

# MSATS PARTICIPANT RIGHTS ADMINISTRATION USER INTERFACE GUIDE

VERSION: 9.04  
DOCUMENT REF: MMSTDPD80  
PREPARED BY: Information Management and Technology (IMT)  
DATE: 7 April 2011  
Final

**Copyright**

Copyright © 2011 Australian Energy Market Operator Limited

All Rights reserved. This entire publication is subject to the laws of copyright and intellectual property Rights. This publication may be printed for personal informational use as long as the copyright notices stay intact, but may not be re-distributed, re-sold, reproduced, stored in a retrievable system or transmitted in any form by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the Australian Energy Market Operator Limited, except as permitted under the Copyright Act 1968.

AEMO is not responsible for and will not be liable to any person in relation to the use of or reliance on any of the information contained in this document.

**Trademark Notices**

Microsoft, Windows and SQL Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates.

Sun and Java are trademarks, registered trademarks, or service marks of Sun Microsystems, Inc. in the U.S. and other countries.

**Disclaimer**

This document is made available to you on the following basis:

1. Purpose – This User Interface Guide (Guide) has been produced by the Australian Energy Market Operator Limited (AEMO) to provide information about the MSATS Participant administrator functions available within the MSATS web portal, as at the date of publication.
2. No substitute – This Guide is not a substitute for, and should not be read in lieu of, the National Electricity Law (NEL), the National Electricity Rules (Rules) or any other relevant laws, codes, rules, procedures or policies. Further, the contents of this Guide do not constitute legal or business advice and should not be relied on as a substitute for obtaining detailed advice about the NEL, the Rules, or any other relevant laws, codes, rules, procedures or policies, or any aspect of the national electricity market or the electricity industry.
3. No Warranty – While AEMO has used due care and skill in the production of this Guide, neither AEMO, nor any of its employees, agents and consultants make any representation or warranty as to the accuracy, reliability, completeness or suitability for particular purposes of the information in this Guide.
4. Limitation of liability - To the extent permitted by law, AEMO and its advisers, consultants and other contributors to this Guide (or their respective associated companies, businesses, partners, directors, officers or employees) shall not be liable for any errors, omissions, defects or misrepresentations in the information contained in this Guide, or for any loss or damage suffered by persons who use or rely on such information (including by reason of negligence, negligent misstatement or otherwise). If any law prohibits the exclusion of such liability, AEMO's liability is limited, at AEMO's option, to the re-supply of the information, provided that this limitation is permitted by law and is fair and reasonable.

**Distribution**

Available to public

**This Document Identification**

Title: MSATS PARTICIPANT RIGHTS ADMINISTRATION USER INTERFACE GUIDE

Version: 9.04

Document ID: MMSTDPD80

Responsible Department: Information Management and Technology (IMT)

Notes: MSATS 3.0 - Build #46.77

Documents made obsolete: The release of this document changes only the version of the MSATS PARTICIPANT RIGHTS ADMINISTRATION USER INTERFACE GUIDE. No documents are made obsolete by releasing this document version.

# Contents

1	Introduction .....	1
1.1	Purpose.....	1
1.2	Audience .....	1
1.3	Scope.....	1
1.3.1	What's in this guide .....	1
1.3.2	Related resources .....	1
1.4	Organisation.....	2
1.4.1	Conventions .....	2
2	MSATS Security Model .....	4
2.1	Entities .....	4
2.1.1	Interactive Entities .....	5
2.1.2	Batch Entities .....	6
2.2	Rights and privileges .....	7
2.3	Users.....	8
2.3.1	AEMO system administrators.....	8
2.3.2	Participant administrators.....	8
2.3.3	Participant users.....	8
2.3.4	Business groups .....	8
3	Maintain Rights .....	10
3.1	Viewing rights.....	10
3.2	Creating a new right .....	12
3.3	Editing a right .....	15
3.4	Removing a right .....	17
4	User Administration .....	18
4.1	Viewing user profiles .....	18
4.2	Creating a new user profile.....	19
4.3	Editing a user profile.....	21
5	Managing the use of Set Participant .....	22
5.1	Retaining multiple user ID logins .....	22
5.2	Transforming from multiple user ID logins to single user ID logins.....	23
5.2.1	Flowchart of Recommended Implementation .....	24
5.2.2	Checklist for implementing single user ID logins .....	26
6	Glossary .....	27
6.1	Abbreviations .....	27
6.2	Special terms .....	27
7	References.....	29



7.1	AEMO's website .....	29
7.2	EITS publications .....	29
7.3	Information centre .....	29

## 1 Introduction

### 1.1 Purpose

This document is a user interface guide for the MSATS participant administrator functions available within the MSATS Web Portal, version 3.0 – software build 46.77. The document is part of the MSATS User Guide Group, see “Related resources” on page 1 for information on other documents in the MSATS group.

### 1.2 Audience

The audience for this guide is:

- Participant administrators (including ombudsman administrators) who maintain a subset of components as assigned by the AEMO system administrator.
- AEMO system administrators who maintain components and ensure that participant access to MSATS is restricted to only the areas they require to complete their duties.
- AEMO users, using the MSATS Web Portal for administration purposes.

### 1.3 Scope

#### 1.3.1 What’s in this guide

This document contains information on how administrators can maintain the MSATS system security by:

- Maintaining MSATS access rights.
- Maintaining user profiles.
- Setting up single user ID logins.

For information about how to:

- Log in or out of the MSATS Web Portal, see “References” on page 29.

#### 1.3.2 Related resources

The MSATS User Guide Group of documents form a detailed guide to the use of the MSATS Web Portal. Each document is targeted towards a specific audience and explains how to navigate and use the menus for each MSATS Web Portal function.

The documents are accessed by clicking the [User Guides](#) link on the MSATS main menu.



The following table provides a description of each document in the MSATS User Guide Group and its intended audience.

Document name	Description	Registered participants	B2B users	Participant admins	Ombudsman organisations	AEMO
MSATS Introduction Guide	An overview of the MSATS Web Portal. Contains a list of Reference Information referred to in this document.	✓	✓	✓	✓	✓
MSATS User Interface Guide	Explains how to use the MSATS participant Web Portal functions	✓	✓	✓	✓	✓
MSATS AEMO User Interface Guide	Explains how to use the MSATS AEMO only Web Portal functions					✓
MSATS B2B User Interface Guide	Explains how to use the B2B functions		✓			✓
MSATS Participant Rights Administration User Interface Guide	Explains how to create and maintain users to provide them access to your data.			✓	✓	✓
MSATS Ombudsman Enquiry User Interface Guide	Explains how to use the Ombudsman Enquiry system.				✓	✓

## 1.4 Organisation

This document is organised in the following way:

- The “MSATS Security Model” on page 4 explains the components for managing and restricting user access to AEMO’s systems.
- The following sections explain how to use each of the administration menus in the MSATS Web Portal.
- The “Managing the use of Set Participant” on page 22 explains how to set-up “single user ID logins” for participant users who have several user IDs and passwords.
- The final sections contain a glossary of abbreviations, special terms and a list of useful references.

### 1.4.1 Conventions



**Important Note:** important information.



**Note:** notes, hints and tips.

**Menu item:** text formatted in this style refers to a menu item in the MSATS Web Portal.

**Button:** text formatted in this style refers to a button to click on a screen.

**Link:** text formatted in this style refers to a link to click on a screen.

**Screen:** text formatted in this style refers to a field or description on a screen.

**“Reference”:** text formatted in this style refers to another document or section in this document.

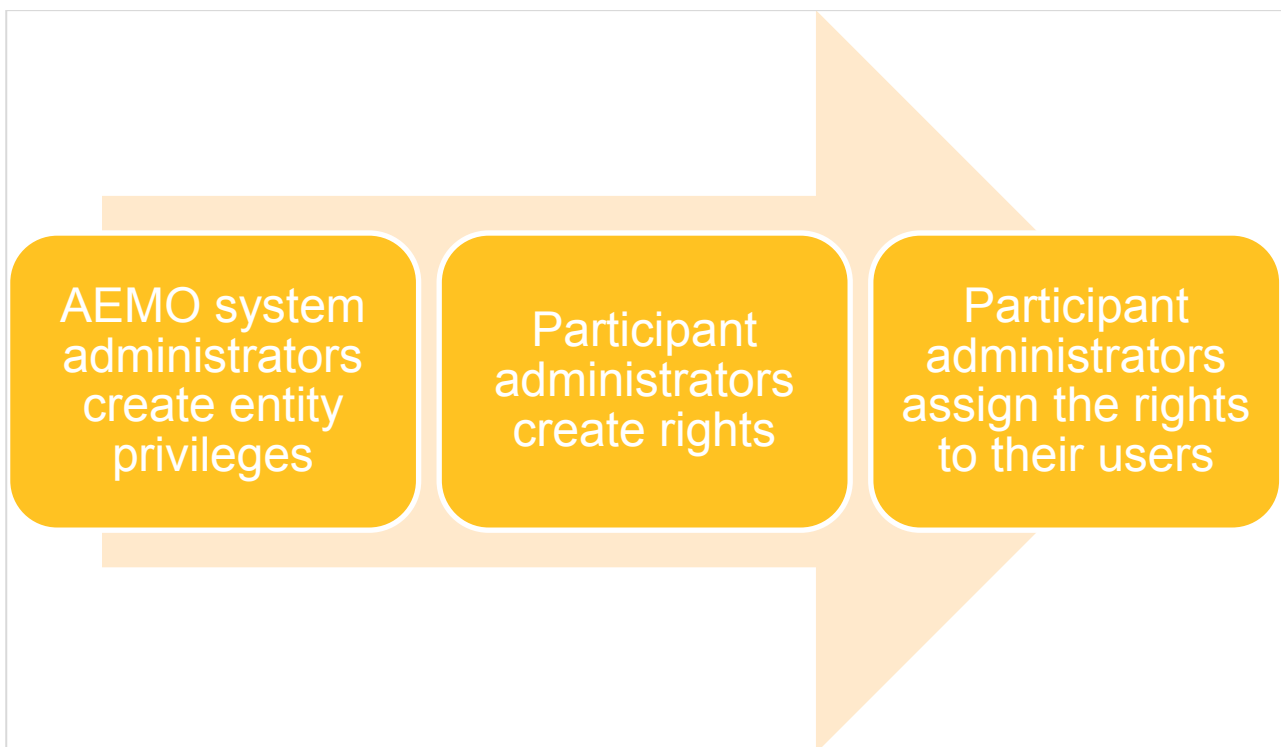
## 2 MSATS Security Model

The MSATS Security Model permits administrators to manage access to AEMO's systems. All users are components of the MSATS Security Model. User IDs are assigned rights, which determine their access privileges, to different areas of AEMO's Web Portals. The components to manage and restrict user access to AEMO's systems are described below.

### 2.1 Entities

Entities are the individual components or building blocks of the MSATS system, representing individual pieces of functionality. Some examples of entities are the menu options available on the MSATS main menu (ombudsman, role assignment, create participant, and CATS reports etc). Entities can be of type "batch" (submitting change requests using the batch handlers) or "interactive" (using AEMO's Web Portals).

AEMO system administrators create entity privileges and assign them to participant administrators. Participant administrators assign these entities to rights, which they assign to their users.



The list of entities available to a participant administrator is determined by their PA right given to them by the AEMO system administrator. Participant administrators cannot assign an entity privilege they are not assigned themselves. Privileges relate to the create, read, update, delete, or execute features of an entity.

The types of entities displayed are also dependent on the type of right chosen—batch, interactive or both. If the selection is changed, the screen refreshes to display the appropriate entities. For example, if the entity type interactive is chosen, the screen refreshes and does not display the batch entities.

### 2.1.1 Interactive Entities

The following table contains a list of common MSATS interactive entities available to participant administrators.

Interactive entity	Description
CATS Reports	Allows users to request any of the CATS reports that are available to participant users. Note that reports output is returned to the participant outbox only.
Codes Maintenance	Giving someone access to this entity with read privileges allows them to view lists of CATS codes online.
Data Load Import	Giving someone access to this entity gives them access to the participant inbox and participant outbox.
MDM Reports	Allows users to request any of the MDM reports that are available to participant users. Note 1: reports output is returned to the participant outbox only. Note 2: that a number of participants have automated systems which transfer these files locally and delete from the participant outbox.
Maintain User Profile	Allows a user to view or change his or her own profile including the description of their User ID, their phone number and email address.
Metering Data	Allows a user to search for and view metering data online.
NMI Discovery	Access to this entity with read privileges allows the use of the NMI Discovery screen.
NMI Master	Access to this entity with read privileges allows the use of the NMI Master screen.
Participant Contacts	Access to this entity allows use of the Participant Contacts screen, either to create, update, delete or view contact records for a participant's own organisation, depending on which privileges they have been given.
Participant Information	Access to this entity with read privileges allows the ability to view lists of all participants online using the participant information option.
Participant Mailbox All	This gives a user access to all files on the participant outbox – not just files created by the user logged on. Note: the user must also have at least read access to Data Load Import.
Participant Queue Monitoring	Access to this entity with read privileges allows a user to monitor the status of: the numbers of change request submitted the number of change request notifications the number of reports in the report queue the number of files waiting to be copied to the outbox and other queues The one entity gives access to all available queues for the participant group.
Participant Relationships	Access to this entity with read privileges allows use of the Participant Relationships Search screen.
Profile Area	Access to this entity with read privileges allows the ability to view information about profile areas.
Profile Data Source	Access to this entity with read privileges allows the ability to view information about profile data sources
Profile Methodology	Access to this entity with read privileges allows the ability to view information about profile methodologies
Profile Name	Access to this entity with read privileges allows the ability to view information about profile names
Rules Maintenance	Access to this entity with read privileges allows the ability to view lists of CATS rules online.

<b>Interactive entity</b>	<b>Description</b>
Settlement Scenarios	Access to this entity with read privileges allows the ability to access the Settlement Scenarios option.
System Calendar	Access to this entity with read privileges allows the ability to view the system calendar to identify national public holidays.
Transactions	<p>Access to this entity with all privileges allows them to create and withdraw change requests and objections and to view notifications and data requests.</p> <p>If the Delete privilege is not checked, the user cannot withdraw change requests or withdraw objections.</p> <p>If the Create privilege is not checked, in addition, the user cannot create or edit a change request or create objections.</p> <p>Allowing the Update privilege but not the Create privilege is meaningless with this entity because updating a change request is, in effect, a create action and if the right does not have access to the Create privilege any user with this right trying to edit a change request receives an error. Update has no meaning for other transaction types.</p> <p>Allowing the read privilege only means the user can search for and view change requests, objections, notifications and data requests.</p>
Uncommitted & Committed Data Cases	Access to this entity with read privileges allows access to the Uncommitted Data Cases and Committed Data Cases options.
User Profile Change Password	Allowing update privileges for this entity allows users to change their passwords. Assign all rights access to this entity if users can change their own passwords.
View Participant Archive	Providing read access to this entity allows a user to view the participant archive file directory provided that the right is also given read access to the Data Load Import entity.

### 2.1.2 Batch Entities

The following table contains a list of common MSATS batch entities available to participant administrators.

<b>Batch entities</b>	<b>Description</b>
CATS Reports Batch	Allows submission of CATS report requests by batch
Change Request	Allows submission of a change request by batch.
Change Withdrawal	Allows withdrawal of a change request by batch.
MDM Meter Data	Allows submission of meter data transactions by batch.
MDM Reports Batch	Allows submission of MDM report requests by batch
NMI data request	Allows submission of NMI discovery Type 2 transactions by batch.
NMI discovery request	Allows submission of NMI Discovery Type 1 transactions by batch.
Objection Request	Allows submission of objections to change requests by batch
Objection Withdrawal	Allows withdrawal of an objection by batch.

## 2.2 Rights and privileges

Rights are a collection of entities and their associated access privileges. A right consists of information about various actions that an owner of a right can perform on each entity in the system. For batch entities there is a single privilege—execute. For interactive entities, there are four kinds of privileges: delete, create, update, and read.

Every user in the system is assigned a right. Their access is limited to the various entities of MSATS that have been assigned to that right. The same right can be assigned to many users; therefore rights allow easier management of security access for groups of users.

Participant administrators can create ordinary rights for participant users or they can create other participant administrator rights by assigning them the same right assigned to them. Once the right is created, it is assigned to the appropriate participant users.

The relationship between the participant administrator and their participant users is hierarchical, with the AEMO system administrator presiding at the top of the hierarchy. All changes to participant administrator rights made by the AEMO system administrator automatically carry through to the participant users underneath the participant administrator. For example, if AEMO removes the ombudsman entity from the participant administrator, then participant users also lose access to the ombudsman entity. This is a cascade update function that can be used by AEMO system administrators to easily update access rights for an entire group of users.

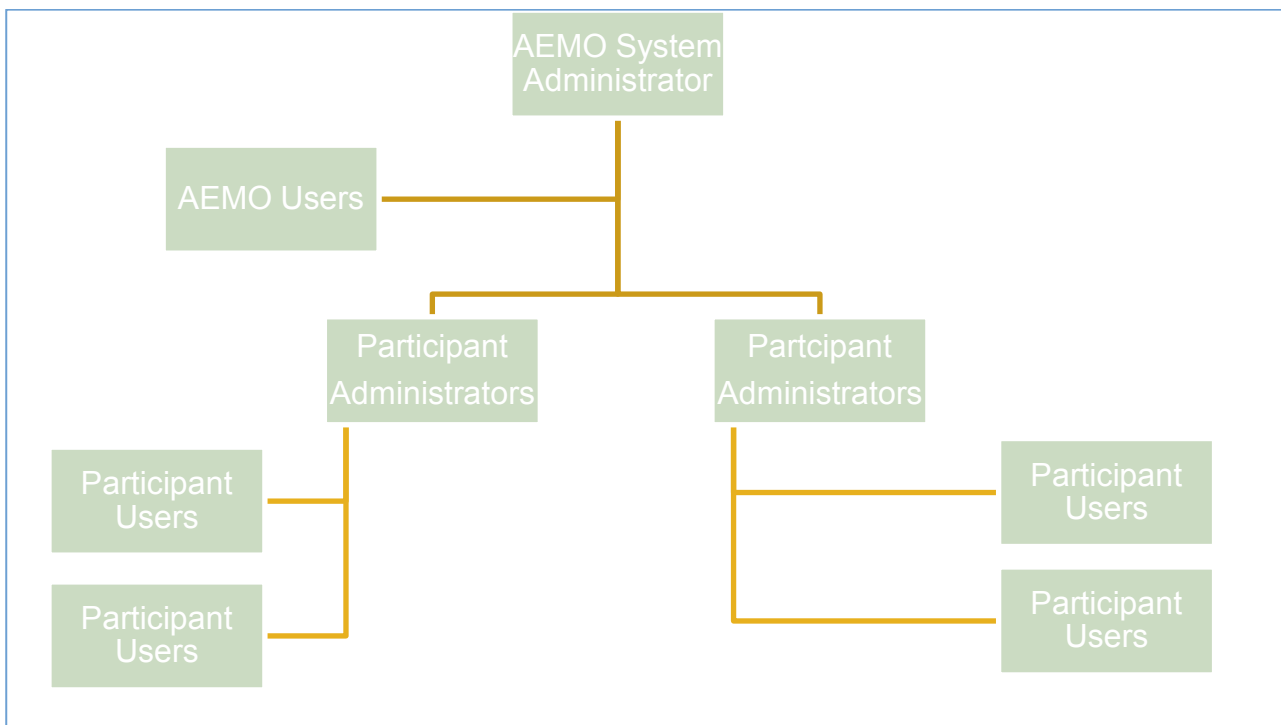


Figure 1: MSATS user hierarchy

This table explains the entity privilege hierarchy:

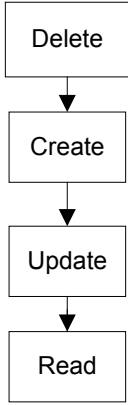
Hierarchy	Privilege	Description
<b>Privilege Hierarchy</b> 	Delete	The privileges in the interactive batch table are linked using a hierarchal relationship. Sitting on top of the hierarchy is the delete privilege. When the delete privilege check box is ticked the create, update and read, privileges are automatically ticked (full user access – low security).
	Create	Second in the privilege hierarchy is create. When create is selected the update and read privileges are automatically ticked. Users have access to create new records, edit records and view records for the entity.
	Update	Third on the hierarchy is update. When update is ticked users can edit and view records for the entity.
	Read	Last on the hierarchy is the read privilege. Checking only the read privilege for an entity ensures users can only view information for the entity (limited user access - high security).

Table 1: Entity privileges

## 2.3 Users

A user is a person who actually uses the system; either the Web Portal (interactive) or by the batch handlers (batch). To use the system each user must be associated with a participant and a right. The right assigned to the user determines the menu options and interfaces the user can access, and what actions (privileges) the user can complete on records.

### 2.3.1 AEMO system administrators

It is the responsibility of AEMO system administrators to create the initial participant administrator ID with the assigned PA right for each organisation. Once the participant administrator is set-up and supplied with their login details, they can create the remaining users for their organisation.



**Note:** AEMO system administrators can view all rights created in MSATS, even rights created by other administrators.

### 2.3.2 Participant administrators

Participant administrators are “super-users” who can manage and perform system administration tasks for their own organisation’s users. They can:

- Create new users.
- Create new rights (only up to the access they have themselves).
- Create new participant administrators by assigning them the same rights as themselves.

### 2.3.3 Participant users

A participant user is assigned rights that are classified as ordinary rights; an ordinary right user can belong to AEMO or participant organisations.

### 2.3.4 Business groups

Setting up a business group allows participant administrators to have visibility of all users in the group, without explicitly allowing visibility for each user. Being in a business group is not mandatory; MSATS allows a participant to exist on its own without belonging to any business group. An example of a business group is the participant IDs PARTID1 and PARTID2, who belong to the same business group of PARTBUSGROUP.

Business groups allow the use of “Single user ID logins”, see, “Managing the use of Set Participant” on page 22.

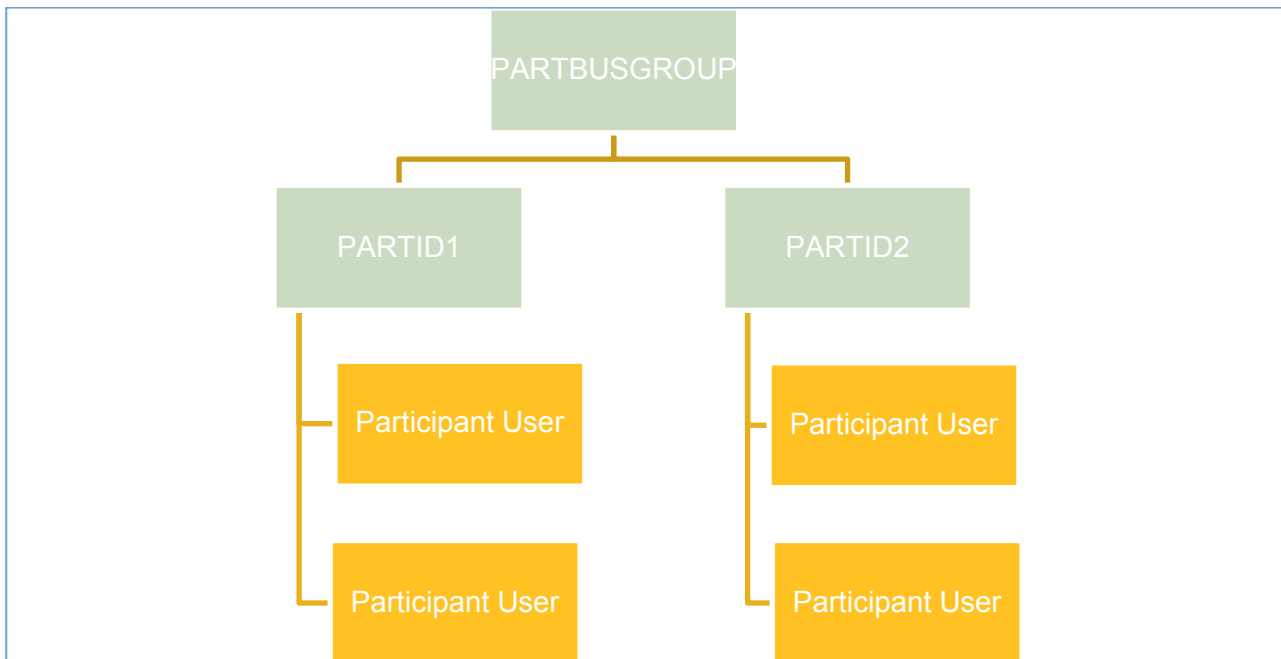


Figure 2: business group example

### 3 Maintain Rights

The **Maintain Rights** menu allows administrators to create and manage sets of rights. Rights allow administrators to group a collection of entities, and their associated privileges, and assign them to their users. For example, if the AEMO system administrator gives a participant administrator access to the Ombudsman and NMI Information menus, the Participant administrator can only allow the users they create to have access to these two menus or less. To learn more, see “MSATS Security Model” on page 4.

#### 3.1 Viewing rights

Using the **Maintain Rights** menu, participant administrators can view rights already created in MSATS.

To view the rights list:

1. On the main menu, click **Administration** and then click **Maintain Rights**.



2. The **Maintain Rights - List** screen displays the **Rights** assigned to users who are visible to the administrator ID shown on the main menu. The **Rights** are sequenced by participant ID and right name. The rights for your own participant ID are at the top of the list. A summary of the right properties display:
  - **Participant** – participant ID and name.
  - **Name** – name given to the right.
  - **Description** – short description of the right.
  - **Type** – if the right allows for batch or interactive access or both.
  - **Administrator** – indicates whether or not the right is an administrator right. The options are: AEMO system administrator, participant administrator or ordinary right.
  - **Activity Status** – indicates whether the right is active or inactive.
  - **Updated On** – the date at which the last update was saved against a right.
  - **Updated By** – the login name of the user who last updated the right.
3. Click the **Participant** drop-down arrow to view the right for one participant or for all participants for whom you have access.

Maintain Rights - List								Participant ID:	POOLTST
								Participant Name:	Pool Testing
Participant: POOLTST - Pool Testing									
Rights: All Participants who have granted rights to own users									
Participant	Name	Description	Type	Administrator	Activity Status	Updated On	Updated By	New	
POOLTST - Pool Testing	ORDINARY RIGHT	Ordinary Right	Batch & Interactive	Ordinary Right	Active	16-Mar-2010	POOLTSTBATCH	• Edit • View	
POOLTST - Pool Testing	PA Right	Rights provided to the Participant Administrator	Batch & Interactive	ParticipantAdmin Right	Active	1-Apr-2010	POOLTSTBATCH	• View	
Ombudsman	ORDINARY RIGHT	Ordinary Right	Interactive	Ordinary Right	Active	16-Mar-2010	POOLTSTBATCH	• Edit • View	
Ombudsman	PA Right	Rights provided to the Participant Administrator	Interactive	ParticipantAdmin Right	Active	1-Apr-2010	POOLTSTBATCH	• View	



**Note:** each right granted by another administrator only has the **View** link in the **Action** column. This allows the administrator in charge of the users, to whom rights are granted, to

check which access other administrators have granted to users. When a new administrator logs in for the first time, they see their administrator right. The administrator then needs to create the ordinary right for their own users.

To view the details of a right:

1. On the main menu, click **Administration** and then click **Maintain Rights**.
2. The **Maintain Rights - List** screen displays. Click **View** in the **Action** column next to the **Right Name**.



**Note:** only the AEMO system administrator can edit other administrator rights, therefore, the **Participant Admin Right** has the **View** link only. Rights granted by other administrators are also viewable only.

Maintain Rights - List								Participant ID:	POOLTST
								Participant Name:	Pool Testing
Participant:		POOLTST - Pool Testing							
Rights		All Participants who have granted rights to own users							
Participant	Name	Description	Type	Administrator	Activity Status	Updated On	Updated By	Action	
POOLTST - Pool Testing	ORDINARY RIGHT	Ordinary Right	Batch & Interactive	Ordinary Right	Active	16-Mar-2010	POOLTSTBATCH	• Edit • View	
POOLTST - Pool Testing	PA Right	Rights provided to the Participant Administrator	Batch & Interactive	ParticipantAdmin Right	Active	1-Apr-2010	POOLTSTBATCH	• View	
Ombudsman	ORDINARY RIGHT	Ordinary Right	Interactive	Ordinary Right	Active	16-Mar-2010	POOLTSTBATCH	• Edit • View	
Ombudsman	PA Right	Rights provided to the Participant Administrator	Interactive	ParticipantAdmin Right	Active	1-Apr-2010	POOLTSTBATCH	• View	

3. The **Maintain Rights - View** screen displays. Details on this screen are read-only and cannot be modified. The **Participant ID - Name** table displays the participants sharing the **Right Name** with your own users listed at the top.

Maintain Rights - View		Participant ID:											
		Participant Name:											
Participant:	Ombudsman												
Rights Name:	OMB_USER												
Description:	Ombudsman User												
Right Type:	Interactive												
Administrator Right:	Ordinary Right												
Activity Status (*):	Active												
Users sharing the given right:	<table border="1"> <thead> <tr> <th>Participant ID - Name</th> <th>User Name</th> </tr> </thead> <tbody> <tr> <td>Ombudsman</td> <td>Sub user</td> </tr> <tr> <td>Ombudsman</td> <td>Sub user</td> </tr> <tr> <td>Ombudsman</td> <td>Sub user</td> </tr> <tr> <td>Ombudsman</td> <td>Sub user</td> </tr> </tbody> </table>			Participant ID - Name	User Name	Ombudsman	Sub user	Ombudsman	Sub user	Ombudsman	Sub user	Ombudsman	Sub user
Participant ID - Name	User Name												
Ombudsman	Sub user												
Ombudsman	Sub user												
Ombudsman	Sub user												
Ombudsman	Sub user												
<b>Interactive:</b>													
Entity Description	Delete	Create	Update Read										
Maintain User Profile	N	N	Y Y										
Ombudsman Enquiry	N	Y	Y Y										
User Profile Change Password	N	N	Y Y										

## 3.2 Creating a new right



**Note:** for help linking rights to user profiles, see “User Administration” on page 18.

To create a new right:

1. On the main menu, click **Administration** and then click **Maintain Rights**.
2. The **Maintain Rights - List** screen displays. Click **New** above the **Action** column.

Maintain Rights - List							Participant ID:	ENGYAUST
							Participant Name:	Energy Australia - Retailer
<b>Rights</b>							<b>New</b>	
Name	Description	Type	Administrator	Activity Status	Updated On	Updated By	Action	
CATS INTERACTIVE	CATS User - Interactive Only	Interactive	Ordinary Right	Active	16-Jun-2004	SYSADMTEST	• Edit • View	
CATS SUPER	CATS Batch & interactive	Batch & Interactive	Ordinary Right	Active	17-Jun-2004	SYSADMTEST	• Edit • View	
CATS TRANSACTIONS	CATS Transactions Interactive	Interactive	Ordinary Right	Active	17-Jun-2004	SYSADMTEST	• Edit • View	
CATS USER	CATS Interactive and Batch	Batch & Interactive	Ordinary Right	Active	17-Jun-2004	SYSADMTEST	• Edit • View	
CREATE PARTICPANT	create participant read only	Batch & Interactive	Ordinary Right	Active	13-Jun-2004	SYSADMTEST	• Edit • View	
ORDINARY CATS	Ordinary CATS user Interactive	Interactive	Ordinary Right	Active	13-Jun-2004	SYSADMTEST	• Edit • View	
PA RIGHT	PA RIGHT	Batch & Interactive	Ordinary Right	Active	4-Mar-2004	SYSADMIN	• Edit • View	
TEST	Testing for Training Purposes	Batch & Interactive	Ordinary Right	Active	15-Jun-2004	SYSADMTEST	• Edit • View	
TRAINING SYS ADMIN	Participant System Administration	Batch & Interactive	ParticipantAdmin Right	Active	16-Jun-2004	SYSADMTEST	• View	

3. The **Maintain Rights – New** screen displays. Click the **Right Type** drop-down arrow and select an option:
  - **All:** both the interactive and batch entity tables are available.
  - **Interactive:** only the interactive entity table is available. The interactive entity table enables the user to assign create, read, update or delete privileges to an entity. This determines the access a user has when they login into the web portal. For ombudsman users, **Interactive** is the only option.
  - **Batch:** only the batch entity table is available. The batch entity table allows a user to assign execute access to batch commands.



**Note:** for help with right types see, “MSATS Security Model” on page 4

4. Type a descriptive name in the **Right Name** field. This name must be unique.
5. Type a detailed **Description**. Include information concerning the role and user group, the right is being created for.
6. Click the **Activity Status** drop-down arrow and select an option:
  - **Active:** if the right is to be used immediately.
  - **Inactive:** if it is not available for use immediately.
7. Set the required privileges for each **Entity Description** by placing a tick in the check box, see “Table 1: Entity privileges”.
  - on:
  - off:

**Note:** the entities shown in this section are examples only and do not represent all available entities. The entities displayed to you may differ from the examples below.

Right Type (\*):

Rights Name (\*):

Description (\*):

Activity Status (\*):

<b>Interactive:</b>				
Entity Description	Delete	Create	Update	Read
CATS Reports	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Codes Maintenance				<input checked="" type="checkbox"/>
Data Load Import (Participant Inbox & Participant Oubox)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
MDM Reports	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Maintain User Profile			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Metering Data	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
NMI Discovery				<input checked="" type="checkbox"/>
NMI Master				<input checked="" type="checkbox"/>
Participant Contacts	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Participant Information				<input checked="" type="checkbox"/>
Participant Mailbox All	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Participant Queue Monitoring				<input checked="" type="checkbox"/>
Participant Relationships				<input checked="" type="checkbox"/>
Profile Area				<input type="checkbox"/>
Profile Data Source				<input type="checkbox"/>
Profile Methodology				<input type="checkbox"/>
Profile Name				<input type="checkbox"/>
Rules Maintenance				<input checked="" type="checkbox"/>
Settlement Scenarios				<input type="checkbox"/>
System Calendar				<input checked="" type="checkbox"/>
Transactions (Change Requests, Objections, Notifications & Data Requests)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Uncommitted & Committed Data Cases				<input type="checkbox"/>
User Profile Change Password			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
View participant archives				<input checked="" type="checkbox"/>

<b>Batch:</b>	
Entity Description	Execute
CATS Reports Batch	<input checked="" type="checkbox"/>
Change Request	<input checked="" type="checkbox"/>

Figure 3: example of the participant administrator maintain rights - new screen

Maintain Rights - New
Participant ID:  
Participant Na

Participant ID & Name : Ombudsman

Right Type (\*): Interactive

Rights Name (\*):

Description (\*):

Activity Status (\*): A - Active

Interactive:				
Entity Description	Delete	Create	Update	Read
Maintain User Profile	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Ombudsman Enquiry	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
User Profile Change Password	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Save
Clear

Figure 4: example of the ombudsman maintain rights - new screen

- Select the **Batch Entities** for the right by selecting the check boxes next to each entity in the **Batch** Table.



**Note:** complete this table only if the **Right Type** is **All** or **Batch**. The entity right type for ombudsman administrators is interactive only.

Batch:	
Entity Description	Execute
CATS Reports Batch	<input checked="" type="checkbox"/>
Change Request	<input checked="" type="checkbox"/>
Change Withdrawal	<input checked="" type="checkbox"/>
MDM Meter Data	<input type="checkbox"/>
MDM Reports Batch	<input type="checkbox"/>
NMI data request	<input checked="" type="checkbox"/>
NMI discovery request	<input checked="" type="checkbox"/>
Objection Request	<input checked="" type="checkbox"/>
Objection Withdrawal	<input checked="" type="checkbox"/>

Save
Clear

- Click **Save**.  
Alternatively, click **Clear** to start again.
- A confirmation message displays, **The Right Record Has Been Saved Successfully** and the new right display in the **Maintain Rights – List** screen. Whoever created the right can edit and view the right.

### 3.3 Editing a right

Participant administrators can edit rights created for their users.

To edit a right:

1. On the main menu, click **Administration** and then click **Maintain Rights**.
2. The **Maintain Rights - List** screen displays. Click **Edit** in the **Action** column next to the **Right Name**.



**Note:** participant administrators can only edit the right for their own users.

Maintain Rights - List							Participant ID:	NEMMCO
							Participant Name:	Australian Energy Market Oper
Rights								
Name	Description	Type	Administrator	Activity Status	Updated On	Updated By	New Action	
CATS INTERACTIVE	CATS User - Interactive Only	Interactive	Ordinary Right	Active	16-Jun-2004	SYSADMTEST	• Edit • View	
CATS SUPER	CATS Batch & interactive	Batch & Interactive	Ordinary Right	Active	17-Jun-2004	SYSADMTEST	• Edit • View	
CATS TRANSACTIONS	CATS Transactions Interactive	Interactive	Ordinary Right	Active	17-Jun-2004	SYSADMTEST	• Edit • View	
CATS USER	CATS Interactive and Batch	Batch & Interactive	Ordinary Right	Active	17-Jun-2004	SYSADMTEST	• Edit • View	
CREATE PARTIPANT	create participant read only	Batch & Interactive	Ordinary Right	Active	13-Jun-2004	SYSADMTEST	• Edit • View	
ORDINARY CATS	Ordinary CATS user Interactive	Interactive	Ordinary Right	Active	13-Jun-2004	SYSADMTEST	• Edit • View	
PA RIGHT	PA RIGHT	Batch & Interactive	Ordinary Right	Active	4-Mar-2004	SYSADMIN	• Edit • View	
TEST	Testing for Training Purposes	Batch & Interactive	Ordinary Right	Active	15-Jun-2004	SYSADMTEST	• Edit • View	
TRAINING SYS ADMIN	Participant System Administration	Batch & Interactive	ParticipantAdmin Right	Active	16-Jun-2004	SYSADMTEST	• View	

3. The **Maintain Rights – Edit** screen displays where you can make your changes. For help with the fields, see “Creating a new right” on page 12.



**Note:** not all fields are available for modification. In the example below the **Participant** and **Administrator Right** fields cannot be modified.

**Maintain Rights - Edit**

Participant ID: NEMMCO  
Participant Name: Australian Energy Market Operator Limited

Participant: NEMMCO - Australian Energy Market Operator Limited  
 Right Type (\*): A - All  
 Rights Name (\*): PA Right  
 Description (\*): Rights provided to the Participant Administrator  
 Administrator Right: ParticipantAdmin Right  
 Activity Status (\*): A - Active

Participants sharing the given right:

Participant ID - Name
AAI2 - AATEST21b
AADG20 - AAI2Test20a
ACTI - Act Distribution

**Interactive:**

Entity Description	Delete	Create	Update	Read
AEMO Utilities	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Active User Sessions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Archival Setup	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

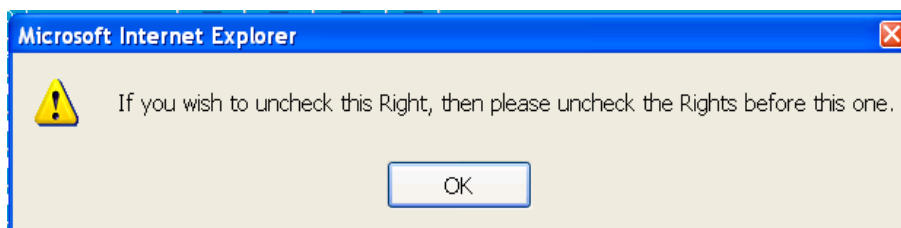
**Batch:**

Entity Description	Execute
CATS Reports Batch	<input checked="" type="checkbox"/>
Change Request	<input checked="" type="checkbox"/>
Change Withdrawal	<input checked="" type="checkbox"/>
MDM Meter Data	<input checked="" type="checkbox"/>
MDM Reports Batch	<input checked="" type="checkbox"/>
NMI data request	<input checked="" type="checkbox"/>
NMI discovery request	<input checked="" type="checkbox"/>
Objection Request	<input checked="" type="checkbox"/>
Objection Withdrawal	<input checked="" type="checkbox"/>

Save Clear

- o Click **Save**. A message displays confirming your changes. When a right is modified and saved, access for all users linked to that right is updated automatically.

If an entity privilege in the interactive entity description table is modified, the entity privilege hierarchy rules must be adhered to. If a privilege is removed out of sequence MSATS displays an error message, see “Table 1: Entity privileges” on page 8.



### 3.4 Removing a right

To remove a right:

1. Follow the instructions for “Editing a right” above.
2. Change the **Activity Status** to **I - Inactive**. For participants assigned the right who are currently logged into MSATS, the change takes effect the next time they login. This is true for any change to a right whilst a participant associated to the right is logged-in.



## 4 User Administration

Administrators can create and manage profile details of their users, users they are specifically given visibility to and to any associated business groups.

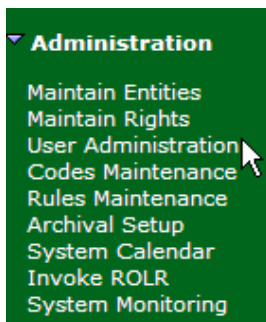
### 4.1 Viewing user profiles

To view user profiles:

1. On the main menu, click **Administration** and then click **User Administration**.



**Note:** ombudsman administrators can only see **Maintain Rights** and **User Administration**.



2. The **User Administration - List** screen displays. Click the **Participant** drop-down arrow to view the right for one participant or for all participants for whom you have access.
3. The **Users** for the selected participant display with the following details:
  - **User ID:** user IDs belonging to the selected participant.
  - **User Name:** user names belonging to the selected participant.
  - **Participant ID – Name:** combined participant ID and name.
  - **Activity Status** – the user’s status, **A** = active and **I** = inactive. Users with an inactive status cannot login to MSATS but an inactive record can be made active again.
  - **Updated On:** the date the details were last modified (not the date the user last logged in).
  - **Updated By** the user name of the person who last modified the user ID details.

User Administration - List						Participant ID:	POOLSNOW
						Participant Name:	Pool Snow
Participant: POOLSNOW - Pool Snow							
User ID	User Name	Participant Id - Name	Activity Status	Updated On	Updated By	Action	
POOLSNOW1	POOLSNOW 1	POOLSNOW - Pool Snow	A	18-Apr-2007	POOLSNOWBATCH	• Edit • View	
POOLSNOW2	Pool snow 2	POOLSNOW - Pool Snow	A	18-Apr-2007	POOLSNOWBATCH	• Edit • View	
POOLSNOWBATCH	POOLSNOW batchuser (NEMMCO)	POOLSNOW - Pool Snow	A	18-Apr-2007	POOLSNOWBATCH	• Edit • View	
POOLSNOWSU	Super User POOLSNOW	POOLSNOW - Pool Snow	A	18-Apr-2007	POOLSNOWBATCH	• Edit • View	
POOLTEST	Pool Test	POOLSNOW - Pool Snow	A	30-Apr-2007	TESTTEST	• Edit • View	

4. To view an individual user’s profile, click **View** in the **Action** column.

TRAINCATS	Training User	Energy Australia - Retailer	A	16-Jun-2004	TRAINCATS	• Edit • View
CONTRABCD	Create Participant Pool	Energy Australia	I	12-Jun-2004	CONTRABCD	• Edit • View

5. The **User Administration – View** screen displays with read-only information that cannot be modified:
  - **Participant ID & Name** of the participant granting the right.

- **Right Name & Description** assigned to the user. If the user has multiple rights they display.
- **User is Visible to Following Participants:** participants who can see the user.

User Administration - View		Participant ID:	POOLSNOW
		Participant Name:	Pool Snow
Participant Id & Name :	POOLSNOW - Pool Snow		
User ID:	POOLTEST		
User Name:	Pool Test		
Phone:	(1) 123		
Email:			
Activity Status:	Active		
Rights:			
Participant Id & Name	Right Name & Description	Granted	
POOLSNOW - Pool Snow	PA Right - Rights provided to the Participant Administrator	<input checked="" type="checkbox"/>	
User is Visible to Following Participants:			
Participant Id	Participant Name	Same Business Group?	

## 4.2 Creating a new user profile

When a new user is created an MSATS user ID and password must be assigned to allow access to the MSATS Web Portal. During the creation process, rights are assigned to the new users that are made visible to one or more other participants outside the business group. This allows use of the **Set Participant** option to switch between different participants; to learn more, click **User Guides** and download the “MSATS Introduction Guide” from the AEMO website.



**Important Note:** revoking the visibility of a user to another participant also revokes all rights granted to the user by the other participant.

To create a new user profile:

1. On the main menu, click **Administration** and then click **User Administration**.
2. The **User Administration - List** screen displays the **Users** list. Click **New** in the **Action** column.

User Administration - List		Participant ID:	POOLSNOW			
		Participant Name:	Pool Snow			
Participant:		POOLSNOW - Pool Snow				
Users						New
User ID	User Name	Participant Id - Name	Activity Status	Updated On	Updated By	Action
POOLSNOW1	POOLSNOW 1	POOLSNOW - Pool Snow	A	18-Apr-2007	POOLSNOWBATCH	• Edit • View
POOLSNOW2	Pool snow 2	POOLSNOW - Pool Snow	A	18-Apr-2007	POOLSNOWBATCH	• Edit • View
POOLSNOWBATCH	PoolSNOW batchuser (NEMMCO)	POOLSNOW - Pool Snow	A	18-Apr-2007	POOLSNOWBATCH	• Edit • View
POOLSNOWSU	Super User POOLSNOW	POOLSNOW - Pool Snow	A	18-Apr-2007	POOLSNOWBATCH	• Edit • View
POOLTEST	Pool Test	POOLSNOW - Pool Snow	A	30-Apr-2007	TESTTEST	• Edit • View

3. The **User Administration – New** screen displays, type a **User ID**. It must be unique and at least 6 alphanumeric characters (containing alphabetic or numeric characters). This is the user ID used to login to AEMO’s Web Portals.

**User Administration - New** Participant ID: POOLTST  
Participant Name: Pool Testing

Participant Id & Name : POOLTST - Pool Testing

User ID (\*):

User Name (\*):

User Password (\*):

Retype Password (\*):

Phone (\*) (09) 99999999:

Email:

Activity Status (\*): A - Active

Participant Id & Name	Right Name & Description	Grant/Revoke
POOLTST - Pool Testing	ORDINARY RIGHT - Ordinary Right	<input type="checkbox"/>
POOLTST - Pool Testing	PA Right - Rights provided to the Participant Administrator	<input type="checkbox"/>

Choose participants to whom user should be visible :  
(Number of participants to whom the user can be visible without those participants granting any rights is limited to 10)

Select Participants (Multiple Allowed)  
 AAA - onload  
 AAAAA - AAAAAATEST

- In the **User Name** field, type the full name of the user. Include the First Name, Middle Name (or Initial) and Surname, for example “John P Smith”.

User Name (\*):

- In the **User Password** field, type the generic password. The password must be at least 6 characters in length. Typing in the **User Password** field, displays only the • character for security purposes. The first time the user logs into MSATS they are prompted to change this password.
- Type the same password in the **Retype Password** field to confirm the correct password.
- Type the user’s **Phone** number (up to 15 digits) along with the area code (up to four digits). The field accepts only numeric characters (no spaces).

Phone (\*) (09) 99999999:

- Type the user’s email address in the **Email** field.
- Click the **Activity Status** drop-down arrow and select **A – Active**. A user cannot login to MSATS if their status is inactive.

Activity Status (\*): A - Active

A - Active  
 I - Inactive

- In the **Rights** table, assign rights to the user by clicking the applicable **Grant/Revoke** check boxes. Only rights created by a participant administrator in your organisation are available for selection, see “Maintain Rights” on page 10.

**Important Note:** granting rights to a participant user who belongs to another participant allows their participant administrator to access the same rights.

Participant Id & Name	Right Name & Description	Grant/Revoke
POOLSNOW - Pool Snow	B2B USER - B2B User Rights	<input type="checkbox"/>
POOLSNOW - Pool Snow	PA Right - Rights provided to the Participant Administrator	<input type="checkbox"/>

- To make the user visible to other participants outside the business group, select the participants from the **Choose Participants to whom the user should be visible** list. To select more than one participant, on your keyboard, hold down the **Ctrl** key and click each participant to highlight them.

Choose participants to whom user should be visible :  
 (Number of participants to whom the user can be visible without those participants granting any rights is limited to 10)

Select Participants (Multiple Allowed)

AAA - onload  
 AAAAA - AAAAAATEST

Save Clear

- Click **Save**. If the information is valid, a confirmation message displays advising the record is saved. The new record displays on the **User Administration – List** screen.

If the information entered is not valid, an error message displays advising of the problem. Rectify the problem and click **Save** again.

### 4.3 Editing a user profile

Administrators can update user details; this includes the ability to change a user's password if required.

To edit a user profile:

- On the main menu, click **Administration** and then click **User Administration**.
- The **User Administration – List** screen displays. Select the user record to modify by clicking **Edit** in the **Action** column.

User Administration - List						Participant ID:	POOLSNOW
						Participant Name:	Pool Snow
Participant:						POOLSNOW - Pool Snow	
User ID	User Name	Participant Id - Name	Activity Status	Updated On	Updated By	New	
POOLSNOW1	POOLSNOW 1	POOLSNOW - Pool Snow	A	18-Apr-2007	POOLSNOWBATCH	• Edit • View	
POOLSNOW2	Pool snow 2	POOLSNOW - Pool Snow	A	18-Apr-2007	POOLSNOWBATCH	• Edit • View	
POOLSNOWBATCH	POOLSNOW batchuser (NEMMCO)	POOLSNOW - Pool Snow	A	18-Apr-2007	POOLSNOWBATCH	• Edit • View	
POOLSNOWSU	Super User POOLSNOW	POOLSNOW - Pool Snow	A	18-Apr-2007	POOLSNOWBATCH	• Edit • View	
POOLTEST	Pool Test	POOLSNOW - Pool Snow	A	30-Apr-2007	TESTTEST	• Edit • View	

- The **User Administration – Edit** screen displays. The edit screen has the same fields available in the **User Administration – New** screen however; the **Participant ID & Name** and the **User ID** fields are read-only and cannot be modified.
  - For a user owned by the participant ID, the **User Password** and **Retype Password** fields are blank. Leave the fields blank if you do not want to change the user's password otherwise enter a new generic password. The next time the user logs into MSATS they are prompted to change this password.
  - For a user owned by the participant ID, any **Rights** granted by other participants display, but do not have check boxes because a participant administrator cannot grant or revoke rights of other participants.
  - For a user *not* owned by the participant ID, any **Rights** granted by other participants do not display.
  - To deactivate the login change the **Activity Status** to **I - Inactive**.
- Make the required changes and Click **Save**.

Click **Clear** to clear the fields and start again or to cancel the changes.



**Note:** participant administrators can reset a user password if it is forgotten or the account is locked. However, only the AEMO system administrator or another administrator in the participant's organisation (that is, another user with administrator rights) can reset an administrator's password.

## 5 Managing the use of Set Participant

Within the MSATS system, it is possible to switch between different participant IDs without having to log out, change an ID and password and log in again. This functionality in AEMO's Web Portals, "Set Participant" enables when participants are assigned to a business group.

All users within a business group are visible to other participants with the same business group. Participant administrators assign rights to each of their users. To make a user visible to participants outside of a business group, the administrator specifically selects participants who are allowed to assign rights to the user. If a user is not visible to participants, the participant administrator should not select any participants who can view that user.

A participant ID belonging to a business group is not compulsory, but then setting up single user ID logins requires cooperation with other administrators. If a participant administrator wants a user to access a participant ID in a business group, but the administrator cannot see that user ID, then the owning administrator for that user ID must explicitly give visibility of that user ID to the relevant participant ID in the business group. When the administrator can see the user ID, then the administrator can grant rights to the user.

Having a single participant ID owning all active user IDs in the business group is not absolutely necessary, but it can simplify management and control. Security management has enough risks without also having to make sure distributed control is fully effective, and stays that way.

A single participant ID owning all the active users can make the transition from multiple user ID logins to single user ID login easier; having the benefit that the owning participant can inform their users to only use their ID for that one participant.

The following sections explain multiple and single user ID logins and how to implement single user ID logins.

### 5.1 Retaining multiple user ID logins

Participant Administrators control the implementation of security and access for their user IDs. Participant administrators can continue working with multiple user ID logins and choose to ignore the "Set Participant" feature of the MSATS Security Model. If so, you do not need to change any of your processes or procedures, and the rest of this section is largely irrelevant to your business.

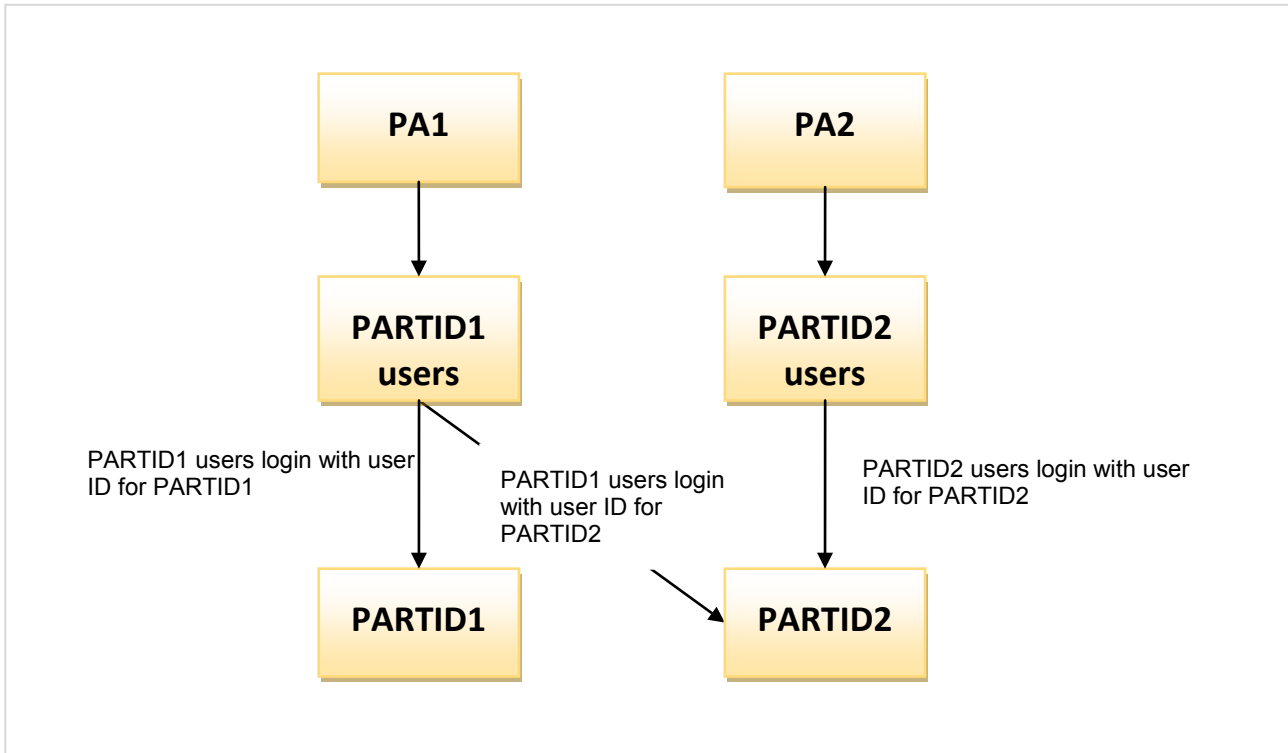


Figure 5: example of multiple user ID logins for each participant ID

- User1 has access to participants, PARTID1 and PARTID 2, using two different logins.
- PA1 has access to PARTID1 users only.
- PA2 has access to PARTID2 users only.

## 5.2 Transforming from multiple user ID logins to single user ID logins

A recommended strategy to transform from multiple user ID logins to single user ID logins is for a participant administrator in each non-owning participant, inactivates all their own user IDs and then grants the appropriate rights to the active user IDs to access the relevant entities for the administrator's participant ID. It is also possible to have a single user ID login for all the administrators in the business group, by having an administrator for each participant grant administrator rights to the one administrator who owns all the active users.

Users having rights assigned by more than one participant can change between participant IDs using "Set Participant", see "References" on page 29.

If any of your users require access to any participant IDs outside your own business group, make the user ID visible to each relevant participant ID. When the administrator for the other participant can see the user ID, then the administrator can grant rights to that user, as deemed appropriate by the other participant's administrators, see "User Administration" on page 18.

There are two options for administrators to set-up single user logins.

- Option 1: allow all PAs in a business group to see all users, is the recommended option for easy management.
- Option 2 is PAs within a business group give access to other PAs to assign rights to their users.

### **5.2.1 Flowchart of Recommended Implementation**

Each participant and business group can use this example as a basis for their own planning, with specific reference to the more general outline above.

The flowchart, Figure 6: migrating to single user ID logins on page 7, has two participants where some participant users have a User ID for each participant. The participants have the IDs of PARTID1 and PARTID2. Each participant has a participant administrator, being PA1 and PA2 respectively.

After migration using this recommended implementation, all the active users (other than PAs) are owned by a single Participant ID. This means all new users created in the business group also need to be created by that single participant ID, to keep the security as simple as possible to manage. It may even be appropriate to have all users in the business group created under a single participant ID, even for those not actually using business facilities of that participant ID; the rights granted under each participant ID determine what the user ID can do.

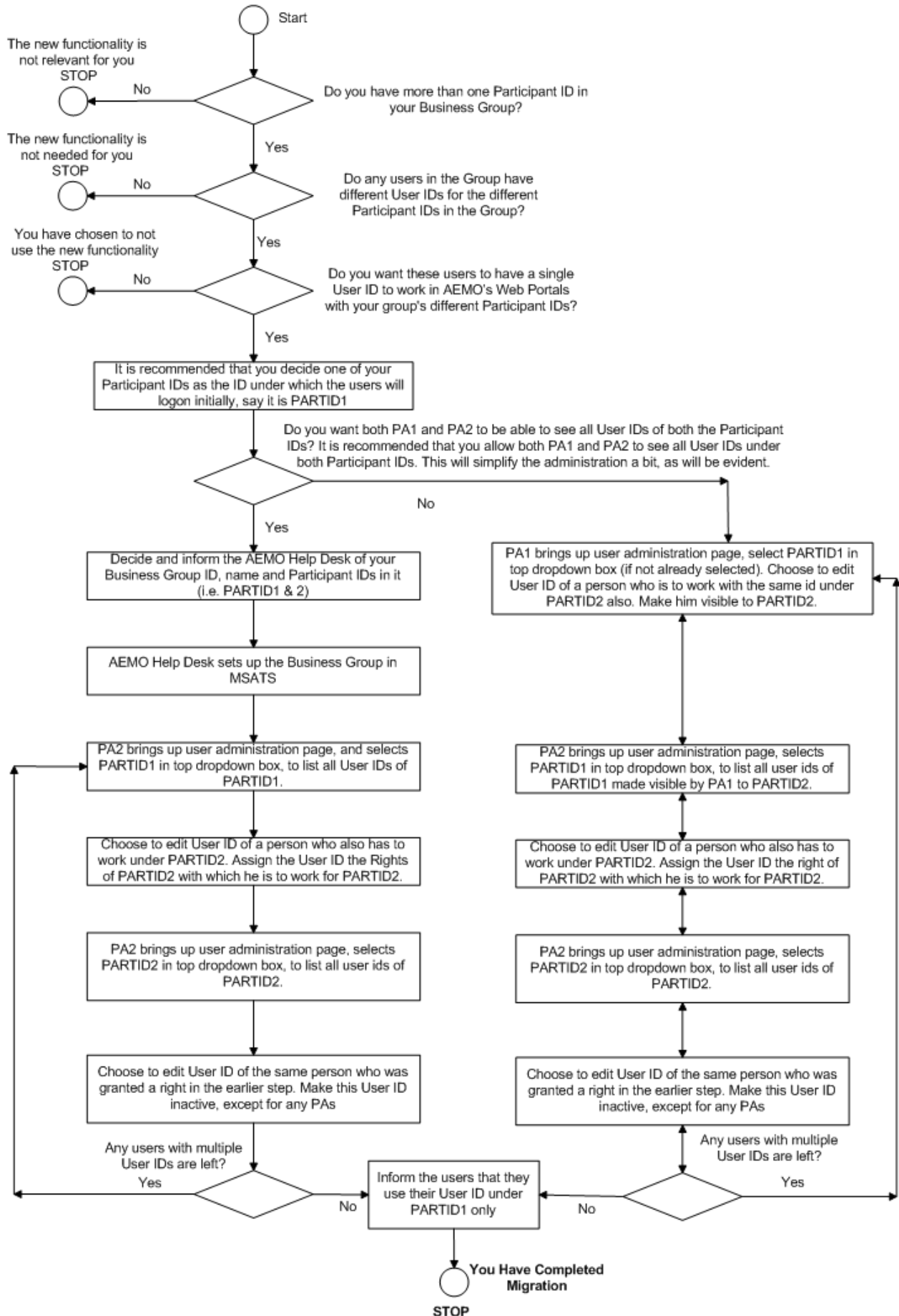


Figure 6: migrating to single user ID logins

## 5.2.2 Checklist for implementing single user ID logins

To convert to single user ID logins, PAs need to address the following:

1. Define the participants of their business group, if required.
2. Decide the “owning” participant for user IDs, considering the security and management factors.
3. Identify any users to be visible to participants outside the business group.
4. Ensure the shared visibility and access does not compromise the security for any part of your business.

Basic steps for setting up single user IDs:

1. Submit the participant IDs in their business group to the AEMO Help Desk. In particular, you need to supply the business group ID and business group name, plus the entire participant IDs to be part of that business group.
2. AEMO sets up the business groups in MSATS.
3. On the MSATS main menu, click **Administration**, and then click **User Administration**.
4. Select the participant from the drop-down list, see “Editing a user profile” on page 21.
5. Select the user from the participant list and click edit to give them access to another participant.
6. Select the other participant you have just granted the user access to and inactivate their user ID for that participant.
7. Advise the user they have a single login and can use **Set Participant** to change participants without logging in and out. For help, see “Using Set Participant” in the “MSATS Introduction Guide”.



**Important Note:** AEMO has made the use of single user ID logins available on the understanding that each participant is responsible for the management of the accesses granted to each and every user. Security is every user’s concern and each participant administrator has a very powerful role in establishing and maintaining effective control of access to sensitive information.

Specific warnings include:

- Be very careful about assigning PA rights to any user.
- Be careful about assigning rights for mailbox, inbox and outbox.

## 6 Glossary

### 6.1 Abbreviations

Abbreviation	Abbreviation Explanation
CATS	Consumer Administration and Transfer Solution.
EMMS	Electricity Market Management System (formerly MMS); software, hardware, network and related processes to implement the NEM.
MSATS	Market Settlement and Transfer Solution.
NEM	National Electricity Market
PA	Participant administrator

Table 1: Abbreviations

### 6.2 Special terms

Term	Definition
AEMO system administrator	Creates the initial participant administrator ID with the PA right assigned, for each organisation.
Batch entity	A right type assigned to a user, allowing the use of the batch handlers in MSATS.
Batch handlers	Allow communications between the MSATS system and participant systems. All communication between MSATS and participants' systems is done using aseXML-formatted messages. When communications are processed using the batch handlers, they undergo the same validity checks as if they were processed using the MSATS Web Portal.
Business Group	Setting up a business group allows participant administrators to have visibility of all users in the group, without explicitly allowing visibility for each individual user. Being in a business group is not mandatory but it allows the use of "Single user ID logins" (see §5).
Entities	Entities are the individual components or building blocks of the MSATS system, representing individual pieces of functionality. Some examples of entities are the menu options available on the MSATS main menu (ombudsman, role assignment, create participant, and CATS reports etc.). Entities can be of type "batch" (submitting change requests using the batch handlers in MSATS) or "interactive" (using AEMO's Web Portals).
Entity privileges	The privileges assigned to an entity by the AEMO system administrator.
Interactive entity	A right type assigned to a user, allowing the use of AEMO's Web Portals.
MSATS Security Model	Permits administrators to manage access to AEMO's systems.
PA Right	The rights assigned to a participant administrator by the AEMO system administrator.
Participant administrator (PA)	Super-users who manage and perform system administration tasks for their own organisation's participant users.
Participant user	A participant organisation's individual user who is assigned ordinary rights.
Privileges	Relate to the create, read, update, delete, or execute features of an entity.
Right	A collection of entities and their associated access privileges. A right consists of information about various actions (read, create, update, delete) that an owner of a right can perform on each entity in the system.

<b>Term</b>	<b>Definition</b>
Right type	Batch, interactive, or both.
Single user ID login	The ability to switch between different participant IDs, without having to log out, change the ID and password, and log in again. This functionality enables when a participant user is assigned to a business group (see §5).

*Table 2: Special terms*

## 7 References

The resources listed in this section contain additional related information that may assist you.



**Note:** it is important to ensure that you are reading the current version of any document.

- AEMO Help Desk: phone: 1300 300 295, option 2; e-mail: [helpdesk@aemo.com.au](mailto:helpdesk@aemo.com.au).
- National Electricity Rules: see the AEMC website <http://www.aemc.gov.au>.

### 7.1 AEMO's website

The following documents are found on AEMO's website:

- "Guide to Market Systems – Gaining Access", for information on access to AEMO's Web Portals. Participants wishing to use AEMO's Web Portals are required to have access to the AEMO Market Systems using the MarketNet Private Network. MarketNet provides information using web interfaces to participants, available from <http://www.aemo.com.au/registration/nemnet.html>.
- "Set Participant": for information about using Set Participant (for example, agents), see the "MSATS Introduction Guide" <http://www.aemo.com.au/electricityops/userguide.html> or the "About Administration" menu in the EMMS Web Portal.

### 7.2 EITS publications

Participant users with the credentials can find the following documents in the secure [EITS Publications](#) area on AEMO's website (application to AEMO's Help Desk or see "About Administration" in the EMMS Web Portal). Documents in "EITS Publications" are available to registered participants only.

- "AEMO CSV Data Format Standard", describes the CSV standard used within flat files provided to participants. Its primary function is to provide sufficient information to allow participants to understand the AEMO CSV data format standard.
- "AEMO's IP Addresses for Participants", provides information about URLs for accessing AEMO's IT systems.
- "Electricity Market Management Systems (EMMS) Web Portal Applications", provides a summary of EMMS Web Portal applications, to assist participants with decisions about AEMO's IT systems.
- "Guide to Market Systems – Maintaining and extending Access", provides high-level, summary information about AEMO's IT systems, to assist participants with decisions about usage of the data interfaces to AEMO's systems.
- "Web Portal Login User Guide": for information on how to log on to AEMO's Web Portals.

### 7.3 Information centre

The AEMO Information Centre provides an information service for all interested parties, from NEM participants to the general public, providing information regarding AEMO NEM operations and the electricity industry generally.

- Telephone: 1300 361 011. E-mail: [infocentre@aemo.com.au](mailto:infocentre@aemo.com.au).