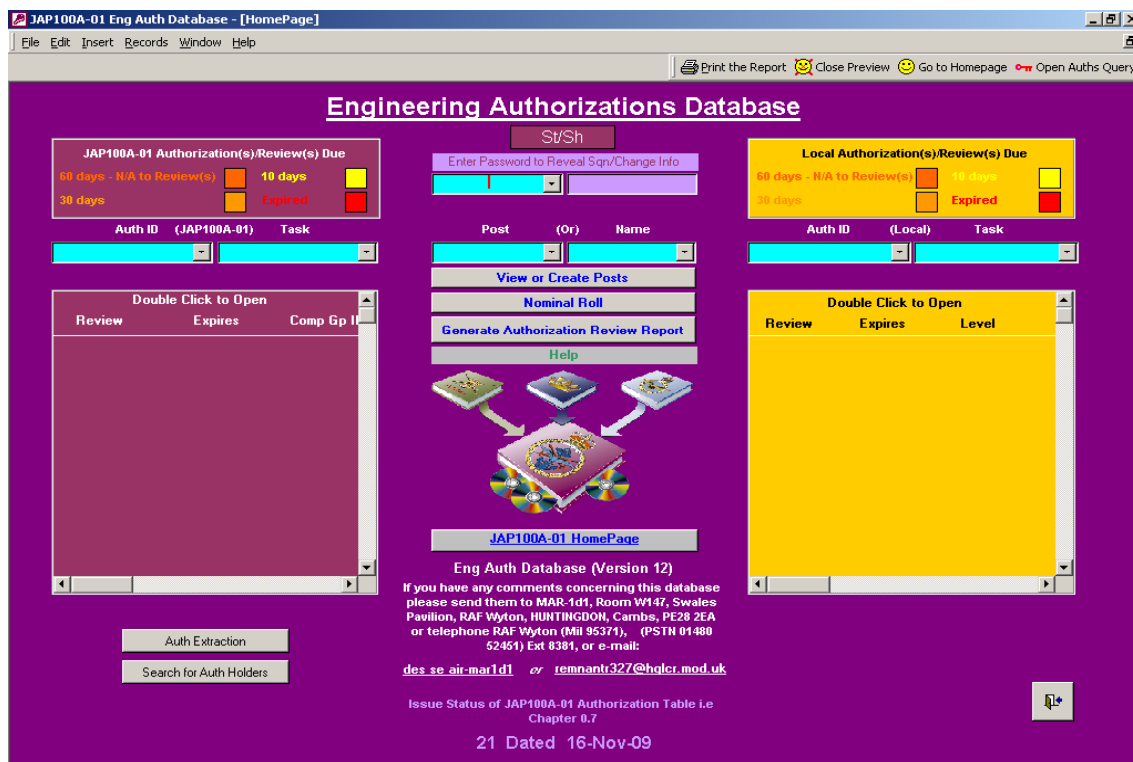


**Note:**

If you are unable to use the "Browse" button you can type the file path directly into the field. Ensure you include .mdb at the end of the address.

You have now carried out the initial set up/installation of the EAD. You should be presented with the following screen:

Figure 9. EAD ▶ Home Page ◀.



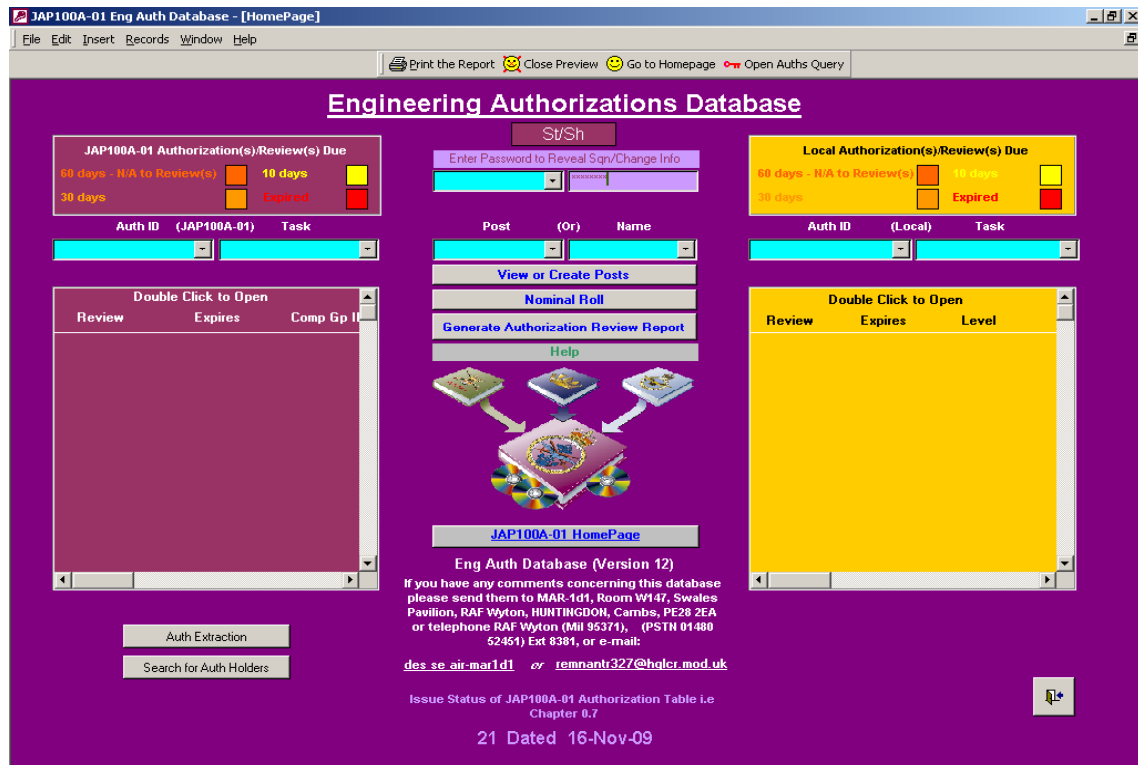
You will note that it has no specific 'Stn/Ship/Unit' and that it is an effectively empty database.



## 2.4 Setting up the Stn/Ship/Unit infrastructure

Before you proceed any further with setting up the EAD, you need to setup the Stn/Ship/Unit. Type in 'password' into the lilac field as ► in Figure 10 ◀ and press return:

Figure 10. Setting up the Stn/Ship/Unit.



After the screen refreshes ►, see Figure 11, ◀ you will note that ► four ◀ new buttons ► have ◀ appeared-

- 1 ► Change Stn/Ship/Unit Info
- 2 Connect or Compact Large Data Tables
- 3 Add Local Authorizations
- 4 Move person

### Note:

For use of "Add Local Authorizations" button see para 3.4. ◀

"Connect Data Tables" is an EAD Help manager function only. ◀

For use of the "Move Person" button see para 4.1.2.

Figure 11. Change Stn/Ship/Unit & Move Person Button Appearance.

Select 'Change Stn/Ship/Unit Info' upon which you will get this screen:

Figure 12. Change Stn/Ship/Unit Location Code.

Select your Stn/Ship/Unit identifier from the dropdown list (shown above) - this list is derived from Chapter 0.6 of the JAP100A-01. Change the password (defaulted to 'password') of the Stn/Ship/Unit – this is the password, which will be used to affect the high level functions of the EAD, by the EAD manager.

You will now need to add the various Sqn/Units at the Stn/Ship/Unit that you wish the EAD to manage. It is suggested that you start with a Headquarters type section, in which you will be able to add the details of the relevant authority level K.

## 2.5 Adding a Sqn/Unit to the Stn/Ship/Unit

Using the 'record' navigation buttons on the Stn/Ship/Unit screen, select the " to go to the next or empty record". Type in the name of the first Sqn/Unit you wish to administer. The Sqn/Unit on the following screenshot is 'Test'. You will need to identify and insert a new password for this Sqn/Unit. If you are upgrading an existing database, the Sqn/Unit information should already be populated. Unless you intend to convert the database to a network wide system you should not need to add any more Sqn/Units.

### Note:

Ensure that the passwords for each of the Sqn/Units of the Stn/Ship/Unit are unique, and are also different to the EAD manager's password.

Figure 13. Adding a Sqn/Unit to your Stn/Ship/Unit EAD.

Continue to add the remaining Sqn/Units to your EAD accordingly. You have now created an empty EAD structure and need to add the relevant authority level K and J's for each section. You cannot do it in the screen above until such time as they have been added to the database. ▶ **Return to EAD Home Page by exiting this screen via the exit icon ◀** .

► Note:

On return to EAD Home Page the following 3 buttons have been removed, Change Stn/Ship/Unit Info, Connect or Compact Large Data Tables and Add Local Authorizations ◀ .

## 2.6 Adding authority level K and J's

### 2.6.1 Adding authority level K

On the EAD ► Home Page ◀ , type the relevant password for the headquarters section in the lilac field and press return. Select the headquarters from the adjacent drop down list. Select 'View or create posts' and you will now be presented with Figure 14. You will need to add, as a first step to populating the Stn/Ship/Unit EAD, the details of the authority level K. Select 'Add a Post' and add the following details (as a minimum):

- 1 Post Title.
- 2 Grade/Appointment. (Select appropriate Level K Grade)
- 3 First Name
- 4 Surname
- 5 Staff/Service No

**Note:**

The Grade/Appointment field is mandatory and must be filled in before any other field can be actioned. It is also mandatory that the fields listed above are completed.

- 6 PQ/Line/LSN/PIC
- 7 Authorization for authority level K - see Figure 15.

Figure 14. Adding Authority Level K.

The screenshot shows a software interface for managing authorizations. The main window is titled 'JAP100A-01 Eng Auth Database - [Post Details]'. It features a menu bar with 'File', 'Edit', 'Insert', 'Records', 'Window', and 'Help'. Below the menu bar, there are tabs for 'JAP100A-01 Authorizations' and 'Local Authorizations'. The 'Local Authorizations' tab is active, displaying a form with various input fields and buttons. The form includes a 'Select Other Post' dropdown, a 'Post Title' field, a 'Sub-Section' dropdown, a 'Location' dropdown (set to 'EngOpsHQ'), a 'PQ/Line/LSN/Pic' field, a 'Tel' field, a 'Grade/Appointment' dropdown, a 'Title' field, a 'First Name' field, a 'Surname' field, and a 'Staff/Service No' field. There are also 'Max Standard' and 'Max Special' notes fields. At the bottom of the form, there are buttons for 'Add Post', 'Delete Post', 'Delete All JAP100A-01 Authorizations', 'Delete All Local Authorizations', 'Move Person', 'Help', 'Preview Local Auths', and 'Preview JAP Auths'. The window also shows a 'Records' section at the bottom with a count of 8 records.

Figure 15. Selecting Authorizations.

JAP100A-01 Eng Auth Database - [Post Details]

File Edit Insert Records Window Help

Print the Report
Close Preview
Go to Homepage
Open Auths Query

JAP100A-01 Authorizations
Local Authorizations

Select Other Post
Local Auths

Post Title
OCFWDSPPT
Grade/Appointment
Wg Cdr
RAF

Sub-Section
Ext ?
Qualifying Training

Location
EngOpsHQ

PQ/Line/LSN/Pic

Tel

See Grade
First Name
IMA
Surname
BOSS

Post Profile
Copy all JAP100A-01 Auths for this Post
Total
Refresh Screen
Global Updates
Select Standard/Special IAW Chapter

Max Standard
K
Max Special
N/A

Notes
See Chapter 1.1.

Notes
Nil.

Level	Task(s)	Authorization Criteria	From	Review	To	Chap	Dep	Type	Grtd?	Print?	Stdg?
JAP-K361		Hold all authority level K authorizations	Nil	28-Apr-08				Standard	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
CompGroupID	JAP101	JAP100A01 Task Requiring Authorization						JAP100A01 Additional Authorization Criteria			
JAP-K205	K	Authorize personnel to be responsible for immediate safety and preservation of aircraft requiring damage assessment	Nil								
JAP-K240	K	Authorize duplicate maintenance forms to be raised if originals lost	Nil								
JAP-K244	K	Authorize extension to RN survival equipment flexible operations	Nil								
JAP-K268	K	Authorize issue of StryShip/Unit Aviation Engineering Standing & Aviation Engineering Routine Orders	Nil								
JAP-K290	K	Issue Aviation Local Technical Instructions	Nil								
JAP-K310	K	Authorize personnel to condition tech eqpt T3/T4 & R3/R4 outside trade boundaries and condition eqpt SCRAF	Nil								
JAP-K319	K	Authorize cannibalization from sustainment fleet	Special auth from IPT								
JAP-K321	K	Dispense with requirement to earth aircraft	Nil								
JAP-K358	K	Auth an auth level J to determine safety precautions taken when foreign military ac land and there is no/sufficient	Nil								
JAP-K361	K	Hold all authority level K authorizations whilst in a Non-Appointed Post, subject to any limitations imposed by the	Nil								
JAP-K370	K	Authorize personnel to authorize cannibalization within StryShip/Unit	Nil								
JAP-K372	K	Authorize personnel to be aircraft TEMPEST Test Team Leader or member	Nil								
JAP-K378	K	Authorize data locking	Nil								
JAP-K379	K	Authorize auditing of electronic data	Nil								
JAP-K381	K	Authorize personnel to be StryShip/Unit Tool Controller	Nil								
JAP-K387	K	Provided extension is permitted in Topic 2N/A/R/11, authorize extensions to explosives maintenance lives by up	Nil								
JAP-K388	K	Provided extension is permitted in Topic 2N/A/R/11, authorize extensions to explosives maintenance lives by up	Nil								
JAP-K408	K	Authorize an authority level J to authorize Battle Damage Repair processes to GSE not detailed in AP 1139-000	Nil								
JAP-K409	K	Authorize use of approved locally manufactured item of GSE/supporting tools iaw JAP 100E-10 Chap 16	Nil								
JAP-K410	K	Authorize personnel to manufacture and certify locally manufactured items of GSE/supporting tools as safe and	Nil								
JAP-K411	K	Authorize personnel to hold GSE inventory iaw JAP 100E-10 Chap 4	Nil								
JAP-K413	K	Authorize personnel to condition Major GSE for transfer/disposal off station/ship/unit iaw JAP 100E-10 Chap 9	Nil								
JAP-K416	K	Authorize personnel to carry out all authority level J/K tasks that do not require additional authorization criteria.	Nil								
JAP-K433	K	Authorize personnel to undertake EFD duties self-supervised	Following award of X annotation to TQA Q-EFD-B qualified personnel								
JAP-K458	K	To authorize personnel to authorize Local Engineering Authorizations only.	The scope of the authorizations covered by this authorization is to be								
JAP-Z454	Z	Top level Auth for Appointed Posts - JPA Use Only	Nil								

Add Post
Delete Post
Delete All JAP100A-01 Authorizations
Delete All Local Authorizations
Move Person
Help
Preview Local Auths
Preview JAP Auths

Record: 8 of 8

Authority level K's get their authorizations by FLC ▶ **Mid Level Instructions** ◀ . Therefore, use the drop down menu on the authorizations screen, and select JAP-K137 for those in an appointed post or JAP-K361 for those in a non-appointed post. (To carry out all authority level K tasks that do not require additional authorization criteria – subject to limitations imposed on subsequent tasks) - as shown in Figure 15.

### 2.6.2 Adding authority level J(s) to the Sgn/Unit nominal roll

On the EAD [▶ Home Page ◀](#), type the relevant password for the relevant Sqn/Unit in the lilac field and press return. Select the Sqn/Unit from the adjacent drop down list. Select 'View or create posts'. Select add a post. Enter the details (see paragraph 2.6.1) of the relevant authority level J. Use the drop down menu on the authorizations screen, and select JAP-J360 for those in an appointed post or JAP-J136 for those in a non-appointed post. If known/identified, it is suggested that you now add the details of the deputy authority level J. (The appropriate Authority Level K must have authorized Deputy Authority Level J's. The database provides the functionality to add any person that can hold Authority Level J as either a standard or special authorization. They will now appear in the drop down boxes on the Sqn/Unit details screens as detailed at [2.6.3](#)). Close the 'Post Details' screen. Repeat for all the Stn/Ship/Unit, Sqn's and Units.

► NOTE: An RAF level J is not an appointed post and cannot be awarded JAP-J360. ◀

### 2.6.3 Adding authority level J(s) and K(s) to the 'Stn/Ship/Unit Info'

From the **► EAD Home Page ◀**, type in the EAD manager's password and select 'Change Stn/Ship/Unit Info'. Navigate to the relevant Sqn/Unit details. Select the authority level K from the drop down list (it is possible to have more than one authority level K at a Stn/Ship/Unit and it is important to select the correct K for the subject Sqn/Unit) - the fields will auto populate. Select the authority level J details from the drop down list, followed by the deputy Authority Level J details. Repeat this process for all the Sqn's/Units. It is mandatory that an Authority Level J and K are entered for each Sqn/Unit; failure to do so will cause problems with the Authorization process and the subsequent print process. Deputy J(s) can be added if required but are not mandatory.

## 2.7 Creating 'Local Authorizations'

► **NOTE:** ◀ Only the EAD Manager can create/amend 'Local Authorizations'.

It is suggested that ► **Local Authorizations** are ◀ created as early on in the life of the EAD as possible. From the EAD ► **Home Page** ◀, select 'Add Local Authorizations'. You will initially see the following screen:

Figure 16. Empty Local Authorizations Screen.

The screenshot displays a software window titled 'JAP100A-01 Eng Auth Database - [Form - Additional Authorizations]'. The main area is a table titled 'Master List of Local Authorizations'. The table has the following columns: 'Strn/Ship/Unit', 'Level', 'LocalAuthID', 'Additional Local Authorization[s] (Click to Sort)', 'Review (Month(s))', 'Reference[s] - "Dbl Click" to +', and 'Granted By'. The table is currently empty. The background of the table area is yellow. There are some input fields and buttons at the top of the table area, including a dropdown for 'Strn/Ship/Unit' with 'AAS' selected, a dropdown for 'Level', a text field for 'LocalAuthID', a text field for 'Additional Local Authorization[s]', a dropdown for 'Review (Month(s))' with '6' selected, a button 'Insert Hyperlink ->', and a dropdown for 'Granted By'. There are also some icons at the bottom left and bottom right of the table area.

Enter the details of the Local Authorization. You will need to identify both the level of the authorization and the details of the person who will award the authorization (note that the drop down list will detail all personnel on the EAD who hold authority level E and above). ► **Figure 17** ◀ shows a partially filled in list of Local Authorizations:

Figure 17. Partially filled In Local Authorizations List.

Strn/Ship/Unit	Level	LocalAuthID	Additional Local Authorization(s) (Click to Sort)	Review (Month(s))	Reference(s) - "Dbl Click" to +	Granted By
VL	B	4	Open Esavian hangar doors	6	Operating Esavian hangar door AE1	845LEVELK
VL	B	5	Operate aircraft passenger steps	6	Operating ac steps AESD	845LEVELK
VL	B	6	Operate dehumidifier and attach to aircraft	6	Operating de-humidification equipm	845LEVELK
VL		(AutoNumber)		6		

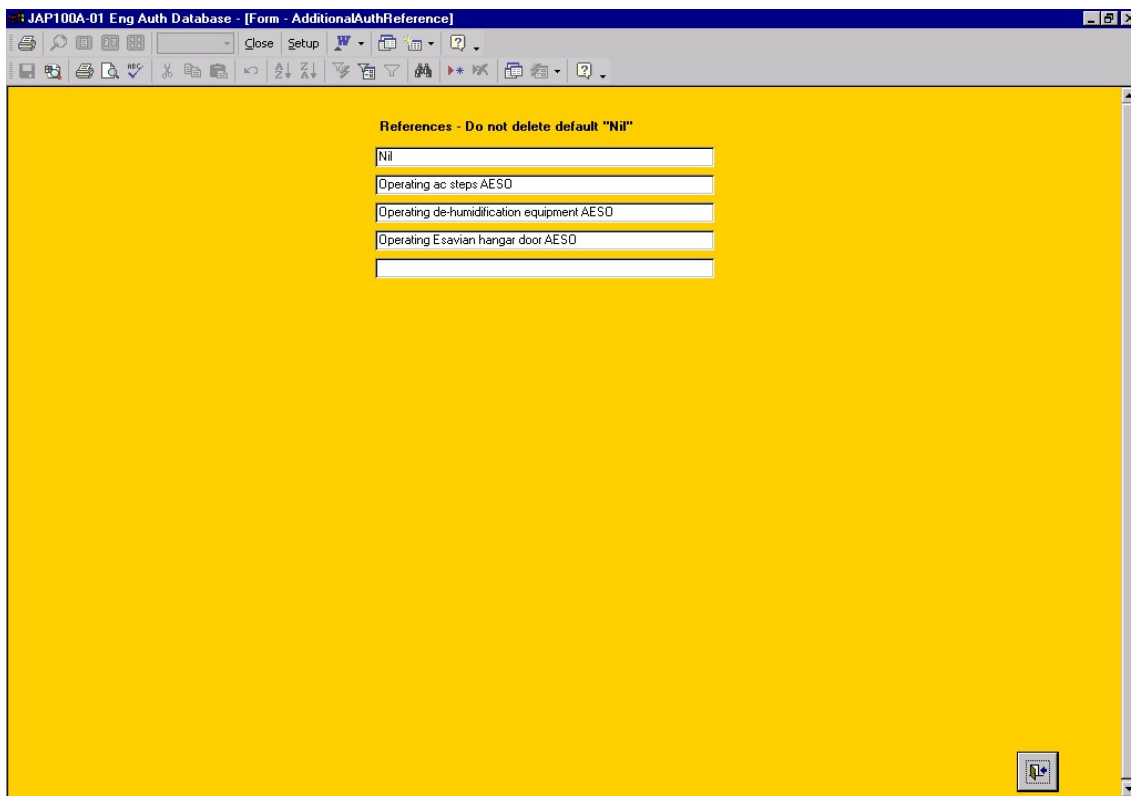
There is a facility to add details of the source of the Local Authorization, i.e. RAF Waddington AESOs, Order 3. This is achieved by double clicking in any of the raised Local authorizations, whereupon you will be shown the following message, prior to the screen at Figure 19 opening:

Figure 18. Local Authorization Source Reference Message.





Figure 19. Adding Source Details of Local Authorization.



JAP100A-01 Eng Auth Database - [Form - AdditionalAuthReference]

References - Do not delete default "Nil"

Nil
Operating ac steps AESO
Operating de-humidification equipment AESO
Operating Esavian hangar door AESO

Additionally, it is further possible to add a hyperlink to the source of the authorization (only applicable if the source is in electronic format) as shown in Figure 17. This process of raising local authorizations should be repeated for all those remaining.

**Note:**

Only the EAD manager will be able to add/amend Local authorizations. Sqn/Unit Managers will only have the facility to append/remove a local authorization against an individual.

***You have now created the bare shell of the EAD for subsequent population by the Sqn/Unit Manager(s).***

## 2.8 Upgrading your EAD to Latest Version

There are two occasions when you will need to upgrade your EAD:

- 1 On changes to the JAP 100A-01 Engineering Authorizations Database.mde i.e. the Front End.
- 2 At each new AL/issue of the JAP 100A-01 a new Chapter 0.7 will be produced – therefore, you will need to update the JAP 100A-01 Eng Auth Back End.mdb file to take account of changes to the authorizations.

### 2.8.1 Upgrading the EAD Front End

Do not overwrite your JAP 100A-01 Eng Auth Stn\_Ship\_Unit BackEnd.mdb file during the upgrade process as you will lose all your existing Stn/Ship/Unit information (remember to always make a backup of this file before carrying out any upgrades to your system).

Carry out the following steps:

- 1 Make a backup of all your 'working' EAD files.

- 1.1 JAP 100A-01 Engineering Authorizations Database.mde
- 1.2 JAP 100A-01 Eng Auth Back End.mdb
- 1.3 JAP 100A-01 Eng Auth Stn\_Ship\_Unit BackEnd.mdb
- 2 Obtain the latest version of the JAP 100A-01 Engineering Authorizations Database.mde from <http://www.jap100a-01.dii.r.mil.uk/AuthDatabase/LatestEngAuthDatabase.htm> or from the latest CDROM of the JAP100A-01 if you do not have access to the website.
- 3 Copy this file to the same location as your existing working version – you will be advised that the file already exists and asked whether you wish to overwrite it. Select yes (this is why you made a backup before carrying out this action).
- 4 Activate the EAD by clicking the new JAP 100A-01 Engineering Authorizations Database.mde file.
- 5 You will need to carry out the link table actions described at Figure 3 and its ensuing paragraphs.

#### 2.8.2 Updating the EAD Authorizations Back End file

- 1 Make a backup of the folder containing your 'working' EAD as per paragraph 2.8.11.
- 2 Obtain the latest version of the JAP 100A-01 Eng Auth Back End.mdb from <http://www.jap100a-01.dii.r.mil.uk/AuthDatabase/LatestEngAuthDatabase.htm>, or from the latest CDROM of the JAP100A-01 if you do not have access to the website.

Copy this file to the same location as your existing working version – you will be advised that the file already exists and whether you wish to overwrite it. Select yes (this is why you made a backup before carrying out this action). There is no requirement to carry out the link table action again for this file.

#### Note:

If copying the files from the CD version you will need to remove the "Read Only" attribute by right clicking on the file, select Properties and remove the tick by "Read Only". This can only be done once you have saved the file to the PC.

## 3 Sqn/Unit Manager

### 3.1 Populating your Sqn/Unit

You should have been provided with a password by the EAD Manager with which you will now be able to access and administer your Sqn/Unit EAD. On the EAD ► **Home Page** ◀ type in this password into the lilac field and press return. Select your Sqn/Unit from the adjacent drop down list and then select 'View or create posts'. You should be presented with the 'Posts' screen, see Figure 14. It is important to remember that the basis of the database is the Sqn/Unit post structure. You should create all the posts with their respective authorizations and change the names of the persons filling that post, as personnel are drafted/posted/appointed. Once a post has been created there should be no need to delete it unless there is an actual manpower audit and it is deemed to be no longer necessary.

Although each person filling a post may not have exactly the same authorizations as the person before, broadly speaking this will be the case. There is a facility to deselect an authorization by un-ticking the granted box thus keeping it in the post profile for future use as necessary or until such time as the individual is qualified. It is suggested that you examine your Sqn/Unit and create a number of post profiles i.e. a squadron may have 20 Air Engineering Mechanics or Senior Aircraftsman all of whom have similar authorizations. Merely create one post "AEM 1" with the necessary generic authorizations and copy these to the subsequent 19 posts you create AEM 2 to AEM 19 etc. For the purpose of this help file it is assumed that you have entered all the post and personal details first to create a Sqn/Unit EAD backbone upon which you will then award authorizations.

### 3.2 Adding personnel to the Sqn/Unit EAD

Select 'Add Post' and proceed to add the following details:

- 1 Post Title
- 2 Grade/Appointment
- 3 First Name
- 4 Surname
- 5 Staff/Service No

**Note:**

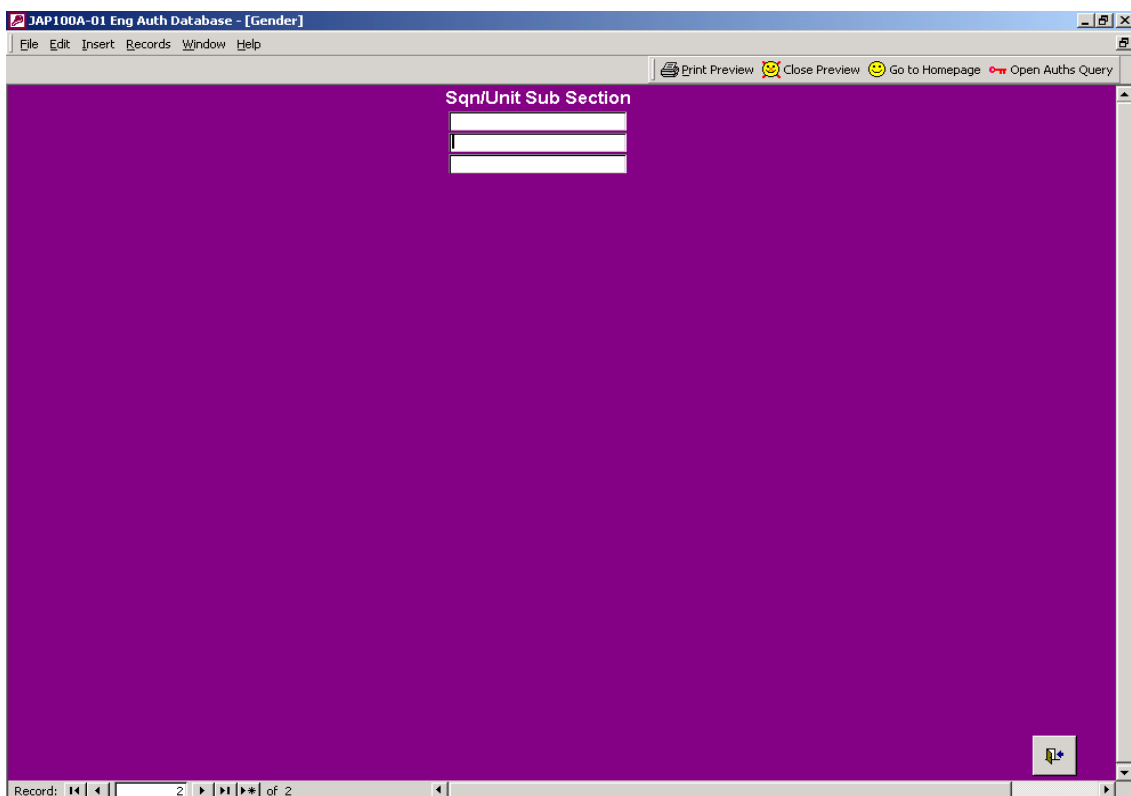
These fields are mandatory and must be completed before any other field may be actioned.

- 6 PQ/Line/LSN/PIC

You have now entered a post into the Sqn/Unit EAD. Repeat the process for all posts in the Sqn/Unit for which the EAD will apply.

To enter a sub section you must first double click on the blank field. The details can then be entered on the screen shown in figure 20.

*Figure 20. Adding a Sqn/Unit Sub Section*



### 3.3 Awarding authorizations against Sqn/Unit personnel

**Note:** Only a signed printed authorization certificate is authoritative.

Access the 'Post' details of your Sqn/Unit EAD. Open the details of the individual concerned by clicking the drop down list 'Select other post'. You can find the individual by either scrolling down to their post or by entering the exact details of the post name. Upon selection, the details will be shown for the individual concerned. You can now append the authorizations to be awarded.

JAP 100A-01 Chapter 0.7 details all current engineering authorizations and includes a [Comp ID](#) reference number and corresponding [Approve ID](#), e.g.:

Comp ID	Task Requiring Authorization	Additional Authorization Criteria	Source Chapter	Auth By	St/Sp	Lim Ref	Approve ID
JAP-C9	Instruct tradesmen in the maintenance of aircraft armament systems.	Appropriate trade or specialization.	<a href="#">Chapter 14.5</a>	K			JAP-K361
JAP-C27	Supervise maintenance of an aircraft armament system.	Must have completed appropriate training for the relevant aircraft type.	<a href="#">Chapter 14.5</a>	J			JAP-J10

Figure 21. Authorization Selection.

Page 19 of 27

Figure 22. Authorization Details.

JAP100A-01 Eng Auth Database - [Post Details]

File Edit Insert Records Window Help

Print the Report Close Preview Go to Homepage Open Auths Query

JAP100A-01 Authorizations Local Authorizations

Select Other Post Local Auths "Add Click" field boxes to add to list Max Standard F Max Special G

Post Title PROPTM1 Grade/Appointment Sgt (inc AGE) RAF Notes Nil Notes Nil

Sub-Section Ext ? Qualifying Training

Location EngOpsHQ Title See Grade First Name IMA

PQ/Line/LSN/Pic Tel Staff/Service No G76276171 Surname SMITH

Post Profile Copy all JAP100A-01 Auths for this Post Total 1 Refresh Screen Global Updates Select Standard/Special IAW Chapter

Level	Task(s)	Authorization Criteria	From	Review	To	Chap	Dep	Type	Gtld?	Print?	Sgd?
JAP-C9	Instruct tradesmen in aircraft armament systems maintenance	Appropriate trade or specialization	28-Apr-08	Review + 1	From + 24	K		Standard			
Limitation(s)				Assessed Competent IAW Reference	14.5	By					
			28-Apr-08	Review + 1	From + 24						
Limitation(s)				Assessed Competent IAW Reference		By					

"Add Click" fields to Revised Calendar

Add Post Delete Post Delete All JAP100A-01 Authorizations Delete All Local Authorizations Move Person Help Preview Local Auths Preview JAP Auths

Record: 8 of 8

The 'from' date is defaulted to the date that the authorization is awarded - this can be amended by double clicking the date shown and using the calendar that appears. You can append a review period for the authorization by clicking the 'Review + 1' button or by double clicking in the date field of 'Review'. The 'to' is defaulted to 24 months when the button is clicked, although, again by double clicking the date field you may select any 'To' date. Repeat this process for any further authorizations to be awarded to the individual. When you have completed this, you will need to check that they are able to be awarded the individual authorizations. By way of example, the following screen shot shows an authorization, which cannot be awarded due to the recipient being of the wrong authority level:

Figure 23. Ineligible Authorization.

Microsoft Access - [Post Details]

JAP100A-01 Authorizations Local Authorizations

Select Other Post: [PROPTM1] Local Auths: [Nil Click] Field Boxes to add to list

Post Title: [PROPTM1] Grade/Appointment: [Sgt (Inc AGE)] Max Standard: [F] Max Special: [G]

Sub-Section: [EngOpsHQ] Ext ? [ ] Qualifying Training: [ ]

PQ/Line/LSN/Pic: [ ] Title: [See Grade] First Name: [IMA] Surname: [SMITH]

Tel: [ ] Staff/Service No: [G76276171]

Post Profile: [Copy all JAP100A-01 Auths for this Post] Total: [2] Refresh Screen: [ ] Global Updates: [ ] Select Standard/Special IAW Chapter: [ ]

Level	Task(s)	Authorization Criteria	From	Review	To	Chap	Dep	Type	Grid?	Print?	Sgd?
JAP-C9	Instruct tradesmen in aircraft armament systems maintenance	Appropriate trade or specialization	28-Apr-08	Today	Review + 1	From + 24	<input type="checkbox"/>	Standard	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Limitation(s)					Assessed Competent IAW Reference	14.5	By				
JAP-H21	Waive flight servicing	When there is no authority level J available	28-Apr-08	Today	Review + 1	From + 24	<input type="checkbox"/>	Standard	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Limitation(s)					Assessed Competent IAW Reference	2.8	By				
			28-Apr-08	Today	Review + 1	From + 24	<input type="checkbox"/>	Standard	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Limitation(s)					Assessed Competent IAW Reference		By				

Record: 2 of 8

Form View

Buttons: Add Post, Delete Post, Delete All JAP100A-01 Authorizations, Delete All Local Authorizations, Move Person, Help, Preview Local Auths, Preview JAP Auths

3.3.2 If the authorization is being awarded by the Deputy level J, then the “Dep” tick box is to be completed. These authorizations may then be printed using the “Preview JAP Auths” button and selecting the “Yes” option from the displayed message box. Please Note: the printouts only show the Auths granted by the relevant J, if a person has been Authorised by both his “J” and his “Deputy J”, you will need to printout using both the “Yes” and “No” options to have all his Auths printed. For this reason, it is advisable to have any Auths granted by a “Deputy J” re-appraised by the “J” when they become available again; the “Dep” tick can then be removed and the subsequent single printout will then show all Auths.

Where the level J/K requests an assessment of competency by another person, prior to awarding the authorization, there is the facility to record their details. If this assessment is not required then there is no requirement to populate this field.

If it is the intention to grant the authorization at this time, then the “Granted” box is to be ticked. There maybe occasions when this box is not ticked; for example if you have created generic post details and the person is not currently eligible to be granted this authorization. To include the authorization in the print then you must ensure that the “Print” box is ticked.

### 3.4 Local authorizations

Local authorizations are awarded by selecting the button ‘Local Auths’ and selecting from the local authorizations screen. This is similar to the JAP authorization process but only allows those authorizations that have been raised by the EAD Manager to be awarded. ▶ Figure 24 ◀ shows the Local Authorizations screen:

Figure 24. Local Authorizations Screen.

Microsoft Access - [Post Details]

JAP100A-01 Authorizations Local Authorizations

Select Other Post: JAP100A-01 "Dbl Click" Field Boxes to add to list

Post Title: PROPTM1 Grade/Appointment: Sgt (inc AGE) RAF

Sub-Section: EngOpsHQ Ext ?

Location: EngOpsHQ

PQ/Line/LSN/Pic: Title: See Grade First Name: IMA Surname: SMITH

Tel: Staff/Service No: G76276171

Post Profile: Copy all Local Auths for this Post Total: 0 Refresh Screen Global Updates

Level(s)	Auth(s)	From	Review	To	Reference(s)	Grid? Print? Sgd?
WAD-B32	9065 - Authority to operate and maintain Major Respiratory Protective equipment within the user Filr/Section - Syllabus 197	28-Apr-08	28-Apr-08		HyperLink to Ref	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>
Delete		Today	Review + 1	From + 24		AEO
Limitation(s)					Certified Competent IAW Ref	By
WAD-J130	Authorise Local Authorisations for personnel within their area of responsibility.	28-Apr-08	28-Oct-08		HyperLink to Ref	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>
Delete		Today	Review + 1	From + 24	Not Eligible	
Limitation(s)					Certified Competent IAW Ref	By
		28-Apr-08			HyperLink to Ref	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>
Delete		Today	Review + 1	From + 24		
Limitation(s)					Certified Competent IAW Ref	By

"Dbl Click" Fields to Reveal Calendar

Add Post Delete Post Delete All JAP100A-01 Authorizations Delete All Local Authorizations Move Person Help Preview Local Auths Preview JAP Auths

Record: 2 of 8

Form View

The following screen shows 2 local authorizations being awarded. One shows correct eligibility and the other is not eligible:

Figure 25. Local Authorizations - Eligibility.

Microsoft Access - [Post Details]

JAP100A-01 Authorizations Local Authorizations

Select Other Post: JAP100A-01 "Dbl Click" Field Boxes to add to list

Post Title: PROPTM1 Grade/Appointment: Sgt (inc AGE) RAF

Sub-Section: EngOpsHQ Ext ?

Location: EngOpsHQ

PQ/Line/LSN/Pic: Title: See Grade First Name: IMA Surname: SMITH

Tel: Staff/Service No: G76276171

Post Profile: Copy all Local Auths for this Post Total: 0 Refresh Screen Global Updates

Level(s)	Auth(s)	From	Review	To	Reference(s)	Grid? Print? Sgd?
		28-Apr-08			HyperLink to Ref	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>
Delete		Today	Review + 1	From + 24		
Limitation(s)					Certified Competent IAW Ref	By

"Dbl Click" Fields to Reveal Calendar

Add Post Delete Post Delete All JAP100A-01 Authorizations Delete All Local Authorizations Move Person Help Preview Local Auths Preview JAP Auths

Record: 2 of 8

Form View

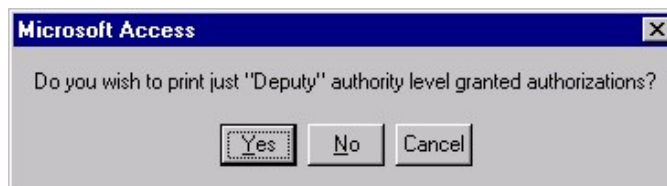


The reason for ineligibility is that the individual is the incorrect authority level to receive the local authorization. You will see that local authorizations carry the same functionality as JAP authorizations and that there is the facility to follow the hyperlinks to its source. Continue to add local authorizations as appropriate.

### 3.5 Printing of individuals Authorization Certificate (JAP and Local)

When you have raised the authorizations against the individual and have checked that they are eligible to hold them, you need to print them off so that the authorization certificates can be signed (thereby making the authorizations valid). To do this, select 'Preview JAP Auths' where you will receive this message screen:

Figure 26. Preview (print) JAP Auths Message Screen.



At this point in your EAD administration you will press 'No' - the help file covers 'Deputy J' authorizations at Para 3.3.2. You will then receive the following screen, which is a print preview of the JAP Auths Certificate:

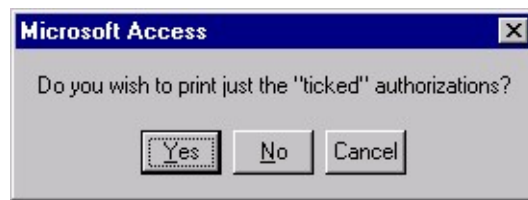
Figure 27. Print Preview of 'Record of Engineering Authorizations'.

The image shows a print preview of a form titled "Record of Engineering Authorizations". The form is part of the "JAP100A-01 Eng Auth Database" application. It contains several sections: a header with reference numbers, a table of tasks with columns for task ID, description, and authorization details, and a signature section at the bottom. The form is displayed in a window with a standard Windows toolbar and a status bar at the bottom indicating "Page 1 of 1".

Task ID	Description	Authorization Details
JAP-0109	To carry out testing operations on aircraft.	02-Apr-04
JAP-0109	Authorized to sign test signature for test work within test boundary.	02-Apr-04
JAP-0112	Carry out flight testing.	02-Apr-04

After viewing the certificate and confirming it contains the correct information, press the 'print' button to obtain the paper certificate. It will need the relevant signatures before it becomes an authoritative document. The local authorizations certificate is obtained by selecting 'Preview Local Auths' whereupon you will receive the following message:

Figure 28. Preview (print) JAP Auths Message Screen.



Select 'Yes' if you wish to preview all the local authorizations that have been granted or pick No to see those that have been assigned but not granted. Whereupon you will receive the following screen:

Figure 29. Print Preview of 'Record of Local Engineering Authorizations'.

JAP100A-01 Eng Auth Database - [Query Post Details]

Ref: JAP100A-01 Chap 4.3

Record of Local Engineering Authorization

Eng Auth Database (Version 2)

Str/Ship/Unit

Post Title: PG/LIN/LSM/PLC No: Max Standard: Max Speed: Title: Grade/Appointment: First Name: Surname: Str/Service No: Auth ID:

RAW ID: (3423424) B: 0: Size Grade: ABA: (BA) BWO RKA: ( )

Level	Additional Local Auth(s)	From	Author	To	Reference(s)	Granted By
VL-8+	Open location hanger doors	02-Apr-04	02-APR-04	02-Apr-06	NA	AB
Unlocked(s)			Certified Competent Rail Ref by:			Req:
VL-86	Operate de-humidifier and attach to aircraft	02-Apr-04	02-APR-04	Eng Wg/ABSO/AC/PLB by 12018er/21er/1		AB
Unlocked(s)			Certified Competent Rail Ref by:	04-LEVELK	BROUW	Req:
Local Auth(s): Signature of Authorization		Grade/Appointment	Name	Signature	Post Title	Date
I authorize the person detailed on this record to carry out the task(s) listed above and understand the responsibilities associated with them, and the implications of using my (specimen) signature/print for given purpose on maintenance documentation.		BA80	BROUW		04-LEVELK	02-Apr-04

Practitioner's Declaration

I certify that I have read the JAP100A-01 Chapter relating to the task(s) listed above and understand the responsibilities associated with them, and the implications of using my (specimen) signature/print for given purpose on maintenance documentation.

Size Grade: MA: BWO RKA: Signature: Name: 02-Apr-04

ABA: ( )

Date & Time Entered: 02-APR-04 14:22:30

Page 1 of 1

### 3.6 Flexibility of raising authorizations

There is a great deal of flexibility built in to the authorizations database with respect to the authorizations listed against an individual. The EAD allows authorizations to be:

- 1 Listed against an individual, but are not actually awarded. This enables the authorizer to control when they become active, i.e. when the individual goes on detachment specific authorizations may be awarded.
- 2 'Limited', i.e. authorization to defer corrective maintenance by raising MOD F703 and MOD F704s being limited to "When operating away from MOB".

Examples of the above are shown in ▶ **Figure 30** ◀:

Figure 30. Flexibility of Authorizations.

**Microsoft Access - [Post Details]**

Print the Report Close Preview Go to Homepage Open Auths Query

JAP100A-01 Authorizations Local Authorizations

Select Other Post Local Auths "Did Click" Field Boxes to add to list Max Standard F Max Special G

Post Title PROPTM1 Grade/Appointment Sgt (Inc AGE) RAF Notes Nil

Sub-Section Ext ? Qualifying Training Nil

Location EngOpsHQ Title See Grade First Name IMA

PQ/Line/LSN/Pic Staff/Service No 676276171 Surname SMITH

Tel

Post Profile Copy all JAP100A-01 Auths for this Post Total 3 Refresh Screen Global Updates Select Standard/Special IAW Chapter

Level	Task(s)	Authorization Criteria	From	Review	To	Chap	Dep	Type	Grid?	Print?	Sgd?
JAP-C9	Instruct tradesmen in aircraft armament systems maintenance	Appropriate trade or specialization	28-Apr-08	Review + 1	From + 24			Standard	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Delete	T		Today	Review + 1	From + 24	K		JAP-K11			
Limitation(s)				Assessed Competent IAW Reference	14.5	By					
JAP-F351	Anticipate scheduled maintenance by any amount of the relevant periodicity unless otherwise constrained by an	Nil	28-Apr-08	Review + 1	From + 24			Standard	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Delete	T		Today	Review + 1	From + 24	J		JAP-J431			
Limitation(s)				Assessed Competent IAW Reference	5.3	By					
JAP-F466	To undertake the duties of an Arising Manager.	Completed platform and GMS specific training.	28-Apr-08	Review + 1	From + 24			Standard	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Delete	T		Today	Review + 1	From + 24	J		JAP-J467			
Limitation(s)				Assessed Competent IAW Reference	7.3.3	By					
			28-Apr-08	Review + 1	From + 24				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Delete	T		Today	Review + 1	From + 24						
Limitation(s)				Assessed Competent IAW Reference		By					

"Did Click" Fields to Reveal Calendar

Add Post Delete Post Delete All JAP100A-01 Authorizations Delete All Local Authorizations Move Person Help Preview Local Auths Preview JAP Auths

Record: 2 of 8

Form View

You should note that the JAP-F466 authorization is shown against the individual, but has not been awarded - shown by the 'Granted' and 'Printed' elements of the authorization not being ticked. The 'Printed' tick box also allows you to print a single authorization if for example one had been added to a profile containing several hundred thus negating the need to re-authorize those already held. Please remember to re-tick the box when all the authorizations for that post require re-authorization.

### 3.7 Multiple personnel with same authorizations

To remove the requirement to individually raise each and every authorization for each and every individual on the Sqn/Unit, the EAD contains a copy and paste system for authorizations. First, select or create the generic 'Post' profile and select 'Copy all JAP 100A-01 Auths for this post'. Upon which you will receive the following message:

Figure 31. Copy and Paste Authorizations Message.



Open or create the relevant post to have the authorizations copied to by either adding a post or using the magenta drop down boxes (top left) to locate a post already in existence in the database:

Figure 32. 'Post' Profile Ready for Authorizations to be Pasted into to.

Note that the 'Copy JAP 100A-01 Auths for this Post' has changed to 'Paste Copied JAP 100A-01 Auths to this Post'. Press this button, upon which you will get the following message:

Figure 33. Confirmation Message Following Pasting of Authorizations



This process may be repeated for as many individuals that have a similar 'Post' profile.

## 4 Things you may wish to do with the EAD

The following is a list of tasks that you may need to do with the EAD:

### 4.1.1 Change the personal details of a 'Post' following the draft/posting of an individual.

When an individual leaves a post, do not delete it merely:

- 1 Overwrite his/her personal details with those of the incoming individual.
- 2 Check the eligibility of the authorizations and withdraw by un-ticking the granted box as required.
- 3 Re-date the 'from', 'Review' and 'To' dates.
- 4 Re-print the authorization certificate for signature.
- 5 There is a tick box that can be checked once confirmation has been received that a particular authorization has been granted and signed in hard copy.

**Note:**

A global update button allows you to quickly refresh the 'From' and 'To' dates for each of the JAP100A-01 authorizations and again for the local authorizations.

**4.1.2 Moving a person within the EAD**

By selecting the "Move Person" button (EAD start up screen for EAD manager or Post Details screen for Sqn/Unit manager) there exists the functionality to move a person from their current Ship/Unit/Establishment to a new location providing it is within the same EAD. It is important that once the person is in their new Ship/Unit/Establishment that their authorizations are reviewed and re-authorized by their new Level J/K as appropriate.

**4.1.3 Identifying who holds a particular authorization.**

The EAD can be used to identify who holds a particular authorization. To obtain this information enter the authorization details in the appropriate field (JAP or Local) on the EAD start up screen (Figure 9). The EAD will automatically return a list with all of the persons holding the requested authorization, as recorded within this particular database.

Alternatively you can click on the "Search for Auth Holders" button on the EAD start up screen (Figure 9). By entering the authorization number at the prompt a list of personnel will be returned. This output will need to be saved as an Excel worksheet. This functionality allows the identification of holders of authorizations that have been superseded or cancelled.

**5 Printer problems**

If you are experiencing difficulties with printing reports to your default printer try the following fix before speaking to your IT section:

1. Ensure the Access application is closed.
2. Click Start, Settings and click Printers.
3. Right click the problem printer and then click Properties.
4. In the Properties dialog box click the Printing Preference button.
5. Click each tab in the Printing Preferences dialog box **without** making any changes.
6. Click OK to close the Printing Preferences dialog box.
7. Click OK to close the Properties dialog box.
8. Restart Access and then try to print the report again.

**6 Your Comments**

Please provide feedback on the usefulness/correctness of this help file and of any omissions that you believe should be included by clicking the following hyperlink:

[E-mail Comment/Observations/Improvements](#)

Or contact us at:

EAD Help, ► **MAA Tech Reg ASPPIC1** ◀ , Room W147, Swales Pavilion,  
RAF Wyton, Huntingdon, Cambs, PE28 2EA  
Phone: 95371 (01480 52451) Ext 8381 or Ext 5386