

ContactWise Security Information

The purpose of this document is to give a high level explanation of the various security options available to an administrator of ContactWise.

Section 1.0 – General Overview

The philosophy of ContactWise security is that all users begin with no rights. All of the security options that can be configured with the Database Administrator are intended to give additional rights to access and/or features in ContactWise. Security rights are cumulative, meaning that a user's rights are determined by combining all effective rights.

ContactWise currently allows administration in the following areas / features of ContactWise:

- General Features
- Contact Access
- Groups
- Properties

Section 1.1 – General Features

The General Features section is where access to the following ContactWise features can be administered:

- Document Merge Utility
- Printing
- Remote Sync

Section 1.1.1 – Document Merge Utility

Giving access to document merge utility allows the affected users to be able to launch the document merge utility which in turn provides access to the following features:

- Add new documents to the local document repository
- Remove documents from the local document repository
- Perform a document merge against a single contact, group, or filter

Section 1.1.2 – Printing

The Printing option refers exclusively to the Report Builder feature which is available from the Print menu on the main screen of ContactWise, an individual contact record, a group, or a filter. Once a user has rights to use the Report Builder feature, they have full access to all Report Builder features which include:

- Running reports
- Creating new reports / folders
- Removing existing reports / folders

Section 1.1.3 – Remote Sync

The Remote Sync option gives the affected users rights to use the Go Remote feature¹. Once a user has gone remote with a selection of contacts, from a group, they have full rights to those contacts regardless of what rights they have been given to those contacts from the master database.

Section 1.2 – Contact Access

Contact Access refers to rights involving access to contacts in the database. This is the option which is used to give certain users certain rights to certain contacts. There are four main contact access options:

- Read
- Write
- Delete
- Modify

Section 1.2.1 – Read

The read right give affected users access to see that the affected contacts are present in the database. This means that if a particular user has rights to read a group of contacts, for example, that that group of contacts will be displayed in the main screen of ContactWise and additional contact listings.

Section 1.2.2 – Write

The write right gives affected users access to create new contacts. This is an important right as users will not be able to create new contacts in ContactWise without it.

¹ Each user wishing to make use of the Go Remote feature must have their local PC configured properly, generally with the assistance of their local network administrator.

Section 1.2.3 – Delete

The delete right gives affected users access to delete existing contacts from ContactWise. Make sure you only give this to users to genuinely need it.

Section 1.2.4 – Modify

The modify right gives affected users access to modify all the information belonging to the affected contacts with the exception of Property fields which are administered separately. Therefore, this right gives affected users the ability to add, delete, and modify phone, address, history, event, comment, group membership, and name information.

Section 1.3 – Groups

The Groups section allows for security administration of public groups in ContactWise. It is important to understand that rights given to groups do NOT affect the members of those groups. Those rights are given through Contact Access. Additionally, private groups are not affected by any of the rights administered through these security rights. All users have full control of their private groups.

Section 1.3.1 – Read

The read right gives affected users the right to see that the affected groups exist in the database. If a user has the right to read a group, that group will appear in all the normal places a group might be listed: Groups, Filters, and Contact Group Tab, etc...

Section 1.3.2 – Write

The write right gives affected users to the right to create new public groups. Without this access right a user will not be able to create new public groups.

Section 1.3.3 – Delete

The delete right gives affected users the right to delete the affected groups.

Section 1.3.4 – Modify

The modify right gives affected users the right to change the name of the affected groups.

Section 1.4 – Properties

The Properties section allows for security administration of property fields in ContactWise. Rights given to affected property fields throughout ContactWise, with the exceptions of Go Remote and Printing as access to those features, are administered separately.

Section 1.4.1 – Read

The read right gives affected users the ability to see that a given property field exists. Without rights to see a given property field, that property field should not appear in any area of ContactWise with the exceptions of the Go Remote and Printing features.

Section 1.4.2 -- Modify

The modify right gives affected users the ability to provide values for the affected property fields for all contacts. This means that if a user has the right to modify a property field, they have the ability to provide a value for that property field for any contact in the database that they can see in the database (see section 1.2.1 for more information about contact visibility).

Section 2.0 – Default Rights

Default rights are the first option in administering security through ContactWise. It is the most generic option available as it will affect all ContactWise users. It also gives you the least amount of flexibility for the same reason. It is available from the far left of the Security tab in the Database Administrator. To change rights simply double click on the desired section and make your selections. Keep in mind that these rights affect all users regardless of what other options have been configured with other security options. Use this section sparingly and only when you are absolutely sure that all users need that particular right or feature access.

Section 3.0 – Assigned Rights

Assigned rights can be assigned to either an LDAP user or an LDAP group. If rights are assigned to an LDAP user, those rights only affect that particular LDAP user. If rights are assigned to an LDAP group, those rights affect all the members of that LDAP group.

Assigned rights can be administered from the Assigned Rights section of the Security tab in the Database Administrator. An LDAP group or user must be selected from the Directory section before rights can be assigned.

Section 3.1 – Assigned Rights: General Features

Assigning rights to general features give the affected users rights to the selected features. See section 1.1 for more information about the General Features rights section.

Section 3.2 – Assigned Rights: Contact Visibility / Access

The contact visibility / access section of assigned rights can be used to give affected users rights to contact visibility / access in three different ways:

- All Contacts
- Individual
- Group

Section 3.2.1 – Contact Visibility / Access: All Contacts

The All Contacts option provides the ability to give the affected users any combination of contact visibility / access rights (read, write, delete, and modify) for all contacts in the database. Section 1.2 has more information regarding the four access rights. It is important to note any given LDAP Group or User can only have ONE All Contacts set of rights. However, it is possible for an LDAP user to inherit the All Contacts set of rights from an LDAP group which it is a member of and have its own All Contacts set of rights. In that situation, the LDAP user's effective rights are determined by combining both sets of All Contacts rights.

Practical Example:

A common use of this option is to give an LDAP group or user the write option in an All Contacts assigned right, which gives the affected users the ability to create new contacts. The benefit of using this method over giving equivalent rights through the Default Rights is that you don't have to give all users contact creation rights; instead you are able to give a select set of LDAP users contact creation access.

Important Note:

The write option is only available from the All Contacts option.

Section 3.2.2 – Contact Visibility / Access: Individual

The individual option provides the ability to give the affected users any combination of contact visibility / access rights (read, delete, and modify) to an individual contact. This option is not commonly used as it only gives a certain set of users rights to a single contact in ContactWise, which is not very common.

Section 3.2.2 – Contact Visibility / Access: Group

The group option provides the ability to give the affected users any combination of contact visibility / access rights (read, write, delete, and modify) to a group of contacts in ContactWise.

Practical Example:

This option is commonly used in conjunction with the Practical Example given in Section 3.2.1. Assigning an LDAP group or user a combination of contact visibility / access rights to all the contacts that are in a particular group gives an administrator the ability to give all users the rights to create new contacts but only be able to read and/or delete and/or modify the contact in a particular group of contacts.

Section 3.3 – Assigned Rights: Groups

The groups section of assigned rights can be used to give affected users rights to public groups in ContactWise in two different ways:

- All Groups
- Individual Group

Section 3.3.1 – Groups: All Groups

The All Groups option provides the ability to give the affected users any combination of group access rights (read, write, delete, and modify) for all public groups in the database. Section 1.3 has more information regarding the four access rights. It is important to note any given LDAP Group or User can only have ONE All Groups set of rights. However, it is possible for an LDAP user to inherit the All Groups set of rights from an LDAP group which it is a member of and have its own All Groups set of rights. In that situation, the LDAP user's effective rights are determined by combining both sets of All Groups rights.

Important Note:

The write option is only available from the All Groups option.

Section 3.3.2 – Groups: Individual Group

The individual group option provides the ability to give the affected users any combination of group access rights (read, delete, and modify) to an individual group.

Section 3.4 – Assigned Rights: Properties

The properties section of assigned rights can be used to give affected users rights to property fields in ContactWise in two different ways:

- All Properties
- Individual Property

Section 3.4.1 – Properties: All Properties

The All Properties option provides the ability to give the affected users any combination of property access rights (read and modify) for all property fields in the database. Section 1.4 has more information regarding the two access rights. It is important to note any given LDAP Group or User can only have ONE All Properties set of rights. However, it is possible for an LDAP user to inherit the All Properties set of rights from an LDAP group which it is a member of and have its own All Properties set of rights. In that situation, the LDAP user's effective rights are determined by combining both sets of All Properties rights.

Important Note:

The write option is only available from the All Properties option.

Section 3.4.2 – Properties: Individual Property

The individual property option provides the ability to give the affected users any combination of property access rights (read and modify) to an individual property.

Section 3.5 – Full Access

The full access option gives the affected users full rights to all four categories of access rights. This feature is intended to be used by administrators that need to give special users full rights.