

Users Permissions

The "Modify Users Permissions" page lets you decide who can access specific features or specific application. For example, a user can have administrative rights for Digital Fax but may not be authorized to restart the Call Recording engine. Permissions can be set for each user and for each IUCS application.

Permissions range from 1 (low) to 10 (high). When a user has permission 1 ("No access") for an application, he/she cannot see it in the IUCS menu after login. Permission 10 ("Complete management") enables administrative access.

For information about each value meaning for a specific application, please refer to its description in this guide.

System Management permissions

Starting from Imagicle Rel 2020.Winter.1, it has been introduced a **System Management** permissions entry, replacing previous **Users Management** permissions. System Management includes five permission levels:

- (1) Base access
- (6) Department users supervisor (Tenant users supervisor, if *multi-tenant*)
- (7) Department users manager (Tenant users supervisor, if *multi-tenant*)
- (9) Complete users management
- (10) Complete management

Base access

This permission level does not allow to view, create, edit or delete any user and cannot manipulate the privileges of any user, for any application.

Department/Tenant users supervisor

System Management's level 6 can view and modify those users belonging to own department (for *single-tenant*) or own tenant (for *multi-tenant*). All fields are changable, but the following read-only fields: "Active Directory username", "Domain", "Remote Authentication Username", "User PIN", "Accesses", "Department", "List of additional departments".

Level 6 supervisor can also assign or modify permission levels of another user, with the following limitations:

- Single tenant
 - ◆ For users belonging to same department/tenant: can assign System Management privilege levels <= 6. If the user has already a higher permission level (like 7 or 9), it can be selected too.
 - ◆ Other applications: can assign any privilege level.
- Multitenant
 - ◆ All applications: can assign all privilege levels <= their current application level. If the user has already a higher permission level, it can be selected too.

- For users belonging to another department/tenant:
 - ◆ Cannot manipulate the privileges.

This permission level does not allow the access to tenants web page: fw/apps/applicationsuite/web/pages/tenants.aspx

Users export to CSV/XML is available, for own department/tenant users only.

Adding, deleting or importing new users from external sources is denied at this level, including synch settings/rules.

Department/Tenant users manager

System Management's level 7 inherits all permissions of level 6 supervisor, plus the possibility to delete or manually add own department/tenant users. New users are automatically assigned to own department/tenant. The following fields are read-only: "Active Directory username", "Domain", "Remote Authentication Username", "User PIN", "Accesses", "Department", "List of additional departments".

Level 7 users manager can also assign or modify permission levels of another user, with the following limitations:

- Single tenant case, for users belonging to same department/tenant:
 - ◆ System Management: can assign all privilege levels <= 7. If the user has already a higher permission level (9 or 10), it can be selected too.
 - ◆ Other applications: can assign any privilege level.
- Multitenant case:
 - ◆ All applications: can assign all privilege levels <= their current application level. If the user has already a higher permission level, it can be selected too.
- Users belonging to another department/tenant:
 - ◆ Cannot manipulate the privileges.

Importing new users from external sources is still denied at this level, including synch settings/rules.

This permission level does not allow the access to tenants web page: fw/apps/applicationsuite/web/pages/tenants.aspx

Complete users management

System Management's level 9 grants full visibility of **all** users, including adding/modifying/deleting any IUCS user, import them from an external source and amend synch settings/rules. All users' fields are changable, including *Department* and *List of additional departments*. Level 9 users manager can also assign any permission level, for any application, except level (10) *System Management*.

Level 9 users manager can't access to IUCS administration menus and he/she doesn't have the permission to invoke administrative APIs to amend IUCS system parameters.

This permission level does allow the access to tenants web page: fw/apps/applicationsuite/web/pages/tenants.aspx

Complete management

System Management's level 10 inherits all permissions of level 9 users manager, plus the possibility to assign level 10 *System Management* permission to all users, full access granted to IUCS administration menus and administrative APIs to amend IUCS system parameters.

Modify permissions for user 101		Default permission
System Management	[default for application] ▼	(1) Base access
Billy Blue's 4	[default for application]	(2) View personal calls
Budget Control	(1) Base access	(2) View own budget
StoneLock	(6) Department users supervisor	(2) Base access
StoneFax	(7) Department users manager	(2) Send / receive faxes
Speedy Enterprise	(9) Complete users management	(2) Base access
IVR Manager Enterprise	(10) Complete management	(2) Change active behavior
IVR module for Queue Manager Enterprise	(10) Complete management	(1) No access
Queue Manager Enterprise	[default for application] ▼	(2) Base access
Blue's CTI Server	[default for application] ▼	(1) No access
Call Recording	[default for application] ▼	(3) Base access
SSAM Enterprise	[default for application] ▼	(1) Base access
Hotel Link	[default for application] ▼	(1) No access

Users with previous legacy **Users management's level 6** (*Edit tenant users*) are migrated during IAS update to **System**

Management level 7 (*Department/Tenant users manager*).

Changing default permissions

If you leave an entry set to "[Default for application]", the users' permissions will be derived by default values. You can edit them by selecting the **Modify Default Permissions** link on the top of the page.

In this way you could grant or revoke access to an application to all the users at a time. If you set a specific permission for a given user, this will override the default. The override will not be affected when you change the default permissions for all users.