User Management

26 Jan 2022

imagicle

Table of Contents

imagicle

User Management

The Users List

To be able to use the Application Suite services, a person **must** be added to the list of known users. E.g., if Mario Rossi wants to send faxes through StoneFax, it is mandatory that you create a user for him in the Users List.

The user properties in the users list control which telephone (device) is owned by the person, if an application is enabled for that person and so on.

The users list also represent the internal contacts ("colleagues") directory.

- All the Application Suite programs share the same Users List
- A user in the users list can be associated to exactly one primary extension, one voicemail number and one fax number
- Those numbers must be unique. E.g. the phone number 303 must appear only once in the users list, either as primary extension, voicemail or fax number.

If you need to associate more than one extension to the same person, you must create secondary users for him/her in the users list.

Usually, users in the users list represent physical persons, but you may want to create virtual users to control specific devices. For example you could create a "showroom" user which is associated to the IP phone of your company's show room.

So the users list is where you should start configuring the Application Suite. You can create the users list:

- Adding them manually, one by one
- Importing them from a file
- Synchronizing the list with an external source, such as Active Directory, OpenLdap, a PBX or a database

You usually edit the users list logging into the web interface as the Main Administrator.

imagicle

Editing Users Manually

Manually Adding or Editing Users

Through the **User Management** link in the **Admin** menu you can add or remove users from you system, edit the details and modify the permissions.

Click on the link on the top of the "User management" page to **create a new user**. Press the **Modify** icon to edit user details. Click the **Delete** icon to permanently remove a single user or the "Delete from database" button (on the bottom of the page) to remove all the selected users, i.e. all the users you filtered through the "Customize search criteria" panel.

User Details

In this web page you can edit all the user's details at once. Some of the information shared between applications (login information, IP telephony data, personal information..) while other fields must be filled only if a specific application is licensed.

Then you will need to fill the other parameters depending on the application you are going to configure.

Please refer to the **basic configuration** section of each application for a detailed description of the relevant fields and their meaning.

Login information

When adding or editing a user, **the only mandatory fields are username and password.** Other login information may be required by some application.

- **Username**: Unique identifier for the UCS user, case-insensitive. It is requested when logging in the web interface. Only digits and the underscore character are allowed.
- **Password**: password requested when logging in the UCS web interface using the UCS username. Case sensitive.
- **Pin**: User PIN for VoiceMail, Phone Lock.
- **Remote Authentication Username**: useful for authentication over a third party LDAP server, such as OpenLDAP. This option is allowed with the assistance of Imagicle Technical Support only

If **Active Directory Username** and **Domain** are filled, the user authentication is made through a LDAP query to the Domain controller. The Domain field must contain a DNS name which the Application Suite server can resolve. In this case the standard Username and Password are ignored. The domain password is stored on the Domain Controller only.

On the contrary, if either Active Directory Username or Domain are blank, the user must login through the UCS Username and Password. You can have some users who use AD authentication and others who use standard UCS authentication at the same time.

In the **Active Directory Username** you must enter the AD username without the domain, e.g. "john.smith". in the domain field, the DNS Domain name, e.g. "mydomain.com".

Note: To be able to log through LDAP authentication, the UC Suite server does **not** need to be joined to the domain. But it **MUST** be able to resolve the DNS name. The first troubleshooting step if LDAP authentication fails is to log onto the server and type at the command prompt "Ping mydomain.com".

Personal Information

- **First Name**, **Last Name**, **Email**, **Mobile Business Number**, **User Address**, and **Home Phone**, are reported on Digital Fax cover pages, Attendant Console internal contacts (colleagues) and Contact Manager web search
- **Preferred language**: controls the language of the Web interface and of the Attendant Console for the user. Valid values are EN, IT, FR, ES, DE. Different users may have different languages.
- **Department**: affects the way the user can access Contact Manager directories. Please check the relevant section of this guide

IP Telephony

- **First Extension Number** and **MAC address**: The first extension number is used by Imagicle applications to be able to tell which physical device is associated to a person. If two users share the same line, the MAC address will be taken into account. MAC addresses must be unique.
- **First extension number alias**: Optional alternative directory number or PSTN number (DID) assigned to the user. This is useful to correctly correlate recordings performed through AudioCodes or other SIPREC-enabled Media Gateways. Call Analytics can leverage it too, to monitor user's phone traffic on an alternative extension number, without consuming an additional user's license.
- **PBX username**: this field needs to be filled if Extension Mobility is enabled on a Cisco PBX. See Speedy configuration for details.
- **Partition**: please refer to Imagicle Billing section

Providing correct IP telephony information allows Imagicle application to tell which IP phone is in use by a person. For example, user John has line 1001 assigned; in the user's list add a user with the name "Mario" and the number 1001 in the extension number. So when Contact Manager must notify an incoming call for line 1001, it will search the right directories and display the message on the right IP Phone.

As a general rule, when a telephony event is raised, Imagicle UC Suite services try to look for the user owning the IP phone:

1. Checking the line that is involved against the First Extension number field
2. If more than one user has the same line in the First Extension number field, or if the line is shared (i.e. assigned to more than one device), they try to tell them by the MAC address

So, filling the MAC address is required only if there is some kind of ambiguity.

For Cisco environments only: if Extension mobility is enabled (through Contact Manager's "Manage Service" page) the IP phone associated to the user will be the one the user is logged onto. The user name entered in the end user list on the PBX must be also typed in the **PBX username** field.

Searching Groups of Users

By default, the "User Management" list shows all the IAS users.

You can restrict the number of items shown in the users table by clicking the **Customize search criteria** link and adding conditions. All the conditions impose restrictions (i.e. are considered in a boolean "and" relation), so the more conditions you add, the fewer will be the items shown.

With filter capabilities you can search users by any of available parameters and use the following conditions:

- Is exactly
- Begins with
- Ends with
- Contains
- Does not begin with
- Does not end with
- Does not contain
- Is empty
- Is not empty

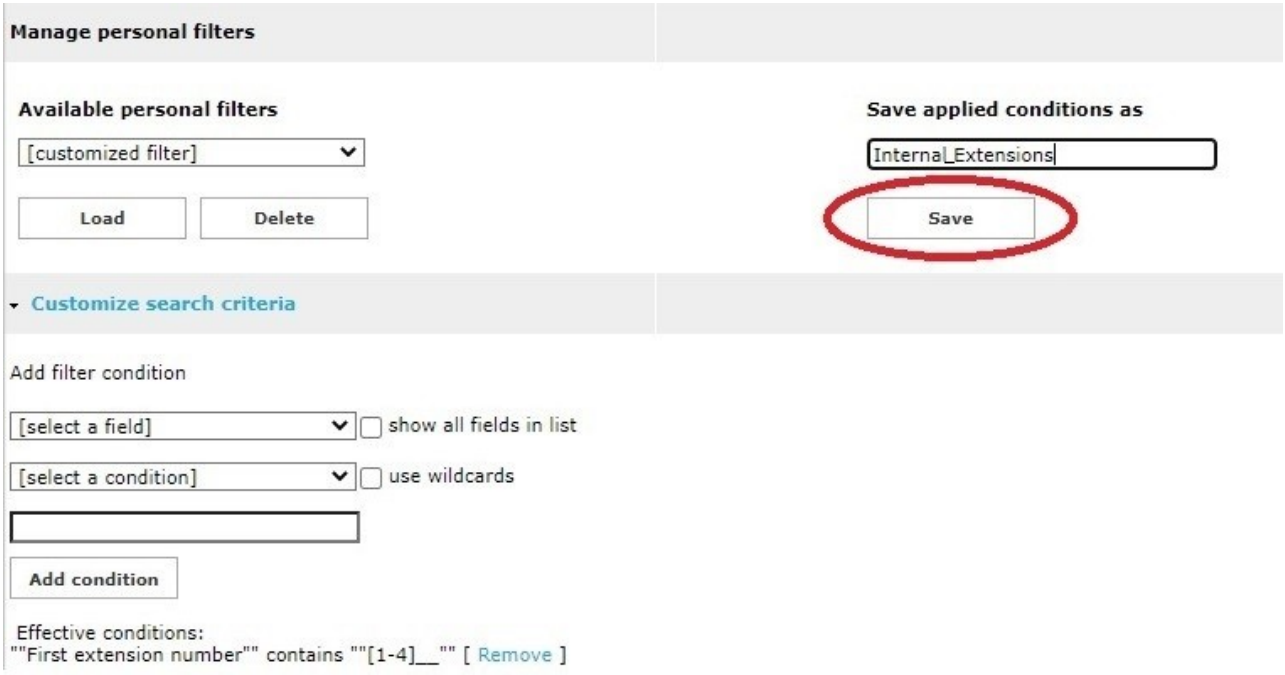
You can use wildcards in the field to be searched by the filter:

- * (asterisk) : means any character sequence of any length
- _ (underscore) : means any single character
- [abc] : means a,b or c character
- [a-z] : means any character from a to z

For example, to select all the users who have a first extension number which is 2xx together with those who have 4xx, use this filter:

```
"First extension number" contains "[24]__" (use wildcards)
```

Filters can also be saved for later use by clicking the "Add or modify personal filters" link.



Importing from CSV files

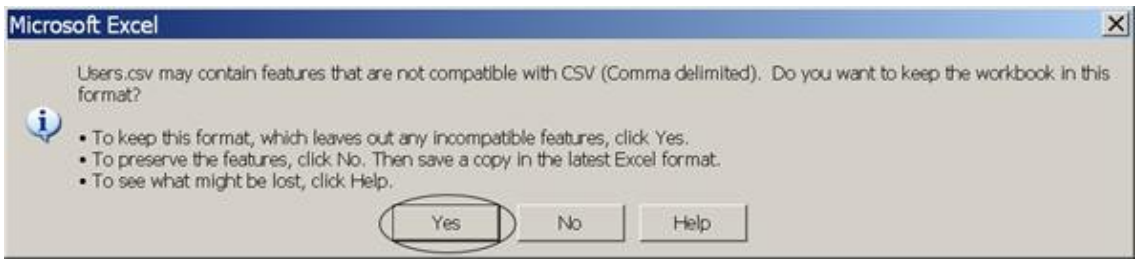
Importing from CSV files and Bulk Editing

To quickly to modify the same property of a group of users (bulk editing), you can export them to a CSV or to a Microsoft Excel XML file, modify it and import it again in the IAS database.

To create a group of users from scratch, you just download a CSV template file from the web interface, fill it with the values, and load it to the IAS database.

Procedure to create a group of users

- Select the "Import users from CSV" link.
- Click the "Template.csv" link and save the file to a temporary folder.
- Open the file with a CSV editor. For example, you can use Microsoft Excelâ ¢.
- Fill all the mandatory fields columns, based on the application you need
- Save the file. If asked to preserve CSV format, press "Yes".



- Return to the "Import Users" page, click "Browse..." to select the file and the press "**Import**". If you are loading a huge number of users, you may have to wait some minutes
- Press the "Import" button. If you are loading a huge number of users, you may have to wait for some minute.

A **green** icon means that all the users have been imported. A **yellow** icon means that some user has been skipped. A **red** icon means that an error occurred.

Reports

When the Import process is completed, the "**Show reports**" link is displayed. All the details can be found in the report file. If a user or a specific column content has been skipped, you'll find the information you need to identify the CSV file row and fix it. Click on the "Download" icon to the left to open the report as a text file.

Preliminary concepts

- A user is considered new if it has an unknown **username**. If the username already exists, the other fields will be overwritten.
- All fields included in the .csv file are overwritten when you import the .csv file in your Application Suite (including empty fields). If you leave a field blank in the CSV file, it means you want it to be erased.
- True/false (boolean) fields are expressed as 1 and 0 in the CSV file
- The CSV file fields must actually be separated by semicolon (Excel standard)
- Some fields may not be included in the import/export process. They are only modifiable from the User Management of the web interface.
- The fields are identified by the column name in the header (i.e. in the first row). Do not change them.
- When a field is populated, its content is validated. For example, if you fill the email field with something which is not an email, the field will be skipped and an error will be recorded in the report.
- Some field values (e.g. the primary extension) should be unique between different columns. It is your responsibility to guarantee this.

CSV File Encoding

When you want to import users which include non-US characters, pay special attention to the file encoding. Supported encodings are:

- ANSI
- UTF-8 with BOM
- Ucs-2 Le / UTF-16 Le

Note: Excel only supports ANSI CSV files. To preserve non-ansi characters you have to save the file as "Unicode text".

Example 1: enable fax for all the users

- Make sure you have some users in the users list.
- Click the "Export for Excel" button and save the file.
- Open the file with Microsoft Excelâ ¢. The field format will be preserved.
- Write the digit "1" in the "Fax Send Enabled", "Fax Receive Enabled", "Fax2Email Enabled", and "Fax2Email Attach Fax" columns of each user.
- Copy the email address from the "E-mail" column to the "Fax2Email Address".
- Select "save as.." and save the file as .CSV.
- In the IAS "user Management", click the "Import Users from CSV" link.
- Click "Browse..." to select the file and the press "Import". If you are loading a huge number of users, you may have to wait for some minute.

Example 2: add voicemail only for the users who have a primary extension which starts by 3

- Click "Customize search criteria" to filter the right users.
- In the drop down boxes choose "First Extension Number" and "Begins With". In the textbox enter "3". Click "Add Condition"
- Click the "Export to CSV" button.
- Fill the "First Extension Number", "Voicemail Number", "Voicemail Address" columns.
- Save the file to disk and import the file as in the examples above. The other users, that is the ones excluded by the filter, will remain unchanged.

The Main Administrator

The Main Administrator

The Main IAS Administrator is a *super user* which always has full permissions (Level 10) on all the applications and is allowed to configure the system. This "first user" is created during setup and cannot be deleted.

The Main Administrator can create other users with extended permissions, so you can have an unlimited number of administrators allowed to manage some or all the applications.

The Main Administrator is not included in the IAS users list. It cannot be associated to a Voip phone, telephone number, fax number, personal email and so on. His purpose is only to perform the configuration of the services. For this reason, this account has no access to the Attendant Console, cannot send faxes, use click to dial, have personal directories...

If you give administrative privileges to a IAS user, he or she will not have such limitations.

Editing the Main Administrator's Details

From top-right "ADMIN" link, available in any web portal's page, the IAS administrator can can change own username and password.

How to reset the main administrator to admin/admin

If you did forget the main administrator password, you can reset it by using one of below options:

IAS version < 2020.Winter.1

- By reinstalling the IAS package in the same folder, choosing a new name and password, or
- By logging onto the IAS server and running the **ResetIasAdmin.exe** application from the **<install dir>\Troubleshooting** folder
- If tool is not available, you can download it from here.

IAS version >= 2020.Winter.1

- By reinstalling the IAS package in the same folder, choosing a new name and password, or
- By logging onto the IAS server and running the **ResetAdminCredentials.bat** batch file from the **<install dir>\System** folder

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

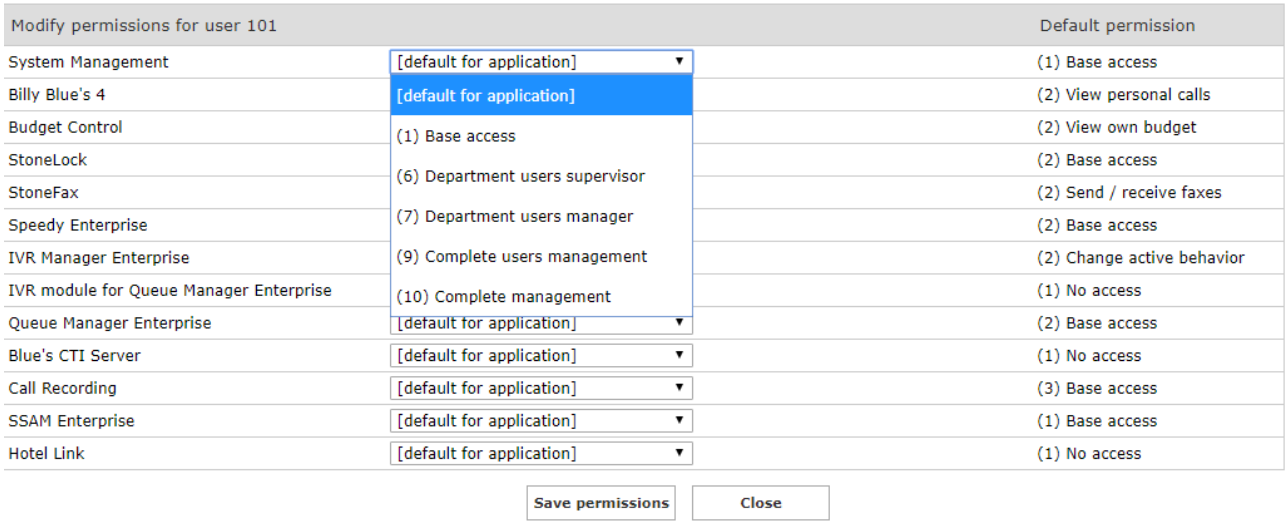
System Management's level 9 grants full visibility of **all** users, including adding/modifying/deleting any IUCS user, import them from an external source and amend synch settings/rules. All users' fields are changable, including *Department* and *List of additional departments*. Level 9 users manager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



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.

Sync Users with External Sources

All the applications included in the Suite share the same users list. This list can be edited manually through the web interface, adding users one by one, or automatically, importing the user list from a CSV file. If you have a large number of users, you might want to keep the user list in sync with an external directory.

The Synchronization Service lets you import users from an external source such as Active Directory, a database or the PBX. Once synchronization is enabled, the service will align the list of users **once a day**. When a new user is added to the external source it is inserted into the IAS users list. When the properties of a user are updated, the changes are written to IAS user data. Data transfer is optimised and only the differences are written to the database.

You could also use the synchronization service to import users once, then disable it and adjust the list manually.

Supported operations and matching criteria

The user synchronization service can perform three types of operation:

- Insert, i.e. adding a new user
- Update, i.e. changing one or more properties of an existing user
- Delete, i.e. removing the user from the list

An Application Suite User list is considered to be the same as an Active Directory User when the "Active directory username" field combined with the "Domain" field value matches the Active directory account. E.g.

- **Active directory account** = John.Smith@yourdomain.com
- **Active directory username** field in User Management = John.Smith
- **Domain** field in User Management = yourdomain.com

By default users which are deleted from the external source are automatically removed from the IAS. This is the main difference between importing users from CSV and synchronization. CSV import does not remove users, while the synchronization does.

If you want to create additional local users which will not be deleted when the sync operation is performed, make sure that the fields used as synchronization key (Active directory username and Domain) are blank.

How to enable Users Synchronization

You can access user synchronization through the web interface by selecting "User Management", then clicking the link "Synchronize users with an external data source" on the top of the page.

On the Welcome screen press the "Begin" button. This will enable the service.

To properly configure user synchronization, you have to:

- Setup the connection to the data source
- Configure the import rules
- Enable alarms (optional)

Configuring the Data Source connection

Click the "Configure Data Source" link and **select the type of external directory** from which you want to import users. These may vary depending on your telephony system. Active Directory is available for all platforms.

Active Directory Connection Configuration

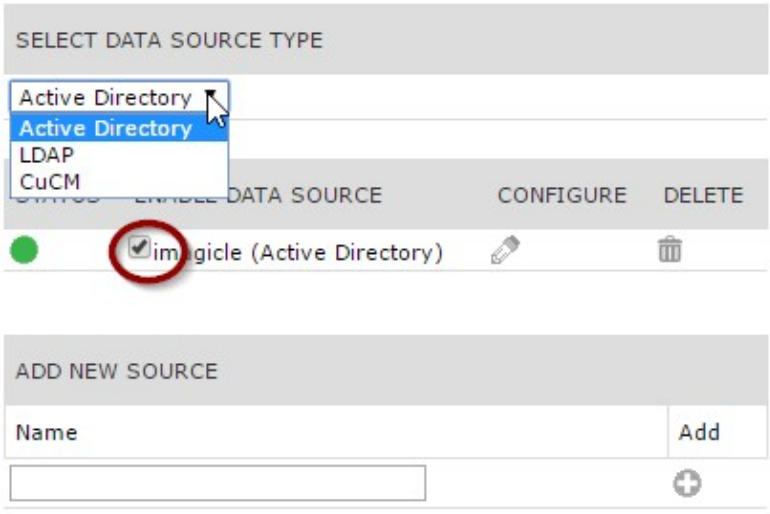
Enter a name for the source, e.g. MyCompanyDC, and press the "Add new source" button. The name must be unique, al least three characters long, and must contain no blanks.

Fill the form fields with these values:

- **Server**: the DNS Name or IP address of the Active Directory server. If you use the DNS name, the Application Suite server must be able to resolve it
- **LDAP object path**: the subtree from which the accounts user will be imported. Basics of LDAP queries can be found on Microsoft web site.
- **Username**: you must enter the credentials of a domain user. This does not need to be an Administrator; any domain user can access the Active Directory
- **Password**: tick the checkbox to the right to show or hide the password characters

Note: If you leave the "LDAP object path" field blank, the "Users" branch will be queried.

Press "Add" and "Back". When the new source has been added, enable it through the checkbox. Once enabled, the service will test the connection parameters.



Active Directory Secure Connection

As of March 2020, Microsoft is updating security requirements for LDAP connections to Active Directory. After this update, Secure LDAP (LDAPS) will become mandatory for all LDAP connections to Active Directory. LDAP connections to Active Directory will not work unless Secure LDAP is configured.

Starting from Spring 2020 release and above, Imagicle follows above Microsoft statement and, for new IAS installations, Secure LDAP using SSL on port 636 is automatically enabled for both authentication and users' synchronization.

If you are upgrading an existing IAS to Spring 2020 or above, the connection is automatically migrated to Secure LDAP and a test is performed to verify AD server reachability. If reachability is granted, then it means Microsoft statement has been respected. If AD can't be reached, then we just leave the connection as it is.

It is also possible to change manually the LDAP authentication settings:

- access to Imagicle server via RDP and edit file C:\Program Files (x86)\StonevoiceAS\Apps\Fw\Settings**FW.Profile.Api.config.xml**
- add a new line, or update the existing one, for the preference Authentication.UseSecureLDAPConnection (see image below)

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  ...
  <preference key="Authentication.UseSecureLDAPConnection" value="SecureThenUnsecure" />
  <!-- OR -->
  <preference key="Authentication.UseSecureLDAPConnection" value="SecureOnly" />
  <!-- OR -->
  <preference key="Authentication.UseSecureLDAPConnection" value="UnSecureOnly" />
```

```
  ...
</configuration>
```

- possible values are:
  - **SecureThenUnsecure**: authentication is tried to be granted using Secure LDAP (LDAPS), if connection failes, authentication is tried again using unsecure LDAP;
  - **SecureOnly**: authentication is tried to be granted using ONLY Secure LDAP (LDAPS);
  - **UnSecureOnly**: authentication is tried to be granted using ONLY unsecure LDAP

Configuring Synchronization Rules

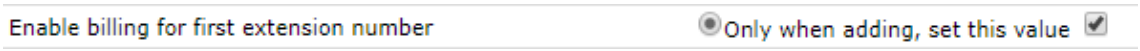
The external directory will not contain all the information needed to fill the Users profile properties. You have to provide the missing values through the web interface.

On the top of this page, select the type of source you want to configure the rules for (Active Directory).

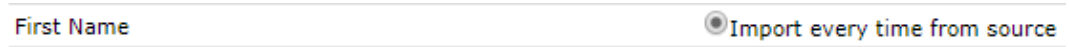
For each field you have the various choices including the following.

- **Only when adding a new user set this value (followed by a textbox)**: this option applies only to **insert** operations. You can specify a default value for the field, which you could modify later from the User Management page, since it will not be overwritten if the user already exists.

- **Only when adding a new user set this value (followed by a checkbox)**: the same as the previous option for boolean fields. Boolean fields can only be set to true (checked) or false (unchecked).



- **Import every time from source**: applies both to insert and update operations. You decided to manage this property from the remote data source, so the value will be synchronized at each cycle.



- **Keep existing value**: the property will not be synchronized. You'll manage the value from the IAS web interface. When the user is created (**insert** operation) the field will be set to blank. During next cycles (**update** operation) the value will remain unchanged.

Other options may involve specifying a prefix to be added to another field value. For instance the First extension number may be imported from the Telephone Number or IP Phone or Skype for Business SIP URI Active Directory fields.

Warning: not all the choices may be available for all the fields. E.g. there is no point in assigning the same default value to a user's personal address.

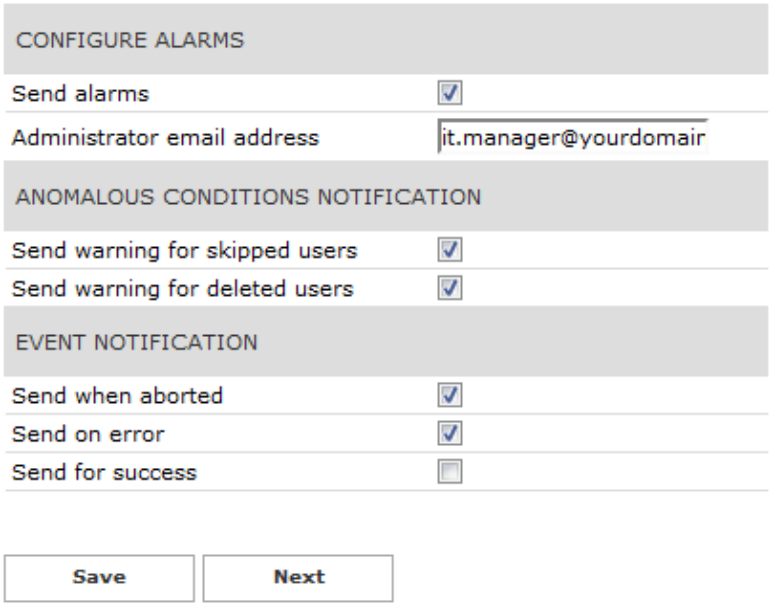
Save the changes

The **Apply** button saves the changes. The **Reload** button undoes the changes. The **Default** button resets to the default values.

Press "Next" or "Back" to continue.

Alarms

The Synchronization service is able to send alarms and warnings should a problem occur during or after synchronization. A brief report is included. The options are pretty self-explanatory. The global SMTP settings are used.



Testing user Synchronization

Once the configuration is complete, you can test it live by pressing the "Run now" button.

Warning: the synchronization process can take a long time if you have a large number of users, depending on the data source type.

To setup the daily schedule, use the "Enable Auto mode" checkbox. Set the hour of the day when you want the service to run, and press save the changes. A countdown will tell you the time left to the beginning of the process.

Reports

Every time the synchronization process is completed, a text report is generated. You can download the report through the web interface. Reports older than 15 days will be automatically removed.

If the synchronization operation is successful, the report contains only statistics. If a user is skipped, details are included so you can edit the user in the data source and try again.

imagicle

```
------------------------------------------------------------
|                          Report                          |
|    Users Data Synchronization with an External Source    |
------------------------------------------------------------

  Start Time: 04/04/2011 17.58.24
  Stop Time: 04/04/2011 17.58.24
  Result: Completed

------------------------------------------------------------
 Statistics:

  Number of Inserted Users: 5
  Number of Updated Users: 30
  Number of Deleted Users: 2
  Number of Skipped Users: 0
  Number of Users in DataBase after sync: 35


------------------------------------------------------------
```

Should an unexpected error be raised, debug information is included in the report. In this case, please send the file to Imagicle Support.

Sync Users with AD

Synchronizing the Users List with Active Directory

Warning: before reading this section, ensure you read and understood general user syncronization concepts and how to synchronize the users list with an external source.

Supported Attributes List

This table list the Active Directory user attributes and shows the UC Suite fields they are mapped to.

- **Active Directory Display Name: label displayed in the Active Directory user interface**
- LDAP Attribute Name: name to be used in LDAP queries, reported for reference but not required to configure IAS
- **UC Suite Field: Label displayed in the adapter's rule configuration UCS web page**
- UC Suite Database name: this is never displayed to the user

General Tab

Active Directory Display Name	LDAP Attribute Name	UC Suite Label	UCSuite Database name	Example Value
First Name	givenName	First Name	user_nome	John
Initials	initials	-	-	JS
Last Name	sn	Last Name	user_cognome	Smith
Display Name	displayName	-	-	"John, Smith"
Description	description	-	-	Sales Manager
Office	physicalDeliveryOfficeName	-	user_office_location	London Office
Telephone Number	telephoneNumber	First Extension Number*	user_telnum, user_amnum	0123 456 789
Telephone Number (Other)	otherTelephone	-	-	0123 4457 89
Email	mail	Email, "Voicemail Address", "Fax to Email Address"	user_mail, user_voicemailaddr, user_pref_fax_mailinaddr	JSmith@domain.com
Web Page	wWWHomePage	-	-	www.johnsmith.com
Web Page (Other)	url	-	-	www.John.net,www.John.org
Password	password	-	-	JohnsPass321
Destination OU	destinationOU	-	-	OU=Sales,DC=Domain,DC=Com
Common Name	CN	-	-	John Smith or %lastname% %firstname%
Modify User if already exists	Modify	-	-	True or False
Delete User	Delete	-	-	True or False

Address Tab

Active	LDAP Attribute Name	UCSuite	UCSuite Database name	Example Value

Directory Display Name		Label		
Street	streetAddress	User address	user_address	10 Downing St;London (Use a semi-colon for carriage return)
PO Box	postOfficeBox	-	-	Po Box 1
City	l *(Lowercase L)*	-	-	London
State/Province	st	-	-	New York
Zip/Postal Code	postalCode	-	-	20013
Country	c	-	-	GB

Account Tab

Active Directory Display Name	LDAP Attribute Name	UCSuite Label	UCSuite Database name	Example Value
User Logon Name	userPrincipalName	Active Directory username, Domain	userPrincipalName, user_ad (without domain), user_domain (without the username), user_authname	JSmith@domain.com
User Logon Name (Pre W2K)	sAMAccountName	PBX username	user_ccmname	JSmith

Telephones Tab

Active Directory Display Name	LDAP Attribute Name	UCSuite Label	UCSuite Database name	Example Value
Home	homePhone	Home phone	user_telcasa	123 123 123
Home (Other)	otherHomePhone	-	-	0123 123 123
Pager	pager	-	-	1234
Pager (Other)	otherPager	-	-	123
Mobile	mobile	Mobile business number	user_mobileBusinessNumber	123 456 789
Mobile (Other)	otherMobile	-	-	123 456 789
Fax	facsimileTelephoneNumber	Fax number	user_faxNumber	123 456 789
Fax (Other)	otherFacsimile TelephoneNumber	-	-	0123 456 789
IP Phone	ipPhone	First Extension Number*	user_telnum, user_amnum	750
IP Phone (Other)	otherIpPhone	-	-	330750
Notes	info	-	-	General information (Use a semi-colon for carriage return)

Organization Tab

Active Directory Display Name	LDAP Attribute Name	UCSuite Label	UCSuite Database name	Example Value
Title	title	-	-	Manager
Department	department	Department	user_department	Sales
Company	company	-	-	Big Corp

Manager	manager	-	-	CN=Ste Jobs,OU=Managers,DC=Domain,DC=Com
Employee ID	employeeID	-	-	
Employee Type	employeeType	-	-	
Employee Number	employeeNumber	-	-	
Car License	carLicense	-	-	
Division	division	-	-	
Middle Name	middleName	-	-	
Room Number	roomNumber	-	-	
Assistant	assistant	-	-	CN=Joe Blog,OU=Managers,DC=Domain,DC=Com
User's Picture**	jpegPhoto / thumbnailPhoto	-	Pictures are saved in SQL DB	JPEG pictures supported. Max 200KB size

* Either telephoneNumber or ipPhone attributes can be imported based on synch rules configuration

** Feature supported from Imagicle 2020.Winter.1 release. Either jpegPhoto or thumbnailPhoto attributes can be imported, based on synch rules configuration

Extension Number Alias Synchronization

This field is by default left empty, If required, you can synch this user's field from the following AD attributes:

- otherTelephone
- otherIpPhone
- telephoneNumber
- ipPhone

Site Name synchronization

Starting from Imagicle UC Suite Summer 2021, we can import Site Name from Active Directory or LDAP, to enable overlapping dial plan across multiple gateways or PBXs.

Depending on the users repository source, the Site Name can be synchronized from one of the following attributes (selectable in the synch rules page):

- Active Directory:
  - department (default)
  - physicalDeliveryOfficeName
  - company
- LDAP:
  - departmentNumber (default)
  - o
  - ou
  - l

Users' pictures synchronization

Starting from Imagicle UC Suite Winter 2020, users' pictures can be synchronized with Active Directory LDAP, to enable two UC Suite features:

- Viewing the user photo in the 'Colleagues' tab of the Imagicle Attendant Console.
- Providing a users' picture repository for Cisco Jabber clients. Please see here.

Depending on the users repository source, the picture can be synchronized from one of the following attributes (selectable in the synch rules page):

- Active Directory:
  - jpegPhoto
  - thumbnailPhoto
- LDAP:
  - jpegPhoto

The default maximum picture size is **200 KB**, bigger pictures will be discarded. If you need to adjust such size threshold, please contact Imagicle Support.

Pictures are saved in the Imagicle database.

imagicle

Syncing Users' Privileges from Imagicle LDAP Module, generic LDAP Server or AD

Description:

This article explains how to synchronize Imagicle permissions with Imagicle LDAP server, generic LDAP or Active Directory privileges.

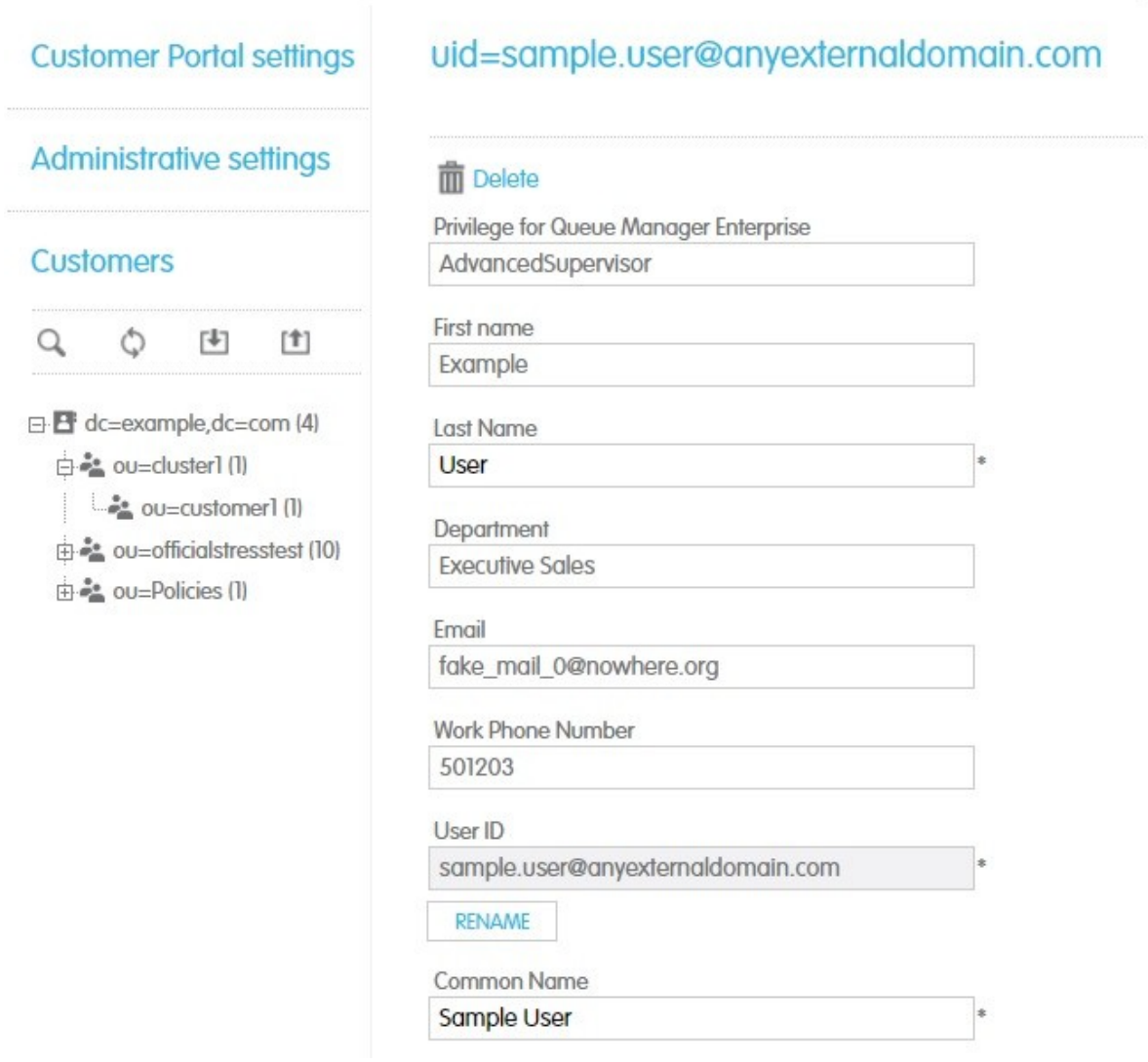
Source configuration

Imagicle LDAP Server

Before starting the synchronization the following steps should be performed on the Imagicle LDAP server:

1. After logging in to the server, go to "Administrative settings" tab and then expand "User fields configuration".
2. Locate the applications privileges under column "Available fields". Note that they start with the prefix "priv":

3. Click or drag the required privilege (privQme for instance), to make it appear as a user attribute. After all the desired privileges are added, click on "Save".
4. Now any existing, newly created or imported user into the Imagicle application suite will have the privileges added in the previous step as additional attributes. Check in the below screenshot the newly added QME privilege (its default value is empty):



The value "Advanced Supervisor" configures relevant use as queue's "Advanced supervisor" on Advanced Queuing application.

The table below lists all available permissions, with configurable privileges for each Imagicle applications:

Att Name	**Description**	**Priv name**
privMai	Users management default users' permission	Default
privMai	No access to users management	BasicUser
privMai	Access to department users list	DepartmentUsersSupervisor
privMai	Access to department users management	DepartmentUsersManager
privMai	Complete users management	CompleteUsersManagement
privMai	System admin	Administrator
Att Name	**Description**	**Priv name**
privBib	Call Analytics default users' permission	Default
privBib	No access to Call Analytics data	NoAccess
privBib	Call Analytics access to own data only	BasicUser

privBib	Call Analytics access to whole own dept. data	DepartmentSupervisor
privBib	Call Analytics access to whole own Cost Center data	CostCenterSupervisor
privBib	Call Analytics access to whole own Office Location data	OfficeLocationSupervisor
privBib	Call Analytics access to whole Call Accounting data	GlobalSupervisor
privBib	Call Analytics Administrator	Administrator
Att Name	**Description**	**Priv name**
privBdg	Budget Control default users' permission	Default
privBdg	No access to Budget Control data	NoAccess
privBdg	Budget Control access to own budget data	BasicUser
privBdg	Budget Control access to whole own dept. budgets	DepartmentManager
privBdg	Budget Control access to whole own Cost Center budgets	CostCenterManager
privBdg	Budget Control Administrator	Administrator
Att Name	**Description**	**Priv name**
privSlo	Phone Lock default users' permission	Default
privSlo	No access to Phone Lock line	NoAccess
privSlo	Phone Lock access to own phone line	BasicUser
privSlo	Phone Lock access to all phone lines associated to own dept.	DepartmentManager
privSlo	Phone Lock Administrator	Administrator
Att Name	**Description**	**Priv name**
privSfx	Digital Fax default users' permission	Default
privSfx	No access to Digital Fax documents	NoAccess
privSfx	Digital Fax access to own fax documents	BasicUser
privSfx	Digital Fax access to all fax documents associated to own dept.	DepartmentManager
privSfx	Digital Fax Administrator	Administrator
Att Name	**Description**	**Description**
privSpd	Contact Manager default users' permission	Default
privSpd	No access to Contact Manager directories	NoAccess
privSpd	Contact Manager access to own directories	BasicUser
privSpd	Contact Manager access to all directories associated to own dept.	DepartmentManager
privSpd	Contact Manager access to all directories	DirectoryManager
privSpd	Contact Manager Administrator	Administrator
Att Name	**Description**	**Priv name**
privIvr	Auto Attendant default users' permission	Default
privIvr	No access to Auto Attendant services	NoAccess
privIvr	Access to Auto Attendant services, only if assigned as AutoAtt Manager	BasicUser
privIvr	Auto Attendant Administrator	Administrator
Att Name	**Description**	**Priv name**
privQme	Advanced Queuing default users' permission	Default
privQme	No access to Advanced Queuing queues	NoAccess
privQme	Access to Advanced Queuing queues, only if assigned as queue Supervisor or Advanced supervisor	BasicUser
privQme	Access to Advanced Queuing queues as Supervisor	Supervisor
privQme	Access to Advanced Queuing queues as Advanced Supervisor	AdvancedSupervisor
privQme	Advanced Queuing Administrator	Administrator
Att Name	**Description**	**Priv name**
privIvy	IVR Manager default users' access	Default
privIvy	No access to IVR Manager scripts	NoAccess

privIvy	IVR Manager Administrator	Administrator
Att Name	**Description**	**Priv name**
privRec	Call Recording default users' permission	Default
privRec	No access to Call Recording data	NoAccess
privRec	Call Recording access to own data only	BasicUser
privRec	Call Analytics access to whole own recording group data	GroupSupervisor
privRec	Call Recording Administrator	Administrator
Att Name	**Description**	**Priv name**
privHtl	Hotel Services default users' access	Default
privHtl	No access to Hotel Services panel and configurations	NoAccess
privHtl	Hotel Services Administrator	Administrator

Generic LDAP server or Active Directory

In case you are not having an Imagicle LDAP Server you can leverage an existing LDAP server or Active Directory server, in this case you need to create custom attributes with the names and the values described above.

It is also possible to use other attributes for the privileges mapping. Please contact Imagicle support for more details.

Privileges Sync

Note: it's not needed to configure/create all the attributes, it's possible to create only the needed one

The following steps describe how to set the Synchronization to import privileges between Imagicle UC Suite and the external server.

In the Imagicle UC Suite interface, assuming that there an LDAP data source already configured:

- Browse to 

-->User Management-->Synchronize users with an external data source-->Configure Sync Rules.
- Change ADAPTER'S RULE TYPE to "LDAP" or "ACTIVE DIRECTORY
- Scroll down to "User permissions" and choose "Import every time from source".
- Click on Save
- Click on "Back" and then click on "Run Now" to start the users synchronization with their privileges. If users are already synced, then this step just synchronizes their privileges and update their permissions accordingly.