


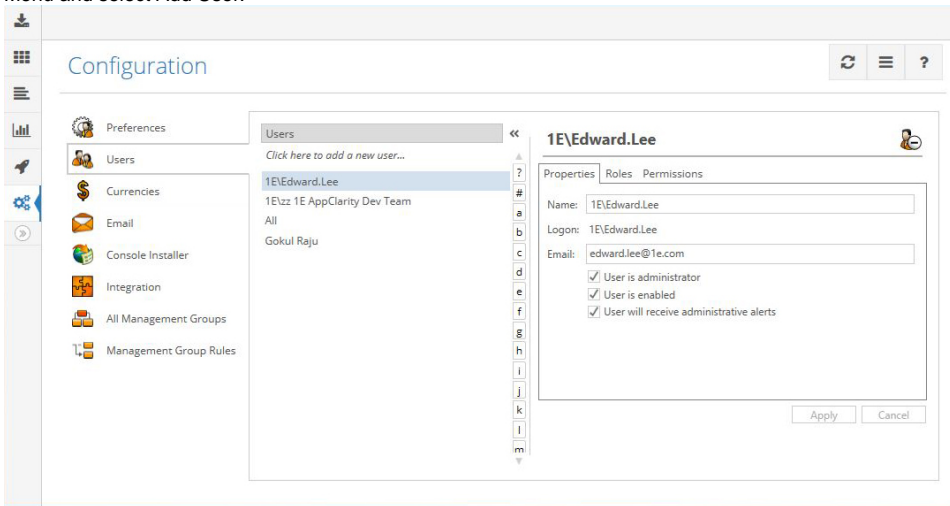
Managing users

You need to add users and set up their access rights in order for them to [get an invitation](#) to download and install the Console. You can determine which screens they see and the tasks they can perform. Initially, there is only the service account and it is the responsibility of this account to add users.

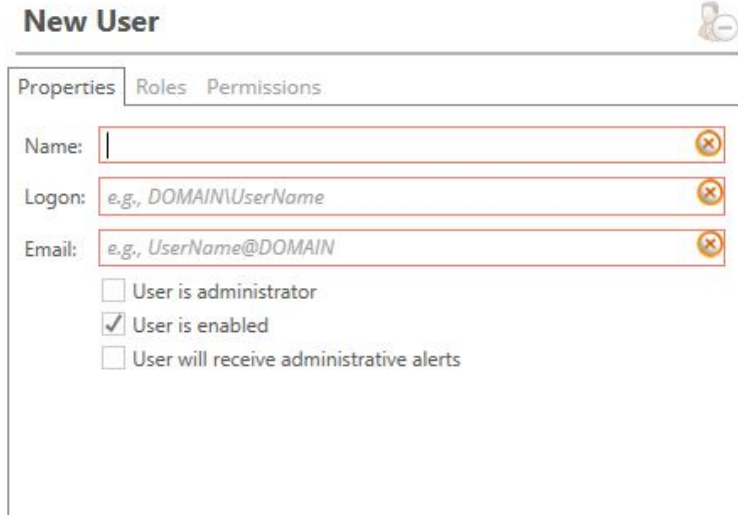
Adding a new user

To add a new user:

1. Click Configuration icon  to the left of the Console.
2. On the Configuration screen, click Users.
3. The simplest way to add a new user is to follow the [Click here to add a new user.. link](#) directly under the list of users Alternatively click the Actions Menu and select Add User.



4. In the New User dialog, populate the attributes for the new user in the Properties tab.



The attributes for the user or group are:

- Name – the name of the user
 - Logon – the domain account for the user or group. This is set and verified when the user is created and cannot be updated.
 - Email – the email address for the user or group – used by AppClarity to send email notifications.
 - User is administrator – users or groups with this permission can view all parts of the AppClarity Console.
 - User is enabled – users or groups can access the AppClarity Console. It is possible for a user to disable their own account. Should this happens, they will lose access to the AppClarity Console. To re-enable their account, they will need to ask another AppClarity administrator to enable them.
 - User will receive administrative alerts – users or groups will receive alerts when licenses are due to expire
5. Click the Roles tab to define the roles for the user. If a user is classified as an administrator (User is administrator is checked in the Properties tab), they have full permissions to view and use the AppClarity Console. If the user is not an administrator, their permissions are determined by the Management Group they are associated with. For example, the Overseas Administrator can view licenses for the Australasia Management Group and not edit them but is able to view and edit Product definitions.

New User



Properties **Roles** Permissions

Group	Role			
	License Viewer	License Editor	Product Viewer	Product Editor
[Global View]	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
[Central]	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Bahaa	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Users may be assigned different roles for different management groups. For example, a user may be allowed to view licenses for the Europe Management Group, edit products for the Americas Product Group and have no role for any of the other Management Groups. If a user has editor permissions, they will inherit the associated view permissions (you cannot edit something you cannot see). In the example above, the Product Viewer checkbox is checked but disabled as the Product Editor role is checked. Similarly, the user will inherit the License Viewer role if they are granted the License Editor role. The features associated with each role is detailed in [features, roles and permissions](#).

- Click the Permissions tab to grant permissions to the user. If a user is classified as an administrator (User is administrator is checked in the Properties tab), they have full permissions to view and use the AppClarity Console.

New User



Properties Roles **Permissions**

User can access Integration Services

You can grant non-administrative users access to integration services which may not have been granted in the management group they are associated with. Tick the User can access Integration Services checkbox to grant the user permissions to use service. This user may or may not have been assigned any roles to access the console but they can access the integration service.

- Click Apply to save the new user. AppClarity will verify the details before creating the new user. To abort, click Cancel.

Features, roles and permissions

The table below details the permissions for each role and their associated features.



Feature/Role		Product Viewer	Product Editor	License Viewer	License Editor	Administrator
Data Capture View						
	View Data Connectors	Y	Y	Y	Y	Y
	Add Data Connectors					Y
	Delete Data Connectors					Y
	Synchronise Data Connectors					Y

	View Applications (Unidentified, Junk, Excluded)					Y
	Link or Unlink Applications					Y
	Include or Exclude Applications					Y
	Import License CSV				Y	Y
	View License Rules			Y	Y	Y
	Activate License Import Rules				Y	Y
	Delete License Import Rules				Y	Y
Products View						
	View Products	Y	Y	Y	Y	Y
	View Compliance Indicators			Y	Y	Y
	View Entitlement Column			Y	Y	Y
	View Compliance Tab			Y	Y	Y
	View Pricing Tab			Y	Y	Y
	View Policy (Software Reclaim) Tab	Y	Y	Y	Y	Y
	Modify Licenseability				Y	Y
	Modify Pricing				Y	Y
	Modify Reclaim Policy		Y			Y
	Modify Categories And Tags					Y
	Modify Notes		Y		Y	Y
	Modify License Managed Setting				Y	Y
Licensing View						
	View Licensing			Y	Y	Y
	Add or Edit Licenses				Y	Y
	View Attachments			Y	Y	Y
	Add or Delete Exclusions				Y	Y
	Modify License Managed Setting				Y	Y
	Modify License Metrics				Y	Y
Automation View						
	View Automation	Y	Y			Y
	Start Automation					Y
	Stop Automation					Y
	View Uninstall Command Lines					Y
	Modify Uninstall Command Lines					Y
Reporting View						
	View Reporting	Y	Y	Y	Y	Y
	Run Overlapping Functionality Adobe Acrobat Report	Y	Y	Y	Y	Y
	Run Labs: Product Suite Optimization Report	Y	Y	Y	Y	Y
	Run Product Installation Report	Y	Y	Y	Y	Y
	Run Shelfware Identification Report			Y	Y	Y
	Run Software Reclaim Savings Report	Y	Y	Y	Y	Y
	Run Specific Device Report	Y	Y			Y
	Run Unused Software Identification Report	Y	Y	Y	Y	Y
	Run Vendor Compliance Report			Y	Y	Y
	Run vmware Report	Y	Y			Y
	Modify Cost on Costing Grid				Y	Y

Configuration View						
	View Preferences	Y	Y	Y	Y	Y
	Edit Preferences	Y	Y	Y	Y	Y
	View Configuration					Y
	View User List					Y
	View User Properties					Y
	Modify User Properties					Y
	View User Permissions					Y
	Modify User Permissions					Y
	Add New User					Y
	Delete User					Y
	View General Configuration Settings					Y
Modify General Configuration Settings					Y	

Deleting an existing user

To delete an existing user:

1. Click the Configuration icon  to the left of the Console.
2. On the Configuration screen, click Users.
3. From the Users list, select the user you want to remove.
4. Click the Delete User icon  located at the top-right of the user's details. Alternatively, click the Actions Menu and choose Delete User.
5. You will be prompted to confirm you actions. Click Yes to remove the user or Cancel to abort. You can prevent this prompt from appearing by unchecking the Always show this message checkbox on the bottom-left.

It is possible for an administrator to remove all users from the Console. Should this happen, they will lose access to the Console. Re-run the AppClarity installer for the AppClarity Service component.