

ISO 27001

The international standard ISO 27001 allows the assurance, confidentiality, and integrity of data and information and the systems that process it. This allows organizations to analyze risk and apply the necessary controls to eliminate it.

If we go to the system configuration, we find the following options that will help us establish a more secure system for our users.

Within the company message option, you can set a warning message from the company, which will appear every time the agent logs in. The system will also display the date and time of the user's last logged-in session.

IMAGEN

Among the security measures it establishes are:

Password expires after a certain number of days. (Modifiable)

- Request mandatory password change after it is updated by the supervisor or for the first time the user logs in.

Account lockout after certain unsuccessful password entry attempts. (Modifiable)

At the time of changing the password, do not allow to use of the last X amount of passwords used. (Modifiable)

The system has three different states for users:

- Asset.
- Inactive.
- Blocked (due to failed login attempts).

The user is disabled if they do not log in to uContact after a certain number of days. (Modifiable)

Password Format sets the complexity that agent passwords should have. Here you can configure if you should have:

- lower case

- Capital letters
 - Numbers
 - Special characters
 - and the minimum length of characters
-

If we go to the creation of agents, we can find the following fields available:

LOGIN SCHEDULE

The possibility of creating a login schedule establishes certain days of the week and hours in which the agent can connect to the system.

TEMPORARY ACCOUNT

There is also the opportunity to create temporary users, that is, an account is created that has a forced expiration on the date established in the fields.

Revision #3

Created 24 January 2023 17:47:15 by Alejandra Vega

Updated 11 June 2023 23:46:23 by Mauricio Coronel