

Security

Authentication and authorisation

CONTACT™ users and user rights assignment

By default users are managed within the CONTACT™ user interface. There are four user levels:

User Level	Rights
General	<ul style="list-style-type: none"> ▪ Message console, basic message handling ▪ Optional editing of customer data ▪ Basic access to operations console ▪ Optional access to manual router ▪ Optional access to broadcast messaging
Team leader	<ul style="list-style-type: none"> ▪ All rights of general user, plus ▪ Ability to view team's performance within operations console
Administrator	<ul style="list-style-type: none"> ▪ All rights of team leader, plus ▪ Full access to operations console for all teams ▪ Administrative access for configuring users, teams, templates, auto responses, etc.
Super user	<ul style="list-style-type: none"> ▪ All rights of administrator, plus ▪ Ability to configure message pipeline ▪ Ability to configure custom fields.

Figure 1: Security levels

Active directory integration

For self-hosted applications CONTACT can be configured to integrate directly with a site's active directory for user authentication and rights assignment. This allows for a single sign-on to the agent desktop.

SSL

CONTACT supports SSL out of the box, and application instances can be deployed using HTTPS only.

SMS and email security

SMS and internet email are both non-encrypted formats. Sensitive information such as credit card numbers or social security numbers should not be transmitted using these media.

Logging and auditing

All user access to the CONTACT application is logged and audited within the CONTACT database and to external log files on the CONTACT servers. Changes to customer data can be optionally audited by enabling a system configuration setting.