

CREATING USERS AND USER GROUPS

Date Created: November 8th, 2017

Date Modified:

Introduction

This procedure document lists the steps to create Users and User Groups in AssetPlanner™ District Administrators can create Users, select Roles and add them to User Groups to define Permissions.

Database Access and Permissions are determined for each User based the following:

User Type: Specifies the general type of User account & access.

User Roles: Allows for additional permissions to be assigned to each User.

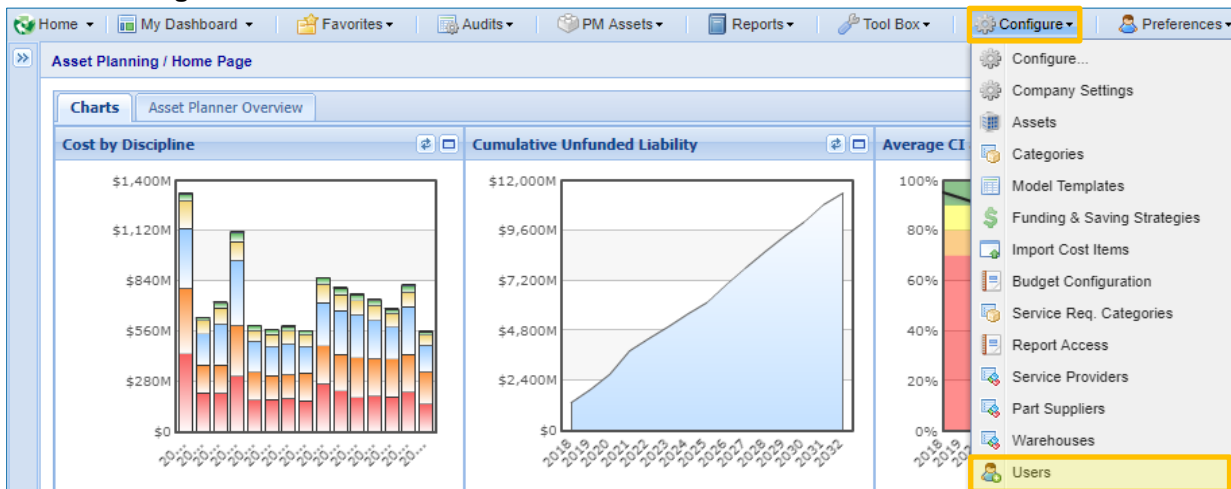
User Groups: Specifies the Module, Assets and Read/Write permissions for a Group of Users.

Follow the steps below to configure the appropriate Permissions & Access for each user.

Creating Users

Step 1

Click on **Configure** from the menu bar and select **Users**



Step 2

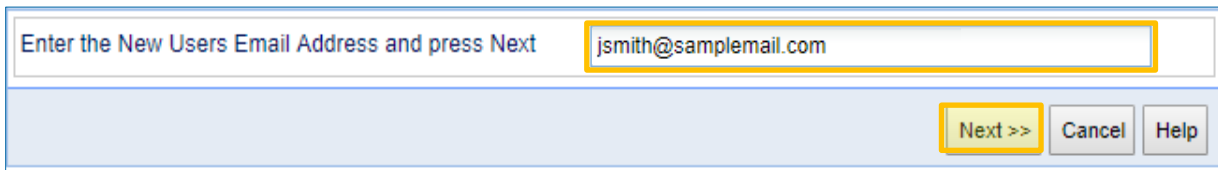
Click on the **Add** button.

The screenshot shows the 'Find Users' form. It has input fields for 'First Name', 'Last Name', 'Email', and 'Department' (a dropdown menu). There is also a 'Disabled Accounts' dropdown menu. At the bottom right, there are three buttons: 'Find', 'Add', and 'Help'. The 'Add' button is highlighted with a yellow box.

Note: Do not enter the Users details in the fields above as these are related to the find feature. Click the Add button and then you will be prompted to enter the Users e-mail on the next screen.

Step 3

Enter the e-mail address of the User you would like to add and click on **Next** to continue.



Enter the New Users Email Address and press Next

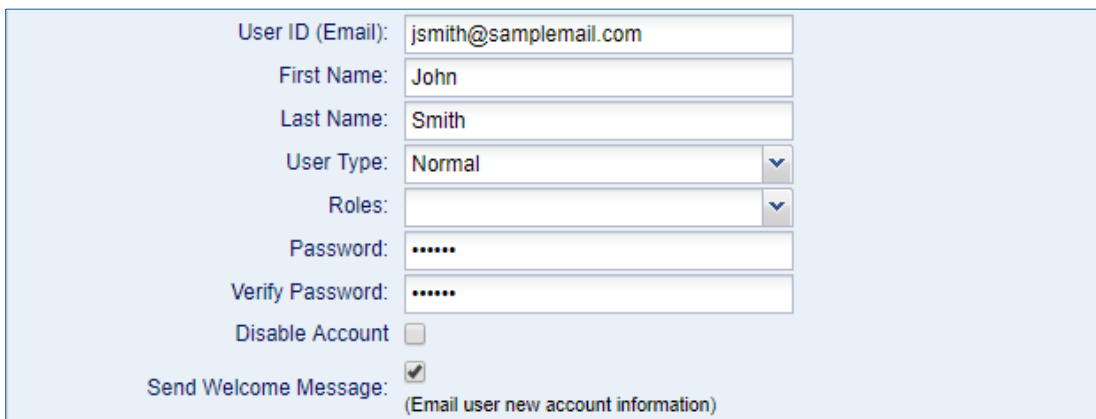
jsmith@samplemail.com

Next >> Cancel Help

Step 4

On the User form enter their **First Name**, **Last Name**, provide them with a temporary **Password** (ex. KDE123) and enter the same value under **Verify Password**.

Ensure that **Send Welcome Message** is checked as this will send an e-mail to the User with instructions on how to login and set up a new password for their account.



User ID (Email): jsmith@samplemail.com

First Name: John

Last Name: Smith

User Type: Normal

Roles:

Password: *****

Verify Password: *****

Disable Account

Send Welcome Message:
(Email user new account information)

District Administrators should first determine if they would like to allow **Read** or **Write** access and then select the User Type, Roles & Group Permissions for each User accordingly.

Read Access: Provides Users with the ability to read and report on the data with no edit rights. Read access is typically provided to support staff who need to view but not modify the data.

Write Access: Provides Users with the ability to read, report and edit the data. Write access is typically provided to a select group of Users who are responsible for managing and maintaining the data.

District Users – Read Access

User Type: Select the **Normal** User Type.

Roles: Do not assign any Roles to Users with Read Access.

If required, you can assign the **Facility Attachments** role to specific users. This will maintain their Read only permissions but will allow them to add pictures or documents to Facilities.

Note: Refer to the **References** section for additional information on User Types and Roles.

District Users – Write Access

User Type: Select the **Normal** User Type.

Roles:

Facility Data Admin: Allows the user to modify the Facility Details and Tabs within the Facility form.

Element Data Admin: Allows the user to modify the Element and Action data within the Published Element inventory.

Note: Depending on the User you may want to assign one of the above Roles or both. For example, you may want to allow modifications of the Element and Action data but want to limit modifications to the Facility Details.

Auditor Users

User Type: Select the **Contractor** User Type.

Roles: Do not assign any roles to Contractor Users.

If required, you can assign the **Contractor Lead Role** to specific Users. This role will give them access to all Audits assigned to their User Group. This Role is typically assigned to a User who is responsible for reviewing Audits assigned to their Group (ex. "Team Lead" - one per Auditor Group).

Note: Contractor Users will only have access to Audits that have been assigned to their account. Users with the Contractor Lead Role will see all Audits assigned to their Group.

Step 5

Click **Save** to add the User to the Database.

The screenshot shows a web form titled "New User Account". At the top left, there is a user icon and the title. Below the title is a toolbar with four buttons: "Save" (highlighted with a yellow box), "Back", "Delete", and "Help". The form has three input fields: "User ID (Email)" with the value "jsmith@samplemail.com", "First Name" with the value "John", and "Last Name" with the value "Smith".

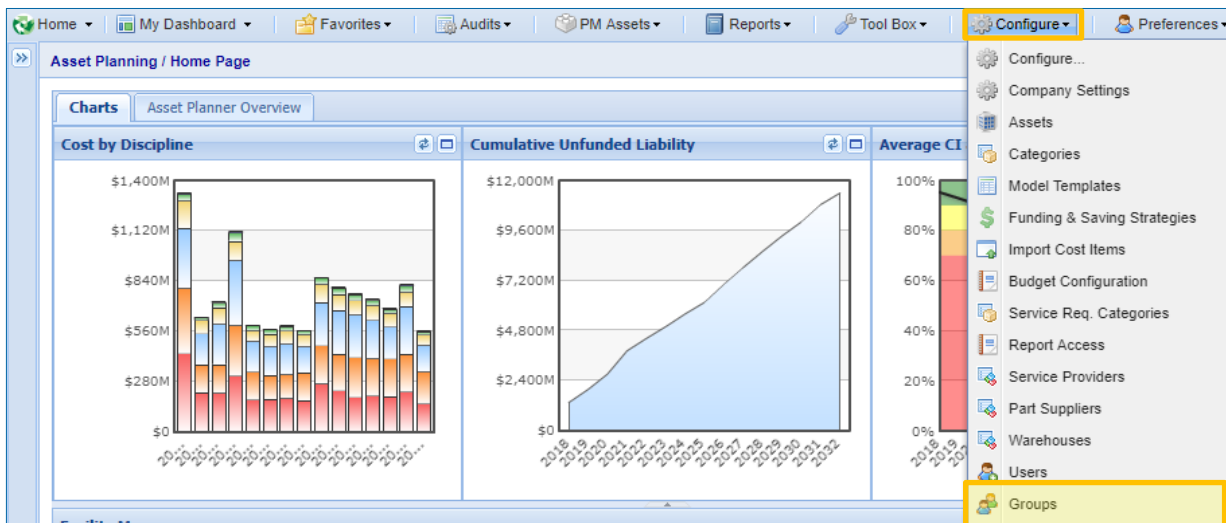
Note: At this point the User will be able to login but will not have access to any Modules or Assets until you add them to a **User Group**.

Creating User Groups

Groups help organize your Users based on common Permissions (Read/Write) to Assets (schools or buildings) within the database. Once a Group and Permissions are established Users can be added or removed and will inherit the permissions of the Group.

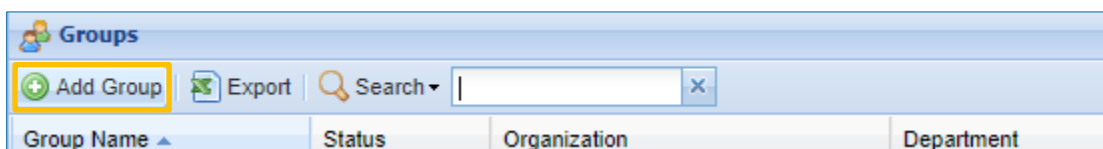
Step 1

Click on **Configure** from the menu bar and select **Groups**



Step 2

Click on **Add Group** to add a new **User Group**.



Step 3

Enter a **Group Name** that briefly describes the general purpose and members of the group. For example: "District Users – Read", "District Users – Write", "Auditor Users" or "Consultant ABC"

Ensure that **Assignable** is checked if you would like to assign Audits to the Group members.

Click **Save** to create the Group.

Manage Group membership and permissions

Save Delete New Group Back

Group Name: * Auditor Users

Description:

Organization: All

Department: Ameresco

Status: * Active

Assignable: (if checked, this group and/or it's members can be assigned to items.)

Step 4

Add Users to the Group by first selecting them under the **Non-Members** listing (list of all Users) and use the **Add >>** button to add them to the **Members** list.

Group Members | Permissions

Non Members

Search [x]

Name	Organization	Department
Adam Hooker		Laurel County
Addison Whitt		Morgan County
Aleisha Ellis		Clark County
Allen Brumfield		Christian County

Page 1 of 1 | Displaying 1 - 445 of 445

Add or Remove

Add >> << Remove << Remove All

Members

Search [x]

Name	Organization	Department
Adam Harasimowicz		Ameresco

Members can be added or removed from a Group at any point using the **Add or Remove** buttons.

Step 5

Once you have added Users to the Group the next step is to assign **Permissions**. This will specify the **Assets** they can view and if they have **Read** or **Write** access to them.

Select the **Permissions** tab and use the check boxes to select the **Assets** to allow access.

Group Members | **Permissions**

Select items

View: Asset Class

- Model TypeIDs
 - Athletic Building
 - Bus Garage
 - Central Office
 - Maintenance Building
 - School
 - Storage Building

Add using:

Module: Asset Planning

Permission: Read

Add or Remove

Add >> << Remove << Remove All

Assigned Permissions

Module	Permis...	Asset	School District	Regional Co-Op	Sc
Asset Pla...	Read				

District User Groups – Write Access

Select Assets using the check boxes. Under **Add Using** set the Module to **Asset Planning**, Permissions to **Write** and click **Add>>** to assign the permissions to the Group.

District User Groups – Read Access

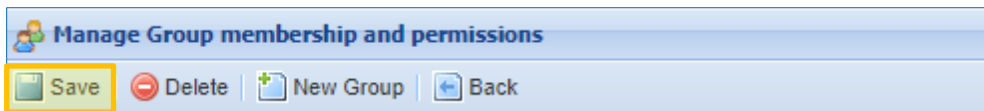
Select Assets using the check boxes. Under **Add Using** set the Module to **Asset Planning**, Permissions to **Read** and click **Add>>** to assign the permissions to the Group.

Auditor User Groups

Select all Assets using the check boxes. Under **Add Using** set the Module to **Asset Planning**, Permissions to **Read** and click **Add>>** to assign the permissions to the Group.

Step 6

Click **Save** to finalize the User Group Members and Permission selection.



Reminders

- It is the Districts Responsibility to maintain and update the User list and User Groups. For example, if a User no longer requires access they should be disabled or deleted.
- Prior to assigning an Audit ensure that the User has an account (Contractor User Type) and is a member of a User Group with Permissions to the Asset they will be Auditing.
- Contractor Users will only see Audits that have been assigned to them. If no Audit has been assigned, they will not see anything in the web Audit Manager or AuditPlanner™

References: User Type & Role Definitions

User Type:

Normal: Normal users are provided with a basic level of permission and access to the database.

Use this role for **District Users** who require read or write access to the database. The use of User Roles & Groups will allow Read or Write capabilities for each Normal User.

Contractor: This role restricts access to items that have been assigned to the user. It is commonly used for outside Contractors or Service Providers who require limited access to the database.

Use this role for **Auditor Users** as it will grant them access to the web Audit Manager and AuditPlanner™. Only Audits assigned to them will be visible in the web & mobile app.

Administrator: This role provides full access to the database and configuration settings and is typically limited to one individual (**District Administrator**)

Configuration: This is a limited administrative role that allows for User Group and User creation / administration (**District Support Staff**)

Note: If you are unsure of the user type, select **Normal** as this is the most commonly used User Type. Remember if you are providing access to a building Auditor you should select **Contractor**.

User Role:

Facility Data Admin: Allows a user to modify the Facility Details and all tabs within the facility form. Normal **District Users** with **Write Access** should have this role.

Element Data Admin: Allows a user to modify the Element and Action data within the Published Element Inventory. Normal **District Users** with **Write Access** should have this role.

Facility Attachments: Allows a user to attach pictures/documents to Facilities. This role is useful for Normal **District Users** with **Read Access** that you would like to allow attachment adding.

Audit Publisher: Allows a user to Publish Audits. This role is for **District Users** that will be involved in the QA/QC process and require permission to Publish Audits.

Contractor Lead: Allows for viewing and access to all Audits assigned to the Users assigned User Group. This role is for **Contractor** users that require an additional level of access to review and modify Audits that are conducted by members of their User Group.

Note: If you are unsure of the User Role to select leave this field blank and it will provide access based on the User Group permissions.