6

Security

This chapter describes the two types of Lookout*Direct* operational security: network security and control security. Viewing security is primarily based in control security. You can use either or both security approaches to control who has access to different processes, control panels, individual controls, and data.

Lookout*Direct* processes can pass data and commands back and forth across a network. Lookout*Direct* security prevents or enables this communication based on who is logged in on each instance of Lookout*Direct* running on the networked computers. Lookout*Direct* network security works between different instances of Lookout*Direct* running on one computer or different computers on the same network.

Network security is based on user and group permissions configured for processes, collections of objects grouped in a folder, or individual objects.

Control security is based on security level parameters set in a given Lookout*Direct* object, usually a control such as a Pot or Switch. This security level is compared to the security level assigned to a user account or a group to prevent or enable access.

A *user account* identifies a single person authorized to log on to Lookout*Direct*. *Groups* consist of collections of users with similar duties and security levels.

Security information for a Lookout*Direct* process is kept in the `.lka` file for that process. You must keep the `.lka` file in the same directory as the `.l4p` file for your security settings to work. If you misplace the `.lka` file, all users will have complete access to all parts of the process.

The user and group account information for Lookout*Direct* 4 is kept in the `Lookout.sec` file, installed in your Windows `SYSTEM` directory.

If you want basic authentication to work between different computers running Lookout*Direct* on your network, you must have an identical `Lookout.sec` file installed on each computer. You can do this by creating a master security file on your main development computer and copying it to all the other computers running Lookout*Direct* on your network.

To preserve user and group account information from versions of Lookout*Direct* prior to Lookout*Direct* 4.0, import the old security file into your new security file using the **Import LookoutDirect 3.x Security File** option in the Lookout*Direct* User Manger. See the Importing Old Security Files into LookoutDirect 4 section for more information on importing old security files.

Permissions and security levels are cumulative in Lookout*Direct*. If you add a user account to a group that has a group security level or permissions different than that assigned to the user account, the user will have the higher of the two security levels or permissions.

Note While it is possible to assign a security level to a user account and then put that user into a group with higher (or lower) security levels, it is not a good practice. To minimize confusion, it is best to assign user accounts to groups with the same security level when possible. Refer to the *Keeping Security Precedence Simple* section of this chapter for information on how different security levels and group permissions interact.

Logging On

Lookout*Direct* requires operators to log on with a predefined name and corresponding password (if any). To log on, use the **File»Log on** command, press <Ctrl-L>, or click on the **Account name** box in the status bar. Collectively, the name and password are known as a *user account*, or account. Each account has a security level and can be included as a member of a group. Because Lookout*Direct* uses account names when logging events to disk and when operators acknowledge alarms, you can identify the operator logged on when an event occurs.

You can programmatically access the name and security level of the currently logged Lookout*Direct* user through the $System object, using the `username` and `seclevel` data members.

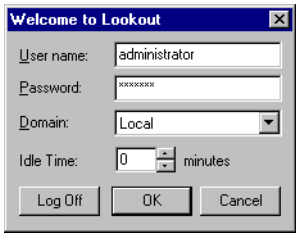
All users must log on to Lookout*Direct*. When nobody has logged on to Lookout*Direct*, Lookout*Direct* shows (nobody) as being logged on in the status bar at the bottom of the main screen. The (nobody) account is built into Lookout*Direct* with a security level of 0 (zero), and cannot be edited.

Note If the (nobody) account is logged on, any functions of client or server processes running that require a security level greater than zero do not receive or report data until someone logs on using an account with a high enough security level.

The first time you start a development version of Lookout*Direct*, the Administrator user account has no password. Any time the Administrator account has no password, Lookout*Direct* opens with Administrator logged in and active, without requiring any login. This is a convenience for you when creating your Lookout*Direct* processes, but you must be sure to assign a password to the Administrator account before allowing others who should not have Administrator privileges to use your copy of Lookout*Direct*.

Note Server and client run-time versions of Lookout*Direct* open with the (nobody) user account logged in, no matter what the password setting for the Administrator account.

After you have added a password to the Administrator account using the Lookout*Direct* User Manager, development versions of Lookout*Direct* open by presenting the **Welcome to Lookout*Direct*** dialog box which requires a Lookout*Direct* user to log in.



Welcome to Lookout

User name: administrator

Password: *******

Domain: Local

Idle Time: 0 minutes

Each time you log on, enter your **User name** and **Password**.

Note If yours is the only account that is a member of the Administrators group, and you forget your password, there is no way to access the **System»User Manger** command, and there is no way to modify account settings. Contact National Instruments for assistance.

Domain—In current versions of Lookout*Direct*, you can only log on to your local domain.

Idle time—The amount of time the computer sits idle (no mouse movement or keyboard action) before Lookout*Direct* automatically logs off the operator. If you enter `0` (zero), idle time is disabled. For security reasons, you might want to use this feature to automatically log off high-level accounts if the computer is left unattended too long. After an account logs off, the account `(nobody)` is logged on. The `(nobody)` account has a security level of 0 (zero).

By default, Lookout*Direct* presents you with the login dialog box every time you open the program. To log off, select **File»Log off** or press <Ctrl-D>. No dialog box appears in response to either of these actions; Lookout*Direct* just logs you off. You can also log off though the login dialog box.

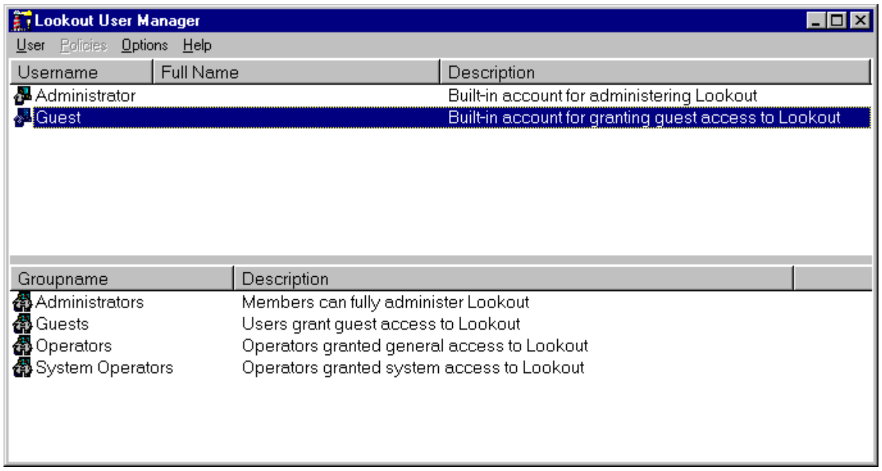
To log on after Lookout*Direct* has automatically logged you out, after someone else has logged off, or just to log in and replace the current user, select **File»Log on** or press <Ctrl-L> on the keyboard.

User Manager

You create individual accounts for operators and developers with the User Manager. Anyone whose account is a member of the Administrators group can create, revise, or delete system user accounts by selecting **Options»User Manager**. The Lookout*Direct* **User Manager** dialog box appears, as shown in the following illustration.

Note For your user accounts to work consistently across your network, you must use the same `Lookout.sec` file for all your installed copies of Lookout*Direct*. After you have created your Lookout`.sec` file, make a copy of it from your `WINDOWS\SYSTEM` directory. Place a copy of the file in the `WINDOWS\SYSTEM` directory of each of your Lookout*Direct* computers.

You should carefully consider users and the security level you assign each one. Assign level 10 access only to those people responsible for system security. Users with security levels of 8 and higher can close process files and exit Lookout*Direct*. Users with security level 9 or higher can edit process files in development versions of Lookout*Direct*.



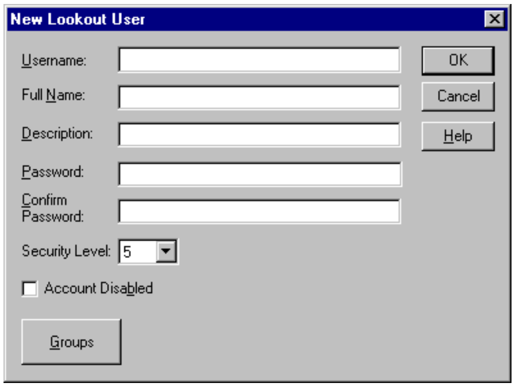
Username	Full Name	Description
Administrator		Built-in account for administering Lookout
Guest		Built-in account for granting guest access to Lookout

Groupname	Description
Administrators	Members can fully administer Lookout
Guests	Users grant guest access to Lookout
Operators	Operators granted general access to Lookout
System Operators	Operators granted system access to Lookout

From this dialog box, you can create and edit the properties of groups, create or edit the properties of user accounts, assign users to one or more groups, and otherwise manage security in Lookout*Direct*.

Creating User Accounts

To create a user account, select **User»New User**. The following dialog box appears.



Security Level: 5

□ Account Disabled

Enter the new user’s domain name in the **Username** field.

Enter the user’s **Full Name**.

You can use the **Description** field for job titles or other relevant information.

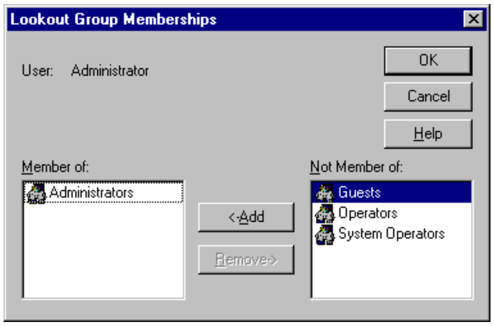
Enter the user’s password in the **Password** field.

Enter the password a second time in the **Confirm Password** field to make sure there was no typing error in the first entry.

Set the new user’s **Security Level**. Lookout*Direct* security levels range from 0 to 10, with 10 being the highest possible security authorization. Assign level 10 access only to those people responsible for system security. Users with security levels of 8 and higher can close process files and exit Lookout*Direct*. Users with security level 9 or higher can edit process files in development versions of Lookout*Direct*.

Select the **Account Disabled** checkbox if you want to disable a user account without removing the user from the system.

Click on the **Groups** button to add this user to various local security groups. The following dialog box appears.



User: Administrator

Member of: Administrators

Not Member of: Guests, Operators, System Operators

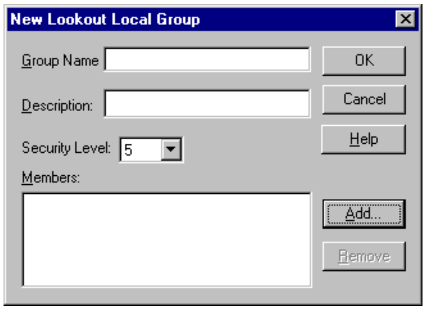
The default groups in Lookout*Direct* are Administrators, Guests, Operators, System Operators, and Everyone. Any groups you have created are also shown.

To enter a user in a group, highlight the group in the **Not Member of** field and click on the **Add** button. To remove a a user from membership in a group, highlight a group in the **Member of** field and click on the **Remove** button.

Note When you add an individual user who has a security level different than that of the group, that user will have the higher of the security levels.

Creating Groups

To create a group, select **User»New Local Group**. The following dialog box appears.



Security Level: 5

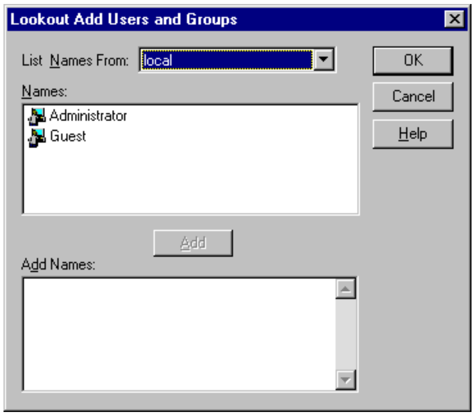
Group Name assigns a name to your new group.

Enter a description of the group in the **Description** field.

Security Level assigns the security level for members of this group.

Note When you add an individual user whose individual account has a security level different than that of the group, that user will have the higher of the two security levels.

To add **Members**, click on the **Add** button. The following dialog box appears.


Lookout Add Users and Groups

List Names From: local

Names:
- Administrator
- Guest

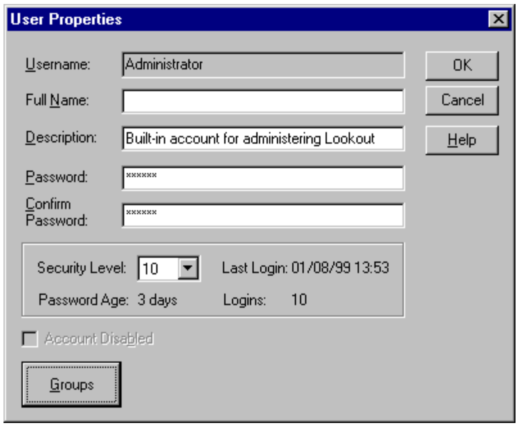
Add Names:

The **List Names From** listbox selects the domain to list user names from. In this version of Lookout*Direct*, you are restricted to your local domain.

Highlight the names you want to add in the **Names** field, and click on the **Add** button to add those users to your group.

Modifying Users and Groups

The dialog boxes for editing users and groups are essentially the same as those for creating users and groups. Open the User Manger, right-click on the user or group you want to edit, and select **Properties**. The following dialog box appears.


User Properties

Username: Administrator

Full Name:

Description: Built-in account for administering Lookout

Password: ******

Confirm Password: ******

Security Level: 10 Last Login: 01/08/99 13:53

Password Age: 3 days Logins: 10

□ Account Disabled

The **User Properties** dialog box displays information about user activity.

Special Users and Groups

Lookout*Direct* comes with several users accounts and groups built-in. The user accounts include Administrator, Guest, and (nobody). The built-in groups include Administrators, Everyone, Guests, Operators, and System Operators. You cannot delete any of these accounts, though you can edit the properties of some of them.

The Administrator account overrides all other security settings and has access to everything in Lookout*Direct*. This override extends to all accounts added to the Administrators group.

You cannot delete the Administrator account or change its security level. You can set the password and enter the name and a description of the Administrator. You can also add or remove user accounts.

The (nobody) account cannot be edited or deleted. This account is what Lookout*Direct* defaults to when no authorized user is logged on. It always has a security level of 0.

The Everyone group is built into Lookout*Direct*. You cannot edit or delete this group in the User Manager. When you first create a process in Lookout*Direct*, it is configured with this group allowed full read and write permissions. Because objects inherit their permission status from the process or folder in which they are created, all the objects you create have this same status until you change them manually, or change the permission status of the process or folder you create them in.

You can edit all the properties of the Guest user account and of the Guests, Operators, and System Operators groups.

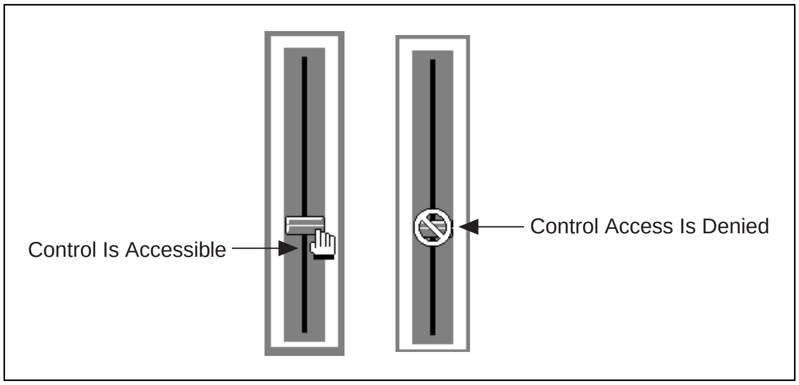
Control Security

Several object classes in Lookout*Direct* support control security, including such control objects as the Pot, Switch, Pushbutton, RadioButtons, and TextEntry, along with a few driver objects. Each class provides some type of control—Pots control numeric output signals, and Switches and Pushbuttons control logical output signals. Each class accepts the **control security level** parameter, which determines whether an operator can control the object. Refer to the online PDF Lookout*Direct Object Reference Manual* for additional information about control object properties.

With control security, Lookout*Direct* compares the security level control of an object to the security level of the currently logged-on account (the operator) to determine if an operator can control (write to) a particular object.

With network security, Lookout*Direct* checks the user account permissions configured for an object or process to determine if an operator can control (write to) a particular object. The user can adjust a control, but the process does not accept the input and the control will return to its original value.

Under control security, if the account security level is equal to or higher than that of the object, the mouse cursor changes into a hand when positioned over the object and the operator can adjust and control the object.



If the account security level is lower than that of the object, the cursor changes into the international symbol for forbidden, and the operator cannot control the object.

You can implement this feature on an object-by-object basis, either through the individual security level set in the object properties dialog box, or by assigning permissions. System integrators can secure high priority Switches, Pots, and Pushbuttons from operators while still allowing operators to adjust lower-level security objects. Refer to the *Configuring Security for Processes and Objects* section for more information on assigning permissions.

Lookout*Direct* globally applies the Control Panel object security setting to all individual objects on that panel and assigns the higher security level (either the control panel or the individual object) when determining whether an operator can access an object. Refer to the discussion of the *Panel* object in the online PDF Lookout*Direct Object Reference Manual* or the online help for additional information.

Viewing Security

Lookout*Direct* provides viewing security for control panels, controllable objects, and system settings. With these security options, you can restrict access to control panels, objects, and Windows system resources.

Control Panels

A Control Panel object defines viewing security for the entire control panel. For example, if you set Viewing security to level 6 on a particular panel, operators with level 5 or lower cannot view that control panel and might not even know that panel exists. If a level 6 (or higher) operator logs on, the control panel instantly becomes available for display. This feature is useful for hiding panels that are rarely used or that contain sensitive information.

Controllable Objects

Controllable objects such as Pots, Switches, Pushbuttons, and so on have a writable data member called `visible`. When `visible` is true, you can see the object on a control panel. When `visible` is false, you cannot see or adjust the object. To ensure that the object is always visible when it is first created, `visible` defaults to true.

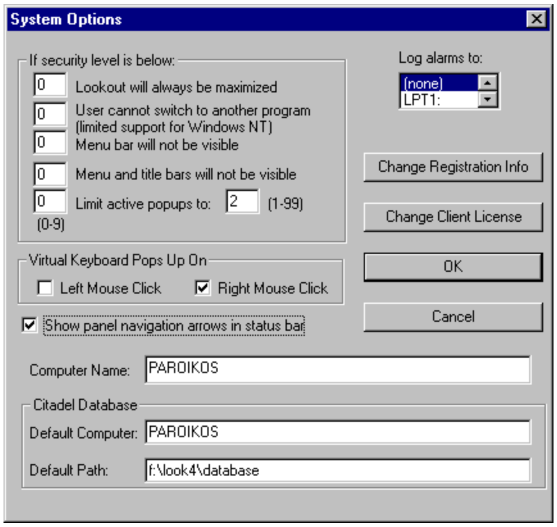
You can connect the `visible` data member of a controllable object (for example, a Pot object) to a controller mode indicator. When the controller is in computer control mode, the `visible` data member of the Pot might be true, allowing the operator to see the Pot and adjust the setpoint. But when the controller is not in computer control mode, the `visible` data member might be false, hiding the Pot from the operator and prohibiting operator control.

You can also use the `username` or `seclevel` data members of the $System object to control the visibility of a control object, depending on the name or security of the person logged on to Lookout*Direct* at any given time.

You can also configure network security permissions on these data members.

System Security Settings

With the **Options»System** menu command, you can define system options in the **System Options** dialog box to keep Lookout*Direct* maximized, the menu bar invisible, title bars invisible, and pop-ups to a minimum.



If security level is below:

0 Lookout will always be maximized

0 User cannot switch to another program (limited support for Windows NT)

0 Menu bar will not be visible

0 Menu and title bars will not be visible

0 Limit active popups to: 2 (1-99)

(0-9)

Log alarms to: (none) LPT1:

Virtual Keyboard Pops Up On

☐ Left Mouse Click ☑ Right Mouse Click

☑ Show panel navigation arrows in status bar

Computer Name: PAROIKOS

Citadel Database

Default Computer: PAROIKOS

Default Path: f:\look4\database

Lookout*Direct* will always be maximized—When you enter a security level, Lookout*Direct* prohibits users below that security level from closing Lookout*Direct*.

Users cannot switch to another program—This prevents an operator from using <Alt-Tab> to switch from Lookout*Direct* to some other program running on the computer. For this feature to work properly under Windows NT, you must install the Lookout*Direct* NT keyboard driver when you install Lookout*Direct*.

Menu bar (and title bars) will not be visible—When you enter a security level, users below that security level cannot view the menu bar or the title bar and, therefore, cannot change to a different Windows application.
This feature is not completely supported under Windows NT 4.0. With Windows NT 4.0, you can still use <Ctrl-Esc> or the Windows key to activate the Windows **Start** menu or <Ctrl-Alt-Delete> to bring up the Task Manager.

Limit active popups to—This option requires two values: a security level and the number of pop-ups. Users below that security level can view up to the specified number of pop-ups at one time. This feature keeps new users from becoming lost.

Network Security

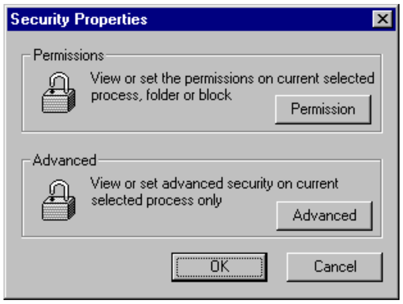
Lookout*Direct* development security is modeled after Windows NT security but is supported for Lookout*Direct* processes running on Windows 98/95 as well. Users with the ability to access processes or elements within a process are organized into groups. You can limit group and user access to processes, folders, and objects.

Configuring Security for Processes and Objects

You can control access privileges by user or group, applying restrictions to processes, folders within a process, or individual objects. You can configure security in the tree views contained in the Lookout*Direct* Object Explorer, the Lookout*Direct* Connection Browser, the **Edit Connections** dialog box, or the **Insert Expression** dialog box.

You cannot configure security for a network node, for your local computer, or for any Lookout*Direct* global objects such as $Keyboard or $System. You must select a process, a folder within a process, or an object within a process or process folder to configure security.

Right-click on the process or object you want to configure security for and select **Configure Security**. The **Security Properties** dialog box appears.


Security Properties

Permissions

View or set the permissions on current selected process, folder or block

Advanced

View or set advanced security on current selected process only

From this box, you can either set **Permissions**, or do **Advanced** security configuration by clicking on the appropriate button.

Permissions

With permissions, you can set individual access privileges for a given process, a folder holding a collection of objects, or individual objects.

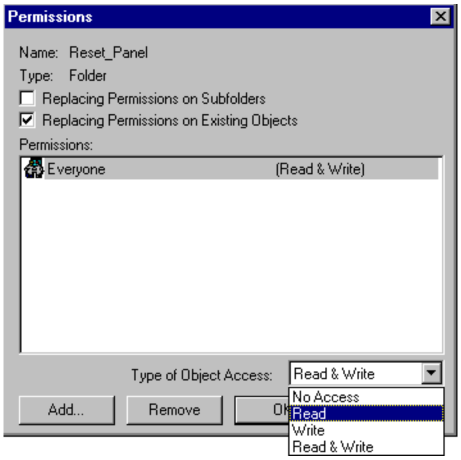
Configure security permissions using either the Lookout*Direct* Object Explorer or the Lookout*Direct* Connection Browser.

Lookout*Direct* objects inherit the permission status of the process or folder in which they are created. When you first create a process in Lookout*Direct*, it has full read and write permission granted to the Everyone group, by default. Any folder or object you create in the process has the same permission.

If you change the permission of the process or of one of the folders, any objects you create after the change have the permission status of the parent process or folder. Changing the permissions of a process or folder does not always change the permissions of an object or folder that already exists in that process, depending on how you set the **Permissions** dialog box options.

If a process has one set of permissions, and a folder under that process has a different set, the objects created under the folder will inherit the permission status of the folder only.

Select **Permission** from the **Security Properties** dialog box. The **Permissions** security properties dialog box appears.



Permissions

Name: Reset_Panel
Type: Folder
□ Replacing Permissions on Subfolders
☑ Replacing Permissions on Existing Objects
Permissions:

Everyone	(Read & Write)

Type of Object Access: Read & Write

The dialog box in the illustration above shows everyone with access to Lookout*Direct* having permission both to read and write all the controls in the `Reset_Panel` folder of the `Server_1` process.

Your options are to substitute individual users or groups for the Everyone group, and give each user or group the appropriate permission. You can refuse access, permit reading or writing only, or allow both reading and writing.

Note Remember that permissions in Lookout*Direct* are cumulative. For your individual user and group permissions to have any effect, you must delete the Everyone group after you set your other permissions. Refer to the *Special Users and Groups* section for more information on the Everyone group.

Select the user or group you want to assign permissions for. Select the appropriate security level in the **Type of Object Access** list in the lower right section of the dialog box. When you are done, select **OK**.

By selecting or disabling **Replacing Permissions on Subfolders** and **Replacing Permissions on Existing Objects**, you can restrict that permission to the process, folder, or object you selected, or extend the permission application in different ways and to different degrees.

In the simplest case, if you have selected an individual object, you can only change the permissions on that object.

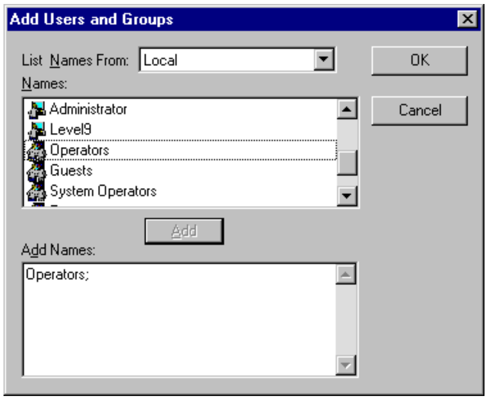
If you selected a process or folder, the options function as shown in the following table.

Table 6-1. Options for Propagating Changes in Security through a Process

Options Selected	Result
neither	Only the selected process, folder, or object has its security configuration changed.
Replacing permissions on subfolders	Changes permissions on the selected process or folder, all the folders under it, and any subfolders under them. This option is disabled when an individual object is selected.
Replacing permissions on existing objects	Changes permissions on all the individual objects contained immediately under the selected process or folder, but does not change permissions on any folder or subfolder, or any object in them. This option is disabled when an individual object is selected.
both	Changes permissions on all the individual objects contained immediately under the selected process or folder, as well as on any folder or subfolder, and all the objects in them.

To remove a user or group entirely from the permissions list, select the user or group and click on the **Remove** button.

To add a user or group, click on the **Add** button. The following dialog box appears.



List Names From: Local

Names:

- Administrator
- Level9
- Operators
- Guests
- System Operators

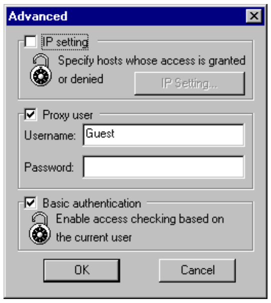
Add Names: Operators;

Select a user or group account in the top window and click on the **Add** button. Click on **OK** when you have selected all the users and groups you want to add.

Configure the security permissions for the added groups as described in the beginning of this section.

Advanced Security

You can set a number of advanced network security options in Lookout*Direct*, but only at the process level. These options are not available on the folder or object level. Click on the **Advanced** button in the **Security Properties** dialog box. The **Advanced** security properties dialog box appears.



☐ IP setting
Specify hosts whose access is granted or denied

☑ Proxy user
Username: Guest
Password:

☑ Basic authentication
Enable access checking based on the current user

There are three advanced security options: **Basic authentication**, **IP setting**, and **Proxy user**.

The default Lookout*Direct* setting is to have both **Proxy user** and **Basic authentication** enabled and the other option turned off.

As with other Lookout*Direct* security settings, the effects of multiple selections in this dialog box are cumulative. In other words, if a user had permission to read under **Basic authentication** and to write under **Proxy user**, then if both options are enabled the user would be able both to read and write.

Basic Authentication

When you select this option, Lookout*Direct* checks the account information of a user logging in to that instance of Lookout*Direct*. Security responds to the security level, individual account, and group permissions of that user account.

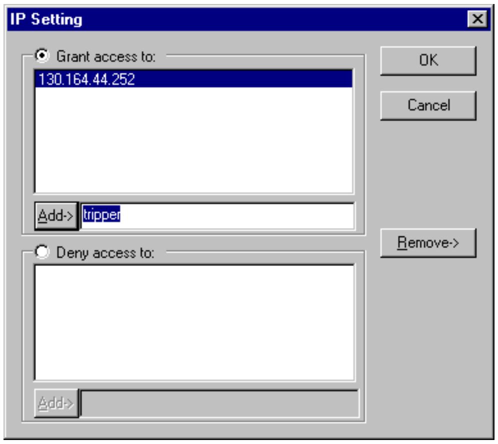
At this time, Lookout*Direct* cannot process the security status of a person logged on to another computer unless you install an identical `Lookout.sec` file on each computer running Lookout*Direct* on your network. Otherwise, if you have base authentication but not proxy access active on a server process, a person attempting to read from or write to a server from a remote computer cannot access the process unless you have configured the permissions for the Everyone group to have such access.

Activating the proxy access option in addition to the basic authentication option greatly increases your security options.

IP Setting

You can configure Lookout*Direct* to grant or deny access to any computer operating at a specific IP address. Click on the **IP setting** checkbox to enable this feature.

To grant or deny access by IP address, click on the **IP setting** button. The **IP Setting** dialog box appears.



IP Setting

● Grant access to: 130.164.44.252

Add-> tripper

○ Deny access to:

Only one of the IP setting options can be active at one time. Select whether you want to grant access or deny access to a given set of computers.

Note The IP access option functions in a literal way. If you choose to grant access to one or more computers using the IP setting option, those will be the only computers able to access the process or object you have applied the restriction to. If you choose to deny access to one or more computers using the IP setting option, all other computers using Lookout*Direct* will be allowed to access the process or object you have applied the restriction to, subject to the other security settings in place.

Enter the IP address you want to add, and click on the **Add** button. You can enter either the IP number itself, or the simple name of the computer. Whether you use the IP number or the simple computer name, the IP address for the computer appears in the list after you accept the entry.

Proxy Access

You can, if you choose, designate a specific local security account whose security level applies for any user accessing processes in your local instance of Lookout*Direct* from another computer (or another instance of Lookout*Direct* running on the local computer).

In other words, no matter who is logged on to another instance of Lookout*Direct*, the proxy account determines external access rights to a process or object operating under this option. The security level of the operator logged into the external instance of Lookout*Direct* is ignored.

The Guest user is built into Lookout*Direct*, specifically provided for this purpose, as well as for providing a visitor with a user account. You can edit the Guest user account properties in the User Manager.

To enable the proxy option, select the **Proxy** checkbox. Enter the **Username** of the account you want to serve as the proxy security account.

You must enter the valid **Password** for the user account for the proxy option to function.

When a user attempts to access your Lookout*Direct* process or objects from another domain, the user’s logon is recorded in the Lookout*Direct* events database. The user will be restricted to the security levels you have configured locally. You must configure any further access restrictions in the client process.

Keeping Security Precedence Simple

The Lookout*Direct* security system is flexible and designed for compatibility both with earlier versions of Lookout*Direct* and with planned future versions. This flexibility carries with it the risk of complexity.

It is not necessary to use every security feature in every Lookout*Direct* process. Keeping your security as simple as possible is the best approach. The following suggestions should help you keep your security simple.

- When converting a Lookout*Direct* process from Lookout*Direct* 3.8.*xx* or earlier, leave the control security in place when possible.
- In cases when you have both security parameters and network permissions set for an object, it is best to make sure that the security level parameters are consistent with permissions.

If you do find yourself with complex security setting interactions, the following principles should help you sort out how your interactions will work.

- User and group permissions are cumulative.

  For example, if user_A is a member of both Operators and System Operators, with the Operators group having read access and the System Operators group having Write access, user_A has both Read and Write access.
- Permissions and control parameter settings are cumulative.

  For example, if a control object has a security parameter set to 7, and user_A’s user account has a security level of 5, user_A cannot access the control. But if user_A is also a member of the Operators group, and the Operators group has a security level of 7, user_A can access the control.

  Additionally, if a control object has a security parameter set to 7, and user_A’s user account has a security level of 5, user_A will nevertheless have read permission if you use network security to grant read permission to user_A's user account.

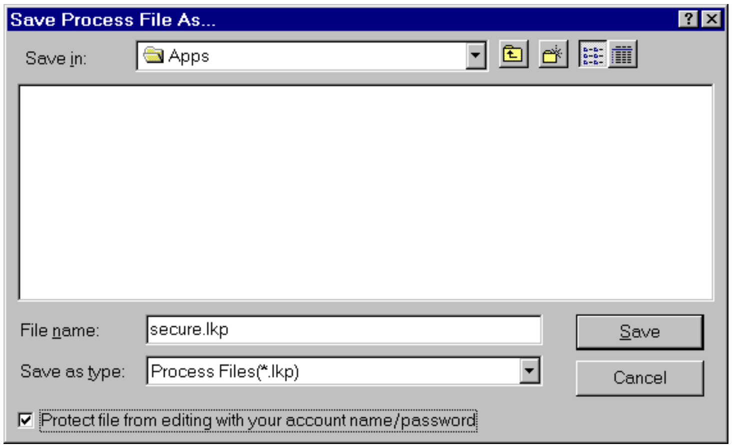
- The no access setting overrides all other permissions granted to a user or the user's group.

  For example, if user_A is granted a read access, and user_A is member of Operators, if the Operators group has been assigned no access, user_A has no access either.

  Additionally, if user_A is a member of both Operators and System Operators, and Operators group has been assigned no access, user_A has no access either—even if the System Operators group has read access.

Process File Edit Security

You can protect your process files from being edited by any other person without using the security accounts. Log in with an account name and a non-empty password, and select **File»Save As** from the menu. The following dialog box appears.



Save Process File As...

Save in: Apps

File name: secure.lkp

Save as type: Process Files(*.lkp)

☑ Protect file from editing with your account name/password

Check the **Protect file from editing with your account name/password** box at the bottom of the dialog box to save the file with your password as protection. To edit the file again, you have to log in under the same account with the same password.

Note You cannot open an encrypted file with an earlier version of Lookout*Direct*, even if you create an account with the same account name and password in that version.

Caution When you protect a process file, Lookout*Direct* does not save the `.LKS` file. Because the `.LKS` file serves as a backup file during application development, you should not use the encrypted-save feature until after you have completed your application and made a backup copy of both the `.LKP` and `.LKS` files on a separate archive disk.

Action Verification

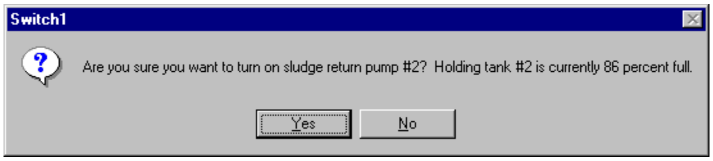
The Switch and Pushbutton object classes support action verification. When you define action verification for an object, Lookout*Direct* displays a message box stating your **Verify** message and prompts you to select either **Yes** or **Cancel**. If you click on **Yes**, Lookout*Direct* completes the previous operator command (for example, flips the switch or presses the pushbutton). If you **Cancel**, Lookout*Direct* ignores the previous operator command.

All action verification parameters accept text expressions, which can contain dynamic data. As an example, consider a switch that controls a pump responsible for filling a storage tank. However, that pump should not fill the tank if the water level is too high. You might enter an expression similar to the following for the switch **Verify On** parameter:

```
“Are you sure you want to turn on sludge return pump #2?
Holding tank #2 is currently ” & DATA_VARIABLE & “ percent
full.”
```

Refer to Chapter 1, *Expressions*, for more information about creating expressions using variables.

The warning message appears every time you turn on the switch. Notice the water level is dynamic—it changes to reflect the value of *`DATA_VARIABLE`* when the switch is flipped.


Switch1

Are you sure you want to turn on sludge return pump #2? Holding tank #2 is currently 86 percent full.

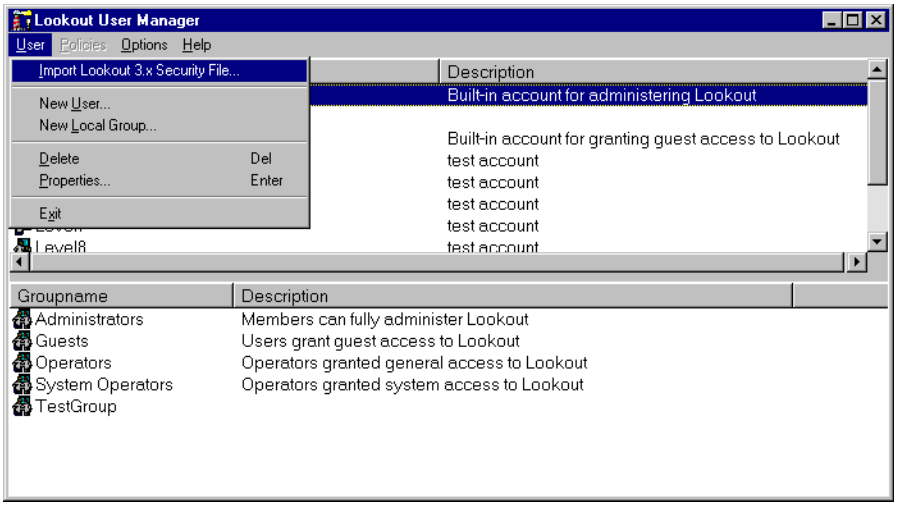
When you turn off the switch, no warning message appears because the **Verify Off** parameter was not specified. If you want to disable the **Verify On** warning message, delete the entire expression from the data field.

Caution Pushbutton verification works in much the same way. However, when you select **Yes**, the pushbutton creates only a momentary output signal. When action verification is enabled, it is impossible to hold the button down for any length of time.

Importing Old Security Files into Lookout*Direct* 4

You can import the user account information from your Lookout*Direct* 3.8 processes into Lookout*Direct* 4 using the Lookout*Direct* User Manager.

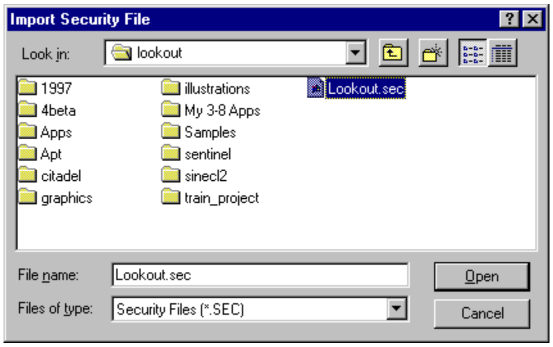
1. Select **Options»User Manager** from the Lookout*Direct* menu. You must be in edit mode for the **User Manager** item to appear in the **Options** menu. The **User Manager** dialog box appears.



Description
Built-in account for administering Lookout
Built-in account for granting guest access to Lookout
test account
test account
test account
test account
test account

Groupname	Description
Administrators	Members can fully administer Lookout
Guests	Users grant guest access to Lookout
Operators	Operators granted general access to Lookout
System Operators	Operators granted system access to Lookout
TestGroup	

2. Select **User»Import LookoutDirect 3.x Security File** from the **User Manager** dialog box. The following dialog box appears.



Look in: lookout

File name: Lookout.sec

Files of type: Security Files (*.SEC)

3. Navigate to your old Lookout*Direct* 3.8 security file `Lookout.sec`, and select it. Lookout*Direct* 3.8 kept the Lookout`.sec` security file in the Lookout*Direct* directory.

4. Click on **Open**.
5. If you have already created any user accounts in Lookout*Direct* 4 that are the same as accounts you used in Lookout*Direct* 3.8, you will receive a message informing you that a user account with that name already exists. You may replace your recently created account, or choose not to use the old account information.
6. Exit the User Manager.

⚠ **Note** Unlike Lookout*Direct* 3.8, Lookout*Direct* 4 maintains the Lookout`.sec` security file in the Windows `System` directory. The Lookout*Direct* 4 User Manager creates a unique identification number for each user account. For Basic Authentication to work properly, you must use the same Lookout`.sec` file for each copy of Lookout*Direct* running on your network. Copy your `Lookout.sec` file to the Windows `System` directory in every computer on which you intend to run Lookout*Direct*.