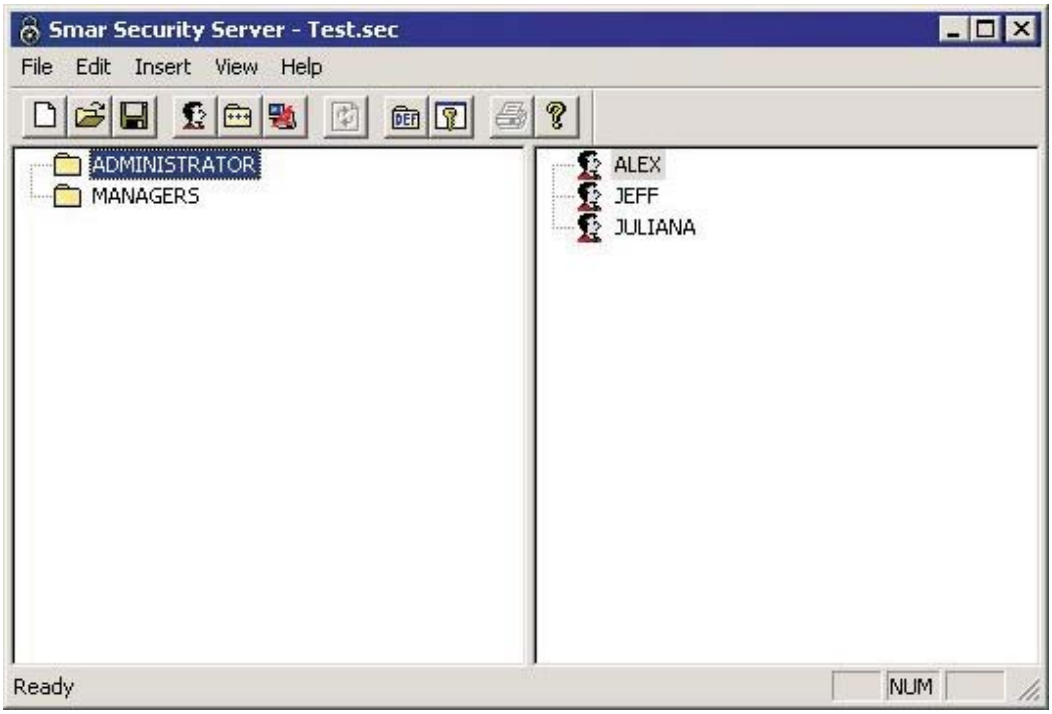
- Security Server

Security Server



Smar
First in Fieldbus

MAY / 06
Security Server
VERSION 8

FOUNDATION™

PVI EWSSVME

www.smar.com

Specifications and information are subject to change without notice.
Up-to-date address information is available on our website.

web: www.smar.com/contactus.asp

TABLE OF CONTENTS

INTRODUCTION TO THE SECURITY SYSTEM

The ProcessView security system provides restricted access to ProcessView functions based on the concept of a logged-in user. A security system administrator configures the system by adding users and assigning them specific ProcessView privileges. In addition, administrators may associate users with certain administrator-defined groups that also have assigned privileges. Thus, a user has the effective rights of all the groups to which he or she belongs plus his or her own private rights.

NOTES
The user/group concept for security assignment is well established in computer operating systems (such as Microsoft Windows NT) and computer networks (such as Novell Netware). This document assumes that the reader has an understanding of these concepts. ProcessView Version 8.0 includes the ability to use SAFLINK biometric authentication instead of or in conjunction with manual user names and passwords. For more information, please see the "Security Using SAFLINK Devices" application note on the ProcessView product CD

Secured Items

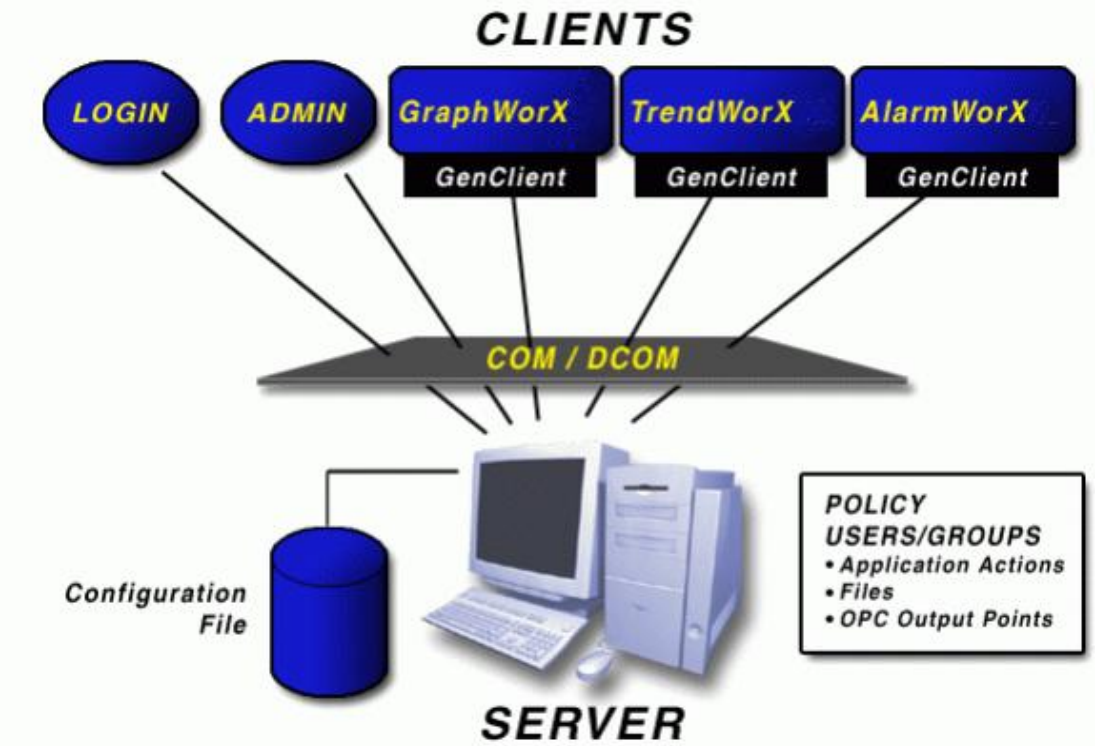
Security protection is applied to the following items within the ProcessView system:

- Application actions
- Process output points
- Critical points
- Alarms
- Files
- Custom strings
- Stations

Security System Components

The security system consists of a Security Server and several security clients. The clients communicate with the server via Microsoft COM/DCOM and therefore can optionally execute on network nodes other than the Security Server Node.

The security system provides two special purpose security clients: one for user login (the Security Login application) and another for administration of the Security Server (the Security Configurator). The rest of the security system clients are the other applications in the ProcessView family (e.g. GraphWorX, TrendWorX, AlarmWorX, etc.). Any stimulus (e.g. a user login or logout) that causes a change in security status will be immediately posted to the affected clients.



Security System Components

Installation

The security system is installed as part of the ProcessView installation. The Security Login client is also installed as part of the Security Server installation.

If you have not configured at least one security administrator, you do not have to enter a password to run the Security Configurator.

Security Server Configuration

The Security Configurator allows Security Server administrators to configure security settings for users and groups. You must enter an administrator password to use the Security Configurator. Configuration of the security system is accomplished by running the Security Server Configurator ("security.exe") in interactive mode. The Security Server may be launched in interactive mode from the ProcessView program group, or from other ProcessView applications while they are in configuration mode.

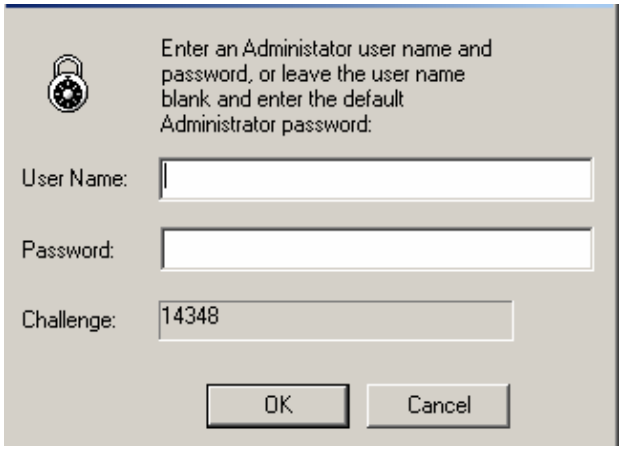
Administration Login

To start the Security Configurator:

1. From the Windows **Start** menu, select **Programs > Smar ProcessView > Tools > Security Configurator.**
2. This opens the **Security Server Administrator Login** dialog box, shown in the figure below. You must enter one of the following to proceed to configuration:

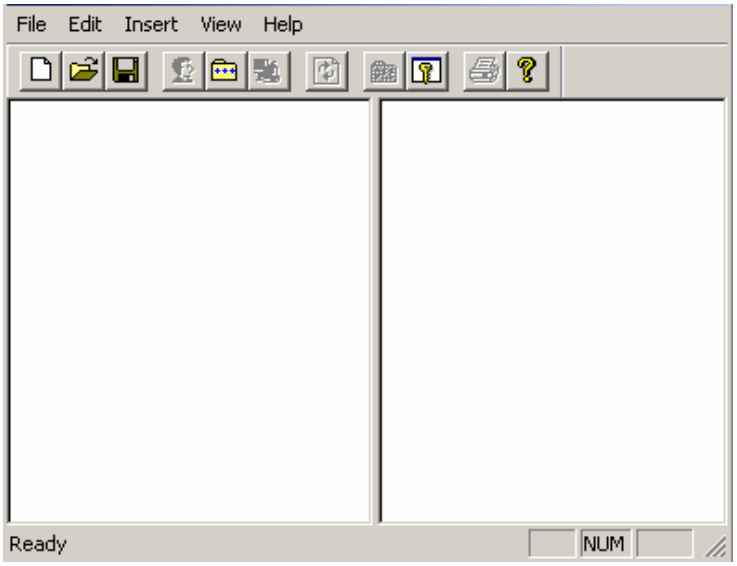
- A **User Name** and **Password** for a user that has previously been configured as a Security Administrator.
- An emergency password you received from technical support based on the challenge code shown in the login dialog box.

NOTE
If you have not configured at least one security administrator, you do not have to enter a password to run the Security Configurator.



Security Server Administrator Login

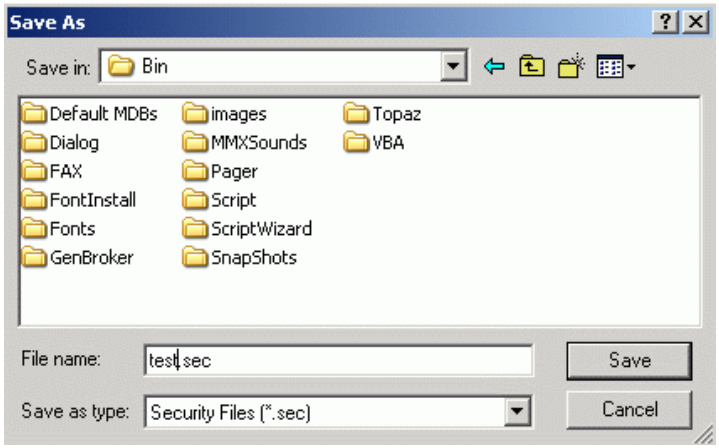
3. When you log in, the **Security Server Configurator** screen opens, as shown in the figure below. The Security Configurator consists of two separate panes. Both panes of the view will be empty when you first log in. Each pane has a tree control. The left tree is the **Group View.** Here the root nodes are groups, and the child nodes are the users that belong to the group. The right tree is the **User View,** in which the root nodes are users, and the child nodes are the groups that have been assigned to each user.



Blank Security Configuration

4. The first time you log in, you will be asked to specify a file name and location for your security configuration file. Future sessions will automatically load this file on startup. To change the name and/or location, choose **Save As** from the **File** menu. You must save the security configuration in a file. Specify a file name in the **Save As** dialog box. This file is saved in your ProcessView installation folder.

NOTE
The most recently used .sec file is always the currently active security configuration.



Saving the Security Configuration

Toolbar

The Security Configurator toolbar, shown below, contains the following command functions. For more information about these functions, please refer to the **Menus** section.

- **New:** Creates a new security configuration (.sec) file.
- **Open:** Opens an existing security configuration (.sec) file.
- **Save:** Saves the current security configuration (.sec) file.
- **New User:** Creates a new security user profile.
- **New Group:** Creates a new security group profile.
- **Associate Users With Groups:** Links a user to a group, or a group to a user.
- **Refresh:** Synchronizes users and groups with the Windows NT security database.
- **Default Group:** Opens the properties dialog box for the default security group.
- **Application Actions:** Defines which users and groups have access rights to specific ProcessView applications and actions.
- **Print:** Prints the current security configuration.
- **About:** Opens the About Box, which contains information about the application.

Security Configurator Toolbar

Menus

The Security Configurator contains the following menus:

- **File**
- **Edit**
- **Insert**
- **View**
- **Help**

File Menu

The **File** menu contains the following commands:

COMMAND	SHORTCUT KEYS	FUNCTION
New	CTRL+N	Creates a new security configuration (.sec) file.
Open	CTRL+O	Opens an existing security configuration (.sec) file.
Save as		Saves the current security configuration (.sec) file with a new name.
Exit		Closes the application.

Edit Menu

The **Edit** menu contains the following commands:

COMMAND	SHORTCUT KEYS	FUNCTION
Edit	Enter	Opens the properties dialog box for the currently selected user or group.
Rename		Renames the currently selected user or group.
Delete	Del	Deletes the currently selected user or group.
Duplicate		Makes a copy of the currently selected user or group.
Global settings		Sets the global security policy and critical points.
Default group		Opens the properties dialog box for the default security group (disabled in basic security mode).
Application actions		Defines which users and groups have access rights to specific ProcessView applications and actions.

Insert Menu

The **Insert** menu contains the following commands.

COMMAND	Function
NEW USER	Creates a new security user profile.
NEW GROUP	Creates a new security group profile.
ASSOCIATE USER & GROUP	Links a user to a group, or a group to a user.

View Menu

The **View** menu contains the following commands.

COMMAND	Function
TOOLBAR	Shows/hides the Security Configurator toolbar.
STATUS BAR	Shows/hides the Security Configurator status bar.
SYNCHRONIZE WITH NT	Synchronizes users and groups with the Windows NT security database.
BASIC MODE	Simple security configuration for beginners.
ADVANCED MODE	Advanced security configuration for experts. Also converts from basic security mode to advanced security mode.

Help Menu

The **Help** menu contains the following commands:

COMMAND	Function
HELP TOPICS	Opens the help documentation associated with this application.
ABOUT APPLICATION	Opens the Smar About Box, which provides the version number and copyright information for this application.

Security Configuration Modes

The Security Server supports three general modes of security configuration. The security mode is specified in the Security Configurator:

- Basic security mode
- Advanced security mode
- Integrated NT security mode

The Security Server can run in "basic" mode or "advanced" mode. **Basic mode** is suggested for first time users of the Security Server. The **advanced mode** is equivalent to the only security mode in previous versions (prior to version 7.x) of ProcessView.

NOTE
You can always convert a basic mode configuration to an advanced mode configuration at any time. However, the conversion from basic mode to advanced mode cannot be reversed (i.e. an advanced configuration cannot be converted to a basic configuration).

The integrated NT security mode automatically synchronizes users and groups with the Windows NT security database. The node on which the Security Server runs must have Windows NT, Windows 2000, Windows XP, or Windows Server 2003, but the client nodes can run on any Windows operating system (i.e. Windows 98, Windows Me, etc.).

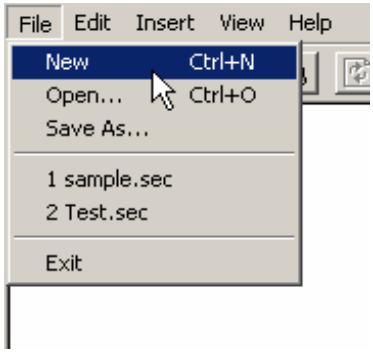
Basic Security Mode

Basic mode limits the configurability of the security system with the aim of easy configuration and predictable runtime results. The following restrictions are imposed when in basic mode:

- The **Default Group** is disabled for editing and allows no access at runtime.
- Only **User Properties** can be edited in the **User** dialog.
- Security access rights are assigned only to groups.
- A user must be associated with one and only one group. In basic mode, this association can be made directly from the **User Properties** dialog box.

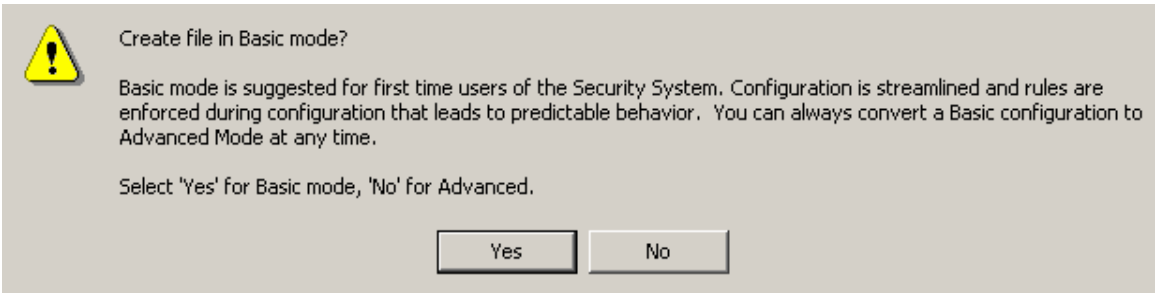
To configure the Security Server in basic mode:

1. In the Security Configurator, select **New** from the **File** menu, as shown in the figure below.



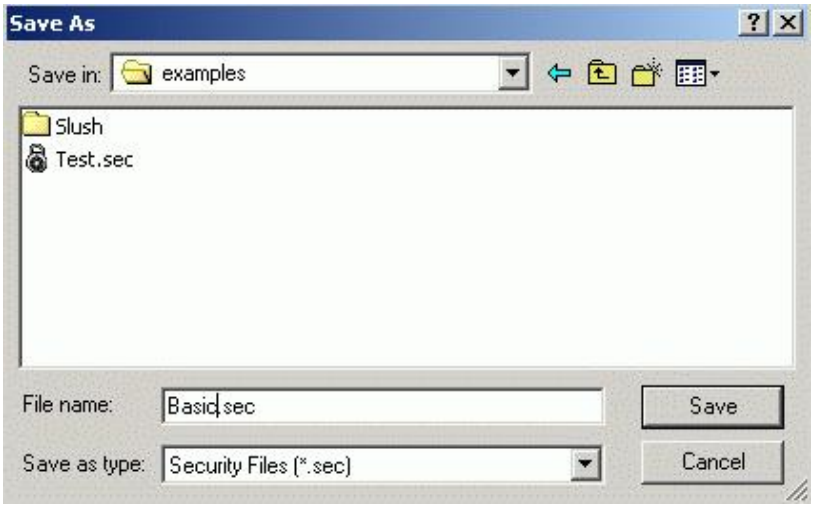
Creating a New Security Configuration

2. A dialog asks you if you want to create the file in basic mode. Click **Yes.**



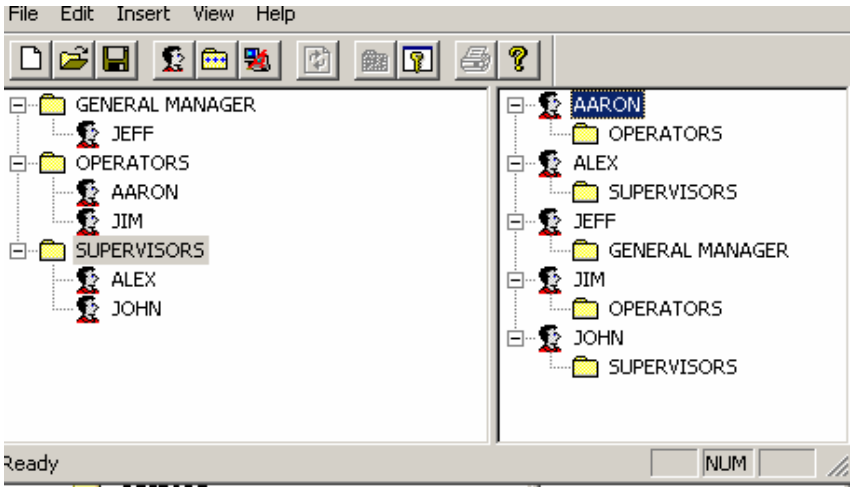
Creating a File in Basic Mode

3. The **Save As** dialog box opens, as shown in the figure below. Give the file a name, and then click **Save.**



Saving the File in Basic Mode

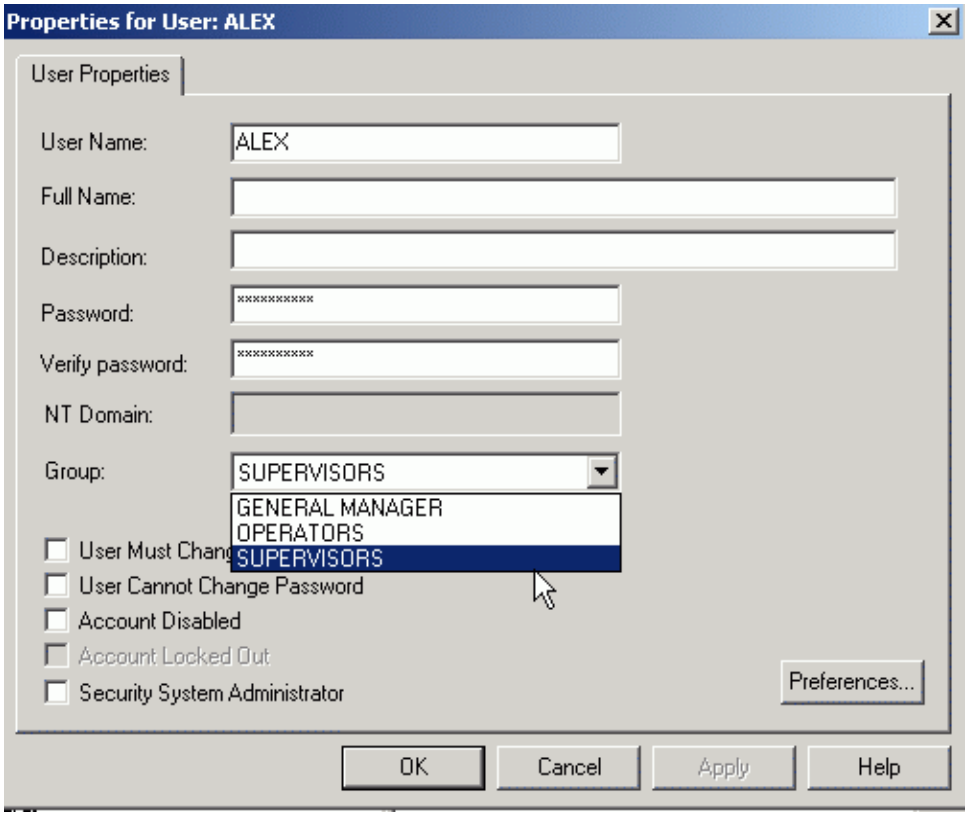
4. Configure users and groups as desired, as shown in the figure below. The **Default Group** is disabled for editing and allows no access at runtime. Thus, you will notice that the **Default Group** command on the **Edit** menu is unavailable.



Security Configuration in Basic Mode

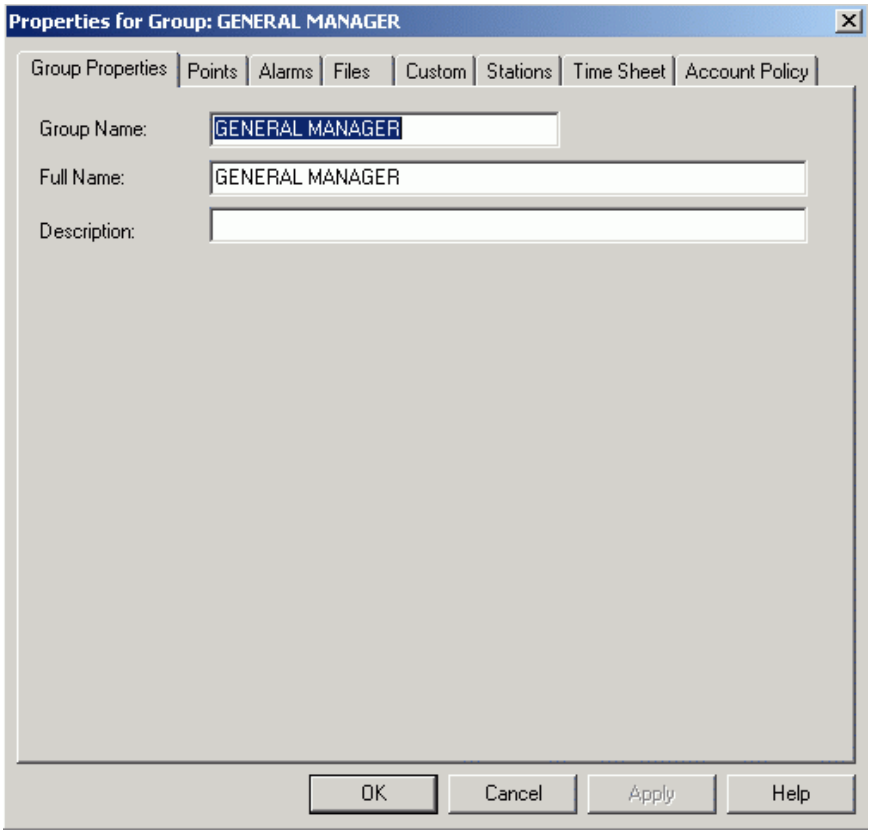
5. In basic security configuration mode, a user must be associated with one and only one group. In basic mode, this association can be made directly from the **User Properties** dialog box, as shown in the figure below. Enter a name and password for the user. You can associate the user with a group by selecting a group from the drop-down list under **Group.**

NOTE
The **Password** field is always filled in by default to disguise the password, but you should always change the password. The **Account Disabled** check box in the **User Properties** dialog is checked by default, so you must uncheck this box in order to activate the user's account.



Editing User Properties in Basic Security Mode

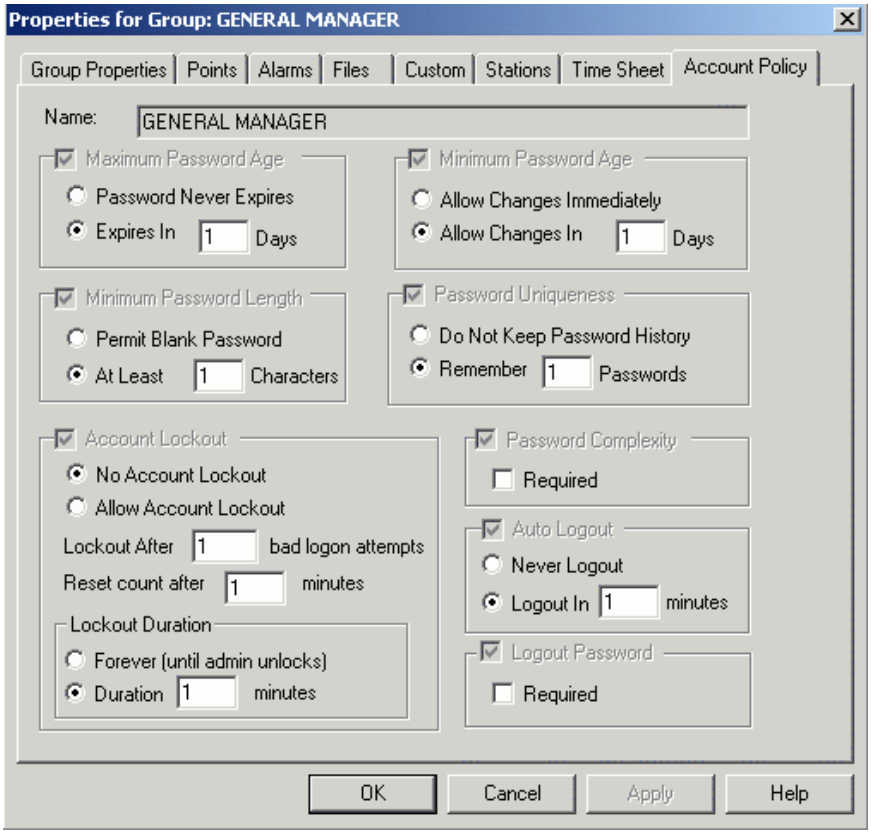
6. In basic security configuration mode, security access rights are assigned only to groups and are configured in the **Group Properties** dialog box, as shown in the figure below.



Editing Group Properties in Basic Security Mode

7. In basic security mode, the main **Account Policy** options are enabled by default, as shown in the figure below.

NOTE
For information about account policy settings, please see the **Account Policy** section.

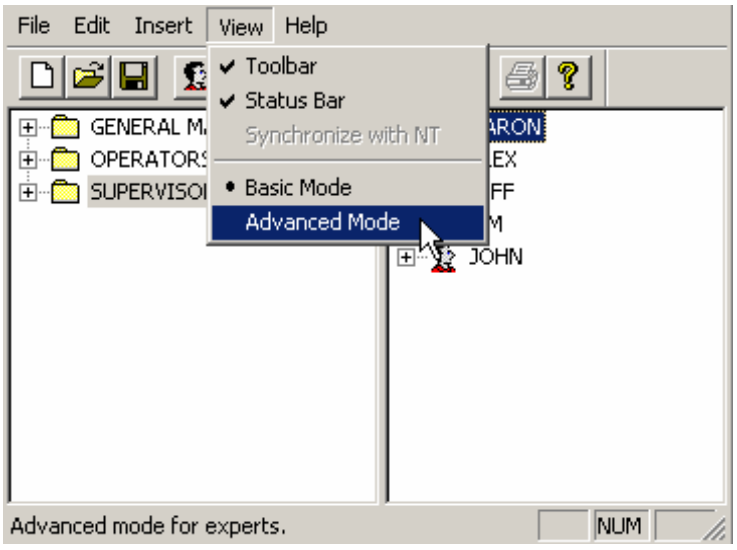


Editing Account Policy in Basic Security Mode

Switching From Basic Mode to Advanced Mode

You can convert a basic mode configuration to an advanced mode configuration at any time:

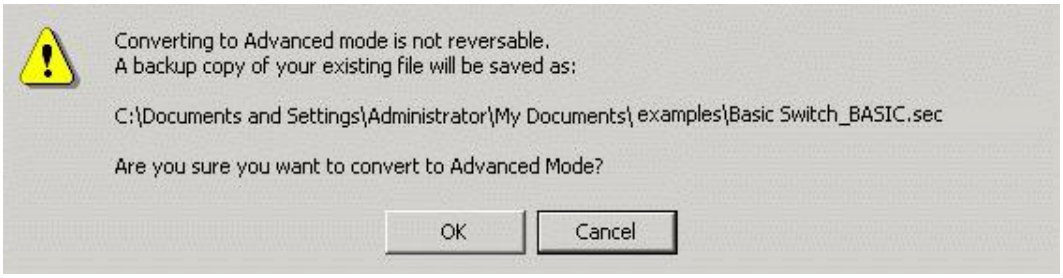
1. Select **Advanced Mode** from the **View** menu, as shown in the figure below.



Switching From Basic Mode to Advanced Mode

2. A warning message appears asking you to confirm the switch to advanced mode, as shown in the figure below. Click **OK** to convert to advanced mode.

NOTE
The conversion from basic mode to advanced mode cannot be reversed (i.e. an advanced configuration cannot be converted to a basic configuration), so the Security Configurator automatically creates a backup copy of your existing basic configuration in the same directory.



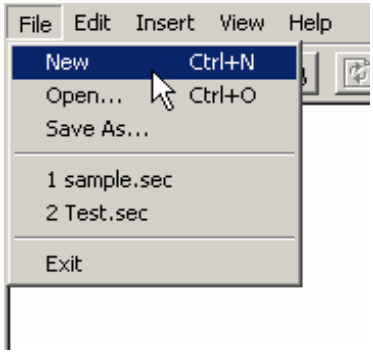
Confirming Switch from Basic Mode to Advanced Mode

Advanced Security Mode

The advanced security configuration mode is equivalent to the only security mode in previous versions (prior to version 7.x) of ProcessView.

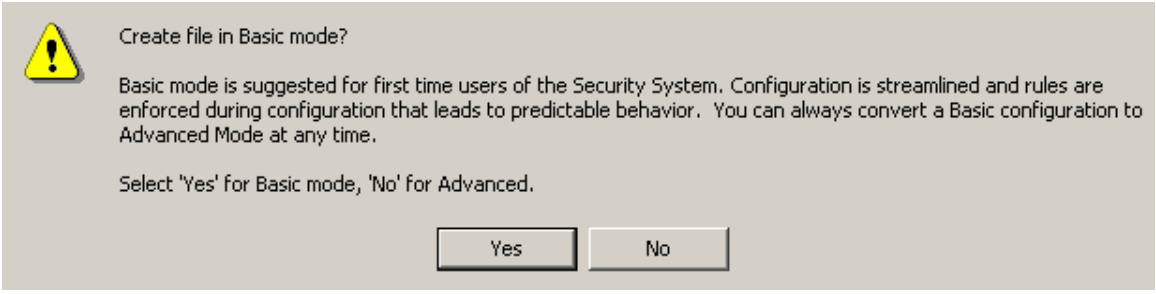
To configure the Security Server in advanced mode:

1. In the Security Configurator, select **New** from the **File** menu, as shown in the figure below.



Creating a New Security Configuration

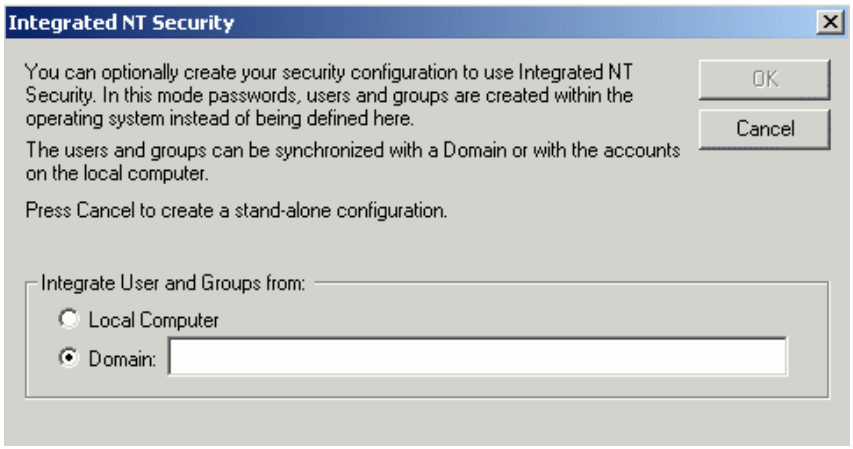
2. A dialog asks you if you want to create the file in basic mode. Click **No.**



Option to Create a File in Basic Mode

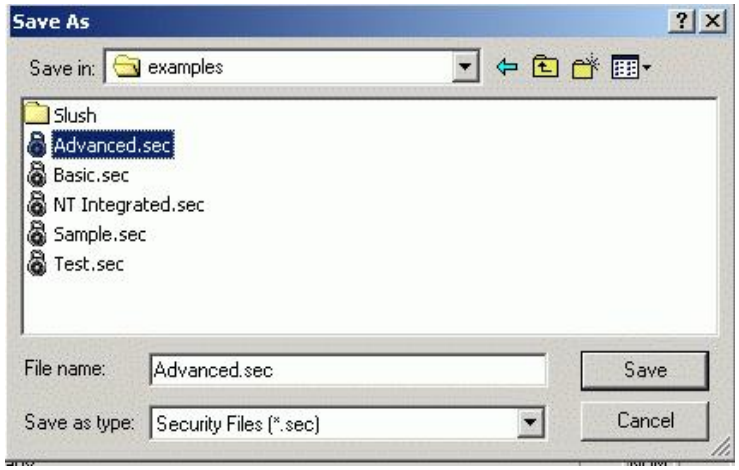
3. You are given an option to create a configuration in integrated NT security mode. Click **Cancel** to create a stand-alone advanced security configuration.

NOTE
For information about NT security, please see the "Integrated NT Security Mode" section.



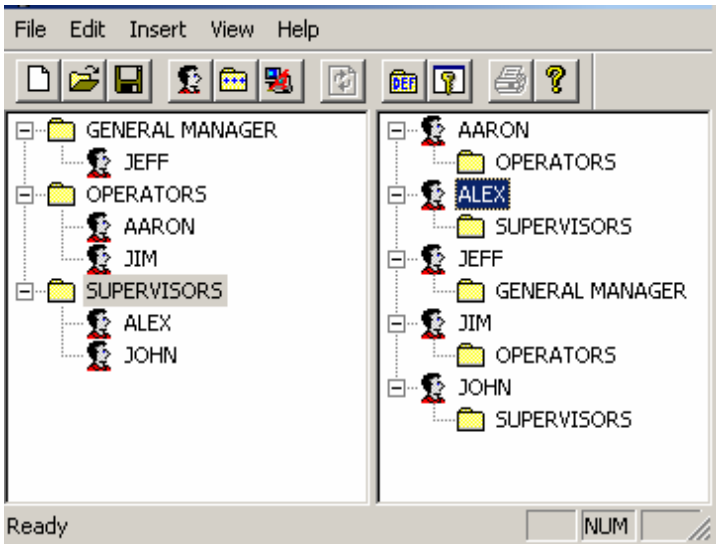
Creating a File in Advanced Mode

4. The **Save As** dialog box opens, as shown in the figure below. Give the file a name, and then click **Save.**



Saving the File in Advanced Mode

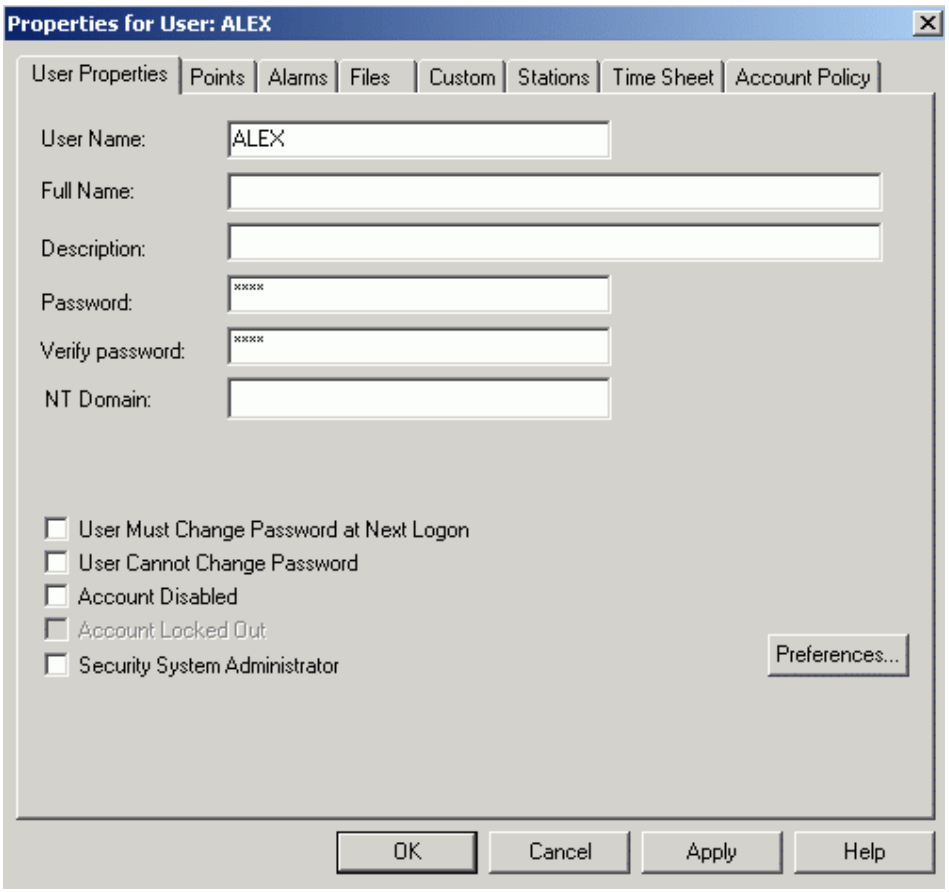
5. Configure users and groups as desired, as shown in the figure below. In advanced mode, the **Default Group** is enabled for editing under the **Edit** menu.



Security Configuration in Advanced Mode

6. In advanced security configuration mode, each user can be associated with multiple groups. Thus, security access rights are assigned to both users and groups and are configured in both the **Group Properties** and **User Properties** dialog boxes, as shown in the figure below. Enter a name and password for the user.

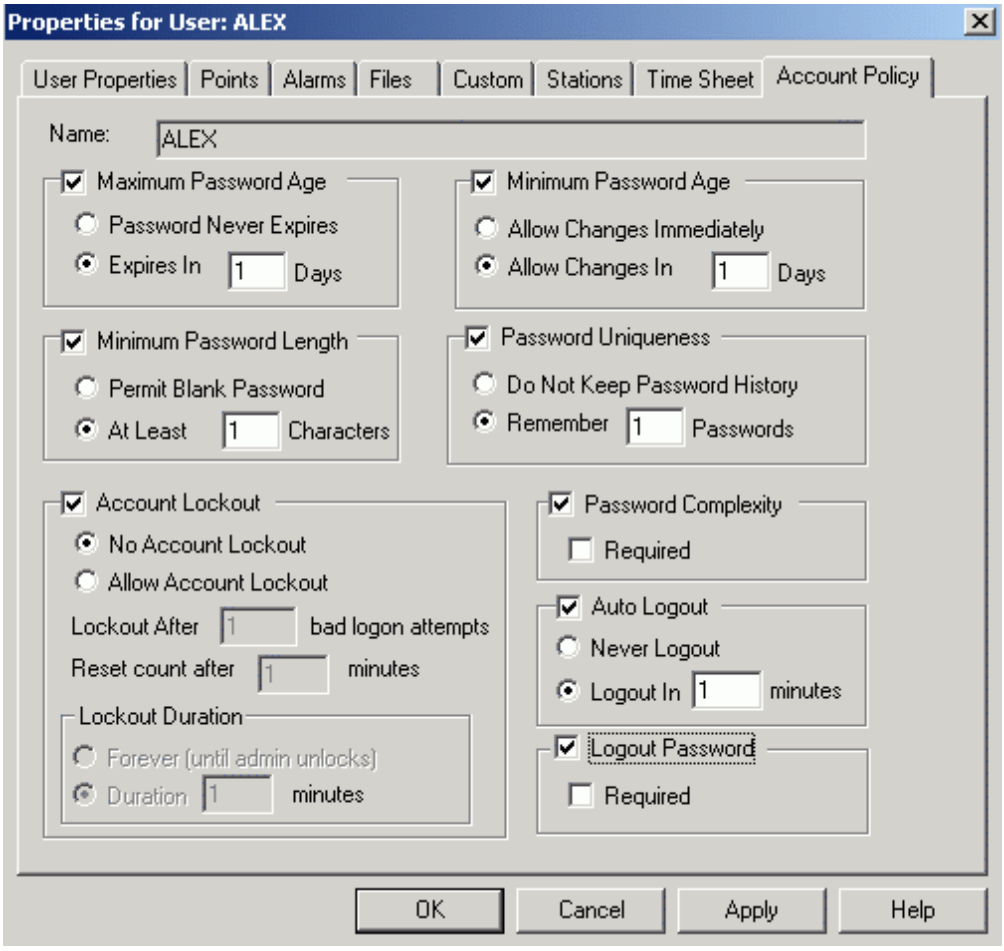
NOTE
The **Password** field is always filled in by default to disguise the password, but you should always change the password. The **Account Disabled** check box in the **User Properties** dialog is checked by default, so you must uncheck this box in order to activate the user's account.



Editing User Properties in Advanced Security Mode

7. In advanced security mode, all **Account Policy** options are available as shown in the figure below.

NOTE
For information about account policy settings, please see the **Account Policy** section.



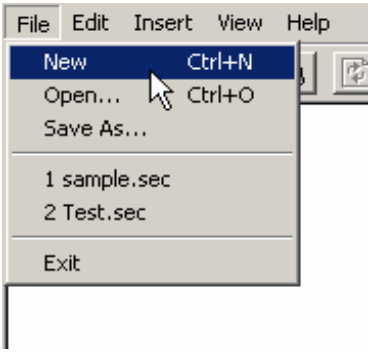
Editing Account Policy in Advanced Security Mode

Integrated NT Security Mode

The integrated NT security mode automatically synchronizes users and groups with the Windows NT security database. The node on which the Security Server runs must have Windows NT, Windows 2000, Windows XP, or Windows Server 2003, but the client nodes can run on any Windows operating system (i.e. Windows 98, Windows Me, etc.).

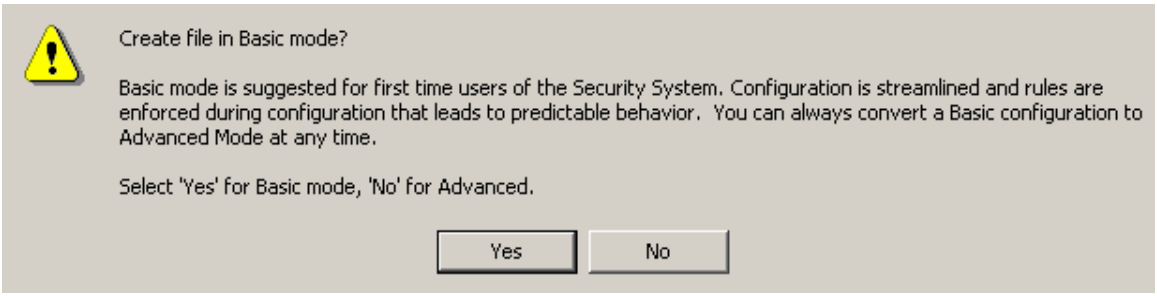
To configure the Security Server in advanced mode:

1. In the Security Configurator, select **New** from the **File** menu, as shown in the figure below.



Creating a New Security Configuration

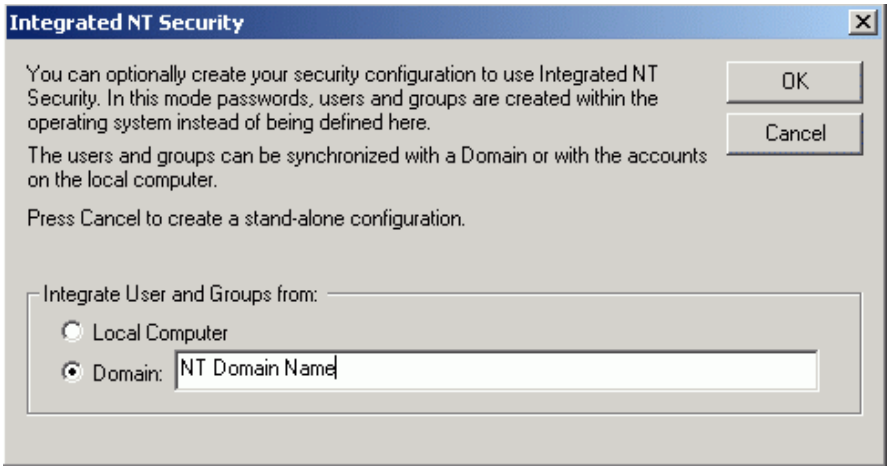
2. A dialog asks you if you want to create the file in basic mode. Click **No.**



Option to Create a File in Basic Mode

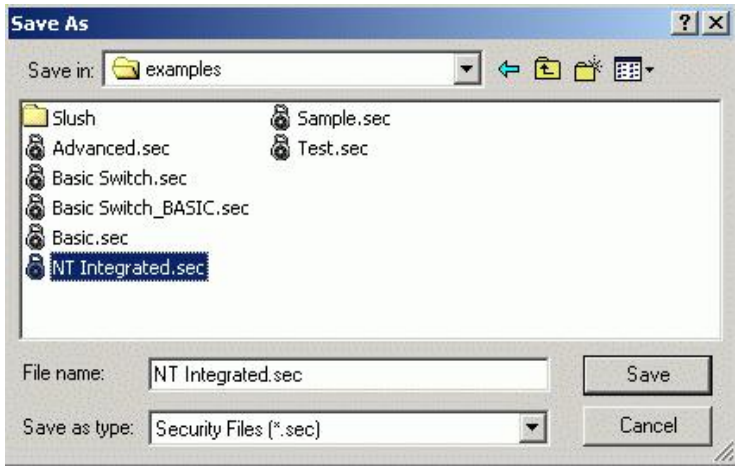
You are given the option to create a configuration in integrated NT security mode. Under **Integrate Users and Groups From,** select the **Domain** field and then enter the NT domain name in the **Domain** field**.** Click **OK.**

NOTES
Security can be configured only for a single NT domain. For testing purposes, you can select **Local Computer.** This creates a simulated integrated NT security configuration. The users and groups will be synchronized with the accounts on the local computer.



Specifying the NT Domain Name

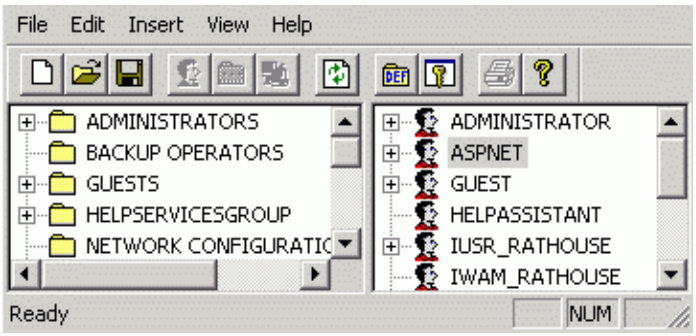
3. The **Save As** dialog box opens, as shown in the figure below. Give the file a name, and then click **Save.**



Saving the File in Integrated NT Mode

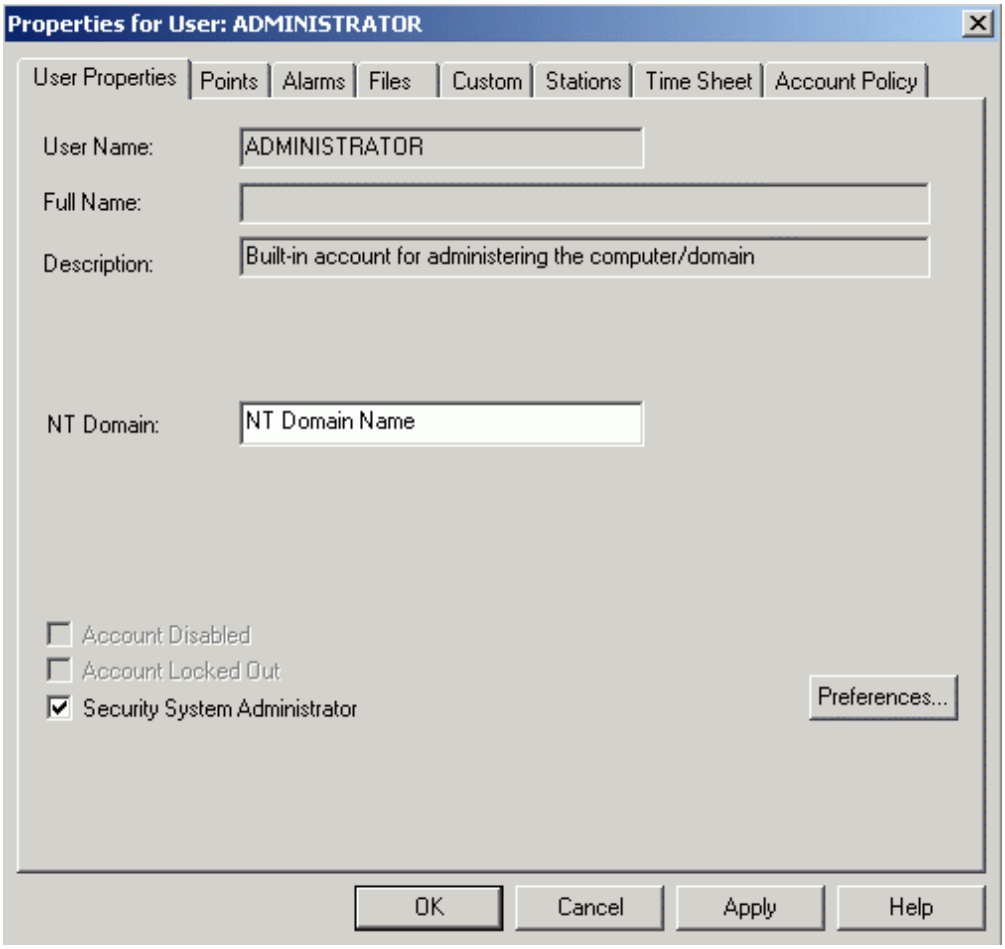
4. The Security Configurator automatically imports and synchronizes all users and groups and their passwords from the specified NT domain's security database. This eliminates the need to manage two different sets of passwords and password policies. In integrated NT security mode, you cannot add or remove users and groups, nor can you remove their associations. A network connection to the domain must be established in order for the Security Configurator to resolve user names and passwords.

NOTE
The Security Server periodically queries the operating system for any user and group changes to keep synchronized. The **NT Synchronization Period** is configured on the **Global Settings** dialog box; a value of 0 disables the automatic synchronization with NT. You can always manually synchronize by selecting **Synchronize With NT** from the **View** menu or by clicking the **Refresh** button on the toolbar.



Security Configuration in Integrated NT Mode

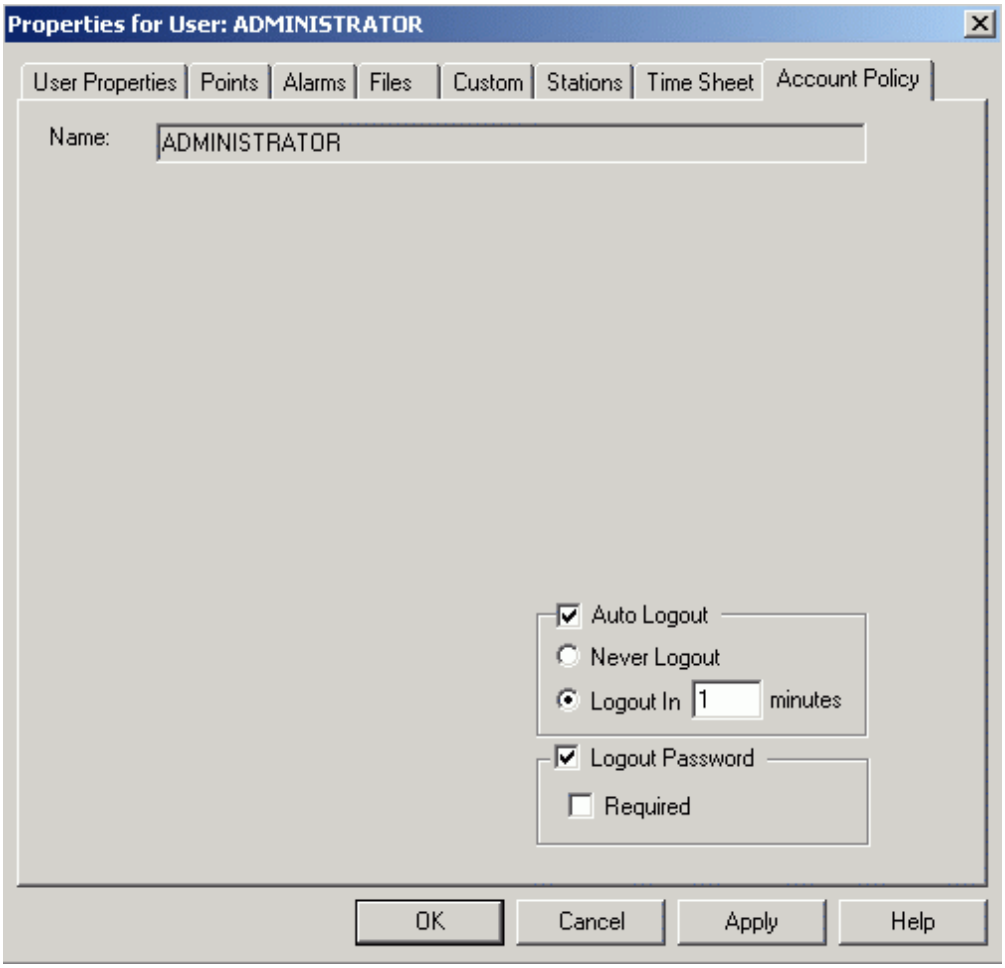
5. In integrated security configuration mode, all user and group associations as well as most security access rights and restrictions are defined by the NT domain's security settings. Thus, the **Group Properties** are read-only, and user options in the **User Properties** dialog boxes are limited, as shown in the figure below. The domain is specified in the **NT Domain** field. The only editable option is to specify a user as the **Security System Administrator.** It is still necessary to manage the access rights for users and groups (i.e. Points, Files, etc.) in the Security Configurator.



Editing User Properties in Integrated NT Security Mode

6. In integrated NT security mode, the **Account Policy** options are limited to **Auto Logout** and **Logout Password,** as shown in the figure below.

NOTE
For information about account policy settings, please see the **Account Policy** section.

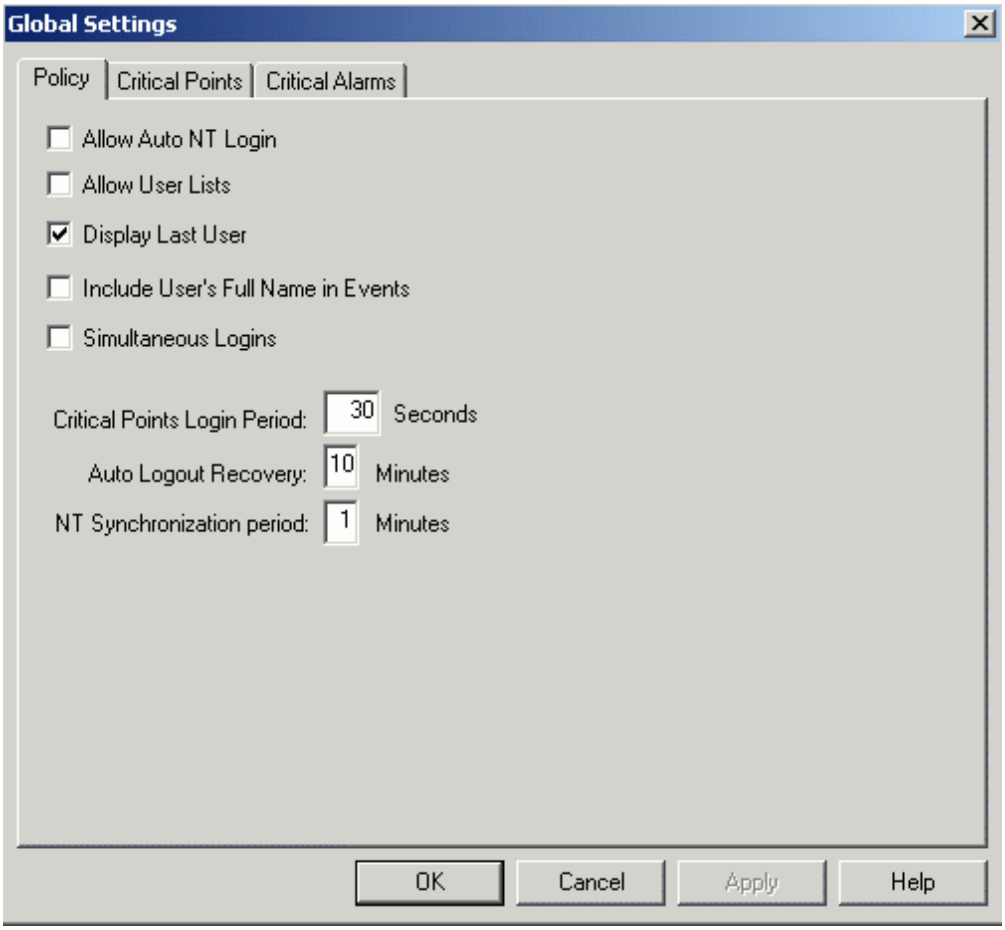


Editing Account Policy in Integrated NT Security Mode

Global Settings

A **Global Settings** menu entry and dialog are used to configure global security policy and critical points. The settings configured here affect the behavior of the security system for all users. In the Security Configurator, select **Global Settings** from the **Edit** menu. This opens the **Global Settings** dialog box, shown in the figure below, which has the following tabs:

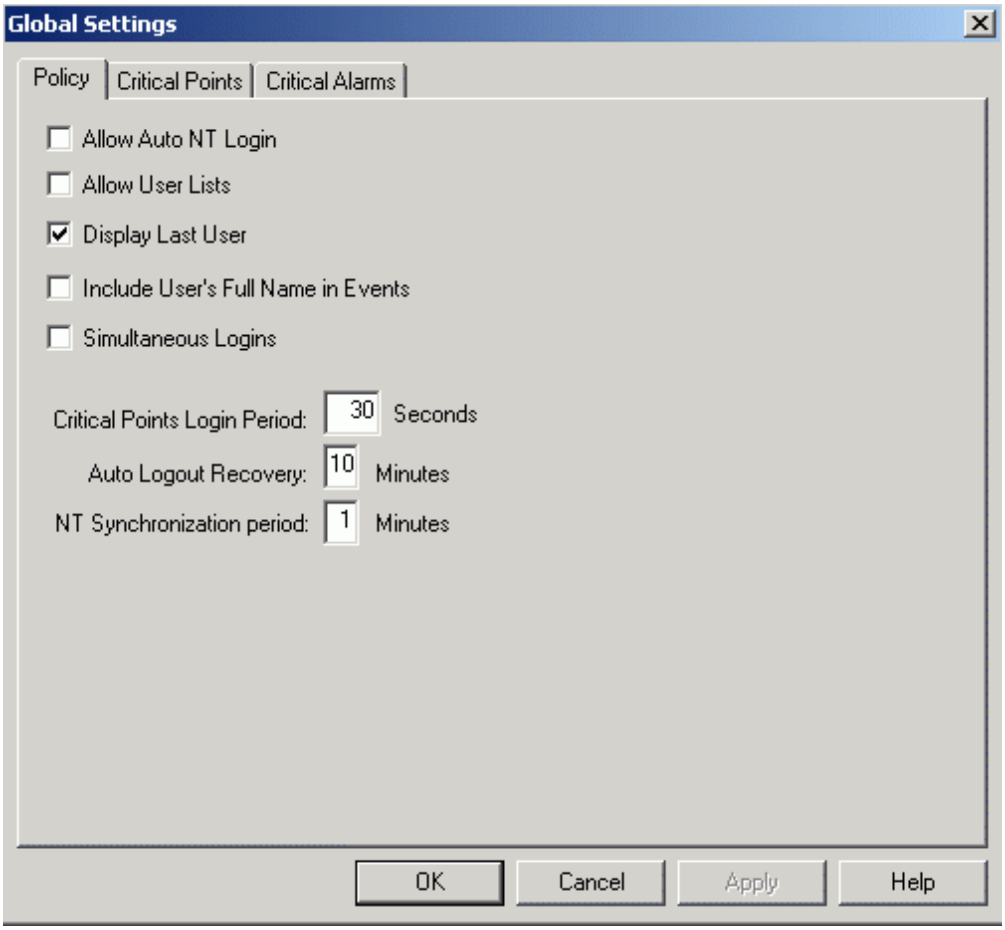
- Policy
- Critical Points
- Critical Alarms



Configuring Global Settings

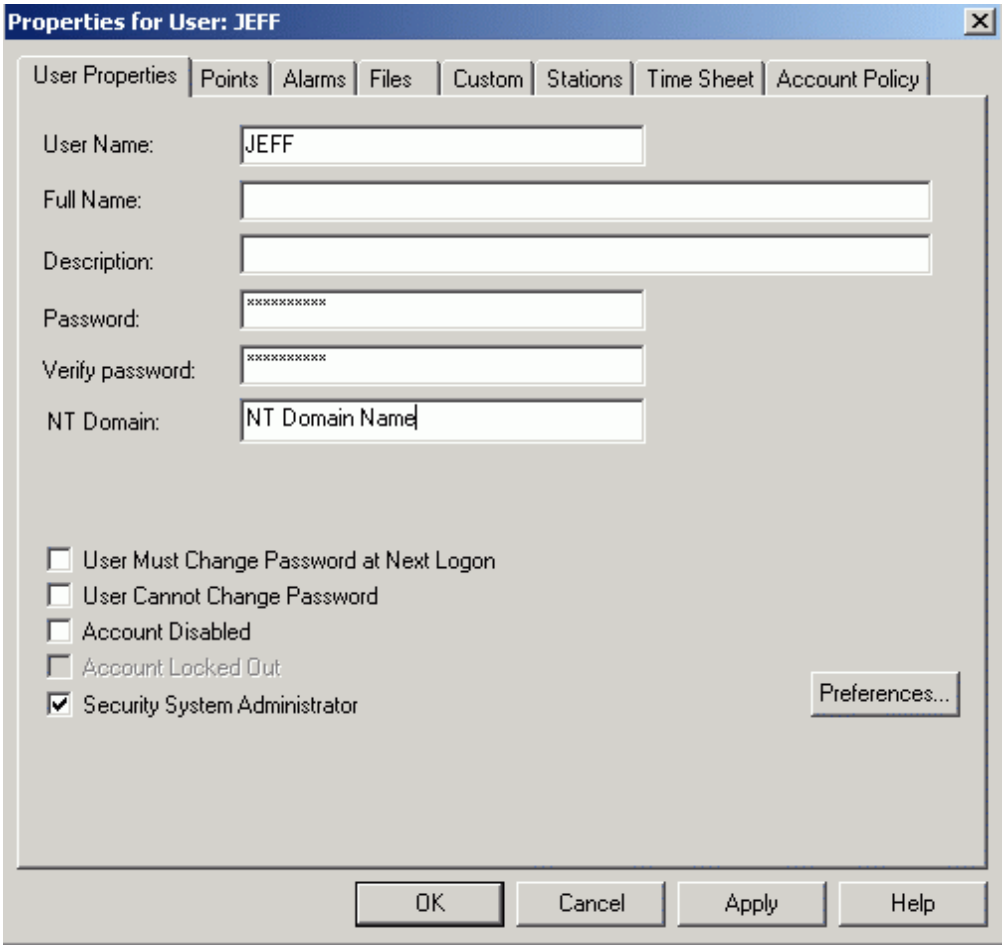
Global Policy

The **Policy** tab of the **Global Settings** dialog box, shown in the figure below, configures the following global security policy settings for all users.



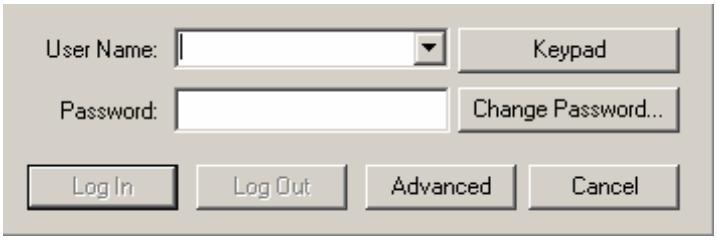
Configuring Global Security Policy Settings

Allow Auto NT Login: When this check box is checked, the **NT Domain** field is enabled in the **User Properties** dialog box, as shown in the figure below. When a domain name is specified, users with matching user names and domain names will be automatically be logged into the Security Server when the Security Login application is launched. This feature eliminates the need for users who have already logged into an NT domain to enter a user name and password a second time to gain access to the Security Server through the Security Login application. This feature, commonly referred to as "single sign-on," is available in all security modes (i.e. basic, advanced, and integrated NT). (Default is off.)



NT Domain Name Field Enabled in User Properties

Allow User Lists: When this box is checked, the **Security Login** dialog in the Security Login application displays a list of all users in a drop-down list next to the **User Name** field, as shown in the figure below. This allows users to log in by selecting their user name from a list instead of typing it in. This is often desirable for touch-screen systems. (Default is off.)



Security Login Dialog Box in Login Application

Display Last User: When this box is checked, the **Security Login** dialog in the Security Login application displays the name of the last user that successfully logged in the **User Name** field. (Default is on.)

Include User's Full Name in Events: When this check box is checked, the user's full name is included in audit messages sent to the GenEvent Server. The format is ***User name (Full Name).***

Simultaneous Logins: When this check box is checked, multiple users can be logged in at the same time from the same node. The rights granted will be the sum of the rights of all of the logged-in users. If **Simultaneous Logins** is not checked and a user logs in when someone is already logged in, the original user will be logged out. (Default is off.)

Critical Points Login Period: Amount of time (in seconds) after logging in that a user will be allowed to manipulate a critical point before being required to log in again.

Auto Logout Recovery: Amount of time (in minutes) after all security related requests from a node have ceased (e.g. when a client node crashes) that users from that node will be logged out. The range is 0-99 minutes, and default is 2 minutes. A value of 0 disables this feature (no auto-logout will occur based on lack of communication).

NT Synchronization Period: The frequency (in minutes) that the users and groups will be synchronized with the NT security database when using the integrated NT Security mode. A value of 0 disables all automatic synchronization. Manual synchronization can be performed any time by selecting **Synchronize With NT** from the **View** menu, or by pressing the **Refresh** button on the toolbar. This field is hidden when not using Integrated NT Security.

NT Domain: This is a read-only field that indicates the NT Domain name from which the Security Server gets its users and groups. This field is hidden when not using Integrated NT Security.

Critical Points

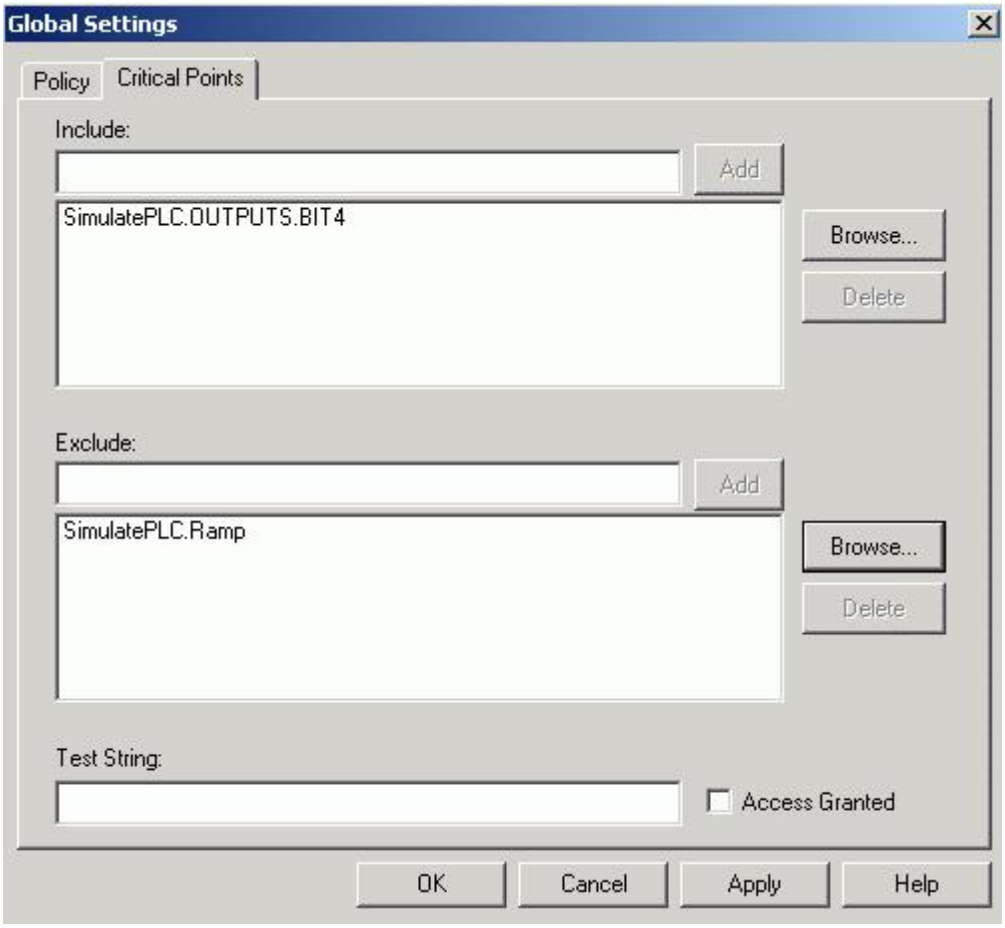
In the **Critical Points** tab of the **Global Settings** dialog box, shown in the figure below, some subset of write-able points (OPC data items) can be designated as "Critical Points." When writing a new value to a critical point, the user will be prompted to login again immediately before writing a new value. This ensures that the person writing the value is the authenticated user.

The critical points use the same include/exclude lists with wildcards concept as the **Points** configuration in the user and group properties dialogs. This allows multiple tags to be specified without listing them individually.

In order for a user to write a new value to a critical point, the following two conditions must be met:

1. The user must be granted rights to the point via his user configuration or via one of the explicit groups he belongs to (rights cannot be granted from the default group).
2. The user must have logged in within the past **Critical Points Login Period** as configured on the **Policy** tab of the **Global Settings** dialog box.

If condition 1 is met, but not condition 2, the client application (e.g. GraphWorX) will launch the **Security Login** dialog, requiring the user to log again and satisfy condition 2.

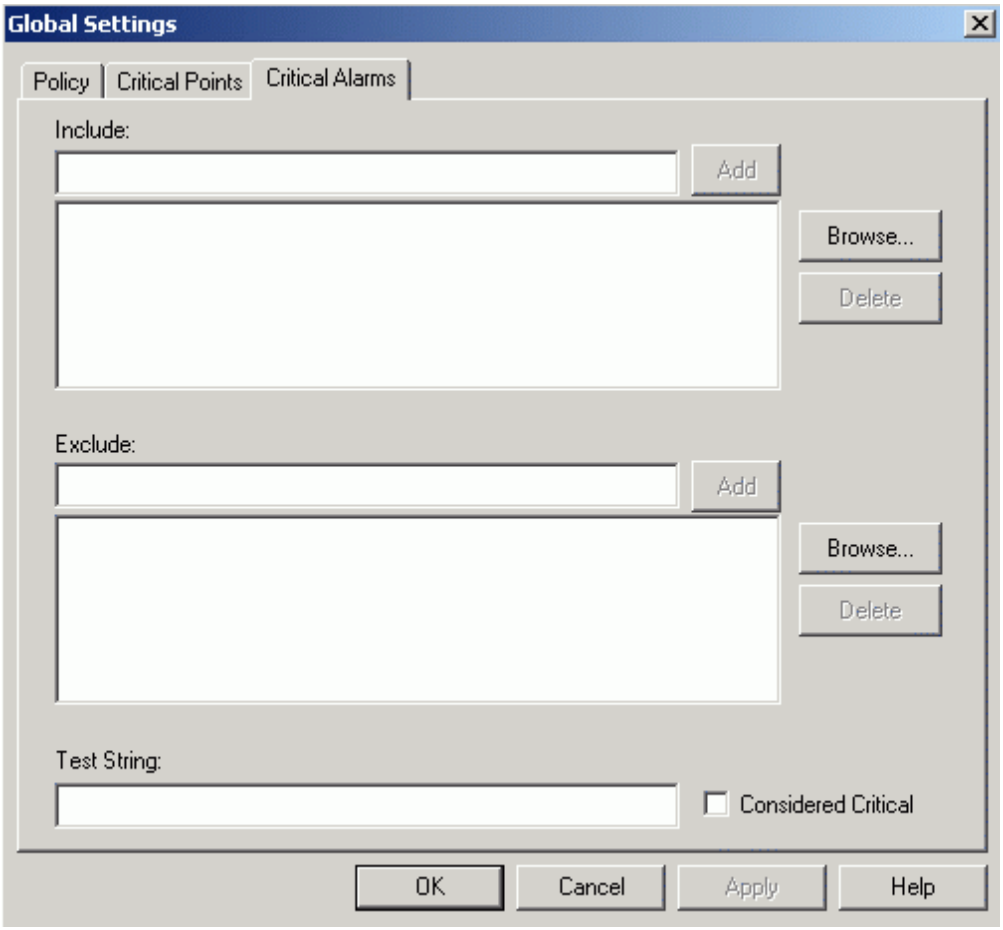


Defining Access to Critical Points

Critical Alarms

In the **Critical Alarms** tab of the **Global Settings** dialog box, shown in the figure below, some subset of alarms can be designated as “Critical Alarms.” When writing a new value to a critical alarm, the user will be prompted to login again immediately before acknowledging an alarm. This ensures that the person acknowledging the alarm is the authenticated user.

The critical alarms use the same include/exclude lists with wildcards concept as the **Alarms** configuration in the user and group properties dialogs. This allows multiple alarms to be specified without listing them individually.



Defining Access to Critical Alarms

Wildcards and Performance Optimization

The security server is a powerful module that provides real-time security for all of the Smar client applications. The security settings are applied with different grades of access. It is possible, for example, to deny the access to a whole display or to a single tag embedded in it. Many of the operations performed from the Smar client applications require a security check in order to be performed. For example, a process point can be visualized in GraphWorX only if the security check for it succeeds. The security check can involve a several string comparison operation in order to grant or deny the access to a specific resource. Thus, before displaying a process point in GraphWorX it is required to check if the process point appears in a tag exclude list. It is also required to check to seed if it belongs to the critical point list. All of these checks are performed through a string comparison between the requested resource name and the lists of restricted resources (e.g. the excluded tag).

The Smar Security Server must perform all of these security checks on the fly each time a tag is requested. The access to a tag could be granted now and denied a fraction of a second later because the security privileges have been changed.

Real-time update means comparing the requested resource with the list of denied resources each time a resource is requested. The whole list of denied resources must be reviewed to find out if the requested resources match one of them.

So the speed is inversely proportional to the number of strings that appear in your denied resource list (i.e. the more strings, the more comparisons are needed, and therefore the longer it takes). All you have to do to optimize the performance of you application is keep this in mind and use as many wildcard characters as possible.

For example, suppose that you want to declare all the tags in the DiskIO branch of the Smar OPC

Simulator tree as a "critical point." You will have to add to the critical point list 50 different tags:
Smar.Simulator.1\DiskIO.D01
Smar.Simulator.1\DiskIO.D02
....
Smar.Simulator.1\DiskIO.D25
Smar.Simulator.1\DiskIO.R01
Smar.Simulator.1\DiskIO.R02
....
Smar.Simulator.1\DiskIO.R25

Now instead of doing this you could simply add the following critical point using a wildcard character:
Smar.Simulator.1\DiskIO.*

In this way the Security Server will have to compare the resource requested from the client with one string instead of 50 different strings. Thus, it will run faster and you will see your data updated quickly.

Wildcards and Pattern Matching

The entries in the include and exclude lists allow pattern matching similar to the Visual Basic LIKE operator. Built-in pattern matching provides a versatile tool for string comparisons. The pattern-matching features allow you to use wildcard characters, character lists, or character ranges, in any combination, to match strings.

Text results in string comparisons are based on a case-insensitive textual sort order determined by your system's locale, for example:
(A=a) < (À=à) < (B=b) < (E=e) < (Ê=ê) < (Z=z) < (Ø=ø)
The following table shows the characters allowed in patterns and what they match:

CHARACTER(S) IN PATTERN	MATCHES IN STRING
?	Any single character.
*	Zero or more characters.
#	Any single digit (0 - 9).
[*charlist*]	Any single character in *charlist.*
[!*charlist*]	Any single character not in *charlist.*

A group of one or more characters (*charlist*) enclosed in brackets ([ ]) can be used to match any single character in string and can include almost any character code, including digits.

NOTE
The special characters left bracket ([), question mark (?), pound sign (#), and asterisk (*) can be used to match themselves directly only by enclosing them in brackets. The right bracket (]) cannot be used within a group to match itself, but it can be used outside a group as an individual character.

In addition to a simple list of characters enclosed in brackets, *charlist* can specify a range of characters by using a hyphen (-) to separate the upper and lower bounds of the range. For example, [A-Z] in pattern results in a match if the corresponding character position in string contains any of the uppercase letters in the range A-Z. Multiple ranges are included within the brackets without any delimiters.

The meaning of a specified range depends on the character ordering valid at run time (as determined by the locale setting of the system the code is running on). The range [A - E] matches A, a, À, à, B, b, E, e. Note that it does not match Ê or ê because accented characters fall after unaccented characters in the sort order.

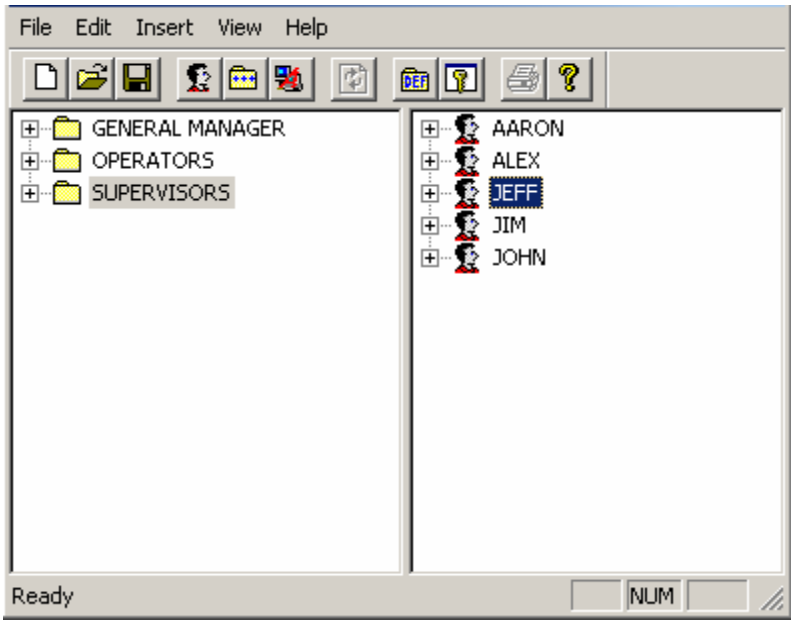
Other important rules for pattern matching include the following:

- An exclamation point (!) at the beginning of *charlist* means that a match is made if any character except the ones in *charlist* is found in string. When used outside brackets, the exclamation point matches itself.

- The hyphen (-) can appear either at the beginning (after an exclamation point if one is used) or at the end of *charlist* to match itself. In any other location, the hyphen is used to identify a range of characters.
- When a range of characters is specified, they must appear in ascending sort order (from lowest to highest). [A-Z] is a valid pattern, but [Z-A] is not.
- The character sequence [] is ignored; it is considered a zero-length string.

Configuring Users and Groups

The Security Configurator consists of two separate panes. Each pane has a tree control. The left tree is the **Group View.** Here the root nodes are groups, and the child nodes are the users that belong to the group. The right tree is the **User View,** in which the root nodes are users, and the child nodes are the groups that have been assigned to each user. Some example groups and users are shown in the figure below.



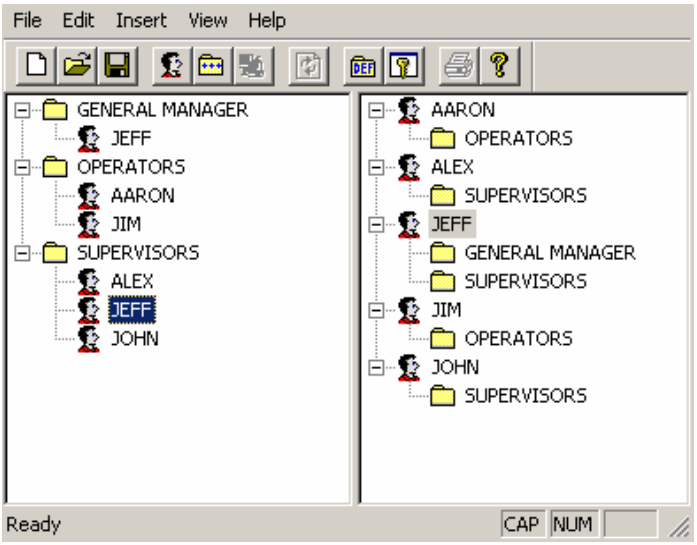
Example Security Configuration

The example security configuration in the figure above shows sample users and groups for a factory. The personnel groups for the factory are:

- General Manager
- Supervisors
- Operators

Each of these groups has one or more users, all of whom need to have access to factory data. There are five different users:

- Aaron (Operator)
- Alex (Supervisor)
- Jeff (General Manager and Supervisor)
- Jim (Operator)
- John (Supervisor)



Configuring Advanced Security for Users and Groups

As you can see in the figure above, you can associate users with various groups to help simplify and organize security management. This way all users associated with a particular group are bound to the restrictions or properties for that group. For example, both Jim and John are supervisors, associated with the **Supervisors** group.

NOTE
Jeff is associated with both the **General Manager** group and the **Supervisors** group. This association of one user with two different groups is possible only in advanced security mode.

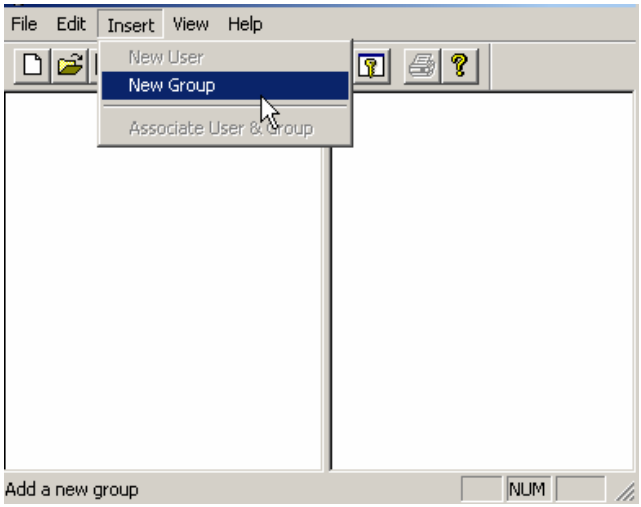
If there are certain files, for example, that only the general manager and supervisors are allowed to view but the operators may not view, the security administrator can use the lock the operators out of those pages by configuring the **Operators** group properties.

You can also configure properties for each user within a group. For example, both Aaron and Jim are operators and are therefore associated with the **Operators** group. However, Aaron's user properties may be configured separately from those of Jim so that each user within the group has unique security restrictions.

Adding a New Security Group

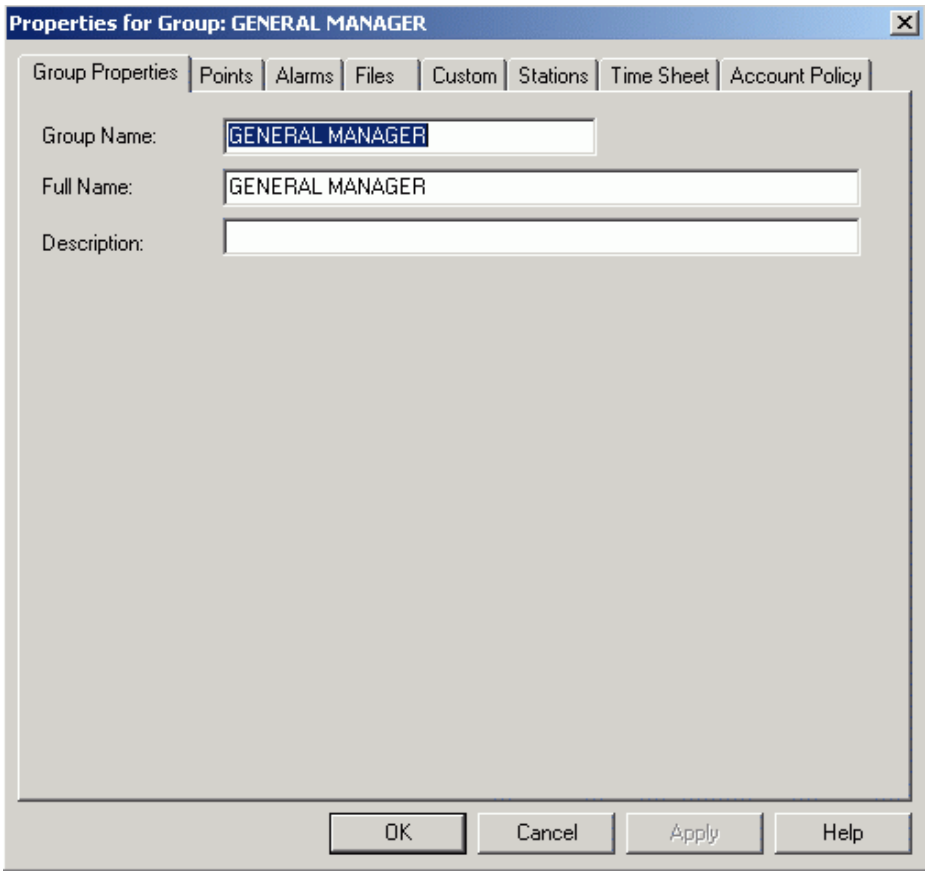
To add a new group to the Security Configurator:

1. Select **New Group** from the **Insert** menu, as shown in the figure below.



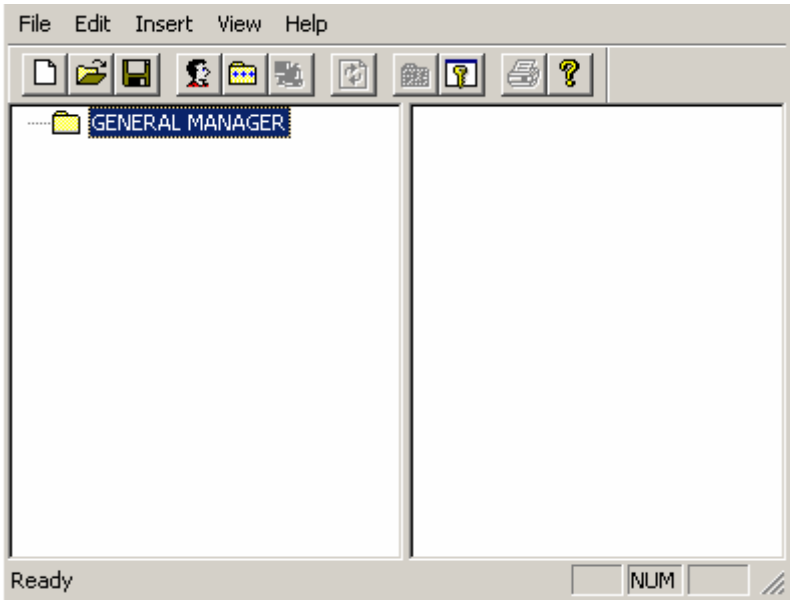
Adding a New Group

2. The **Properties** dialog box for the new group appears, as shown in the figure below. Give the group a name, and then click **OK.**



Properties for New Group

3. This adds the new group under the **Group View** tree. The name is highlighted, as shown in the figure below.

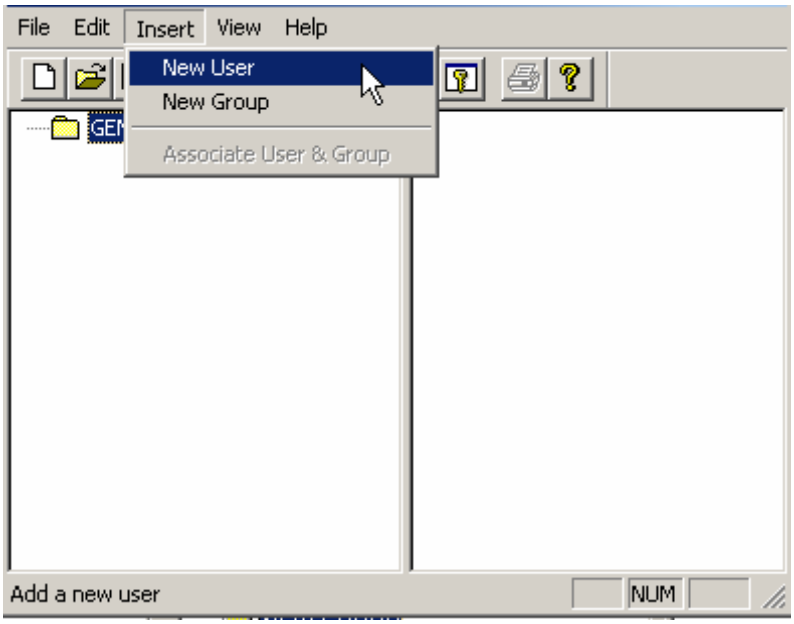


New Group Added to Group Tree

Adding a New User Profile

To add a new user profile to the Security Configurator:

1. Click the **New User** from the **Insert** menu, as shown in the figure below.



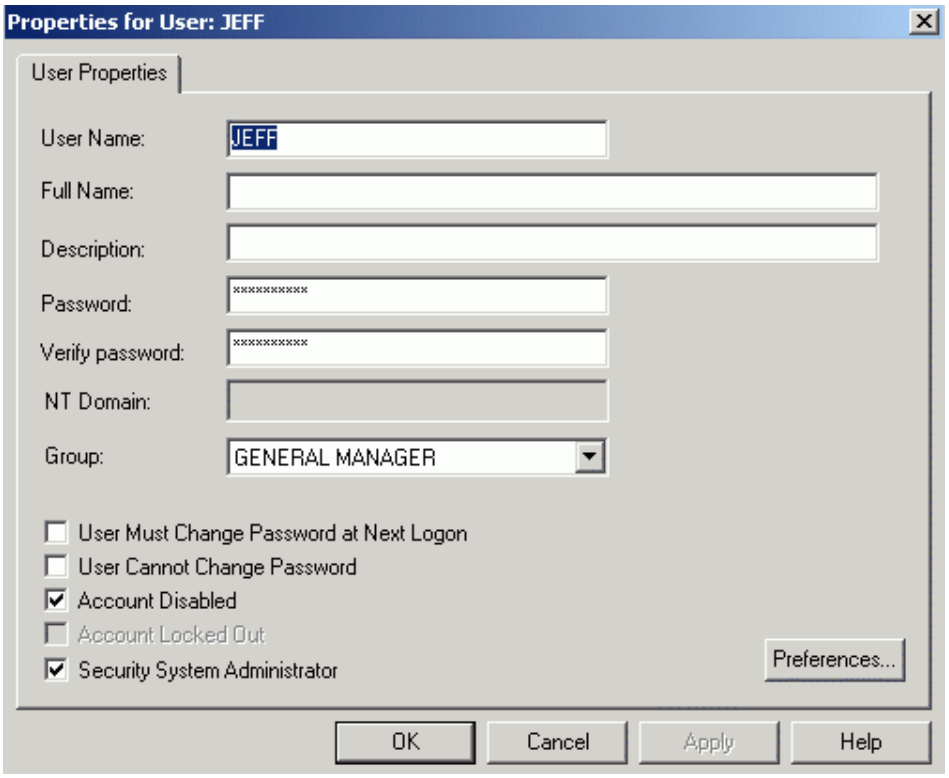
Adding a New User Profile

2. The **Properties** dialog box for the new user appears, as shown in the figure below. Enter a name and password for the user.

NOTE
The **Password** field is always filled in by default to disguise the password, but you should always change the password.

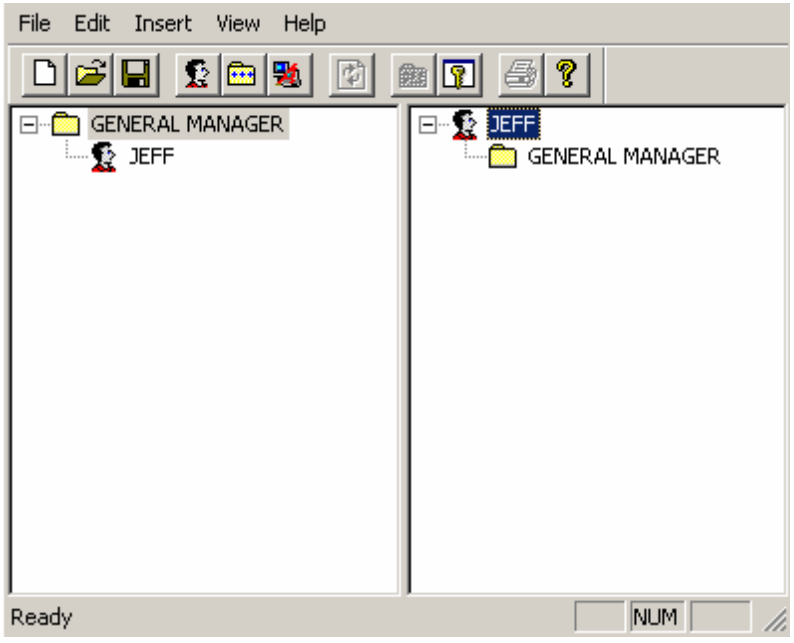
3. The **Account Disabled** check box is checked by default, so you must uncheck this box in order to activate the user's account. Give the user a name, and then click **OK.**

4. **Note:** In basic mode, you can associate the user with a group by selecting a group from the drop-down list under **Group.** In NT integrated security mode, you can specify a domain for the user in the **NT Domain** field.



Properties for New User

5. The new user is added to the **User View** tree, as shown in the figure below. Notice that (in basic security mode) the user is associated with the group you specified in the **User Properties** dialog box.



New User Added to User Tree

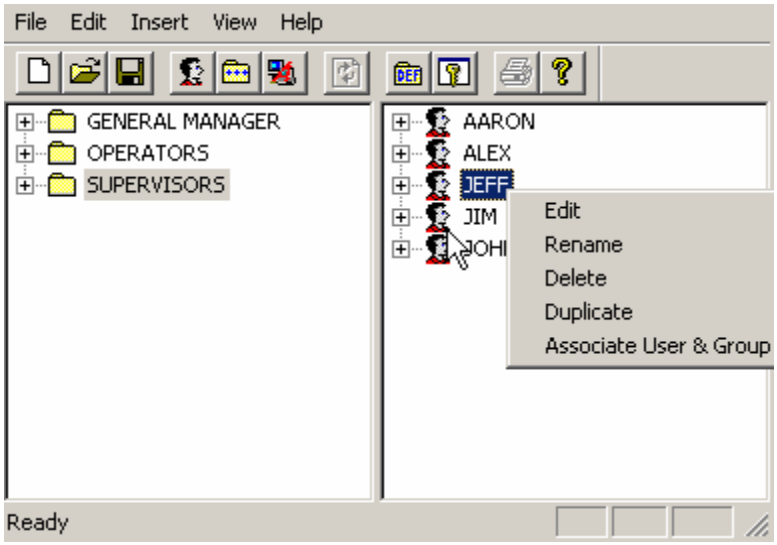
Duplicating Users and Groups

The **Edit** menu in the Security Configurator has a **Duplicate** command that is enabled when a group is selected in the Group tree or a user is selected in the User tree. Selecting **Duplicate** makes a copy of the selected user or group.

To duplicate a user or a group in the Security Configurator

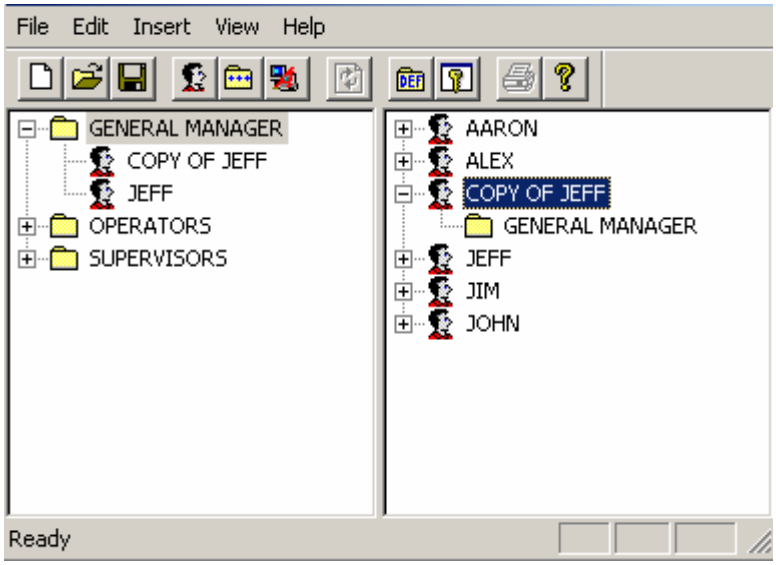
1. Select the desired group in the **Group View** tree, or the desired user in the **User View** tree.
2. Right-click on the item and select **Duplicate** from the pop-up menu, as shown in the figure below.

NOTE
Selecting a child item in the tree instead of a root item (i.e. you select a user in the group tree or a group in the user tree) and performing a delete, as described above, removes the child item from the parent (dissociates the group from the user) but does not actually delete it.



Duplicating Users and Groups

3. A copy of the user or group appears in the Security Configurator, as shown in the figure below. The name of the new item is the name of the source item with “COPY OF” pretended. When a user is duplicated, all of the groups associated with the original user are automatically associated with the new user. When a group is duplicated, users associated with the original group are not automatically associated with the new group.



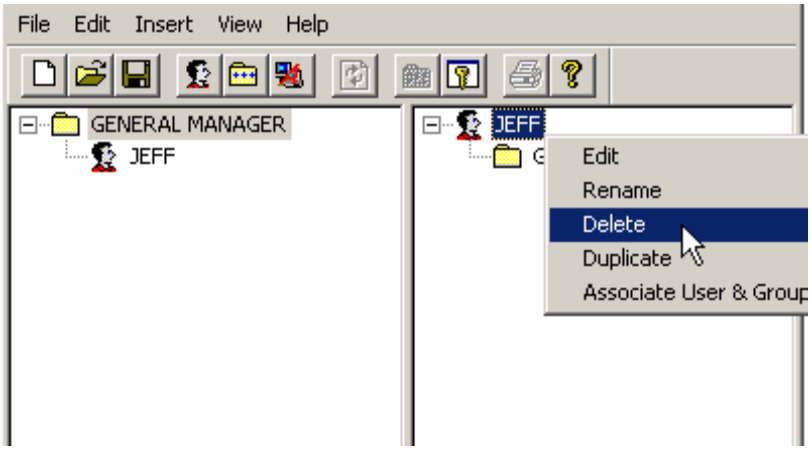
User Duplicated

Deleting Users and Groups

To delete a user or a group from the Security Configurator

1. Select the desired group in the **Group View** tree, or the desired user in the **User View** tree.
2. Right-click on the item and select **Delete** from the pop-up menu, as shown in the figure below.

NOTE
Selecting a child item in the tree instead of a root item (i.e. you select a user in the group tree or a group in the user tree) and performing a delete, as described above, removes the child item from the parent (dissociates the group from the user) but does not actually delete it.



Deleting Users and Groups

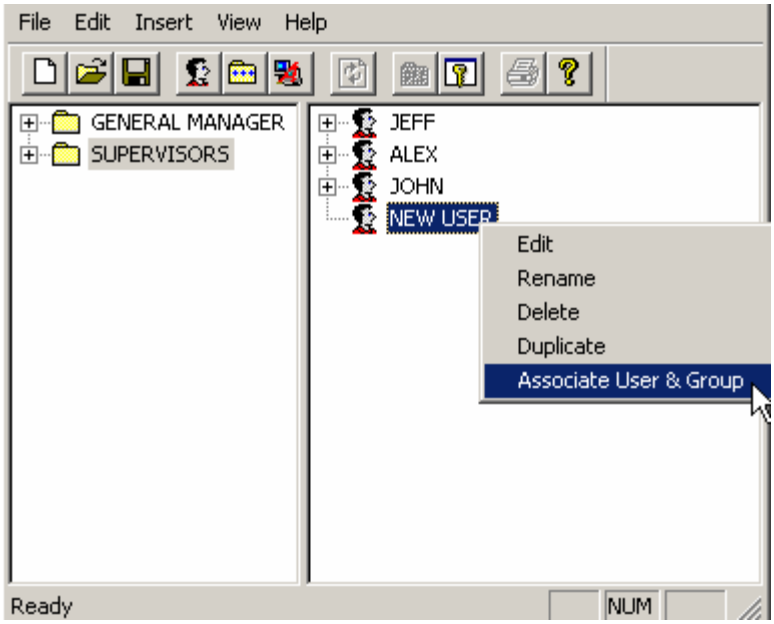
3. You are then asked to confirm the deletion, as shown in the figure below. Click **OK** to delete the user or group.

Confirming Deletion of a User or Group

Associating Users and Groups

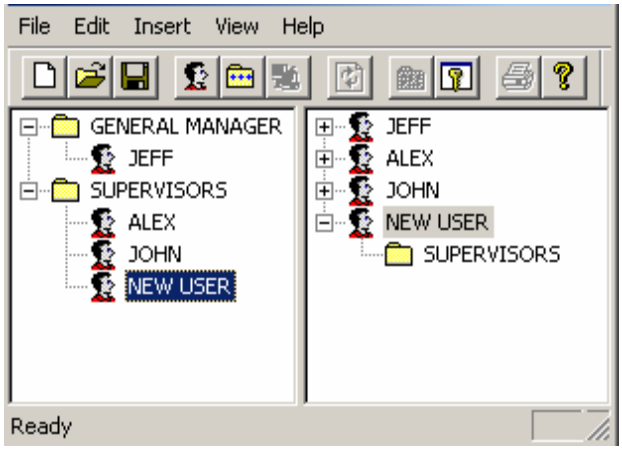
To associate a user with a group in the Security Configurator:

1. In the **Group View** tree, select the group with which you want to associate the user.
2. In the **User View** tree, select the user to be associated with the group. Right-click and select **Associate User and Group** from the pop-up menu, as shown in the figure below.



Associating a User with a Group

3. When a user and group are associated, the user appears as a child item under the group tree in the left pane, and the group appears as a child item under the user tree in the right pane, as shown in the figure below. In this example, the "New User" has been associated with the group "Supervisors."

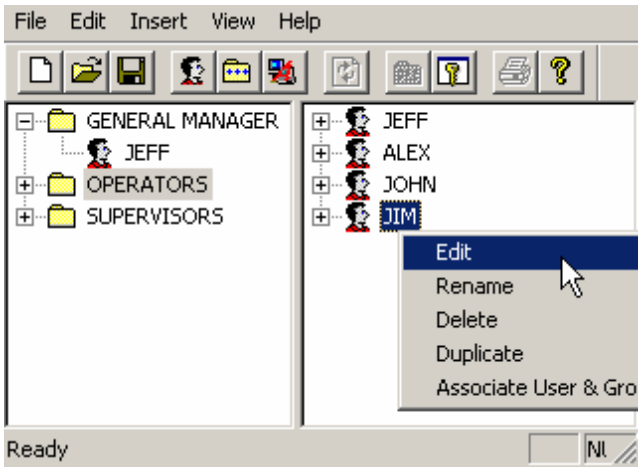


Viewing User and Group Associations

Basic Security Mode

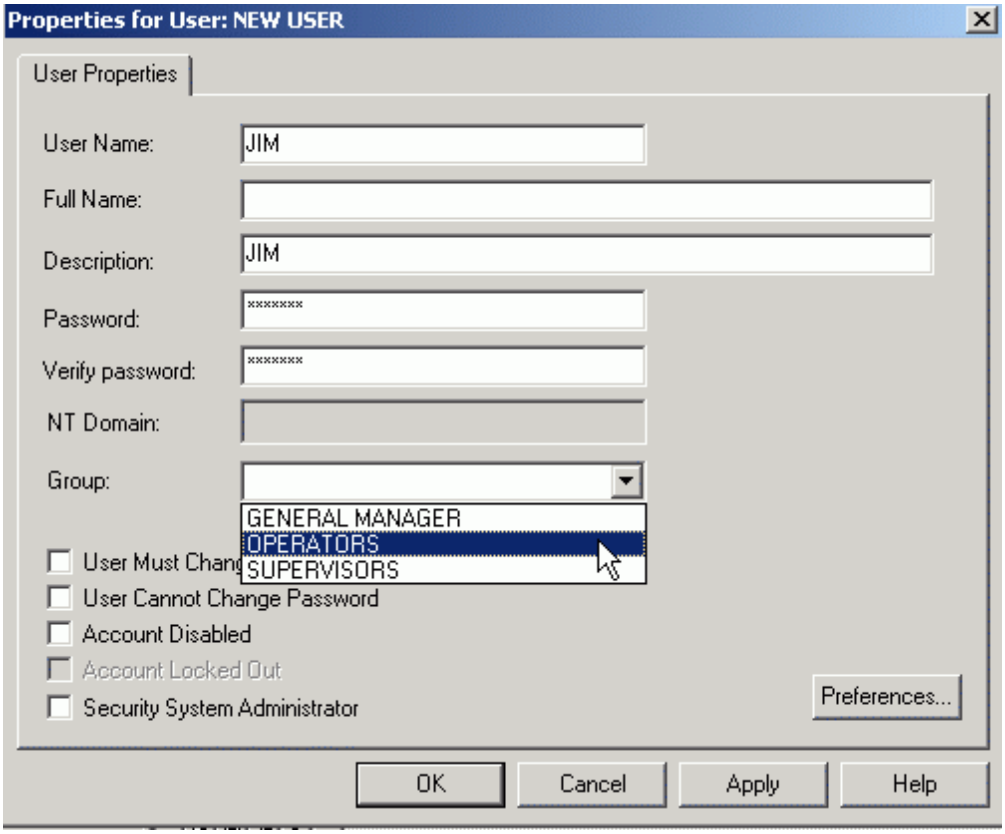
In basic security configuration mode, a user must be associated with one and only one group. In basic mode, this association can be made directly from the **User Properties** dialog box. To associate a user with a group in basic mode:

1. In the **Group View** tree, select the group with which you want to associate the user.
2. In the **User View** tree, select the user to be associated with the group. Right-click and select **Edit** from the pop-up menu, as shown in the figure below.



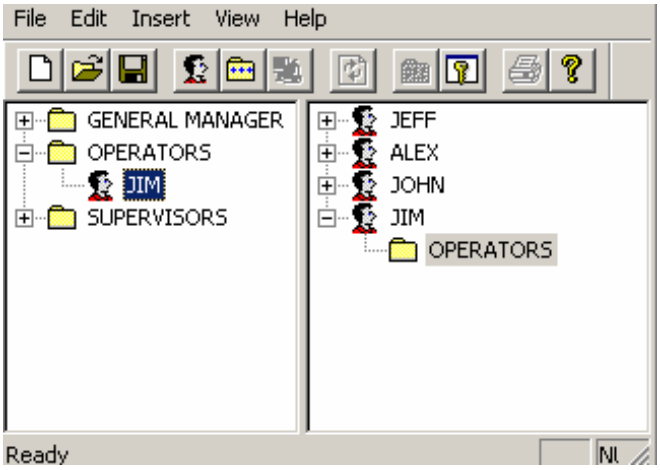
Editing User Properties

3. The **Properties** dialog box for the user appears, as shown in the figure below. You can associate the user with a group by selecting a group from the drop-down list under **Group.** Click **OK.**



Associating a User with a Group: Basic Mode

4. When a user and group are associated, the user appears as a child item under the group tree in the left pane, and the group appears as a child item under the user tree in the right pane, as shown in the figure below. In this example, the user "Jim" has been associated with the group "Operators."



Viewing User and Group Associations

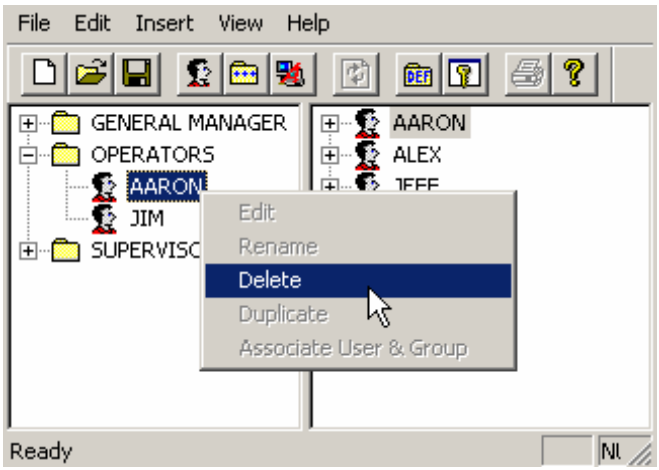
Removing Associations Between Users and Groups

To remove the association between a user and a group in the Security Configurator:

1. Select the user child item under the desired group in the left pane, or select the group child item under the desired user in the right pane.

2. Right-click the user or group to be dissociated under and select **Delete** from the pop-up menu, as shown in the figure below.
3. When the association is removed, the child user under the group in the left pane is removed, and the child group under the user in the left pane is removed.

NOTE
Performing this operation never deletes the selected user or group. Only their association is removed.

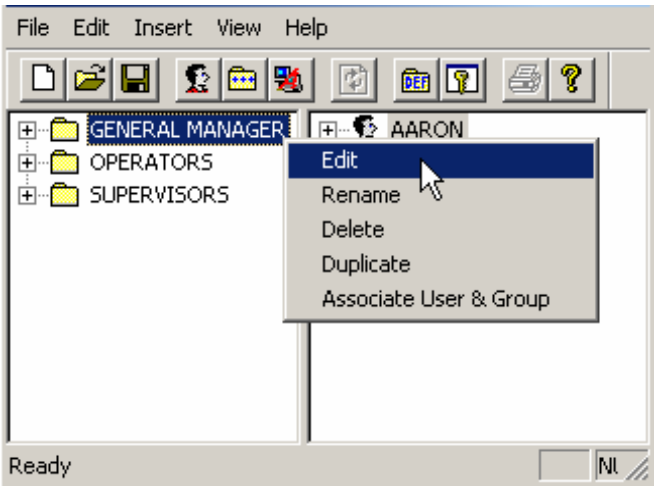


Removing Associations Between Users and Groups

Editing Group Properties

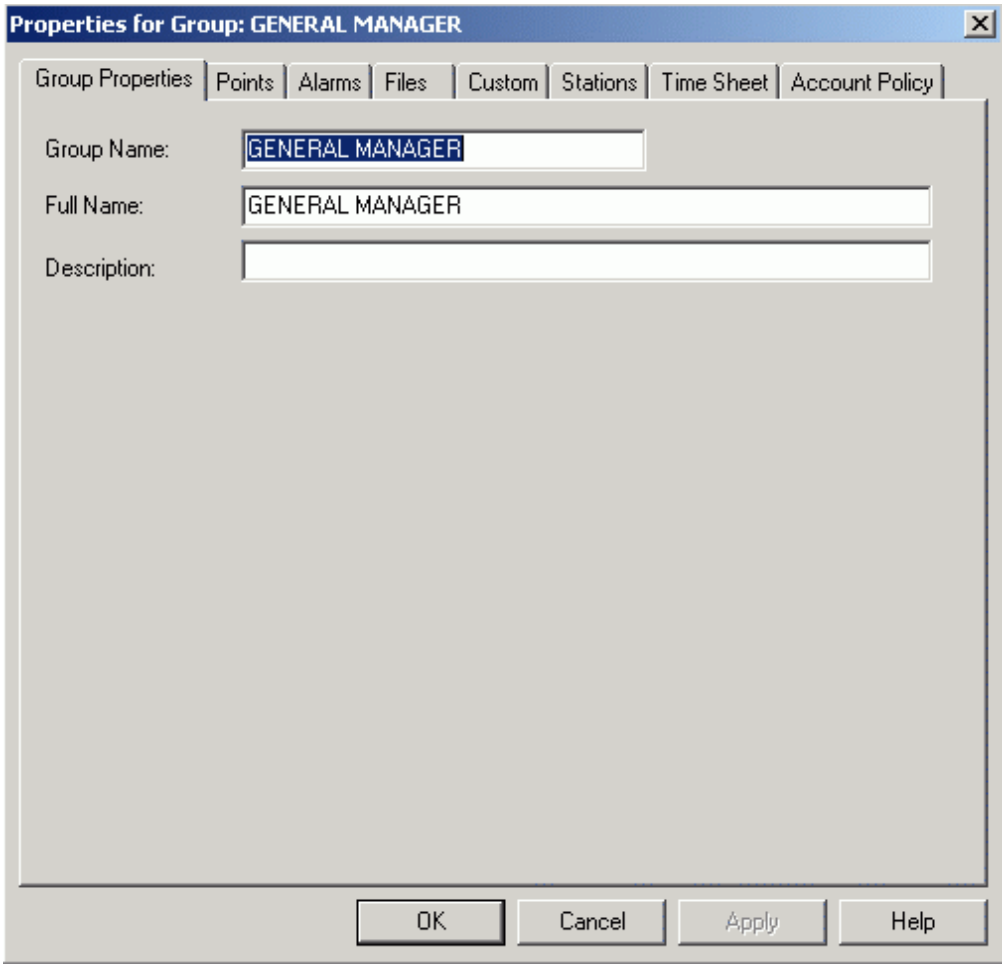
To edit the properties assigned to a group in the Security Configurator:

1. Select the desired group in the group tree.
2. Right-click on the group or user and select **Edit** from the pop-up menu, as shown in the figure below.



Editing Group Properties

3. This opens the **Properties for Group** dialog box, shown in the figure below, which is used to configure group security restrictions.



Properties for Group

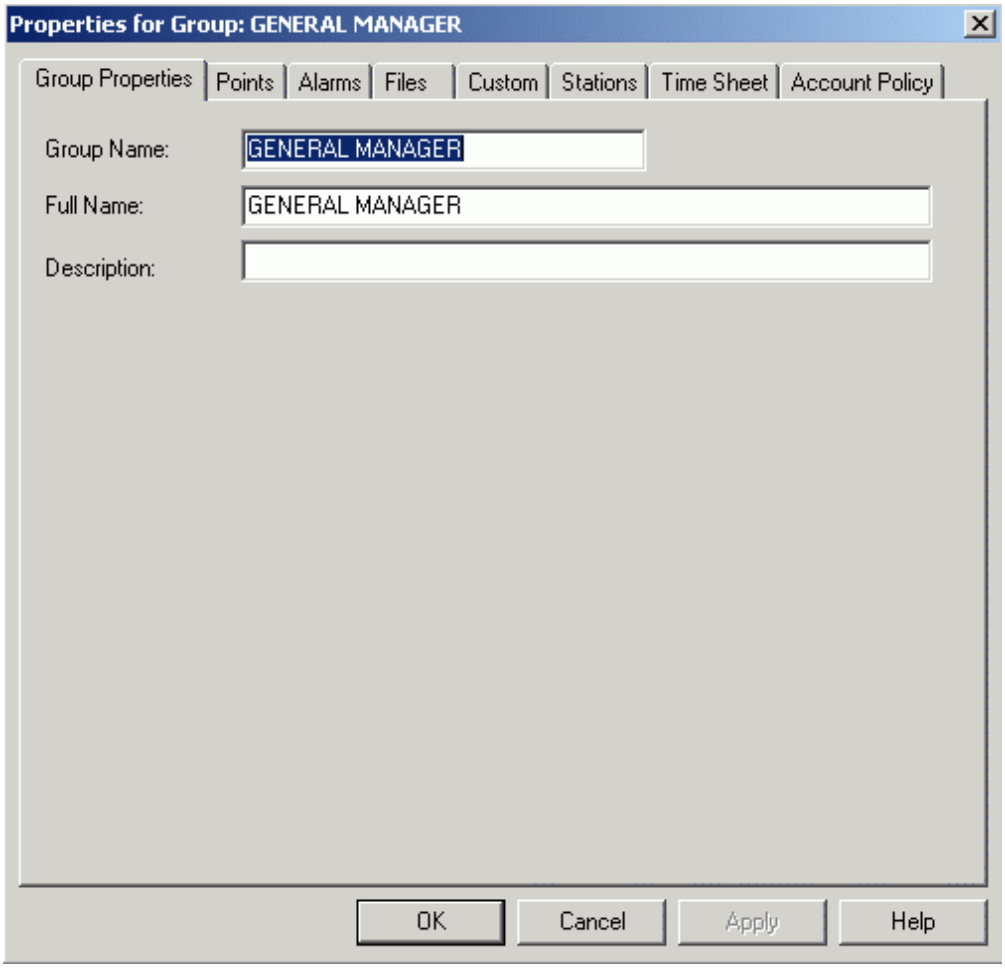
The **Properties for Group** dialog box contains the following tabs:

- **Group Properties**
- **Points**
- **Alarms**
- **Files**
- **Custom**
- **Stations**
- **Time Sheet**
- **Account Policy**

Group Properties

The **Properties for Group** dialog box, shown in the figure below, contains the following fields:

FIELD	DESCRIPTION
Group Name	Short name that uniquely identifies this group within the system.
Full Name	The full name for this group (optional).
Description	Optional.

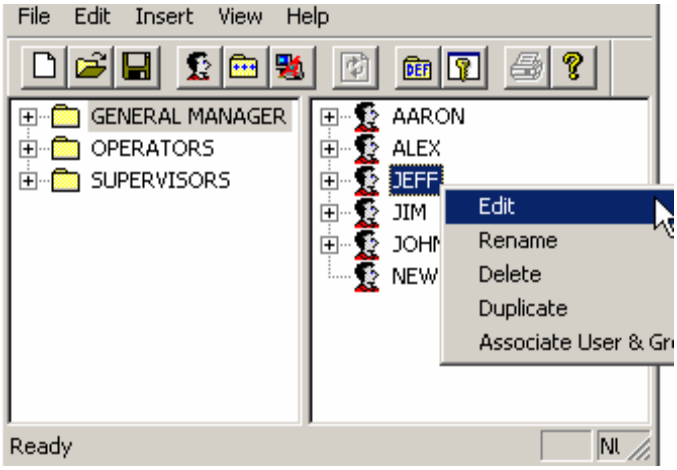


Properties for Group

Editing User Properties

To edit the properties assigned to a user in the Security Configurator:

1. Select the desired user in the user tree.
2. Right-click on the user and select **Edit** from the pop-up menu, as shown in the figure below.



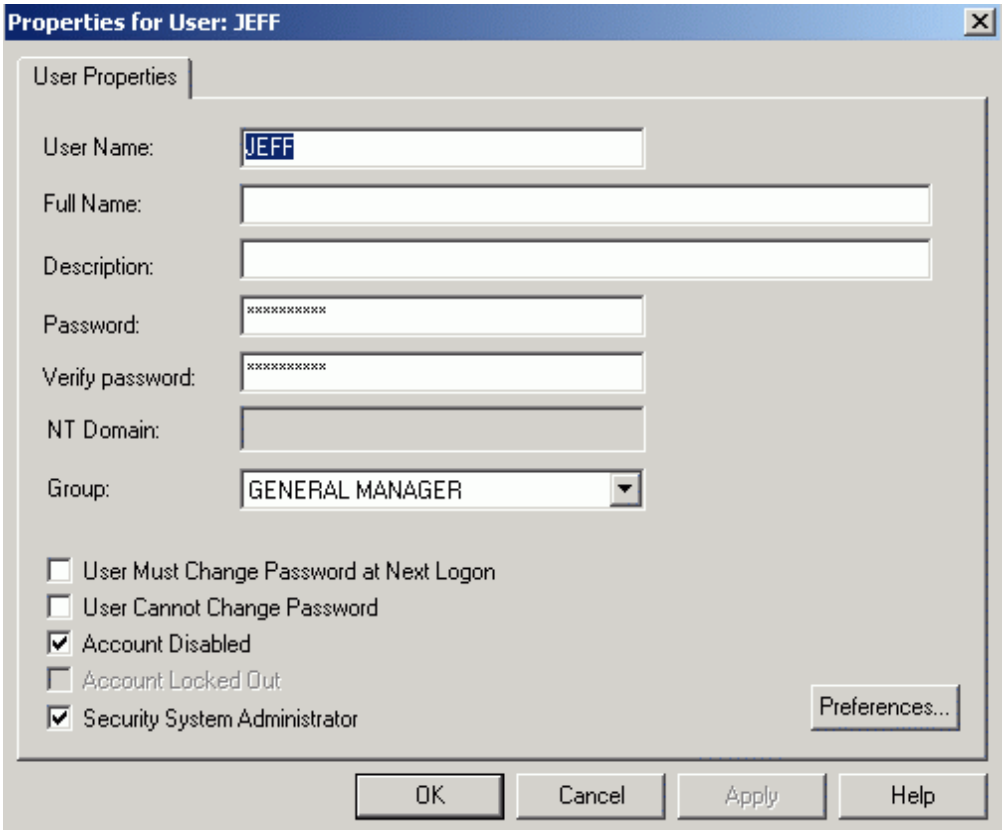
Editing User Properties

3. This opens the **Properties for User** dialog box, shown in the figure below, which is used to configure user security restrictions.

NOTE
The **Password** field is always filled in by default to disguise the password, but you should always change the password.

4. The **Account Disabled** check box is checked by default, so you must uncheck this box in order to activate the user's account. Click **OK.**

NOTE
In basic mode, you can associate the user with a group by selecting a group from the drop-down list under **Group.** In NT integrated security mode, you can specify a domain for the user in the **NT Domain** field.



Properties for User (Basic Mode)

In basic security mode, only the **User Properties** tab can be configured in the **Properties for User** dialog box, as shown in the figure above, because all other properties are configured in the group with which the user is associated.

In advanced security mode, the **Properties for User** dialog box contains the following tabs:

- **User Properties**
- **Points**
- **Alarms**
- **Files**
- **Custom**
- **Stations**
- **Time Sheet**

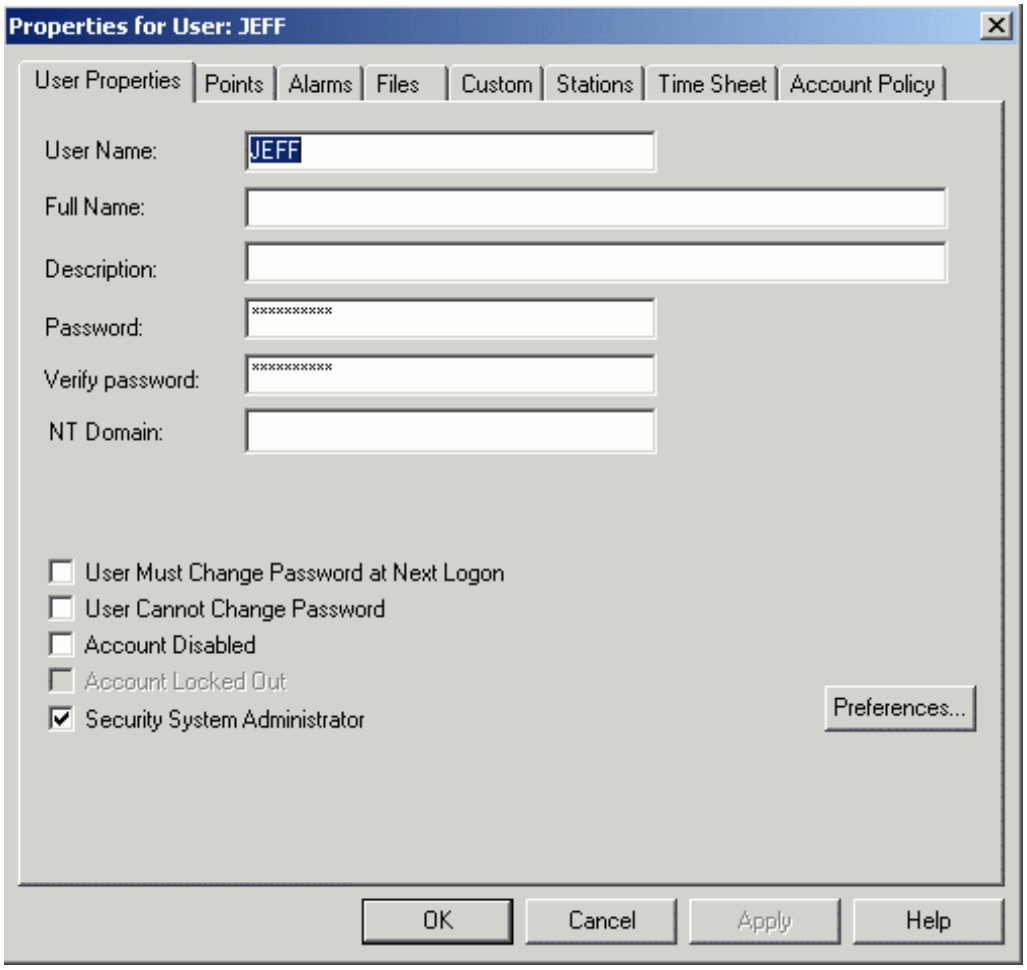
- **Account Policy**

User Properties

The properties for users and groups vary slightly. In basic security mode, only the **User Properties** tab can be configured in the **Properties for User** dialog box, because all other properties are configured in the group with which the user is associated.

In advanced security mode, the group fields are a subset of the user fields, and the **Properties for User** dialog box, shown in the figure below, contains the following fields:

FIELD	DESCRIPTION
User Name	Short name that the user types when logging on to the system.
Full Name	The user's full name for reference only (optional).
Description	Optional.
Password	The password the user must type to log in to the Security Server. This field is case-sensitive; no spaces are allowed.
Verify Password	If you change the **Password** field, you must type the exact same password into this field.
User Must Change Password at Next Logon	When checked, the user must change his or her password at the time of the next logon. This is often used when a new user created. The administrator enters a default password for the new user and checks this field to require a "real" password to be entered on first logon.
User Cannot Change Password	When checked, the user's password can only be changed from this dialog, and not from the Login Client.
Account Disabled	Checking this check box has the same effect as deleting the user without the permanence of an actual delete. The **Account Disabled** check box is checked by default, so you must uncheck this box in order to activate the user's account.
Account Locked Out	This field is normally unchecked and disabled. Should the account become locked out (see the account lockout description in the **Account Policy** tab), the field would be enabled and checked. From here, the administrator can uncheck the field to re-enable the user logon.
Security System Administrator	When checked, this user is allowed to log in as a Security System Administrator to configure all aspects of the security system.

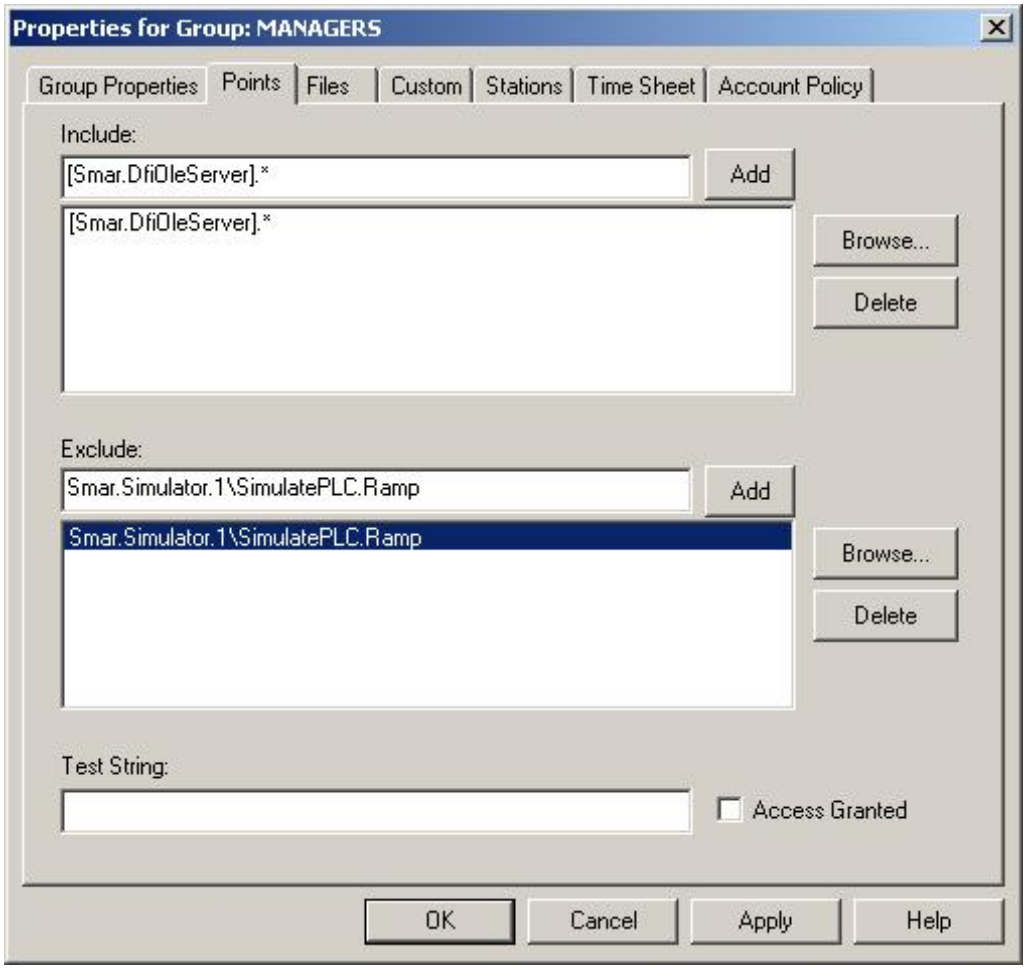


Properties for User (Advanced Mode)

Process Output Points

A ProcessView application that is configured to send outputs to points in OPC servers will disable them if denied by the Security Server. As with the file names, OPC point names with or without wildcards are placed in include or exclude lists for each user or group.

Before a ProcessView client outputs a process value to an OPC server, the unique string that identifies the OPC output point is sent to the Security Server to determine if the write should be allowed based on the currently logged-in user(s) and or the groups to which they belong. The **Points** tab of the **Properties** dialog box, shown in the figure below, is used to configure which OPC output points are allowed to be written to by users and groups.



Points Configuration

The **Points** property page is divided into two sections, **Include** and **Exclude.** Each section contains an edit field and a list box. You can select strings by using the **Browse** buttons. Pressing the **Enter** key with the cursor in the edit field or clicking the **Add** button adds the edit field text to the list box. When an entry in the list box is selected, pressing the **Delete** key or clicking the **Delete** button deletes the selected entry.

If you type a string in the **Test String** field, the **Access Granted** check box indicates if access would be given to the user if the access to the "test string" was requested. The test is made using only the include and exclude lists that are visible.

During runtime, when a ProcessView client sends an OPC point string to the Security Server for access testing (granted or denied), the include and exclude lists are string compared as follows for each active user and group until access is granted:

1. Compare the OPC point string with each string in the include list until a match is found. If no match is found, access is denied.
2. If a match is found in the include list, compare the OPC point string with every string in the exclude list. If no match is found in the exclude list, access to the point is granted, and no further testing of active groups and users is performed.

NOTE
The exclude list entries can only remove rights granted in their corresponding include list. For example if user *Aaron* belongs to the group *Operators,* and *Operators* grants access to OPC point *xyz,* adding point *xyz* to *Aaron's* exclude list has no effect.

Wildcards and Pattern Matching
The entries in the include and exclude lists allow pattern matching similar to the Visual Basic LIKE operator. Built-in pattern matching provides a versatile tool for string comparisons. The pattern-matching features allow you to use wildcard characters, character lists, or character ranges, in any combination, to match strings.

Text results in string comparisons are based on a case-insensitive textual sort order determined by your system's locale, for example:
(A=a) < (À=à) < (B=b) < (E=e) < (Ê=ê) < (Z=z) < (Ø=ø)

The following table shows the characters allowed in patterns and what they match:

CHARACTER(S) IN PATTERN	MATCHES IN STRING
?	Any single character.
*	Zero or more characters.
#	Any single digit (0 - 9).
[*charlist*]	Any single character in *charlist.*
[!*charlist*]	Any single character not in *charlist.*

A group of one or more characters (*charlist*) enclosed in brackets ([ ]) can be used to match any single character in string and can include almost any character code, including digits.

NOTE
The special characters left bracket ([), question mark (?), pound sign (#), and asterisk (*) can be used to match themselves directly only by enclosing them in brackets. The right bracket (]) cannot be used within a group to match itself, but it can be used outside a group as an individual character.

In addition to a simple list of characters enclosed in brackets, *charlist* can specify a range of characters by using a hyphen (-) to separate the upper and lower bounds of the range. For example, [A-Z] in pattern results in a match if the corresponding character position in string contains any of the uppercase letters in the range A-Z. Multiple ranges are included within the brackets without any delimiters.

The meaning of a specified range depends on the character ordering valid at run time (as determined by the locale setting of the system the code is running on). The range [A - E] matches A, a, À, à, B, b, E, e. Note that it does not match Ê or ê because accented characters fall after unaccented characters in the sort order.

Other important rules for pattern matching include the following:

- An exclamation point (!) at the beginning of *charlist* means that a match is made if any character except the ones in *charlist* is found in string. When used outside brackets, the exclamation point matches itself.
- The hyphen (-) can appear either at the beginning (after an exclamation point if one is used) or at the end of *charlist* to match itself. In any other location, the hyphen is used to identify a range of characters.
- When a range of characters is specified, they must appear in ascending sort order (from lowest to highest). [A-Z] is a valid pattern, but [Z-A] is not.
- The character sequence [] is ignored; it is considered a zero-length string.

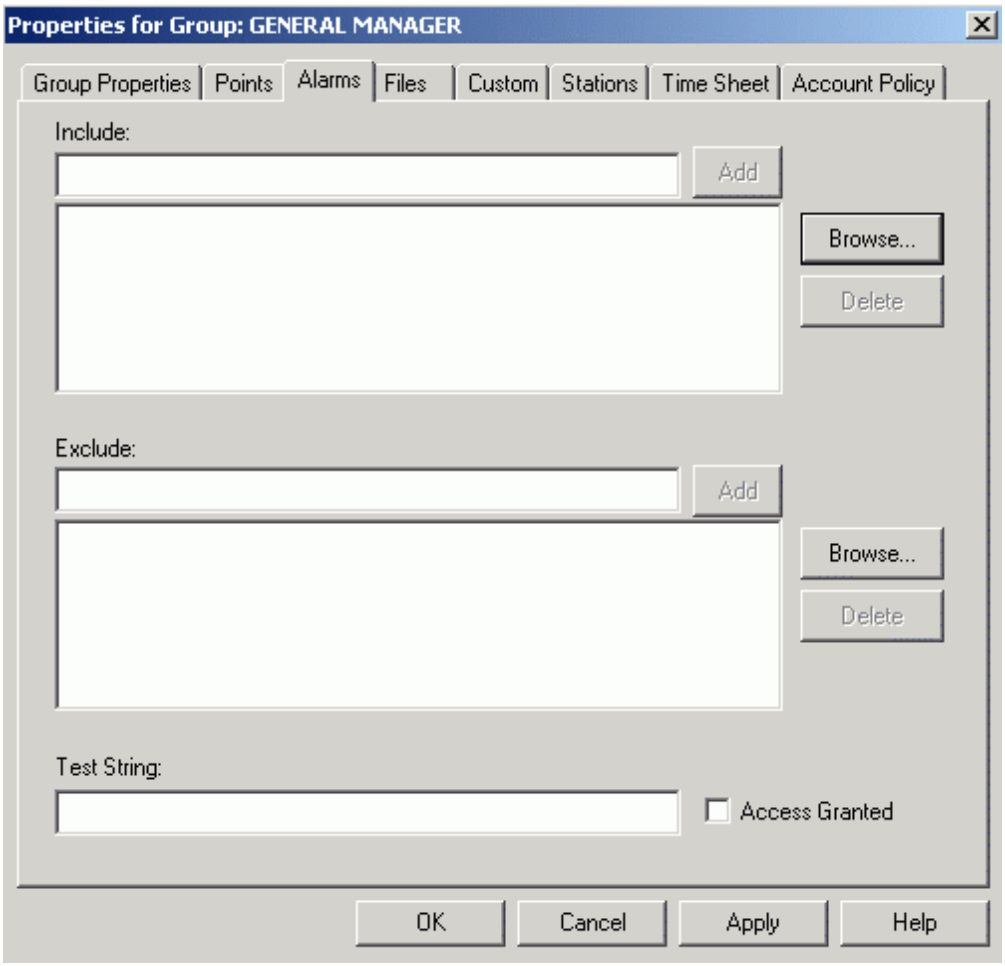
Alarms

Single alarms or groups of alarms may be protected. Alarm names with or without wildcards are placed in include or exclude lists for each user or group. (Include and exclude lists are commonly used by file backup programs to specify a backup set.)

A ProcessView application will query the Security Server for alarm access before opening a file.

The **Alarms** property page is used to control access to alarm acknowledgement during runtime.

The runtime processing and wildcard pattern matching for the Points property page apply here as well.



Alarm Configuration

Files

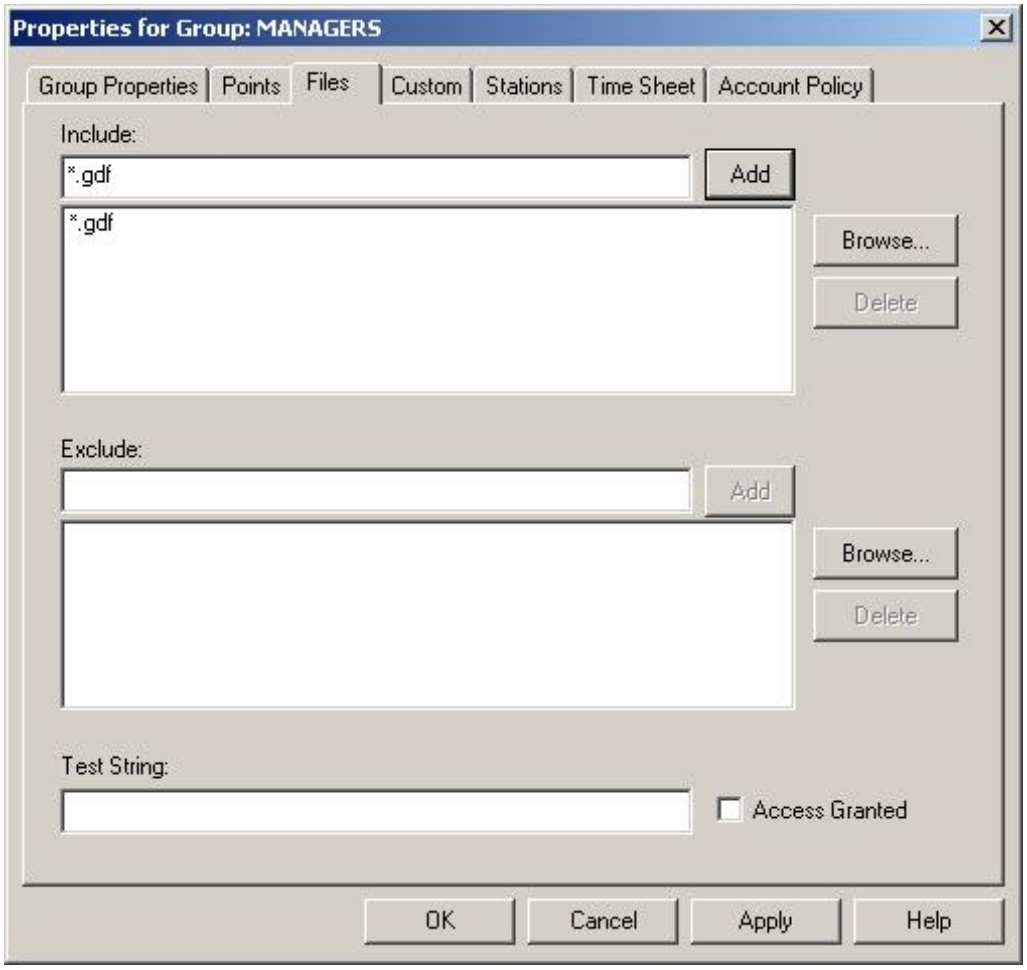
Single files or groups of files may be protected. File names with or without wildcards are placed in include or exclude lists for each user or group. (Include and exclude lists are commonly used by file backup programs to specify a backup set.)

A ProcessView application will query the Security Server for file access before opening a file. Typical files that will be secured are GraphWorX display files.

The **Files** property page is used to control access to files that ProcessView clients may open during runtime. For example, entries here would typically be used to restrict certain users or groups from viewing specific GraphWorX displays.

The runtime processing and wildcard pattern matching for the Points property page apply here as well with the following differences:

- The pattern matching is done on the file extension, separate from the file name, to match the DOS wildcard semantics. For example, the wildcard string to indicate all files is *.*
- File names entered without a path are considered a match no matter what directory they are in.



File Configuration

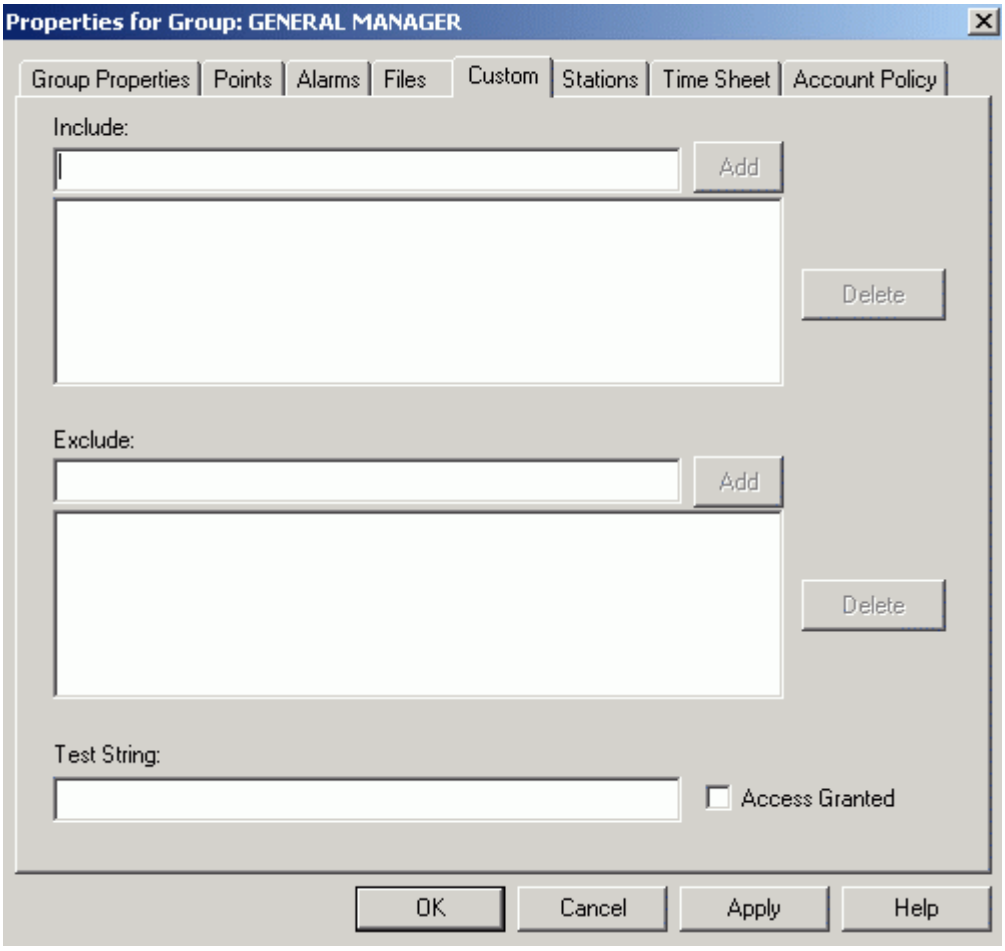
Custom Strings

VBA Scripts may use custom defined strings as security tokens that are evaluated by the Security Server. As with the file names, custom strings with or without wildcards are placed in include or exclude lists for each user or group.

The **Custom** property page, shown below, is used to include or exclude strings that will be tested in runtime by VBA scripts executing within ProcessView clients. The meaning of these strings and the functionality they protect are controlled entirely by the author of the VBA script.

The runtime processing and wildcard pattern matching apply here as well.

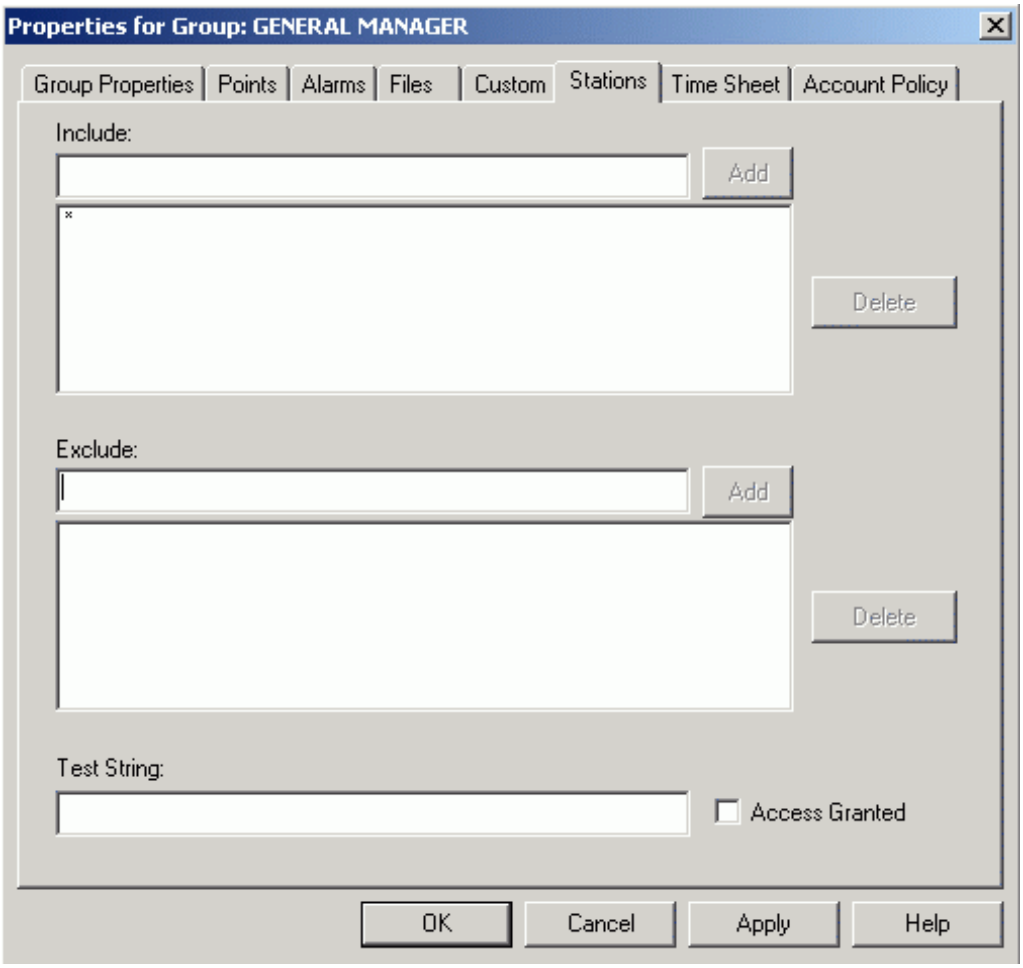
For example, from a GraphWorX VBA script, a custom security item is tested by calling the method **TestCustomSecurityItem(BSTR customString)** in the **GwxDisplay** object.



Custom Configuration

Stations

The **Stations** property page is used to grant or restrict access from specific nodes on the network. Each node on a Microsoft network is identified by a unique computer name.



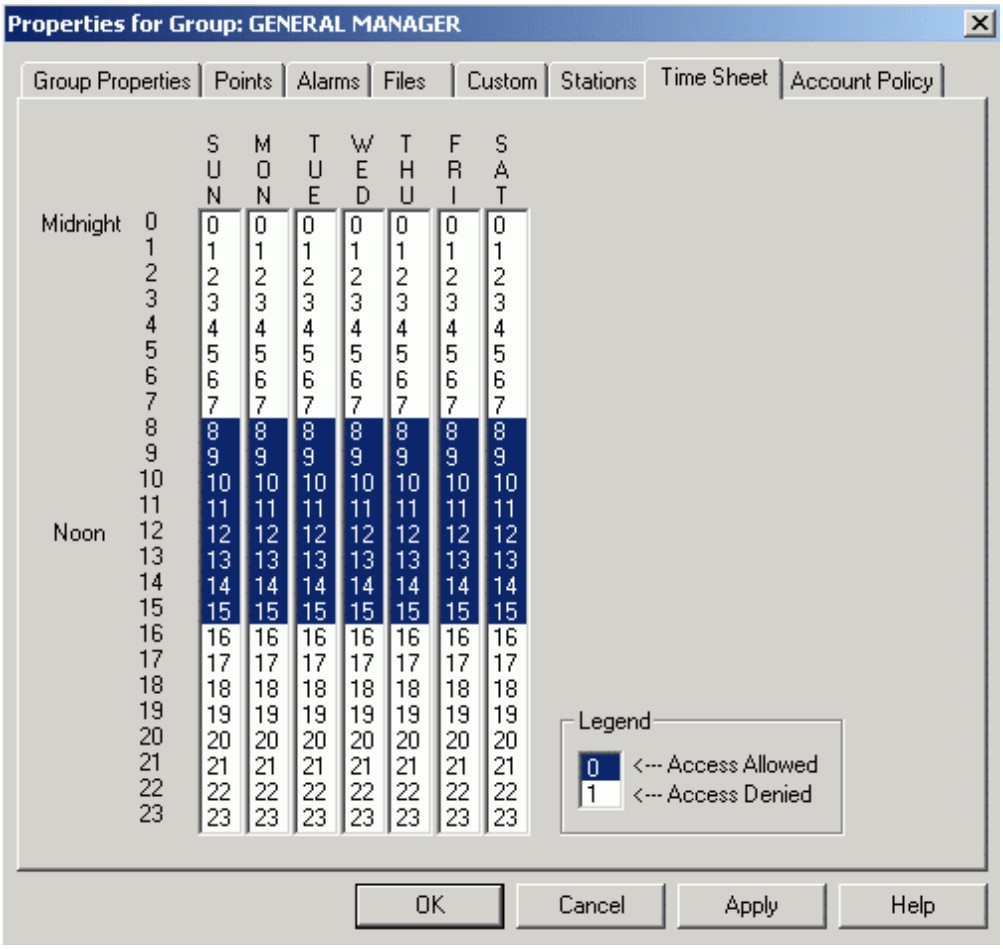
Station Configuration

The wildcard pattern matching described for the **Points** property page also applies here, but the runtime processing is slightly different, and the processing differs for users and groups. When a ProcessView client passes a Point, File, or Custom string to the Security Server for access testing, the station name where the client is running is also passed. For the currently logged-in user(s), the station include and exclude lists are searched for access from the client's station. If access from that station is denied for that user, the access request is instantly denied. The Point, File, or Custom string is never tested, nor are any of the groups to which the user belongs. This has the same effect as if the user had never logged in!

Unlike the user case, testing for station restrictions in groups only affects the current group (i.e. if access is denied for a group, then other active groups are still tested).

Time Sheet

The **Time Sheet** property page allows time-of-day restrictions on an hourly basis for users and groups. For hours that are selected (highlighted) in the lists, access is allowed. For hours that are not selected, access is denied. The figure below shows a configuration that allows access from 8 AM to 4 PM each day.

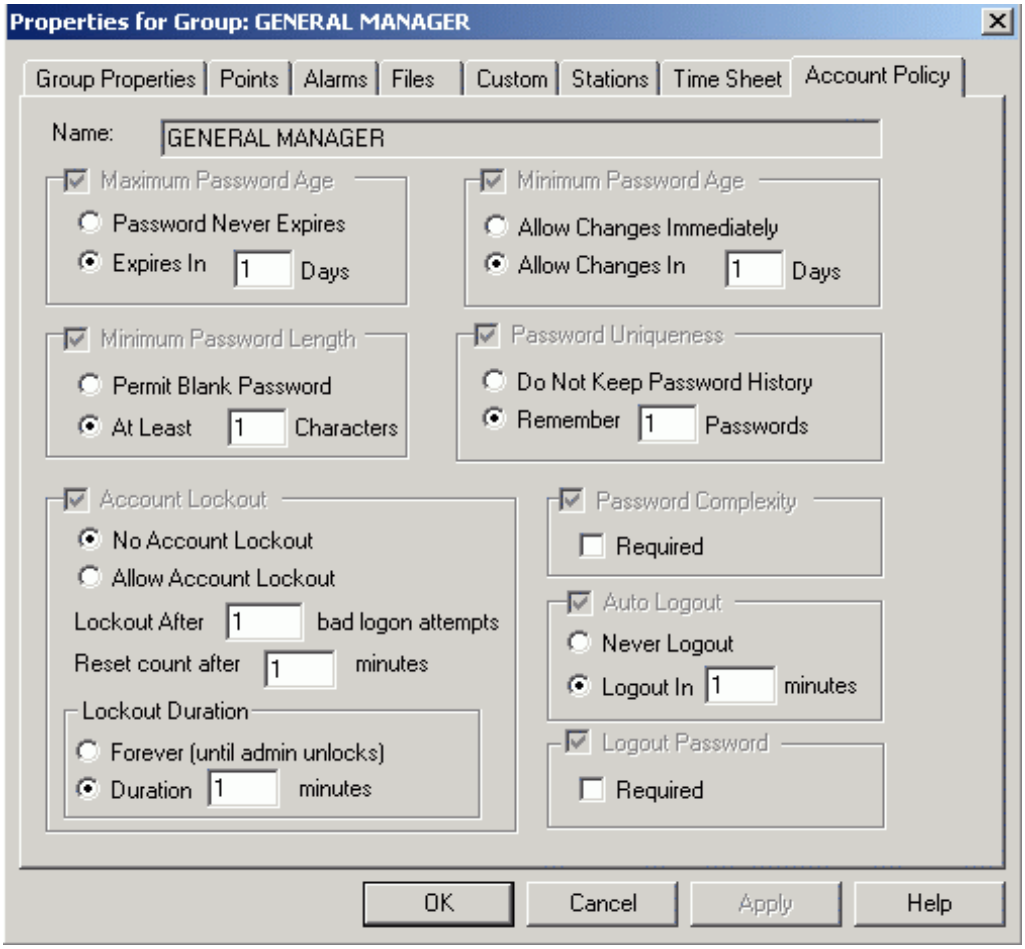


Time Configuration

Account Policy

The **Account Policy** property page is used to show how passwords must be used, and whether user accounts are automatically locked out after a series of incorrect login attempts. The base policy (i.e. the most restrictive) for the system is set in the default group (see the "Editing the Default Group" section). For users and groups other than the default group, each policy can selectively be enabled and set for that user or group.

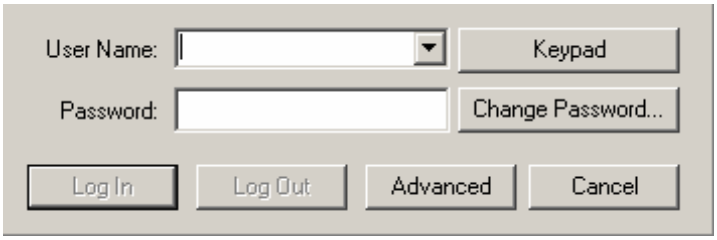
During runtime, if more than one policy setting is in effect, the least restrictive is used. For this reason, the policy set in the default group must be the most restrictive. Individual users and groups can be made less restrictive than the default, but never more restrictive.



Account Policy Configuration

FIELD	DESCRIPTION
Maximum Password Age	Sets a time limit for a password, after which the user must change to a new password. If this is selected, the **Expires in** value can range from 1 to 999 days. To make the password permanent, select **Password Never Expires.**
Minimum Password Age	Sets the period of time a password must be in effect before the user can change it. If this is selected, the value can range from 1 to 999 days. To allow the user to change the password at any time, select **Allow Changes Immediately.** **Note:** Do not allow immediate changes if a **Password Uniqueness** value is entered.
Minimum Password Length	In the **At Least** field, this specifies the fewest number of characters a password can contain. If this is selected, the value can range from 1 to 14 characters. If **Permit Blank Password** is selected, there is no minimum password length.
Password Uniqueness	The number of new passwords that must be used by a user account before an old password can be reused. If **Remember Passwords** is selected, the value can range from 1 to 24 passwords. If **Do Not Keep Password History** is selected, there is no password uniqueness. **Note:** For uniqueness to be effective, an age value should be specified for **Minimum Password Age** (**Allow Immediate Changes** should not be selected).
No Account Lockout	When selected, user accounts are never locked out, no matter how many incorrect login attempts are made on a user account.

FIELD	DESCRIPTION
Account Lockout	If selected, all user accounts are subjected to lockout. If too many incorrect login attempts are made on a user account, no more than a specified amount of time between these, the account is locked out. If you select **Account Lockout,** you should also do the following: In **Lockout After,** type the number of incorrect login attempts that will cause the account to be locked. The range is 1 to 999. In **Reset Count After,** type the number of minutes that must pass between any two login attempts to ensure that a lockout will not occur. The range is 1 to 999. Click **Duration** and type the number of minutes that locked accounts will remain locked before automatically becoming unlocked. The range is 1 to 999. Or, select **Forever** in **Lockout Duration** to keep locked accounts locked out until an administrator unlocks them.
Password Complexity	This option mimics the NT test for complexity. The password must: Not contain all or part of the user's account name. Be at least six characters in length. Contain characters from three of the following four categories: English upper case characters (A-Z) English lower case characters (a-z) Base 10 digits (0-9) Non-alphanumeric (For example, !,$#,%)
Auto Logout	If selected, sets the number of minutes from the time of user login, before the system automatically logs the user off. The range is 1 to 999 minutes.
Logout Password	To log out of the Security Server, the user specified in the **User Name** field of the **Security Login** dialog of the Security Login application must click the **Log Out** button, as shown in the figure below. When a **Logout Password** is required in the user's account policies, the user must type in his or her password when logging out.

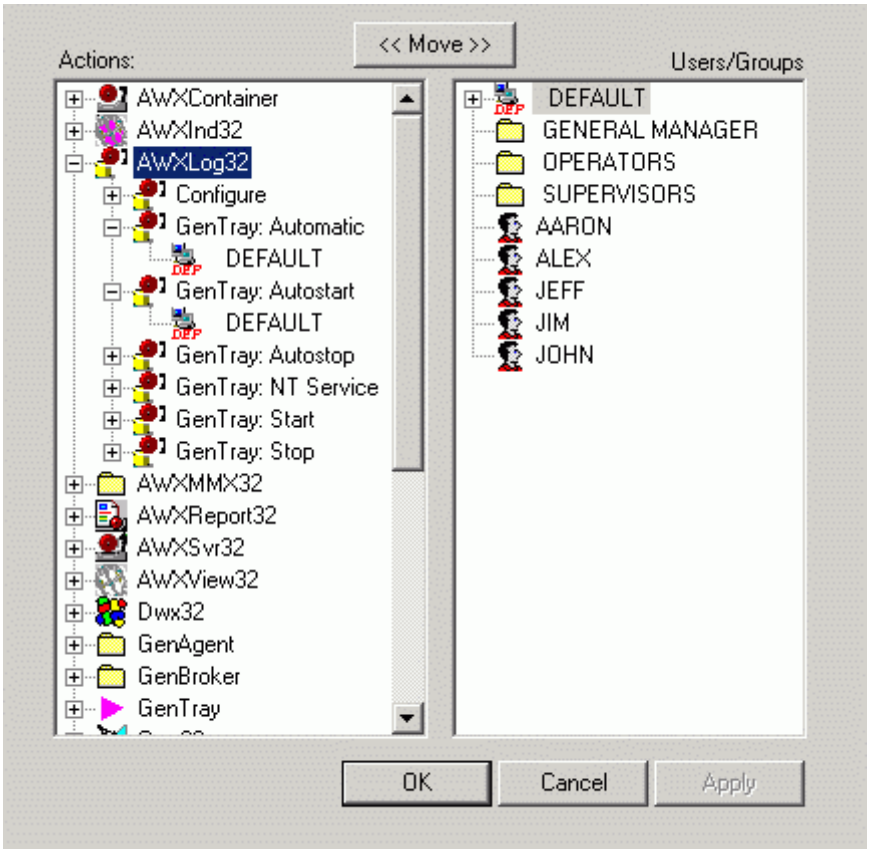


Security Login Dialog Box in Security Login Application

Assigning Application Actions

Each ProcessView application may supply a static list of functions to be secured. For example, functions such as adding trend pens in TrendWorX or entering configuration mode in GraphWorX are commonly disallowed for operators via the security system.

Each ProcessView client provides a list of application functions that can be protected through the security system. To configure which users and groups have access to specific application actions, select **Application Actions** from the **Edit** menu in the Security Configurator. This opens the **Actions/User Association** dialog box, shown below.



Assigning Application Actions

The dialog box has two tree controls. The parent items in the **Actions** (left) tree control are the ProcessView application names. The child items of the application names are the application functions that can be protected. The child items of the application functions are the users and groups that are granted access to the function.

The parent items in the **Users/Groups** tree control on the right are the users and groups defined in the security system. The child items of the users and groups are the ProcessView application names. The child items of the application names are the application functions that are allowed for the parent user or group.

To grant access to a single application function to a user or group:

1. In the left tree control, select the application function to be assigned.
2. In the right tree control, select the user or group that should have access to the application function selected in the left tree.
3. Click the **Move** button.

To grant access to all application functions of a ProcessView client:

1. In the left tree control, select the application name.
2. In the right tree control, select the user or group that should have access to the all of application's functions selected in the left tree.
3. Click the **Move** button.

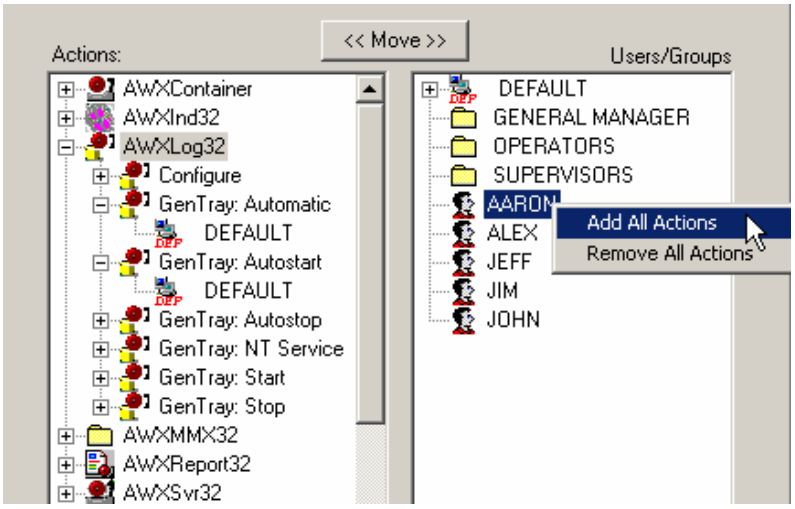
To remove access rights to an application action, select the user or group name in the left tree or select the application name or function in the right tree, and then press the **Delete** key.

NOTE
This operation never deletes the user, group or application function. Only their association is removed.

Adding and Removing All Application Actions

Right-clicking on a user or group in the right pane of the **Applications Actions** dialog shows a pop-up menu with two entries, as shown in the figure below.

- **Add All Actions:** Associates all actions with the selected user or group.
- **Remove All Actions:** Deletes the selected user or group from all actions.



Adding and Removing All Application Actions

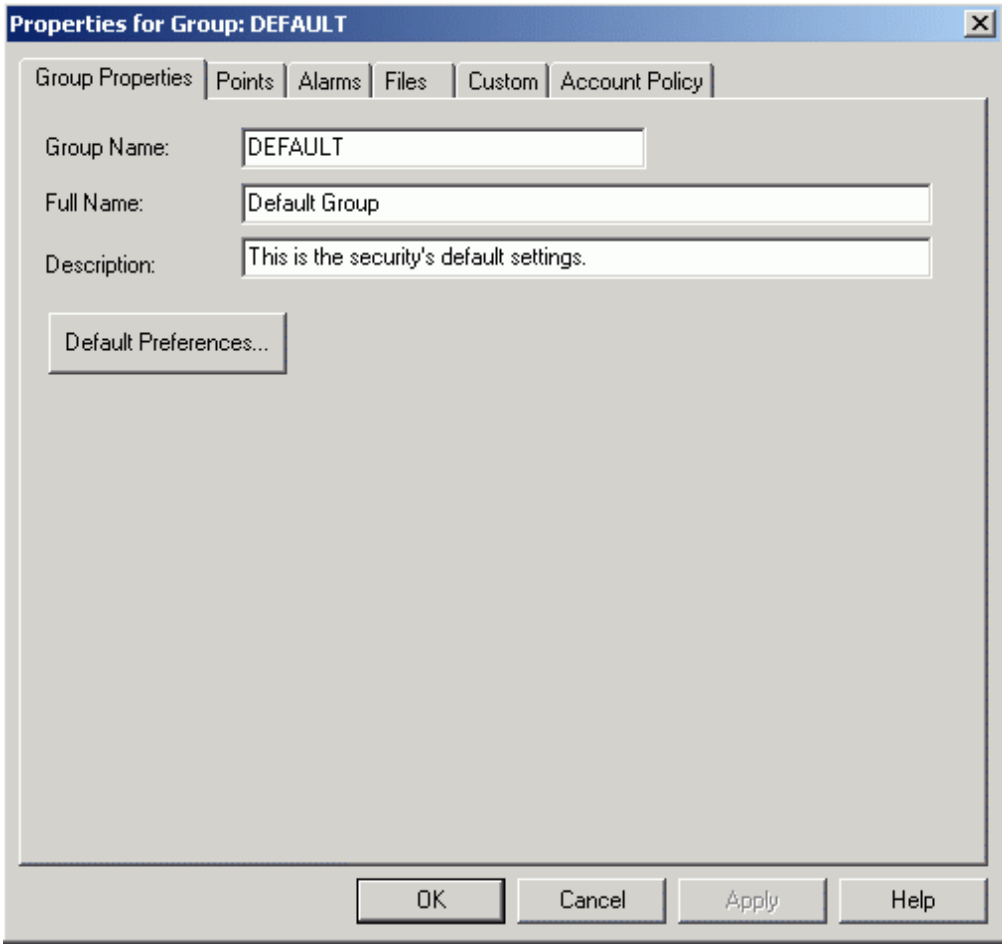
Editing the Default Group

The system **default group** (available in advanced security configuration mode only) is used to assign access rights that are granted regardless of whether any users are logged in. When the Security Server is first installed, the default group has full access to everything. The first step in configuring the security system is to remove most if not all access rights assigned to the default group.

NOTE
You must configure the default group to have minimum access rights, because individual users and groups can only add access rights but can never remove rights already granted in the default group**.**

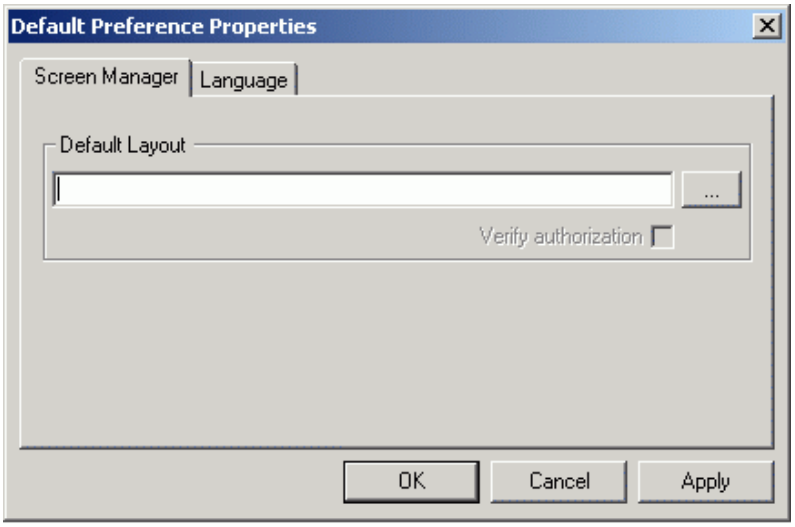
To edit the default group, select **Default Group** from the **Edit** menu in the Security Configurator. This opens the **Properties** dialog box for the default group, as shown below. The same property pages used to edit ordinary groups are used for the default group, with the following differences:

- There is no **Stations** property page. Default access is valid for all stations.
- There is no **Time Sheet** property page. Default access is valid for all hours.
- **Account Policy** must be set in the default group.



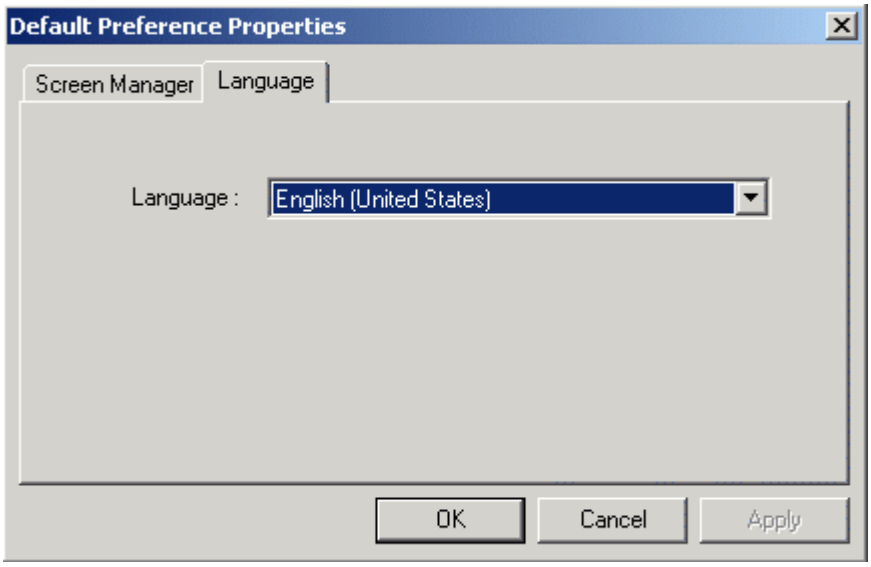
Properties for Default Group

Clicking the **Default Preferences** button opens the **Default Preference Properties** dialog box, shown below. In the **Screen Manager** tab, you can browse for a default Screen Manager layout (.pwf) file.



Default Preferences Properties: Screen Manager Tab

The **Language** tab, shown below, allows you to select the language for the default group.



Default Preferences Properties: Language Tab

Security Login Utility

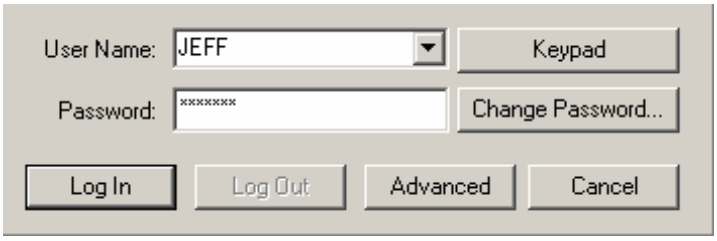
To log in to the security system, start the Security Login Utility:

1. From the Windows **Start** menu, select **Programs > Smar ProcessView > Security Login.**

NOTE
You can also start the Security Login Utility from other ProcessView applications during runtime mode.

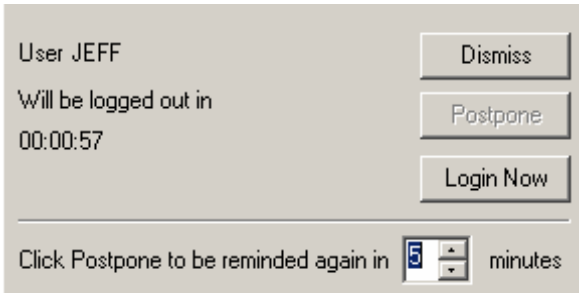
2. This opens the **Security Login** dialog box, shown below. Enter the **User Name** and **Password.** You can use the **Keypad** if necessary. Click the **Log In** button.

NOTE
Passwords are case sensitive



Security Login Dialog Box

If the login attempt is successful, the dialog closes and the Security Login Utility is now running. Depending on the user account policy settings, the user may be logged out automatically. To log in again, the user must click the **Login Now** button, as shown in the figure below.



Auto Logout Reminder

Login Dialog Parameters

The **Security Login** dialog box contains the following parameters:
User Name: When the login dialog is displayed, the edit field will be populated in one of the following ways:

1. With the name of a logged in user if one or more users are logged in.
2. With the name of the last user who logged in from this node if no one is currently logged in. The last user name will only be displayed if allowed by the Global Policy in the Security Server.

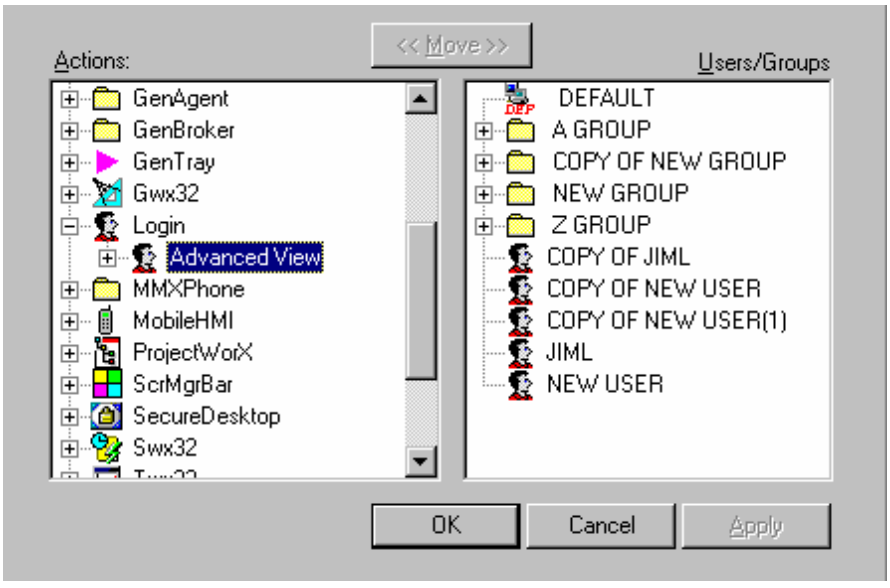
The drop-down list contains the names of the users currently logged in from this node. The list will optionally contain a list of all available users in the Security Server if the **Global Policy** in the security configuration allows **User Lists.** This is largely to remove the burden of typing user names when using touch screens.

Password: Passwords are case sensitive. The user may have to type in his or her password on logout, depending on the security policy for the logged-in user.

Log In: Clicking this button sends the **User Name** and **Password** to the Security Server for login. After a successful login, the dialog is closed and the login application remains running in hidden mode.

Log Out: The user specified in the **User Name** field will be logged out. The user may have to type in his or her password on logout, depending on the security policy for the logged in user.

Advanced: This button closes the dialog and makes the hidden Security Login application main window visible. This button is disabled if the current logged in user(s) do not have permission to use **Login Advanced** mode, which is an application action configured in the Security Configurator, as shown in the figure below.



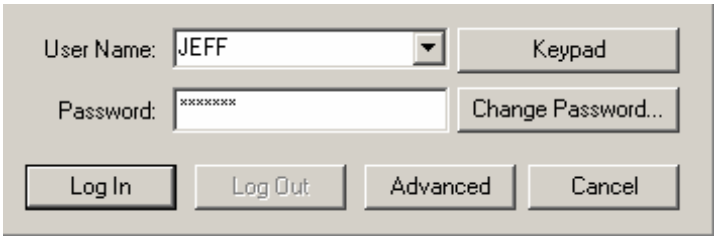
Login Application Action Configured in Security Server

Cancel: Closes the dialog. If no logged-in users remain from this node, the Security Login application will close, otherwise it remains running in hidden mode.

Keypad: Pops up QUERTY key entry pad. This is useful for touch-screen systems.
Change Password: Displays the Change Password dialog box.

Main Window

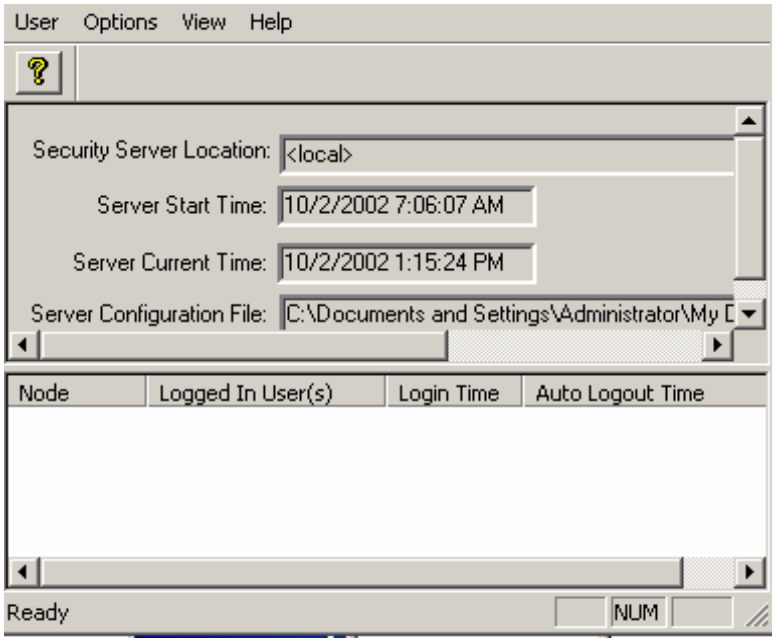
The Security Login client application interface is hidden by default and is displayed only in advanced mode. To view the full Login client interface, click the **Advanced** button on the **Security Login** dialog box, as shown in the figure below. This opens the main window for Security Login Utility.



Security Login Dialog Box

The main window of the Login Utility is divided into two panes, as shown in the figure below. The upper pane contains the status of the Security Server to which the Login Utility is connected. The following display-only fields are shown and updated:

FIELD	DESCRIPTION
Security Server Location	The name of the workstation where the Security Server is running and to which the Login Utility is connected. It is "**<local>"** if the Security Server is running on the same workstation as the Login Utility.
Server Start Time	Date and time the Security Server was started. Time is converted to the local time of the user workstation if the Security Server is in a different time zone.
Server Current Time	Current date and time as reported by the Security Server on the last update. Time is converted to the local time of the user workstation if the Security Server is in a different time zone.
Server Configuration File	Name and path of the configuration file currently being used by the Security Server.



Login Utility Main Window

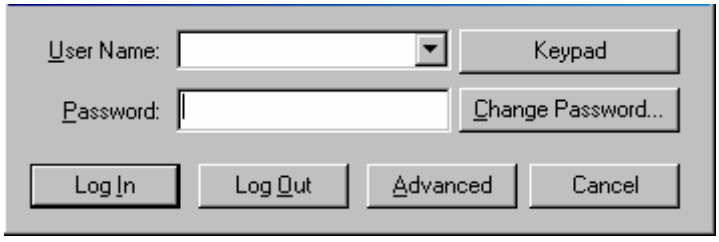
The lower pane contains a list of users that are currently logged in. The list includes the following information:

- The node name.
- The user name.
- The time the user last logged in.
- The time at which the Security Server will automatically log the user out. If this field is blank, the user will never be logged out automatically.

The lower pane shows all users logged into the Security Server from all nodes, provided the current user is a security system administrator. The **Node** column indicates the location of the logged in user. For non-administrative users, the view shows just the users logged in from the local node.

Logout

To logout from the security system, select **Logout** from the **User** menu. If a single user is logged in, the user will be logged out. If more than one user is logged in, the **Security Logout** dialog will open as shown below, allowing you to select the user to be logged out. Click the **Log Out** button. The user specified in the **User Name** field will be logged out. The user may have to type in his or her password on logout, depending on the security policy for the logged in user.

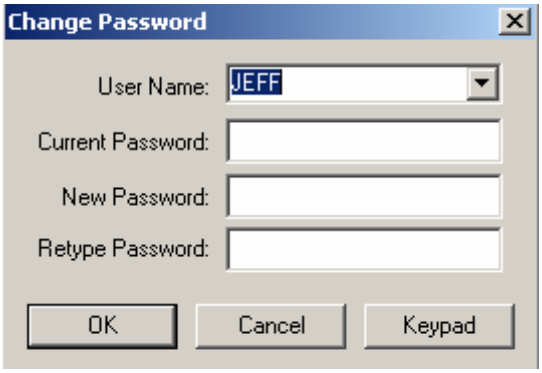


User Logout Dialog

Change Password

To change the password, select **Change Password** from the **User** menu. This opens the **Change Password** dialog box, shown below. Enter the user name, the current password, and the new password. Then retype the password to confirm it. Click **OK.**

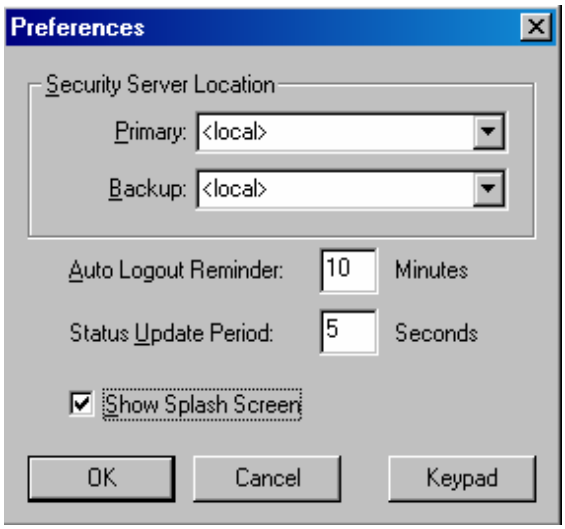
NOTE
Users may be restricted from changing their passwords from the Security Login Utility.



Change Password Dialog Box

Login Utility Preferences

You can set the Login preferences by choosing **Preferences** from the **Options** menu. This opens the **Preferences** dialog box, shown below.



Preferences Dialog Box

FIELD	DESCRIPTION
Security Server Location	Enter the names of the primary and backup nodes to which the Login Utility should connect in order to run the Security Server. This is "<local>" by default. **Note:** Expanding the drop-down list will cause all nodes on the network to be searched for installed Security Servers. This can take a long time. If you know the name of the workstation, it is much faster to type it in.
Auto Logout Reminder	The number of minutes prior to a Security Server auto logout that a user should be reminded to re-login. The range is 0 to 60 minutes. Enter 0 for no popup reminder window.
Status Update Period	The period between updates of the Server Status in the main window. The range is 1 to 60 seconds.
Show Splash Screen	Hides/shows the Security Login splash screen (default is to show the splash screen).

WebHMI Security

The **Symbol Library** in GraphWorX contains a symbol category file called "WebHMI Security Login.sdf," which contains several symbols that, when dragged into a GraphWorX display, allow users to gain access to the Security Server.

All the symbols use VBScript to call the Security Server on the remote WebHMI Server and get back security information. You do not need to know VBScript to use this symbol. You can directly drag and drop the symbol that you need from the Symbol Library into your display, but you also have the freedom to use the Script Editor toolbar in GraphWorX to change the source code associated with each of these symbols. Or you can copy the code and attach it to your own symbols.

All of the scripts associated with these symbols create an instance of the “Smar Login ActiveX” and call methods of this object or access properties. The complete automation for the “Smar Login ActiveX” is described below.

These symbols are shown in the figure below.

WebHMI Security ActiveX Symbols in GraphWorX

Logging Into the Security Server

The WebHMI Security Login ActiveX symbol button, shown in the figure below, enables WebHMI users on remote client machines to log in to the Security Server. For example, if the "Login" symbol button is placed in a GraphWorX display, the user can simply click on the symbol (button) in runtime mode to launch the Security Login dialog box, as shown in the figure below.

Security Login Symbol Button

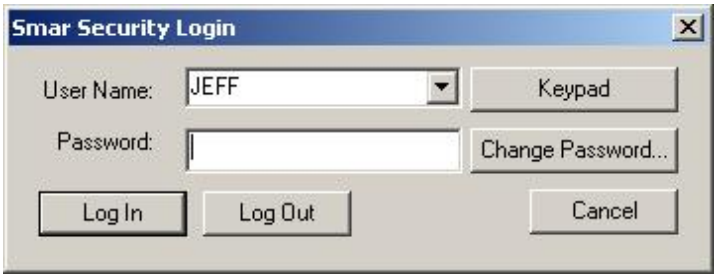
The **Security Login** dialog is basically the same as the one for the Security Login Utility, except that the **Advanced** login mode is disabled, as shown in the figure below. The WebHMI Security Login ActiveX also includes full keypad support (ideal for touch-screen systems). The Login ActiveX allows simultaneous login of many users (this must be enabled on the Security Server global settings).

The drop-down list for the user name can show:

- The complete list of users in the system.
- The list of the currently logged users.
- The name of the last logged user.

All of these features must be enabled on the Security Server in order to work.
For more information, please see the Security Configurator Help documentation.

NOTE
When you log into the Security Server using the Login ActiveX, you do not get any warning messages when the security session is about to expire. If your security session expires, then the Login ActiveX will automatically be displayed again.



Logging Into the Security Server

Changing the Security Server Password

If you should wish to change your password you can do it by clicking on the Change Password button on the login ActiveX dialog, or you can do it directly by using the Change Password symbol button and dragging it into your GraphWorX display.

Change Password Button

Clicking the **Change Password** button opens the **Security Password Change** dialog box, as shown in the figure below. Type your new password in the **New Password** and **Retype Password** fields, and then click the **OK** button.

Changing the Security Password

Viewing the Logged User List

To view a list of users currently logged in to the Security Server, click the Logged User List symbol button in your GraphWorX display, as shown in the figure below.

Logged Users List Button

The **Security** window will appear, as shown in the figure below. The **Security** window allows you to view the list of users that have logged in.

Security Window

Logging out of the Security Server

To log out everyone who has logged in, you can use the **Log Out All Users** symbol button shown in the figure below.

Logout All Button

You can also logout one specific user with a simple click on the **Logout User** button, as shown in the figure below.

Logout User Button

NOTE
You have to specify the user to be logged out in the VBScript code associated with this button. You can do it by editing the script with the Script Editor toolbar in GraphWorX.

Security OLE Automation

The OLE Automation interface for the WebHMI Security ActiveX is compatible with VBA and VBScript. You can perform login/logout operations directly trough scripting without displaying any user interface. The WebHMI Security ActiveX contains the following OLE Automation interfaces:

LoginDlg()
Launches the login dialog.

ChangePwdDlg()
Launches the dialog to change the password.

ShowLoggedInUsers()

Launches the dialog to show a list of the usesr currently logged into the Security Server.

Logout()
Logs out all currently logged users.

SetTimeout(LONG nSec)
Sets the timeout for all of the GenClient calls to the Security Server.

ShowResultMsgs(BOOL bShow)
Enables / disables the message box with the result (e.g. "failed to log on to the Security Server").

LoginUser(BSTR username, BSTR password)
Logs in one specific user through code.

LogoutUser (BSTR username)
Logs out a specific user through code.

GetLoggedInUsersNames (BSTR usernames)
Gets the list of currently logged users. The string “usernames” is filled with the comma-separated list of currently logged user names. Note that by default the Security Server does not allow concurrent login of multiple users; the concurrent login option must be enabled from the Security Server Configurator. Please refer to the Security Server documentation for additional details.

Launching the Security Login ActiveX Through Scripting

The Security Login ActiveX can be programmatically created and initialized from VBA Script, VBScript and JScript. The GraphWorX Symbol Library contains a category named “WebHMI Security Login” located under the “VBAScriptSymbol” folder, which is filled with samples of each of the automation interfaces listed above. Please refer to the aforementioned samples for additional information on how to use the Login ActiveX through scripting.
The following code sample has been extracted from the Symbol Library; this sample shows how to launch the Login ActiveX from VBScript. The code runs on WebHMI too:

```
Set t = CreateObject ("Smar.LoginActiveX")
If t Is Nothing Then
    MsgBox "An error has occurred while trying to launch the login dialog."
Else
    t.LoginDlg()
End If
```

The following code sample has been extracted from the Symbol Library; this sample shows how to get the list of currently logged users from VBScript. The code runs on WebHMI too:

```
Set t = CreateObject ("Smar.LoginActiveX")
If t Is Nothing Then
    MsgBox "An error has occurred while trying to launch the login dialog."
Else
  t.GetLoggedInUsersNames str
    MsgBox str
End If
```