Akeni Enterprise Server
Administration Guide

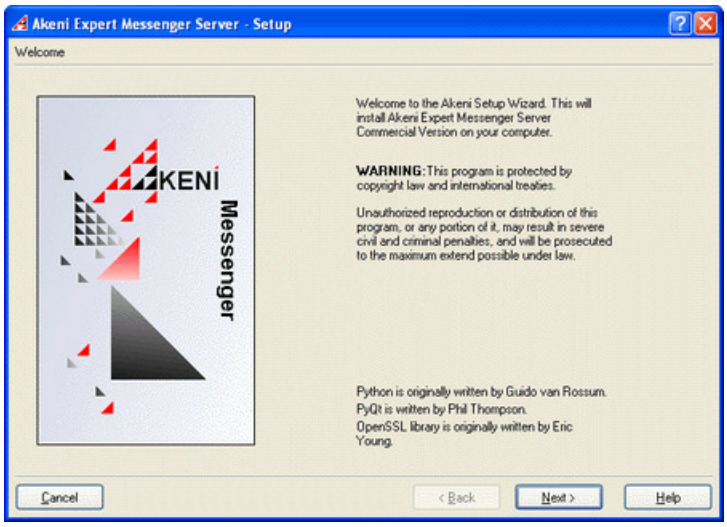
(Version 1.2)

Contents

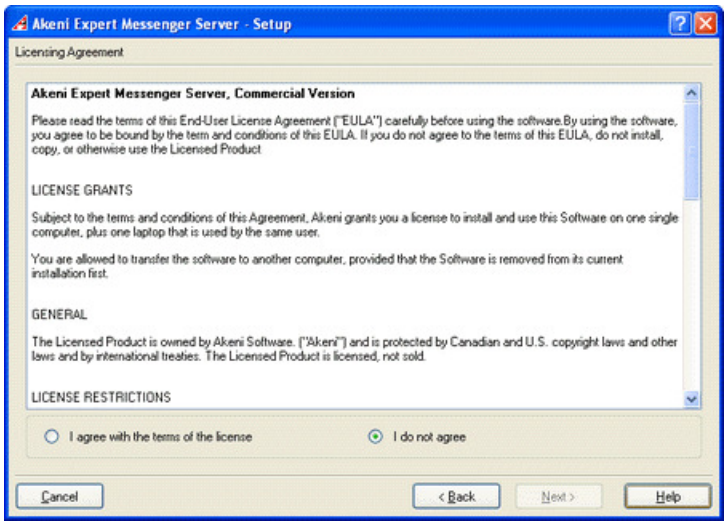
Chapter 1: Getting Started

1.1 Enterprise Server Installation

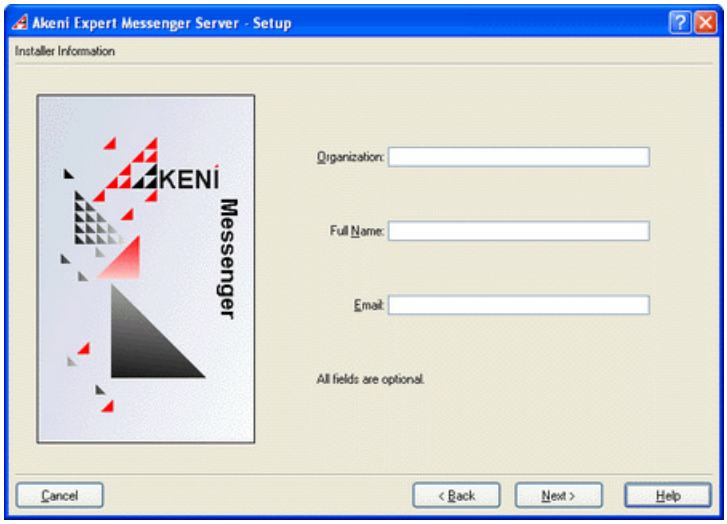
1. Select the Akeni Enterprise Server installation file that matches your operating system and double-click on the file.
2. If you are installing the commercial version of the software, or you have received an extended evaluation license key, please make sure that you have placed the license key file in the **same directory** as the installer.
3. A welcome window will appear with information pertaining to the Akeni product, press the "Next" button to proceed.



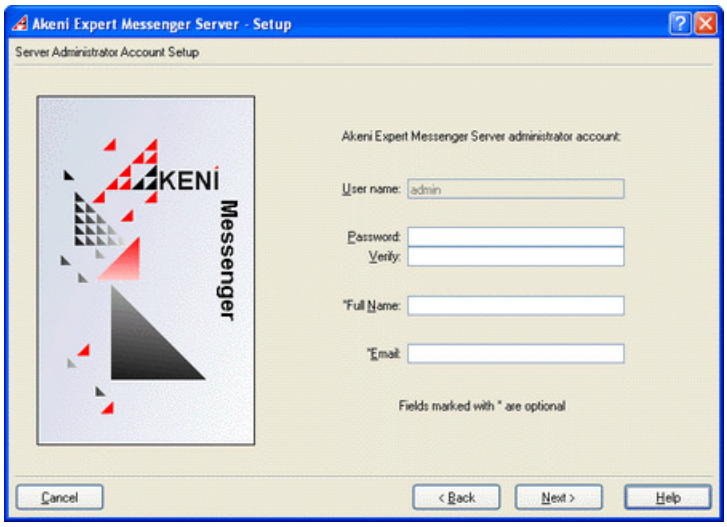
4. The license agreement will now appear. If you accept the license agreement, select "I agree with the terms of the license" and press the "Next" button to continue. Otherwise, press the "Cancel" button to exit the installation.



5. The installer information window will now appear. Enter the applicable information and press the "Next" button to continue.

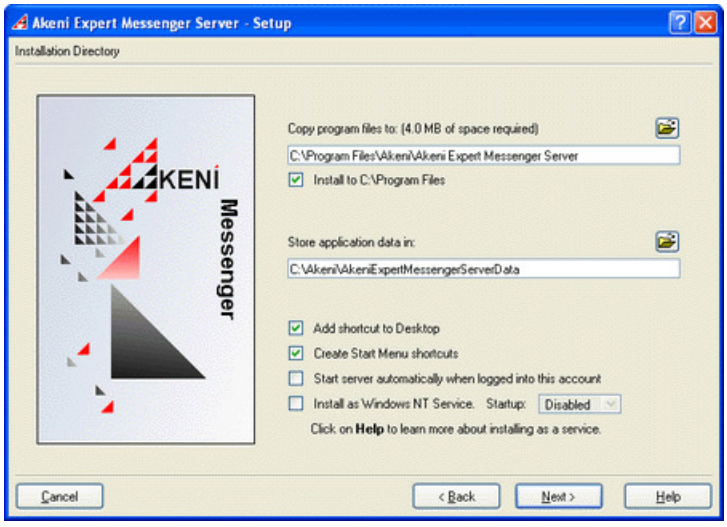


6. Enter the password for system administrator account "admin" and enter the password again to verify the password. You will have re-install the program if you lost your password (but your data will still be intact)

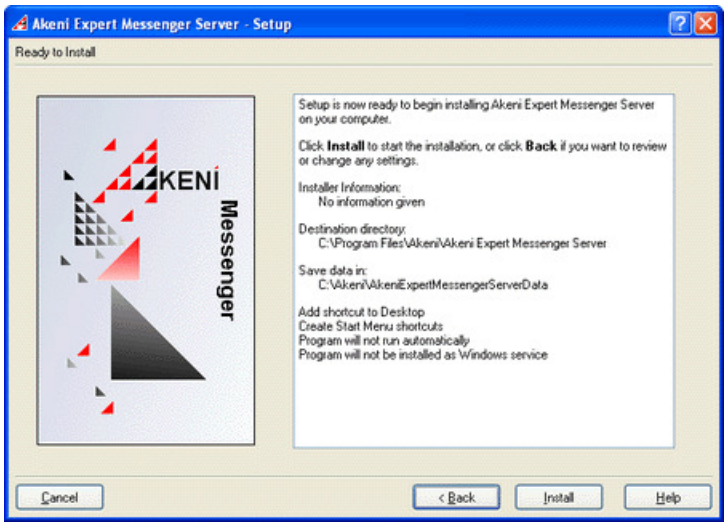


7. Select the location where you wish Akeni to be installed and where the application data should be stored. Other options include:
    - Add shortcut to Desktop – This will add a shortcut icon to your desktop.
    - Create Start Menu shortcuts – This will add Akeni to your Start menu list.
    - Start server automatically when logged into this account – This will automatically launch Akeni when you login to your system.
    - Install as Windows NT Service – This option is available on Windows NT/2000/XP, and it will allow the server to run in the background when the machine is booted, without having to log into the system. You can only install as a Service when you are logged in as the system administrator.

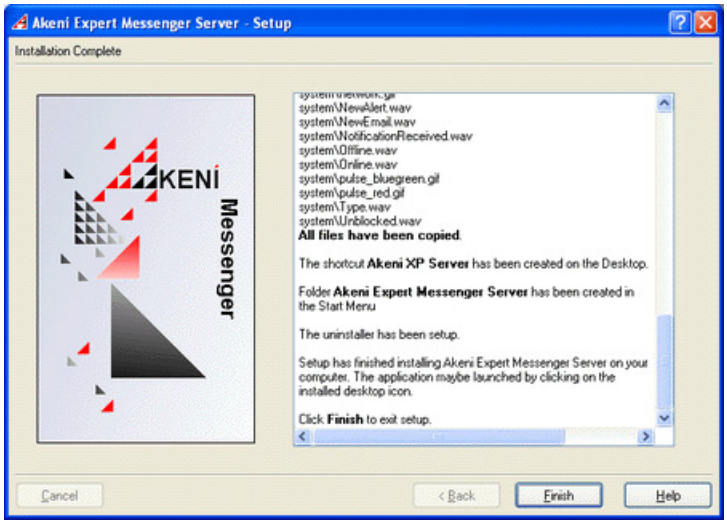
   Press the "Next" button to proceed.



8. You're now ready to install. The preview window will list the options that you have selected. If you wish to make changes, press the "Back" button. Otherwise, press the "Install" button to proceed.



9. Akeni Enterprise Server has now been installed. To complete the process, press the "Finish" button.



10. The AD (Active Directory) / LDAP Wizard will now be launched automatically (Please make sure that you do not click on the Enterprise Server desktop icon and launch the server before you have finished running this wizard.)

    For security reason, it is best to run the server with LDAP encryption set to LDAPS (LDAP over SSL) or StartSSL. If for some reason you can not get SSL to work then it is best to run the server on the same computer as your AD / LDAP server so that the password is not transmitted in the clear over the network.

    The hostname should be the FQDN (Fully Qualified Domain Name) of your AD/LDAP server. This must be the same as the FQDN on your LDAP/AD server's SSL certificate or the SSL server certificate verification will fail. If you are not using any encryption then it is OK to set it to the numeric IP address as well. If you are running the server on the same computer as your AD/LDAP without encryption then you can also set it to "localhost".

    If you are running on Microsoft Windows and you want to run the LDAP session over SSL then you must install the public key of the SSL certificate of your AD on the machine that is running the Enterprise Messaging server. The easiest way to do this is to point your Internet Explorer Web Browser to your AD server and then use it to import the certificate. For example, suppose your AD server is at ldap.yourcompany.com, then you should type "https://ldap.yourcompany.com:636" (note that it is "http**s**" not "http") into the address bar of your browser and then tell the browser to accept the certificate offered by the server.

    In order to make sure that the host information you just entered is correct, you need to enter the DN (Distinguishing Name) of an user on your AD/LDAP that you know the password of.

    If you are using MS Active Directory, you can add the **ADSI snap-in** to the management console (MMC) to help you get the DN of the users. You can find the snap-in in the support folder of your Windows 2000/2003 server installer CD.

    The procedure is discussed in an article at
    http://www.microsoft.com/resources/documentation/Windows/2000/server/reskit/en-us/Default.asp?url=/resources/do

    There is also more information at

http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/8c76ff67-9e9d-4fc7-bfac-ffedee

You may also want to download a free LDAP browser from http://www.ldapbrowser.com to help you figure out the structure of you LDAP / AD server. Note that you can install the browser on any Windows 2000/XP machine that can connect to your LDAP server via TCP/IP.

When using Active Directory, the DN for someone whose user name is **mark** is probably **CN=mark,CN=Users,DC=yourdomain,DC=com** or **CN=mark,OU=Office Users,DC=yourdomain,DC=com**.

Once you have entered the correct LDAP/AD host parameter you can now go to the next page, where you need to enter the following information:

- The DN and the password of the account that will be used to lookup contact information (such as the name, phone number, email address, etc.) for each user. It is recommended that you create a special account with read only access to this information just for this purpose. Please also note that the password for this account **will stored in the clear**, so make sure that the ldap.conf file is readable only by the account used to run this server
- The search base (container) for all the user objects. This is the DN from which the search should begin. For Active Directory, this would be the container where all your users resides. If your LDAP database is very large, then you will get better performance if the search is done using a base DN that has more depth. You can also try to set the search scope to **One Level** if all the users are only one level deep from the base DN.
- The search filter is useful when you have different LDAP object mixed together with your user object. The filter will limit the search so that only user object will be returned. A good filter is to use is "**(&(objectclass=organizationalPerson)(CN=%s))**
- The user name of the account that will map to the "admin" account used by Enterprise Messenger. For example, suppose Alice Smith with LDAP password "secret" has been assigned as the administrator of Enterprise Messenger System. Then you should enter "Alice Smith" in there, assuming that Alice's DN is **CN=Alice Smith, OU=users,DC=akeni,DC=com** (assuming that you have already set the search base to OU=users,DC=akeni,DC=com)

The third step in the LDAP wizard is to setup the mapping of the field from your LDAP / AD to the fields used by Enterprise Messenger. All the field names are optional and you can leave them blank.

The last step in the LDAP Wizard is to create the accounts from the values that the system can find from your LDAP/AD using the parameters you have entered in step 2. You can delete users that you do not wish to have access to the messaging system by deleting their names from the list. You can use the control and shift key to select multiple entries. If you deleted a user by mistake then simply reload the page again.

The user name used by the message system needs to be lower case alphanumeric plus the special characters [. + - _ - @], but can not include any spaces. This means that in order to bind to the LDAP / AD you need to change a mixed case user name to all lower case and replace the space with '+'. For example "Alice Smith" will have the user name "alice+smith".

Please note that by default, any user who have a valid account on your LDAP / AD will have access to Enterprise Messenger because the account is created automatically when the user's account information have been authenticated against the LDAP/AD. If you do not want this behavior then you need to go to the Enterprise Messenger Server Console, choose (Files | Configuration) and disable the option **Allow anyone with a valid LDAP account to sign-on**.

1.2 Launching Akeni Enterprise Server

1. Depending on the options you selected during installation, you can start Akeni Enterprise Server in the following methods:

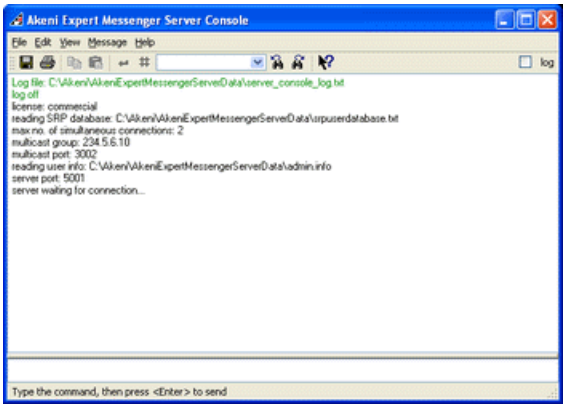
   - Double click on the “Akeni Enterprise Server” icon on your desktop.

   OR

   - Press the “Start” button on your system tray.
   - Select “Programs -> Akeni Enterprise Messenger Server -> Akeni Enterprise Server”.

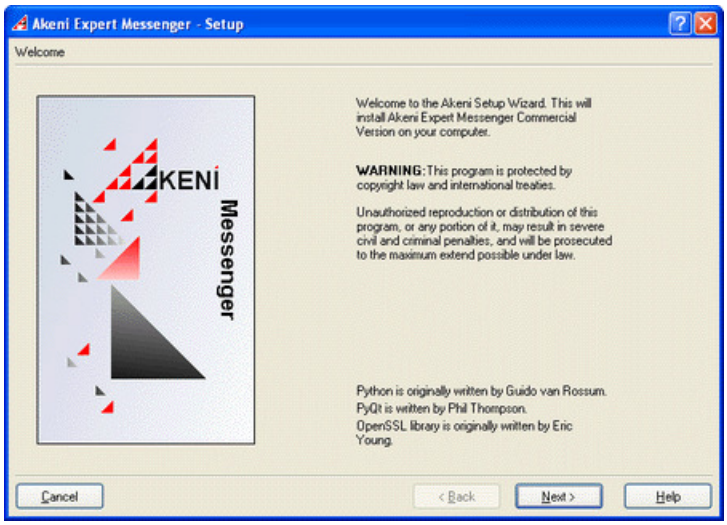
   OR

   - Press the “Start” button on your system tray.
   - Select “Programs -> Akeni Enterprise Messenger Server -> Start Service”.
   - (You will see this option only if you installed the server as a Windows NT Service.)

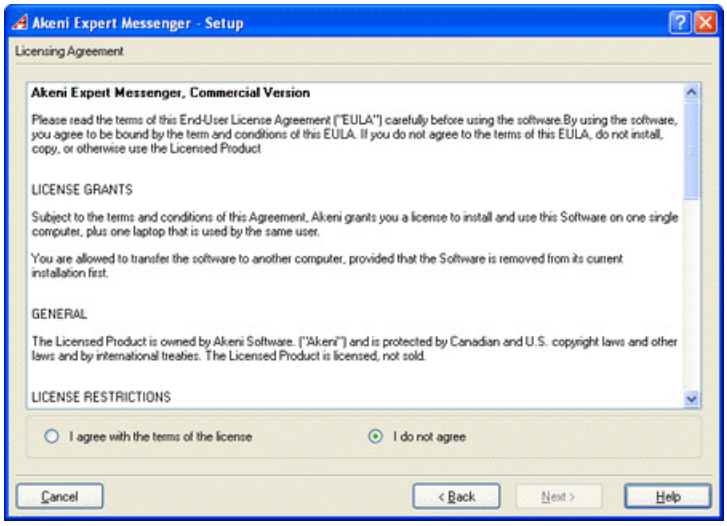


1.3 Enterprise Client Installation

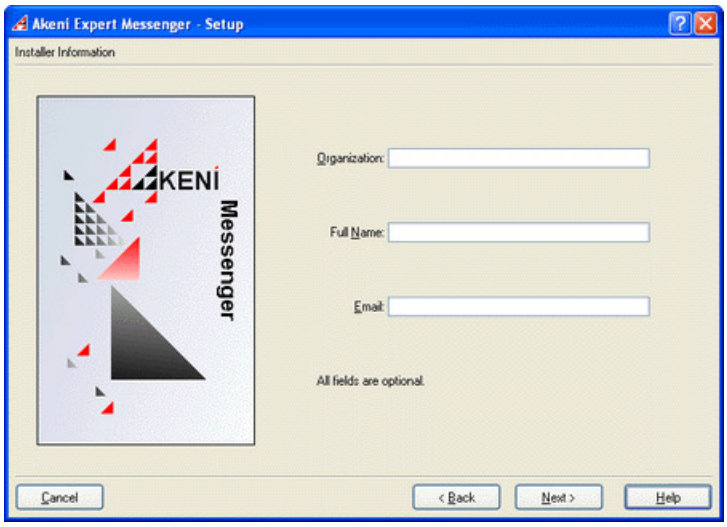
1. Select the Akeni Enterprise Client installation file that matches your operating system and double-click on the file.
2. If you are installing the commercial version of the software, or you have received an extended evaluation license key, please make sure that you have placed the license key file in the **same directory** as the installer.
3. A welcome window will appear with information pertaining to the Akeni product, press the "Next" button to proceed.



4. The license agreement will now appear. If you accept the license agreement, select "I agree with the terms of the license" and press the "Next" button to continue. Otherwise, press the "Cancel" button to exit the installation.

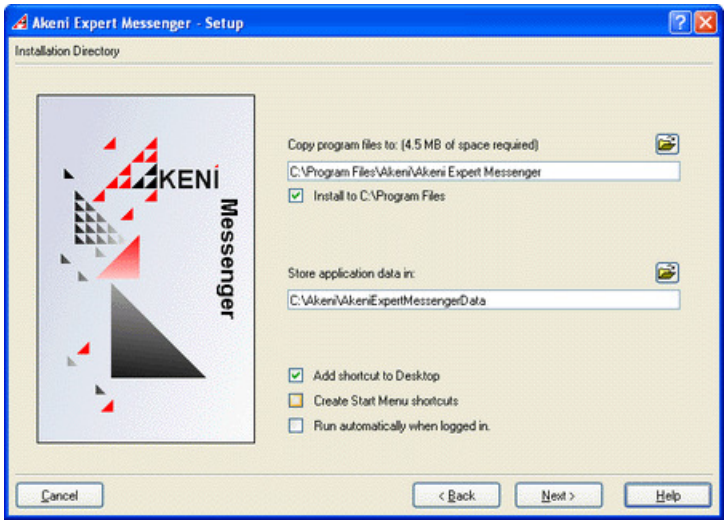


5. The installer information window will now appear. Enter the applicable information and press the "Next" button to continue.

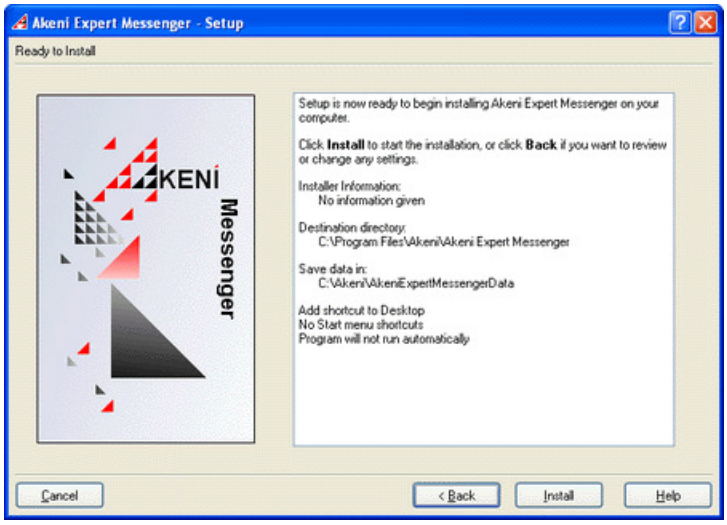


6. Select the location where you wish Akeni to be installed and where the application data should be stored. Other options include:
    - Add shortcut to Desktop – This will add a shortcut icon to your desktop.
    - Create Start Menu shortcuts – This will add Akeni to your Start menu list.
    - Run this program when Windows starts – This will automatically launch Akeni when you login to your system.

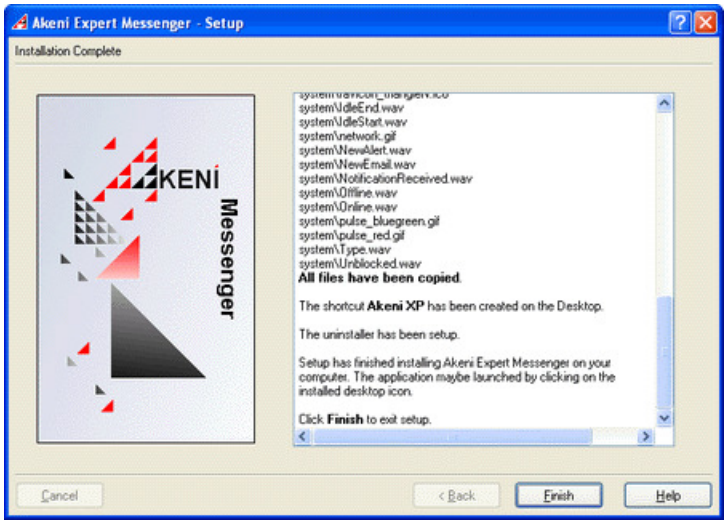
   Press the "Next" button to proceed.



7. You're now ready to install. The preview window will list the options that you have selected. If you wish to make changes, press the "Back" button. Otherwise, press the "Install" button to proceed.



8. Akeni Enterprise Client has now been installed. To complete the process, press the “Finish” button.



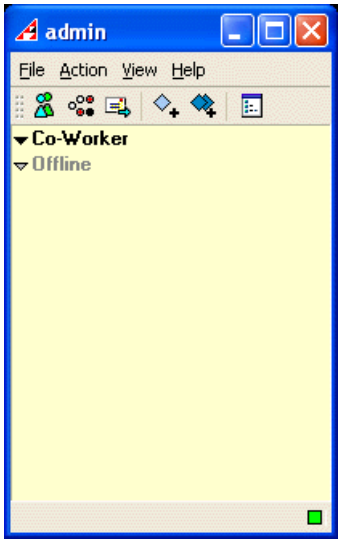
1.4 Launching Akeni Enterprise Client

1. Depending on the options you selected during installation, you can start Akeni Enterprise Client in the following methods:
    - Double click on the “Akeni Enterprise” icon on your desktop.

    OR

    - Press the “Start” button on your system tray.
    - Select “Programs -> Akeni Enterprise Messenger -> Akeni Enterprise”.

2. Enter the "admin" account password to login to server as the Akeni Enterprise Server administrator:

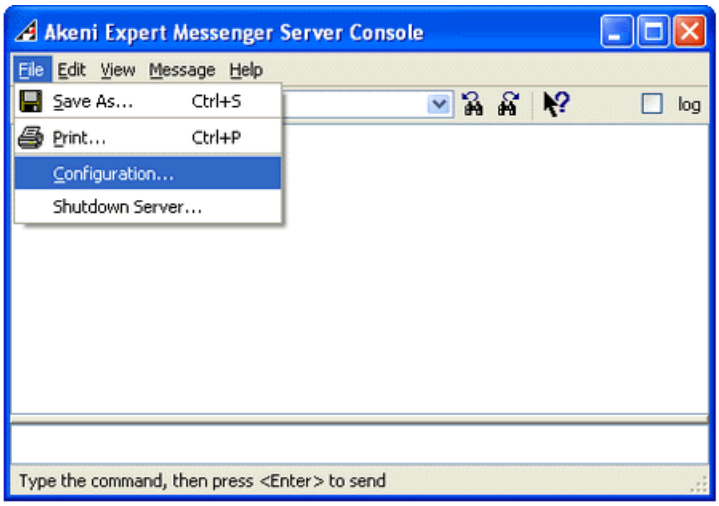


Chapter 2: Server Administration

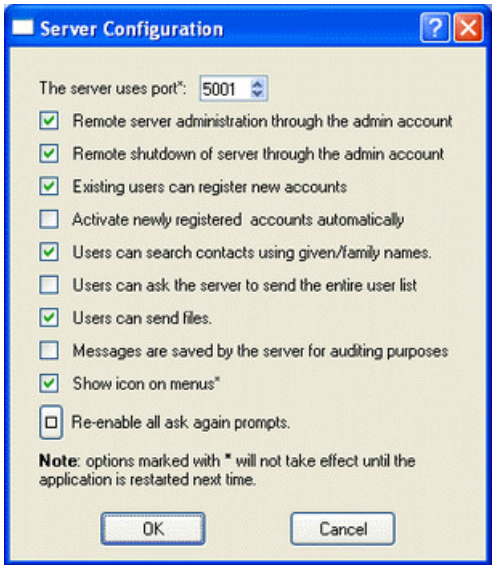
2.1 Setting Up Your Server Configuration

To view your server configuration settings:

1. Select "File -> Configuration...".



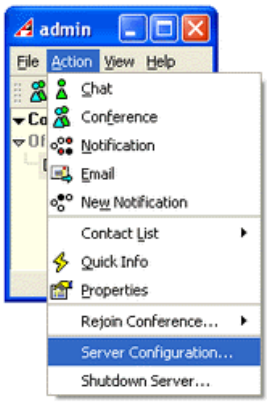
2. This will pop up the "Console Configuration Dialog" window where you can configure your server parameters.



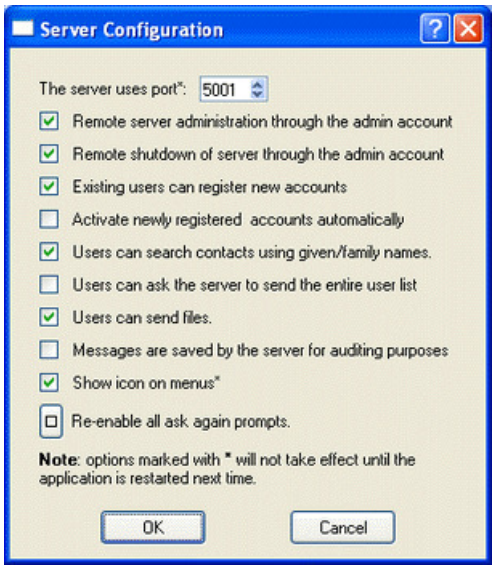
2.1.1 Remote server administration through the admin account

Set the check box if you would like to enable "Remote server administration through the admin account". This would allow the "admin" account to remotely access the server configuration from any workstation with Akeni Enterprise Client installed. If this is not checked, then you can access the admin account through the client only from the computer where the server is running.

1. Select “Action -> Server Configuration...”.



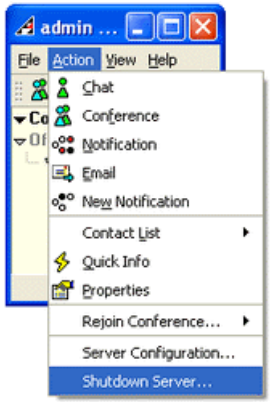
2. This will pop up the “Console Configuration Dialog” window where you can remotely configure your server parameters.



2.1.2 Remote shutdown of server through the admin account

Set the check box if you would like to enable "Remote shutdown of server through the admin account". This would allow the "admin" account to remotely shutdown the server from any workstation with Akeni Enterprise Client installed.

1. Select “Action -> Shutdown Server...”.

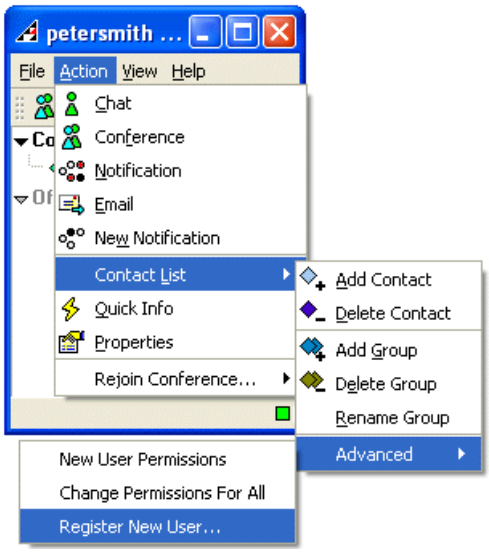


2. This will pop up the “Shutdown Confirmation Dialog” window where you will enter the "admin" password.

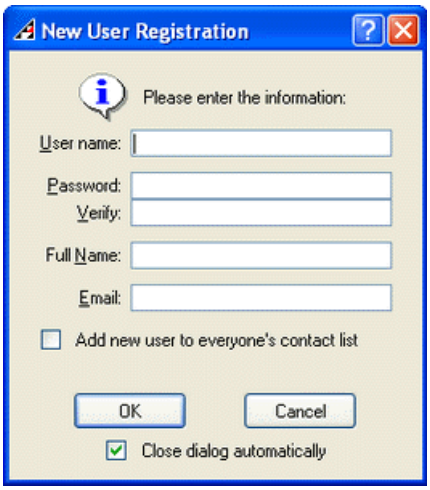
2.1.3 "Existing users can register new accounts" and "Activate newly registered accounts automatically"

Set the check box if you would like to enable "Existing users can register new accounts". This would allow existing users to register new user accounts. Important warning: If you have also enabled the "Activate newly registered accounts automatically" check box, then existing users can register new users and activate the new accounts WITHOUT the "admin" approval. It is best to leave "Activate newly registered accounts automatically" off except when the server is running entirely within a trusted LAN and no external access is allowed.

1. from any existing client account, Select “Action -> Contact List -> Advanced -> Register New User...”.



2. This will pop up the “New User Registration Dialog” where user can enter the new account information.



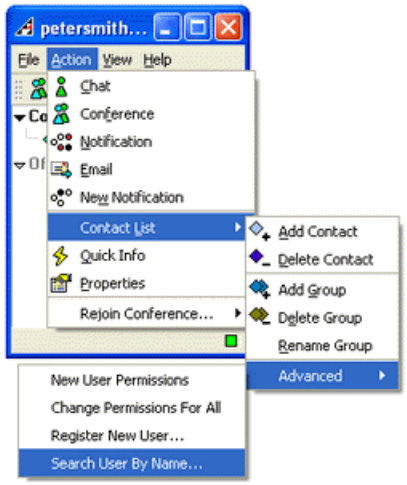
3. If you set the check box "Add new user to everyone's contact list" then this new user will be automatically added on everyone's contact list.

2.1.4 "Users can search contacts using given/family names"

Set the check box if you would like to enable "Users can search contacts using given/family names". This would allow a user

to search other users using given/family names.

1. from client account, Select "Action -> Contact List -> Advanced -> Search User By Name...".

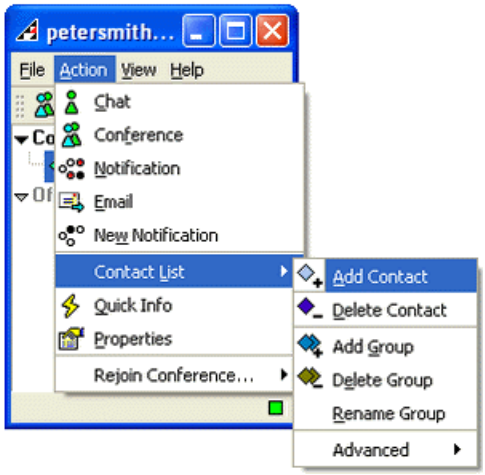


2. This will pop up the "Search User By Name Dialog" where user can enter the new account information.

2.1.5 "Users can ask the server to send the entire user list"

Set the check box if you would like to enable "Users can ask the server to send the entire user list". Important Warning: this feature would allow a user to ask the server to send the entire user list so that the user can add selected users into contact list. This might cause your server's user list to be exposed to the internet so the administrator might want to disable this feature if the Enterprise Server is connected to the internet.

1. from client account, Select "Action -> Contact List -> Advanced -> Search User By Name...".



2. This will pop up the "Add To Contact List Dialog", if the user enters blank and presses the return key, then the server will send the entire user list.

2.1.6 "Messages are saved by the server for auditing purposes"

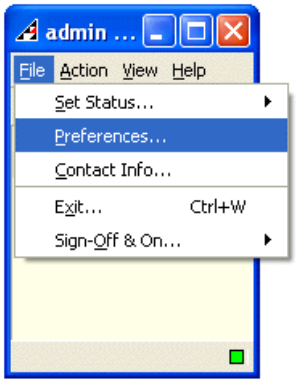
Important Warning: The server will Automatically Shutdown once you have changed this parameter. Please do this operation during non-business hours or send warning messages to all users before changing this parameter. Set the check box if you would like to enable "messages are saved by the server for auditing purposes". If this feature is enabled, then the server will store all the messages passed between the users for auditing purposes.

Important Warning: all logs are stored as unencrypted files, so the administrator should make sure that the files are stored in a secured location where normal users can not read them, preferrably using an encrypted file system. These logs should be backup and then removed from the system to minimize potential exposure.

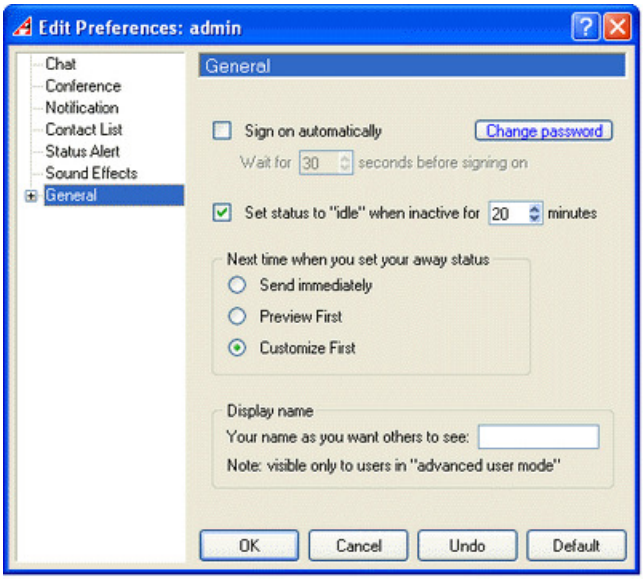
2.2 Change Password of Admin

To change the password of "Admin" account:

1. Select “File -> Preferences...”.



2. This will pop up the “Preferences Dialog”, then choose "General".



3. Then press the "Change Password" button and it will pop up the “Change Password Dialog”.

Chapter 3: User/Group Account Management

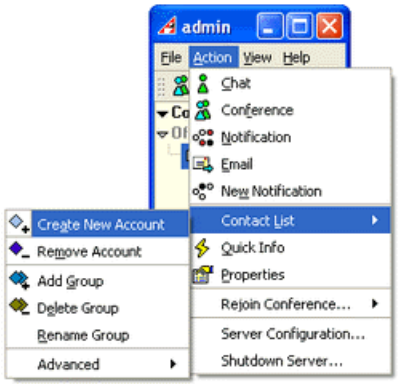
3.1 New User Registration

For a new user registration, do the following:

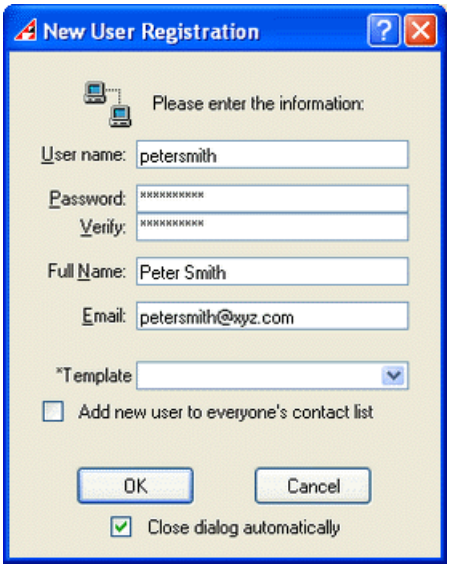
1. Click on the add user icon.

   OR

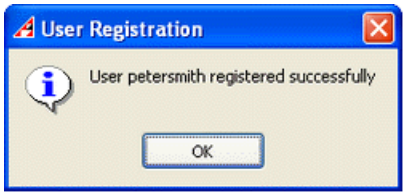
   - Select “Action -> Contact List -> Create New Account”.



2. The add new user dialog will now appear.
3. Now you can enter the user's account information. In this example, a new user "petersmith" is being created



4. After you have entered the user's information successfully, you should see the following message



You can also specify the name of a user to be used as a template for the new user. The new user will have the same contact list as the exiting user that is being used as the template. The new user will also be added automatically to the contact list of every user on the template. The new user and the user being used as the template will also be added to each other's contact list. The new user will also be created with the same access priviledge as the template. Any existing user can be used as a template, but please also see the note about using a special "template user" below. If the "Add new user to everyone's contact list" option is also checked, then the new user will be created using the template as outlined above, then he/she will be added to everyone's contact list, and everybody else not on the template will be placed into the default "Co-Workers" group.

A user template is created just like any other user account, except that the name starts with the special character '%'. This account will behave just like any other account (you can even login to this account) except for the following two points.

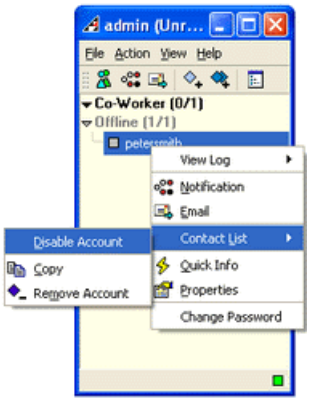
When a new user, say "bob" is created using the "%manager" account, then bob's contact list will be exactly the same as %manager's (and %manager itself will not be in there)

A template user will NOT be added to other user's account when the template is created. Suppose "%sales" is created using account "alice" as the template. Then everyone on alice's contact list will be in the "%sales" template, but "%sales" will not appear in their accounts.

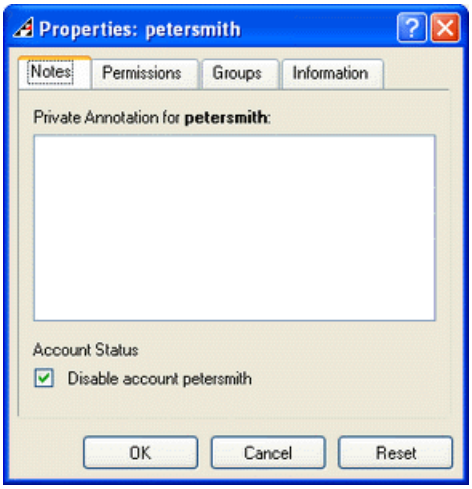
3.2 Disable User's Account

To disable a user's account, do the following:

1. Select the user account you want to disable and then right mouse click. In this example a user petersmith's account is being disabled
    - Select “Contact List -> Disable Account”.



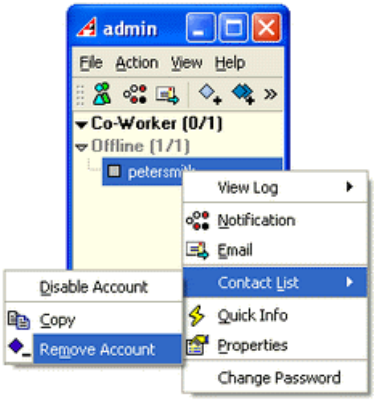
2. The properties dialog will now appear, in this example it is showing "disable account petersmith" check box is set. Press OK to disable the account



3.3 Remove User from Server

To permanently remove a user from the server, do the following:

1. Select the user you want to remove and then right mouse click. In this example a user "petersmith" is being removed
    - Select "Contact List -> Remove Account".

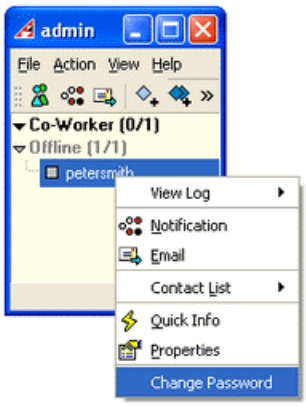


2. The remove user warning dialog will now appear.

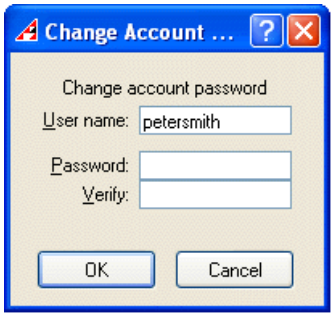
3.4 Change User Password

To change the password of a user, do the following:

1. Select the user you want to remove and then right mouse click. In this example a user "petersmith" password is being changed
    - Select “Change Password”.



2. Now the change password dialog will appear

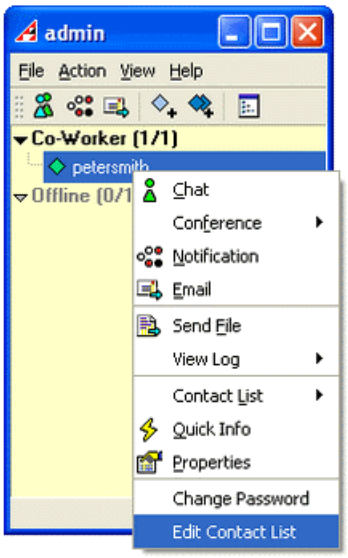


3.5 Change User's Contact List

Please note that the user must be offline for the admin to modify his/her account. If the user is online, then he/she will be logged off by the system. While the admin is modifying the contact list, the user's account will be disabled (if it was enabled)

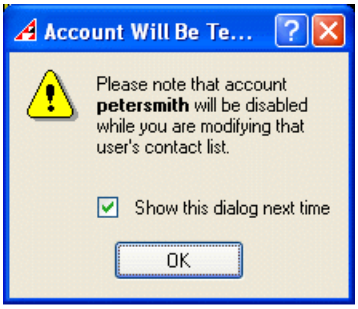
To modify the contact list of a user, do the following:

1. Select the user you want to modify and then right mouse click. In this example a user "petersmith" contact list is selected to be modified
    - Select “Edit Contact List”.

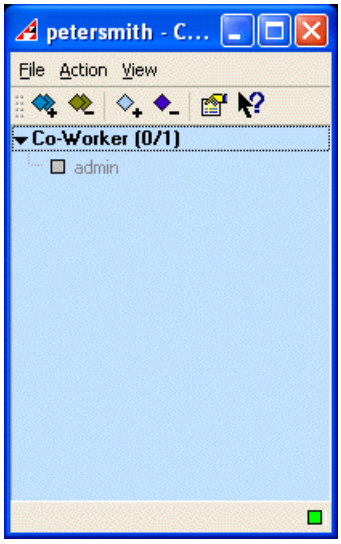


2. If the user was online, then the following dialog will ask you if you want to force the user offline

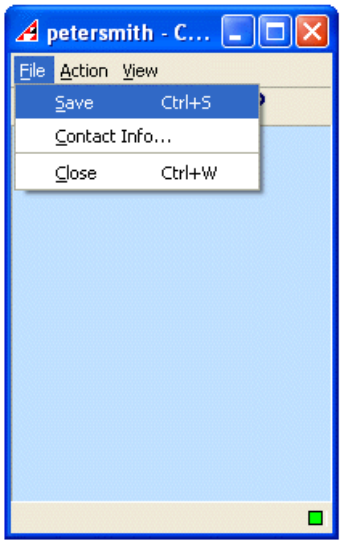
3. If you pressed yes, then the following dialog will inform you that the user's account is temporarily disabled.



4. Now you can modify the user's contact list. You can also drag-and-drop users from the admin's contact list into the user's contact list



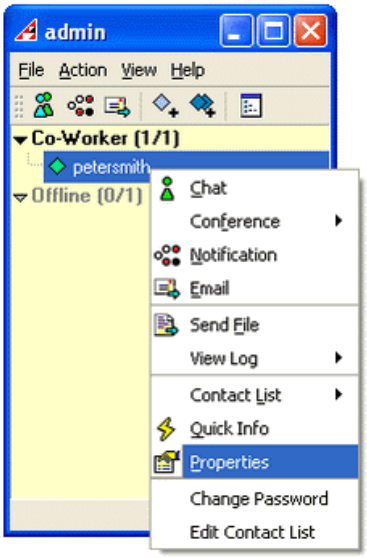
5. Once you have finished modifying the user's contact list, then from the File menu, select "Save"



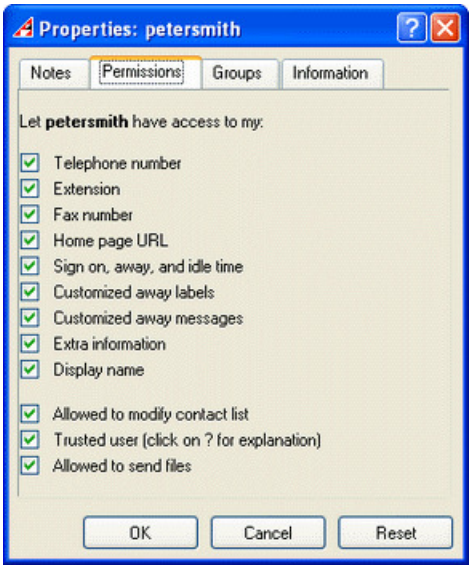
3.6 Change User's Account Access Rights

To change the Account Access Rights of a user, do the following:

1. Select the user you want to change the Account Access Rights and then right mouse click. In this example a user "petersmith" access rights is being changed
    - Select “Properties”.



2. Now select the "Permission" tab, and the following will appear. In this example, the user is allowed to modify contact list, it is a trusted user, and the user is allowed to send files



Allowed to modify contact list: If this option is unchecked then the user can not modify his/her contact list. Only the admin will be able to do that.

Trusted User: Only trusted users are allowed to contact anyone in their contact list (i.e., to start chat/conference, send notification/files, etc). If this option is unchecked then the user can **only chat and send notification to a trusted user (but can not start a conference)**. Two untrusted users can not contact each another directly.

This is useful, for example, in a school computer lab so that teachers can talk to students and students to teachers, but students can not chat with each other.This can also be used to setup guest accounts (along with the ability to modify the contact list disabled) in the system so that they can only contact a limited number of users (say their sales contacts) but not other guests.

Allowed To Send Files: if this option is enabled, then the user is allowed to send files

By default, all new users are created with all options enabled. To change the default option for new uses, login as admin and choose Action | Contact | Advanced | New Permissions. Note that this is for users that are created without the use of templates. When a template is used new users are created with the access rights specified for the template.

3.7 Change Group Access Rights

Besides specifying the access rights on a per user basis, the admin can also specify the access rights on a per group basis. To set the acess rights for a group,

If the "override" column is checked, then the group access right will override the user's individual access right. For example. If the override column is checked and the option "Allowed to modify contact list" itself is unchecked for group "Guest" (i.e.,

the "Guest" group can not modifiy its contact list") then if user alice is put into group "Guest" then she can not change her contact list, regardless of the setting for the alice account set via the user's own property page.

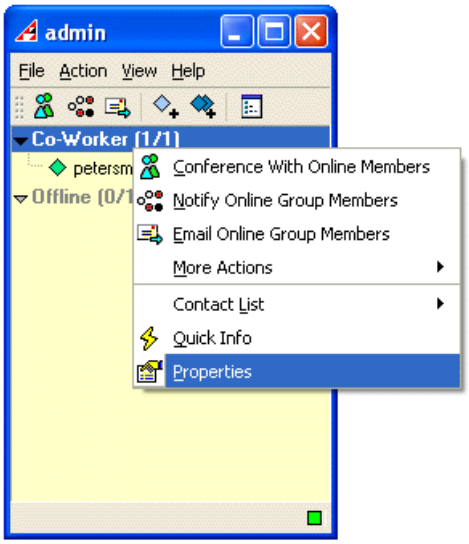
If a user belongs to more than one group, then the access level is the union of the access right of all the groups that he/she belongs to. For example, if alice is in both group "Sales" and "Manager", and if people in "Sales" are not allowed to modify their contact list but users in "Manager" are allowed to, then alice is allowed to modify her contact list.

New groups are created with "override" unchecked, so that the users in these groups simply have their own individual access rights.

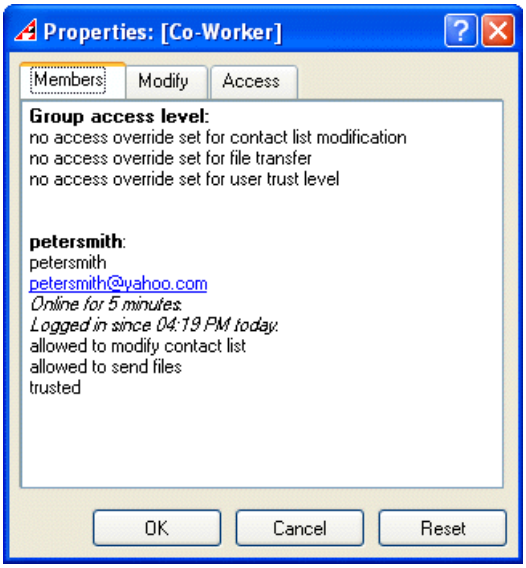
The access level of each user is then the access level set for that user level, in combination with the access level set for the groups that the user belongs to. To see this "effective accessl level", you can right click on the users and select "Property", then go to the "Information" tab. At the bottom you can see the "effect access level" of the users, which can be different from the access set in the "Permissions" page if the group access level is turned on. You can also see this information from the tooltip and the quick info for the users.

To change the Group Access Rights, do the following:

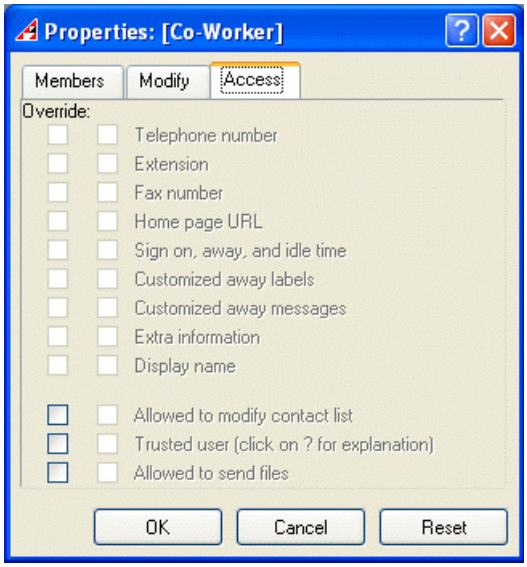
1. Select the group you want to modify the access rights and then right mouse click.
    - Select "Properties".



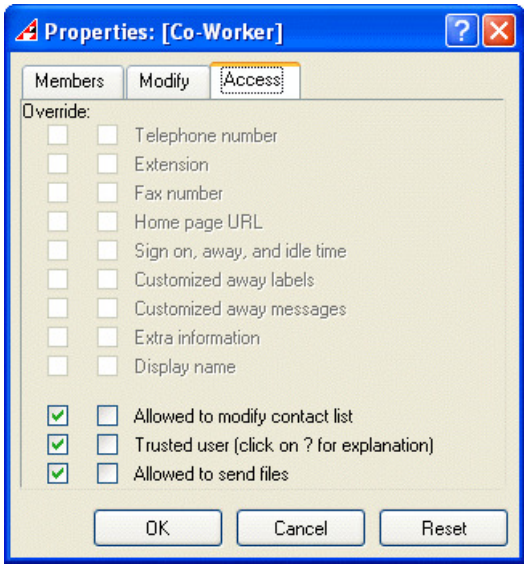
2. The following dialog will be displayed showing the details of the access rights of the group and also its user's individial access rights.



3. To modify the access rights of the group, change to the "Access" tab and the following dialog will appear.



4. To override the group access rights to NOT allowed to modify contact list, NOT trusted user, and NOT allowed to send files, you should set the override check box as follows:



5. To override the group access rights to ALLOWED to modify contact list, IS a TRUSTED user, and ALLOWED to send files, you should set the override check box as follows