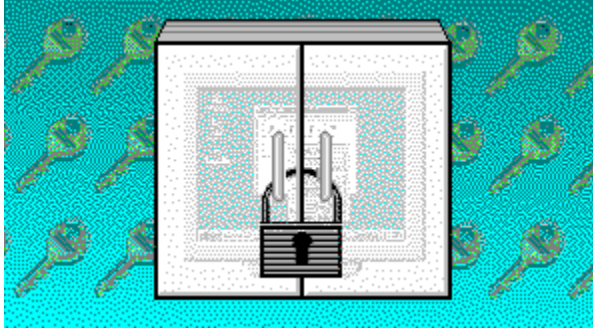


## Centralizing ReachOut Security

```
{button  
  Related  
  Topics,AL(  
  `How_Spe  
  cify_Gener  
  al_Reach  
  Out_Secur  
  ity_Setting  
  s;How_Set  
  _Up_a_Ce  
  ntralized_  
  Copy;Auto  
  mating_Re  
  achOut_In  
  stallations;  
  Troublesh  
  oting_Rea  
  chOut_Sec  
  urity;Prote  
  cting_Your  
  _Computer  
  _From_Un  
  authorized  
  _Access;H  
  ow_Specif  
  y_Security  
  _Settings_  
  fro_an_Ind  
  ividual_Co  
  nnection;S  
  haring_Re  
  achOut_on  
  _a_Networ  
  k;Help_sec  
  _Overview  
  ;How_Spe  
  cify_Share  
  d_ReachO  
  ut_Securit  
  y_Settings;  
  Master_Pa  
  ssword;l  
  DATAPAT  
  H')}
```

The easiest way to maintain ReachOut security on a network is to install one centralized copy of ReachOut that is accessed by users on different workstations. You can install ReachOut on a network drive and just set the security options there. Then have users install their copies of ReachOut directly from the network, using ReachOut's [public installation](#) feature. To ensure security, you will want to limit access to the network or shared folder where ReachOut is installed. Follow these simple steps to set up a secure copy of ReachOut:

1. Run SETUP SHARED to install ReachOut onto a network or shared folder.
2. [Open Supervisor Security](#) and make any global security changes.
3. If you do not want users to be able to create [connection icons](#) or to change their own configuration and security settings, make the appropriate selections on the *Application* tab of Supervisor Security and make the appropriate settings. To make all ReachOut users share the same connection icons that you store somewhere on the network, add the DATAPATH command to the ReachOut installation script you create in step 4.
4. If you want to customize the installation of ReachOut, open the text file named ROINST, and add any installation script commands on separate lines after the word PUBLIC. The install commands specified in this file will automatically be executed when the user runs SETUP.EXE.  
**Note:** Don't delete the PUBLIC command from the installation script. If you delete it, then whoever installs ReachOut from this shared folder will get a regular version of ReachOut that will not be affected by the Supervisor Security settings.
5. Give users read-only access to the network ReachOut folder.



ReachOut Supervisor Security provides a way for a system administrator to enable or disable most ReachOut security features. Supervisor Security controls features such as password life and login confirmation, and you can use it to impose various restrictions on both calling and waiting computers. If a security option exists in both the main ReachOut security options and in Supervisor Security, then the main ReachOut security setting can never be less restrictive than the Supervisor Security setting.

### ***Security Over the Internet***

If your network has a connection to the Internet, you will probably want to set up a [firewall](#) to prevent Internet access from unauthorized users.

<b>Supervisor</b>	{button
<b>Security</b>	Related
<b>Main</b>	Topics,AL(
<b>Window</b>	`Help_sec
	_MainInde
	x;Help_sec
	_Security;
	Help_sec_
	Password;
	Help_sec_
	Config;Hel
	p_sec_Au
	dit')}

The main window of ReachOut Supervisor Security may display any of five different groups of options. You can display a different set of options just by choosing the appropriate tab.

- **Connect**  
Use this page to set security options that apply when users make connections.
- **Disconnect**  
Use this page to set security options that apply whenever a user disconnects from a computer.
- **Session**  
Use this page to set remote control and ReachOut Explorer security options that apply while two computers are connected.
- **Application**  
Use this page to determine who may access the ReachOut program and make changes to its settings. Access levels can be defined for three different areas of ReachOut: *security*, *options/configuration*, and *connection icons*.
- **Waiting**  
Use this page to allow or prevent ReachOut computers from waiting for calls using specific [connection types](#).



## Control Menu

**Restore** {button  
Related  
Topics,AL(  
`VIEWING  
\_CONTRO  
L\_MINIMIZ  
E;VIEWIN  
G\_CONTR  
OL\_MAXI  
MIZE')}

Returns the ReachOut Supervisor Security window to its normal size.


This command is only available if Supervisor Security is minimized.



## Control Menu

### Move

```
{button  
  Related  
  Topics.AL(  
    `VIEWING  
    _CONTRO  
    L_RESTO  
    RE;VIEWI  
    NG_CONT  
    ROL_SIZE  
    ;VIEWING  
    _CONTRO  
    L_MINIMIZ  
    E')}
```

Turns the mouse pointer into a Move pointer  so you can use the arrow keys on your keyboard to move the window.

This command is not available if Supervisor Security is minimized.



## Control Menu

### Size

```
{button  
  Related  
  Topics,AL(  
    `VIEWING  
    _CONTRO  
    L_MOVE;  
    VIEWING_  
    CONTROL  
    _MAXIMIZ  
    E')}
```

The Size command is not available in ReachOut Supervisor Security.



## Control Menu

**Minimize**  
**e**

```
{button  
  Related  
  Topics,AL(  
    `VIEWING  
    _CONTRO  
    L_RESTO  
    RE;VIEWI  
    NG_CONT  
    ROL_SIZE  
    ;VIEWING  
    _CONTRO  
    L_MAXIMI  
    ZE;VIEWI  
    NG_CONT  
    ROL_CLO  
    SE')}}}
```

Reduces the ReachOut Supervisor Security window to an icon on the Windows taskbar.

This command is not available if Supervisor Security is already minimized.



*Minimize* is also on the title bar.



## Control Menu

**Maximize**  
**e**

```
{button  
  Related  
  Topics,AL(  
    `VIEWING  
    _CONTRO  
    L_RESTO  
    RE;VIEWI  
    NG_CONT  
    ROL_SIZE  
    ;VIEWING  
    _CONTRO  
    L_MINIMIZ  
    E;Help_Wi  
    ndows')}}
```

The *Maximize* command is not available in ReachOut Supervisor Security.





## Control Menu

**About** {button  
**ReachO** Related  
**ut** Topics,AL(  
"")}

Displays license and version information for ReachOut Supervisor Security.



## Control Menu

### Help Topics

```
{button  
  Related  
  Topics,AL(  
    'Getting_H  
    elp')}
```

Displays the list of ReachOut Supervisor Security Help topics.

For Help on a specific page of the dialog box, you can choose the *Help* button at the bottom of the ReachOut Supervisor Security window.



## Control Menu

### Close

{button  
Related  
Topics,AL(  
"")}

Closes Supervisor Security without saving your changes.

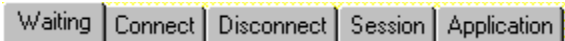
You can also use the *Cancel* button at the bottom of the ReachOut Supervisor Security window.

KEYBOARD: ALT+F4

KEYBOARD: ESC

## ReachOut Supervisor Security (Dialog Box)

```
{button  
  Related  
  Topics,AL(  
    `Superviso  
    r Security  
    screen;ID  
    H_OPTIO  
    NS_PAGE  
    _WAITING  
    `)}}
```



Use this page to determine which [connection types](#) you want ReachOut computers to be able to wait for calls on.

If you check any box to allow waiting for calls on that connection type, then each user may decide to wait for that type of call at his or her discretion.

### Modem

Check this box to allow ReachOut computers to wait for calls over a modem.

### NetBIOS (NetBEUI)

Check this box to allow ReachOut computers to wait for calls over a NetBIOS-compatible network.

NetBIOS compatibility is usually installed by default with Windows.

### NetWare (IPX/SPX)

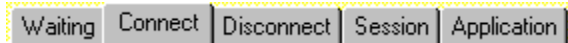
Check this box to allow ReachOut computers to wait for calls over a NetWare-compatible network.

### Internet (TCP/IP)

Check this box to allow ReachOut computers to wait for calls over the Internet or any TCP/IP network.

## ReachOut Supervisor Security (Dialog Box)

```
{button  
  Related  
  Topics,AL(  
    `Superviso  
    r Security  
    screen;ID  
    H_SECUR  
    ITY_CON  
    NECT')}
```



Use this page to protect computers from unauthorized access. Any security option that you activate here is in effect on all [publicly installed](#) ReachOut computers.

If you leave a security option turned off, each user may set that option at his or her discretion.

### Must prompt before accepting an incoming call

Check this box if you want ReachOut users to be notified when [remote computers](#) try to connect to them. At that time, the user will be able to allow or deny access to that computer.

### Must wait seconds for a response

Check this box to force a timeout period for the confirmation prompt that appears when a caller tries to connect, then set the number of seconds ReachOut should wait for the user at the waiting computer to respond to the confirmation prompt. If nobody at the waiting computer responds, ReachOut will either allow the caller to complete the connection, or disconnect the caller—depending on the how the waiting computer's *If no response* option is set up.

If you do not check this box, each ReachOut user may set an individual timeout period.

This option is available only if *Must prompt before accepting an incoming call* is checked.

### Force disconnect if no response

Check this box if you do not want to allow callers to connect to waiting computers if the confirmation response time has elapsed and no one has responded to the prompt. You might choose this setting if you do not want anyone to log on to a computer without the explicit knowledge and permission of a user at that computer.

- If *Force disconnect if no response* is checked, ReachOut will break the connection.
- If *Force disconnect if no response* is NOT checked, the caller will be allowed to connect, unless the user at the waiting computer has turned this option on.

This option is available only if *Must prompt before accepting an incoming call* is checked.

### Callback required

Check this box to force callbacks to connecting computers. When a user sets a callback, the waiting computer automatically disconnects and calls back the calling computer whenever a connection attempt is made. A user at the waiting computer needs to define the callback phone number or ReachOut computer name in the individual user account.

If this field is checked and a user does not have any user accounts that do not specify callbacks, then those remote users will not be able to connect to the computer.

**Note:** Callbacks work only with local Windows user accounts, not those defined on a Windows NT domain. To ensure that callback security will work correctly, you might want to set the *Authenticate caller* option to *On local computer only*.

### Don't allow caller to set callback number/name

Check this box to prevent users from connecting with passwords that allow them to enter callback numbers or names. When you check this box, user accounts that specify *Set by caller* for the callback choice become unusable. This forces users to call from a known location specified in the user account.

### Authenticate caller

Choose where you want waiting ReachOut computers to look for user accounts to validate connecting callers.

- **Using default NT process**

Choose this option to let in all callers with Windows user accounts that are defined either on the waiting computer itself or on the domain containing the waiting computer.

- **On local computer only**

Choose this option to let in only callers who have Windows user accounts on the waiting computer itself. Callers with user accounts defined only on the domain will not be able to connect. You might want to choose this option if callbacks are required, since callbacks only work with local user accounts.

- **On domain**

Choose this option to let in only callers who have Windows user accounts that are defined on a specific domain. Callers with user accounts defined only on the waiting computer will not be able to connect.

### **Must log off current user and prompt for new logon**

Check this box to force remote callers to log on to waiting computers when they start remote control. This means the caller's rights are restricted by the caller's user account, and the caller cannot gain access to the rights of the user at the waiting computer simply by making a ReachOut connection.

A user at the waiting computer can continue to use the computer locally while the caller works remotely, but while the caller is connected the waiting user only has the access privileges normally granted to the caller.

**Note:** This setting does not affect callers who only use ReachOut Explorer. For file transfers, each connected user has the rights assigned by that person's user account.

**Important!** For this setting to work properly, each user must have ReachOut configured to start waiting for calls when the computer starts. After you activate the Supervisor Security setting, tell each ReachOut user to do the following:

1. From the ReachOut *Configure* menu, choose *Options*.  
This will synchronize the user's settings with the Supervisor Security settings.
2. Close ReachOut and restart the computer.

### **Lock out all callers**

Check this box to prevent callers from connecting after a certain number of incorrect user names or passwords have been entered. Use the second field to set the maximum number of consecutive failed logon attempts allowed (up to 100). If this box is not checked, users could try hundreds of passwords in an attempt to gain access to a waiting computer.

When the IntruderGuard is activated, no remote computers can connect until a user at the waiting computer resets the IntruderGuard by clicking *OK* in the resulting message box.

## ReachOut Supervisor Security (Dialog Box)

```
{button  
  Related  
  Topics,AL(  
    `Superviso  
    r Security  
    screen;Re  
    achOut_P  
    asswords;  
    Calling_Ba  
    ck;How_C  
    hange_Yo  
    ur_Passwo  
    rd;Master_  
    Password;l  
    DH_SECU  
    RITY_DIS  
    CONNECT  
  )}
```



Use this page to set security options that apply when a caller disconnects from a ReachOut computer.

If you leave a security option turned off, each user may set that option at his or her discretion.

### Force disconnect after no activity

Check this box to have ReachOut automatically disconnect when there is no activity for the amount of time you specify. This is useful if user leaves the computer and forgets to disconnect. It can save money if users connect over long distance phone lines. It also prevents a user from accidentally tying up a waiting computer.

### Must wait before disconnecting

Check this box to set the length of time (in minutes) that there should be no activity before ReachOut automatically disconnects. If you do not check this box, each ReachOut user may set an individual timeout period.

This option is only available if *Force disconnect after no activity* is checked.

### Disconnect action override

Choose what you want a computer to do when a caller disconnects.

- **User defined**

Choose this option if you do not want to force logoff security. The user at each waiting computer may decide what to choose here.

**Note:** If you choose *User defined*, a user might decide to allow whoever is logged on to stay logged on even after the ReachOut connection is broken. If you do not want this to happen, you must choose one of the other options.

- **Log the caller off the computer**

Choose this option if you want to automatically log the caller off Windows when ReachOut is disconnected.

**Note:** If the user has set ReachOut to leave the current user logged on instead of logging on the [remote](#) caller, then the current user is the one who is logged off when ReachOut is disconnected. To force the caller to be logged on instead, check the *Must log off current user and prompt for new logon* option on the *Connect* tab.

- **Restart the computer and prompt for new logon**

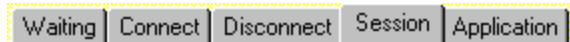
Choose this option if you want ReachOut to automatically restart the waiting computer when ReachOut is disconnected. This also logs off all users. Having the computer restart can be useful in situations where an error occurs during the connection, preventing ReachOut access to the computer. If ReachOut restarts the computer and a user checks *when computer starts* on the *Waiting* page of the Options dialog box (available from the *Configure* menu), then callers will be able to connect again once the computer restarts.

#### Notes

- If more than one caller is connected, ReachOut waits until the last caller has disconnected before restarting the computer.
- Even if a waiting computer is not set up to restart automatically, callers can cause waiting computers to restart upon disconnection.

## ReachOut Supervisor Security (Dialog Box)

```
{button  
  Related  
  Topics,AL(  
    `Superviso  
    r Security  
    screen;Co  
    nfirming_C  
    onnection_  
    Attempts;l  
    DH_SECU  
    RITY_SES  
    SION`)}  
}
```



Use this page to set security options that apply while two computers are connected.

If you leave a security option turned off, each user may set that option at his or her discretion.

### Don't allow computers to be remotely controlled

Check this box to prevent callers from using ReachOut remote control. With remote control, the caller can take control of the computer.

### Don't allow files to be accessed using ReachOut Explorer

Check this box to prevent callers from accessing files with ReachOut Explorer.

If you don't check this box, then depending on the level of access users have, they may be able to create, copy, and delete files and folders with ReachOut Explorer.

### Clear computer's display

Check this box to blank a computer's screen while a caller is connected to it with ReachOut. This allows the caller to work securely on the computer from a [remote](#) location, without other people seeing what the caller is working on.

When you choose this option, *Ignore computer's keyboard and mouse* is automatically enabled.

### Ignore computer's keyboard and mouse

Check this box to disable a computer's keyboard and mouse while a remote caller is connected to it with ReachOut. This prevents user input conflicts while remote callers are trying to control the computer.

### Ignore caller's keyboard and mouse

Check this box to prevent callers from using the keyboard and mouse to remotely control computers. This effectively disables remote control, though the caller can still see the remote desktop. To turn off the display as well, disable remote control by checking the box labeled *Don't allow computers to be remotely controlled*.

### Don't allow remote clipboard access

Check this box to prevent callers from copying and pasting information between computers while they are using remote control.

**Note:** If you want to prevent the caller from retrieving data from the computer, you will probably want to disable the use of ReachOut Explorer as well.

### Must check for viruses on transferred files

Check this box to have ReachOut scan files for viruses when they are copied to or from a hosting computer. This only takes about one second per file.

### Limit caller access rights

Check this box to choose the maximum level of access that you want callers to have to files with ReachOut Explorer. If you do not check this box, each ReachOut user may set maximum access rights individually.

Click a selection below for a description:

- [Full Control](#)
- [Change](#)



- [Read/Write](#)
- [Read Only](#)

**Note:** To disable file access with ReachOut Explorer altogether, check the box labeled *Don't allow files to be accessed using ReachOut Explorer* at the top of this dialog box.

### Connection time override

Check the *Limit to* box to limit the amount of time a caller can be connected to a ReachOut computer. Type or choose a number in the first *Limit to* field, then select a unit of time from the list. Time can be measured in minutes, hours, days, weeks, or months. Use the last field to set the period of time over which the maximum connection time is in effect. For example, you can specify a maximum connection time of 2 hours per day. If you want to set an absolute maximum connect time (not renewed after any time period), choose *total* from the *per* list.

#### Notes:

- For each user on a waiting computer, the period of time over which you define a connection time limit starts when the user makes the first connection to that computer.
- Changing this value affects the connection time limit only on new connections that are subsequently made; it does not affect currently connected users until they disconnect.

## How to Specify Shared ReachOut Security Settings

```
{button  
  Related  
  Topics,AL(  
    `How_Spe  
    cify_Gener  
    al_Reach  
    Out_Secur  
    ity_Setting  
    s;How_Sp  
    ecify_Secu  
    rity_Settin  
    gs_fro_an  
    _Individual  
    _Connecti  
    on;Help_s  
    ec_MainIn  
    dex;Sharin  
    g_ReachO  
    ut_on_a_N  
    etwork;Pre  
    venting_R  
    eachOut_  
    Users_Fro  
    m_Changi  
    ng_Securit  
    y_Settings'  
  )}
```

1. Set up a shared copy of ReachOut.
2. [Open Supervisor Security](#).
3. Make the desired changes.  
The security settings are divided into different pages. You can display a different screen by choosing any of the tabs at the top of the window.
4. Choose *OK*.  
The changes you made apply to all copies of ReachOut that were [publicly installed](#) from the shared copy.

## How to Specify Maximum File Rights for Any Waiting Computer

```
{button  
  Related  
  Topics,AL(  
    `Help_sec  
    _Security;  
    How_Set_  
    Default_Ac  
    cess_to_L  
    ocal_Files;  
    How_Restr  
    ict_a_Calle  
    rs_File_Ri  
    ghts;How_  
    Hide_Fold  
    ers')}}}
```

1. [Open Supervisor Security.](#)
2. Choose the *Session* tab.
3. Check the box labeled *Limit caller access rights*.
4. From the *Limit caller access rights* list, choose the maximum file rights you want to allow. Users at waiting computers will not be able to set less restrictive file rights than you choose here.  
To allow the user at each waiting computer to set any level of file access, choose *Full Control*.
5. Choose *OK*.

**Note:** To prevent the use of ReachOut Explorer altogether, check the box labeled *Don't allow files to be accessed using ReachOut Explorer* at the top of the dialog box.

**How to Make  
ReachOut  
Check for  
Viruses When  
a File Is  
Transferred to  
Any  
ReachOut  
Computer**

```
{button  
  Related  
  Topics,AL(  
    `Help_sec  
    _Security;  
    How_Mak  
    e_ReachO  
    ut_Check_  
    for_Viruse  
    s;How_Au  
    dit_File_Tr  
    ansfers')}}}
```

1. [Open Supervisor Security.](#)
2. Choose the *Session* tab.
3. Check the box labeled *Must check for viruses on transferred files.*
4. Choose *OK.*

**How to Guard  
Against  
Multiple  
Connection  
Attempts to  
Any  
ReachOut  
Computer**

```
{button  
  Related  
  Topics,AL(  
    `Help_sec  
    _Security;  
    How_Guar  
    d_Against  
    _Multiple_  
    Connectio  
    n_Attempt  
    s')}}}
```

1. [Open Supervisor Security.](#)
2. Choose the *Connect* tab.
3. Check the box labeled *Lock out all callers*.
4. In the *Lock out all callers* field, type the maximum number of consecutive times that an invalid user name or password can be entered by users trying to connect to a waiting computer. For the global IntruderGuard, ReachOut counts all consecutive invalid connection attempts, even if they are from different users.
5. Choose *OK*.

## How to Disable Input on Waiting Computers While They Are Connected

```
{button  
  Related  
  Topics,AL(  
    `Help_sec  
    _Security;  
    How_Blan  
    k_the_Dis  
    play_on_  
    Waiting_C  
    omputers;  
    How_Dis  
    able_Input_  
    on_Calling  
    _Computer  
    s;How_Dis  
    able_Input  
    _on_a_Re  
    mote_Com  
    puter')}}}
```

1. [Open Supervisor Security](#).
2. Choose the *Session* tab.
3. Under *Remote control hosting overrides*, check the box labeled *Ignore computer's keyboard and mouse*.
4. Choose *OK*.

## How to Disable Input on Calling Computers During Remote Control

```
{button  
  Related  
  Topics,AL(  
    `Help_sec  
    _Security;  
    How_Dis  
    able_Input_t  
    o_the_Vie  
    wing_Wind  
    ow;How_D  
    isable_Inp  
    ut_on_Wai  
    ting_Comp  
    uters;How  
    _Prevent_  
    a_Caller_F  
    rom_Disab  
    ling_Input')  
}
```

1. [Open Supervisor Security](#).
2. Choose the *Session* tab.
3. Under *Remote control hosting overrides*, check the box labeled *Ignore caller's keyboard and mouse*.
4. Choose *OK*.

## How to Set User Confirmation Options for All Waiting Computers

```
{button  
  Related  
  Topics,AL(  
    `Help_sec  
    _Config;H  
    ow_Confir  
    m;How_M  
    ake_Reac  
    hOut_Disc  
    onnect_if_t  
    he_Caller_  
    Is_Not_Co  
    nfirm;Co  
    nfirming_C  
    onnection_  
    Attempts'}}
```

1. [Open Supervisor Security](#).
2. Choose the *Connect* tab.
3. Under *Confirmation override*, check the options you want to apply all waiting computers.
4. Choose *OK*.



## How to Make Each Waiting Computer Call Back the Connecting User

```
{button  
  Related  
  Topics,AL(  
    `Help_sec  
    _Password  
    ;How_Mak  
    e_ReachO  
    ut_Automa  
    tically_Call  
    _Back;Ho  
    w_Prevent  
    _Users_Wi  
    thout_Call  
    backs_Fro  
    m_Connec  
    ting;How_  
    Disable_AI  
    l_Callback  
    _Prompts;  
    Calling_Ba  
    ck;How_M  
    ake_Reac  
    hOut_Allo  
    w_Local_o  
    r_Domain')  
  }
```

1. [Open Supervisor Security.](#)
2. Choose the *Connect* tab.
3. Under *Callback override*, check the box labeled *Callback required*.
4. Choose *OK*.

### Notes:

- You should inform all users that any user accounts that do not specify a callback number or name cannot be used while this setting is turned on.
- Callbacks work only with local Windows user accounts, not those defined on a Windows NT domain. To ensure that callback security will work correctly, you might want to set the *Authenticate caller* option to *On local computer only* on the *Connect* page of ReachOut security.

## How to Make Each Waiting Computer Restart After It Disconnects

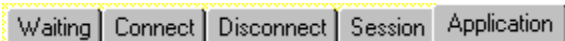
```
{button  
  Related  
  Topics,AL(  
    `Help_sec  
    _Security;  
    How_Mak  
    e_the_Wai  
    ting_Comp  
    uter_Resta  
    rt;CONNE  
    CTION_DI  
    SCONNE  
    CT')}
```

1. [Open Supervisor Security](#).
2. Choose the *Disconnect* tab.
3. Under *Disconnect action override*, choose *Restart the computer and prompt for new logon*.
4. Choose *OK*.

**Note:** The user at each waiting computer can make ReachOut automatically wait for calls when the computer restarts. The user does not have to be logged onto Windows or onto the network for ReachOut to be able to receive calls.

## ReachOut Supervisor Security (Dialog Box)

```
{button  
  Related  
  Topics,AL(  
    `Superviso  
    r Security  
    screen;Re  
    achOut_P  
    asswords;  
    Calling_Ba  
    ck;How_C  
    hange_Yo  
    ur_Passwo  
    rd;Master_  
    Password;  
    How_Mak  
    e_ReachO  
    ut_Wait_fo  
    r_Calls_W  
    hen_the_C  
    omputer_S  
    tarts;IDH_  
    SECURIT  
    Y_APPLIC  
    ATION')}
```



Use this page to determine who may access the ReachOut program and make changes to its settings. Access levels can be defined for three different areas of ReachOut: *security*, *options/configuration*, and *connection icons*.

**Note:** Users in the “Administrators” group always have full control over all ReachOut settings, unless those settings are individually disabled by the ReachOut supervisor. To limit control of a particular group of settings to Administrators only, check the appropriate box and choose *Administrators* from the list. To give control to another group of users in addition to Administrators, choose the other group from the list. If you do not want users to have access to the ReachOut settings on their own computers, you must personally administer their computers and remove them from the “Administrators” group. Be aware, however, that because of Windows NT security restrictions, members of the “Users” group cannot run ReachOut unless you set it to start waiting for calls when the computer starts. To learn how, click the *Related Topics* button above.

### Limit who may edit ReachOut security

Check this box to limit access to ReachOut’s security options by selecting a user group from the list. Only those users who log onto the computer as a member of this group will be able to change ReachOut security settings.

### Limit who may edit ReachOut options/configuration

Check this box to limit access to ReachOut’s general options and configuration settings by selecting a user group from the list. Only those users who log onto the computer as a member of this group will be able to change ReachOut modem, network, and other configuration settings.

### Limit who may edit ReachOut connection icons

Check this box to limit access to ReachOut’s [connection icons](#) by selecting a user group from the list. Only those users who log onto the computer as a member of this group will be able to create, delete, or change the properties of ReachOut connection icons.

## How to Make ReachOut Allow Local or Domain User Accounts

{button  
Related  
Topics,AL(  
`Calling\_B  
ack')}

1. [Open Supervisor Security.](#)
2. On the *Connect* page, choose the option you want under *Authenticate caller*.
3. If you chose *On domain*, you can specify the name of a domain to use.  
Only callers with user accounts on this domain will be allowed to connect with ReachOut.
4. Choose *OK*.

## Preventing ReachOut Users From Changing Settings

```
{button  
  Related  
  Topics,AL(  
    `Help_sec  
    _Overview  
    ;Master_P  
    assword;;  
    How_Mak  
    e_ReachO  
    ut_Wait_fo  
    r_Calls_W  
    hen_the_C  
    omputer_S  
    tarts')}}}
```

The [ReachOut supervisor](#) can prevent all ReachOut users who have done a [public installation](#) from changing configuration and security settings or changing [connection icons](#).

To do this, [open ReachOut Supervisor Security](#) and choose the *Application* tab. You can limit access to three different sets of ReachOut options:

- Security
- Options and configuration
- Connection icons

To limit access, you must also make sure users are not members of the “Administrators” group on their computers. Users in the “Administrators” group always have full control over all ReachOut settings, unless those settings are individually disabled by the ReachOut supervisor. Be aware, however, that because of Windows NT security restrictions, members of the “Users” group cannot run ReachOut unless you set it to start waiting for calls when the computer starts. To learn how, click the *Related Topics* button above.

**Enter Shared  
Computer  
Password  
(Dialog Box)** {button  
Related  
Topics,AL(  
`CONFIGU  
RE\_SECU  
RITY;Wind  
ows\_NT\_P  
asswords;  
Help\_sec\_  
MainIndex;  
How\_Set\_  
Up\_a\_Cen  
tralized\_C  
opy'})}

During the shared installation of ReachOut, if you chose to save the ReachOut security settings on a computer other than the shared computer or your local computer, the Enter Network Password dialog box might appear when you try to view the security settings. To access these settings, you must log on to the computer where the Registry settings are stored.

**Computer Name**

This area displays the name of the shared computer where the ReachOut security settings are stored.

**Connect As**

Type your user name on the shared computer.

**Password**

Type your password to log on to the shared computer.

Remember that passwords are case-sensitive.

