

## CHAPTER 3

# Using InTouch Security

InTouch gives you the option of selecting either traditional InTouch-based security, operating system-based security or ArchestrA-based security. All InTouch security methods are configurable with application granularity, meaning that you can operate two applications with different security settings on the same computer.

All three security methods are compatible with Network Application Development (NAD) distribution of applications. InTouch-based security works with NAD as it did in previous versions of InTouch. For more information on NAD, see Network Application Development (NAD). ArchestrA-based security is centralized regardless of whether NAD is used or not.

If the authentication mode is operating system-based, then the user names will be the Windows Domain Name / User name pairs. If the mode is ArchestrA-based, then the security related activities would be configured externally in the Integrated Development Environment (IDE). For more information on the IDE, see the Wonderware® ArchestrA™ Integrated Development Environment (IDE) Guide.

## Contents

- Using InTouch-Based Security
- Using Operating System-Based Security
- Using ArchestrA-Based Security
- Creating a Custom Security Log on Window
- InTouch Security Script Functions

## Using InTouch-Based Security

Applying security to your application is optional. The default security setting for InTouch applications is "None." However, by applying security to your application, you can control specific functions that an operator is allowed to perform by linking those functions to internal tagnames. In addition, when you establish security on your application, audit trails can be created that tie the operator to all alarms/events that occur during the time he/she is logged on to the system.

Security is based on the concept of the operator "logging on" to the application, typing his/her name and password. You must configure a user name, password, and access level for each operator.

There is no association between Microsoft operating system security and InTouch security.

When you create a new application, by default, the user name is set to "Administrator" with an access level of 9999 (which allows access to all security commands). After you add a new user name to the security list and restart WindowMaker or WindowViewer, the default user name is automatically reset to "None" with an access level of "0" (which prevents access to the **Configure Users** command in both WindowMaker and WindowViewer). However, the Administrator account and password remain and can still be used.

After an operator logs on to the application, access to any protected function will be granted upon verification of the operator's password and access level against the value specified for the internal security tagname linked to the function.

For example, you can control access to a window, or the visibility of an object and so on, by specifying that the logged on operator's "Access Level" must be greater than 2000.

The operator can log on to the application by executing the **Log on** menu command under **Security** in the WindowViewer **Special** menu (if the **Special** menu is displayed), or you can create a custom log on window with touch-sensitive input objects that are linked to internal security tagnames.

The commands used to establish security on an application are located under **Security** on the **Special** menu in both WindowMaker and WindowViewer. The security commands are used to log on and off the application, change passwords and to configure the list of valid user names, passwords and access levels.

## Using the Security Internal Tagnames

After you implement security for your application, there are several internal security tagnames that you can use on buttons, in animation link expressions or QuickScripts, and so on, to control whether or not the logged on operator is allowed to perform specific functions:

Tagname	Type	Valid Values	Access
\$AccessLevel	System Integer	0-9999	Read Only
\$Operator	System Message	16-characters max	Read Only
\$ChangePassword	System Discrete	1 or 0	Read Write
\$ConfigureUsers	System Discrete	1 or 0	Read Write

Tagname	Type	Valid Values	Access
\$InactivityTimeout	System Discrete	1 or 0	Read Only
\$InactivityWarning	System Discrete	1 or 0	Read Only
\$OperatorEntered	System Message	16 characters max	Read Write
\$PasswordEntered	System Message	16 characters max	Read Write

For example, to make an object become visible based on the logged on user's access level, the following statement could be used in a visibility animation link expression:

```
$AccessLevel >= 2000;
```

Or, a QuickScript can be bounded by an IF statement:

```
IF $Operator == "DayShift" THEN
    Show "Control Panel Window";
    {and other lines that only execute for the DayShift
     Operator}
ENDIF;
```

You can also control an object's touch functionality based upon the value of an internal security tagname by using the **Disable** animation link. For example:

Object Disabled -> Discrete Value

Expression:

`$AccessLevel == 0 OR $Operator == "none"`

Disabled State

☐ On ☒ Off

OK Cancel Clear

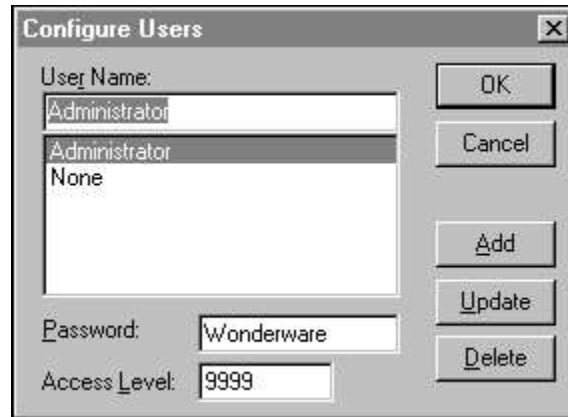
By using this expression, if no one is logged on, the object or button is secured from tampering.

For more information on the internal security tagnames, see your online *InTouch Reference Guide*.

## Configuring the User and Security Levels

To configure security for the operators of your application

1. On the **Special** menu, point to **Security**, then click **Configure Users**. The **Configure Users** dialog box appears.'



---

**Tip** If you right-click any of the text entry boxes in any dialog box, a menu appears displaying the commands that you can apply to the selected text.

---

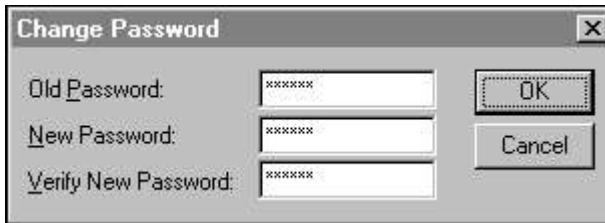
2. In the **User Name** box, type the name that you want to assign to the operator.
3. In the **Password** box, type a password (up to 16 characters).
4. In the **Access Level** box, type a value (lowest = 0 to highest = 9999).
5. Click **Add** to add the user name to the security list.
6. To **modify** an existing user name, select the desired name in the **User Name** list. Type your changes and then click **Update** to accept the changes.
7. To **delete** a user name, select it in the list and then click **Delete**.

The **None** and **Administrator** names are reserved and only the password of the Administrator may be changed. Once you have configured user names for your application, you should change the Administrator name's password since it will more than likely become commonly known to most users of the system. The Administrator default access level (9999) is the highest and allows access to everything including the Configure Users menu command.

## Changing a Security Log On Password

### To change the password for an operator

1. On the **Special** menu, point to **Security** and then click **Change Password**. The **Change Password** dialog box appears.



If you right-click any of the text entry boxes in any dialog box, a menu appears displaying the commands that you can apply to the selected text.

2. In the **Old Password** field, type the old password.
3. In the **New Password** field, type the new password (up to 16 characters).
4. In the **Verify Password** field, type the new password again.
5. Click **OK**.

To prevent anyone who may be watching the operator from seeing the password, the information entered is displayed on the screen as asterisks.

---

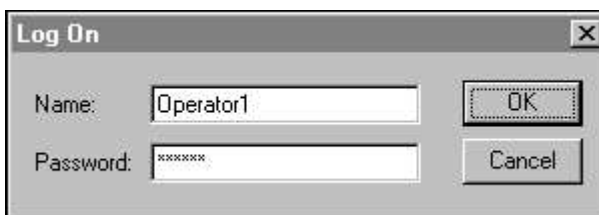
**Tip** If you do not plan on displaying the **Special** menu in WindowViewer, you can create a discrete button and link it to the **\$ChangePassword** internal tagname. Do so in order to set the **\$ChangePassword** tagname equal to 1 to cause the **Change Password** dialog box to be displayed. Once displayed, the operator can change his/her password.

---

## Logging on to an InTouch-Secured Application

### To log on to an application

1. On the **Special** menu, point to **Security** and then, click **Log On**. The **Log On** dialog box appears.



2. In the **Name** box, type your user name.
3. In the **Password** box, type your password.

4. Click **OK**.

If the information is entered incorrectly or is invalid, a message box indicating that log on failed appears.

If log on is successful, the **\$AccessLevel** internal tagname will be set to its predefined value (configured in the security user list).

---

**Note** See also PostLogonDialog().

---

## Logging Off an InTouch-Secured Application

### To log off the application

- On the **Special** menu, point to **Security** and then click **Log Off**.

When this command is executed, the "User Name" is reset to "None" with an Access Level of "0."

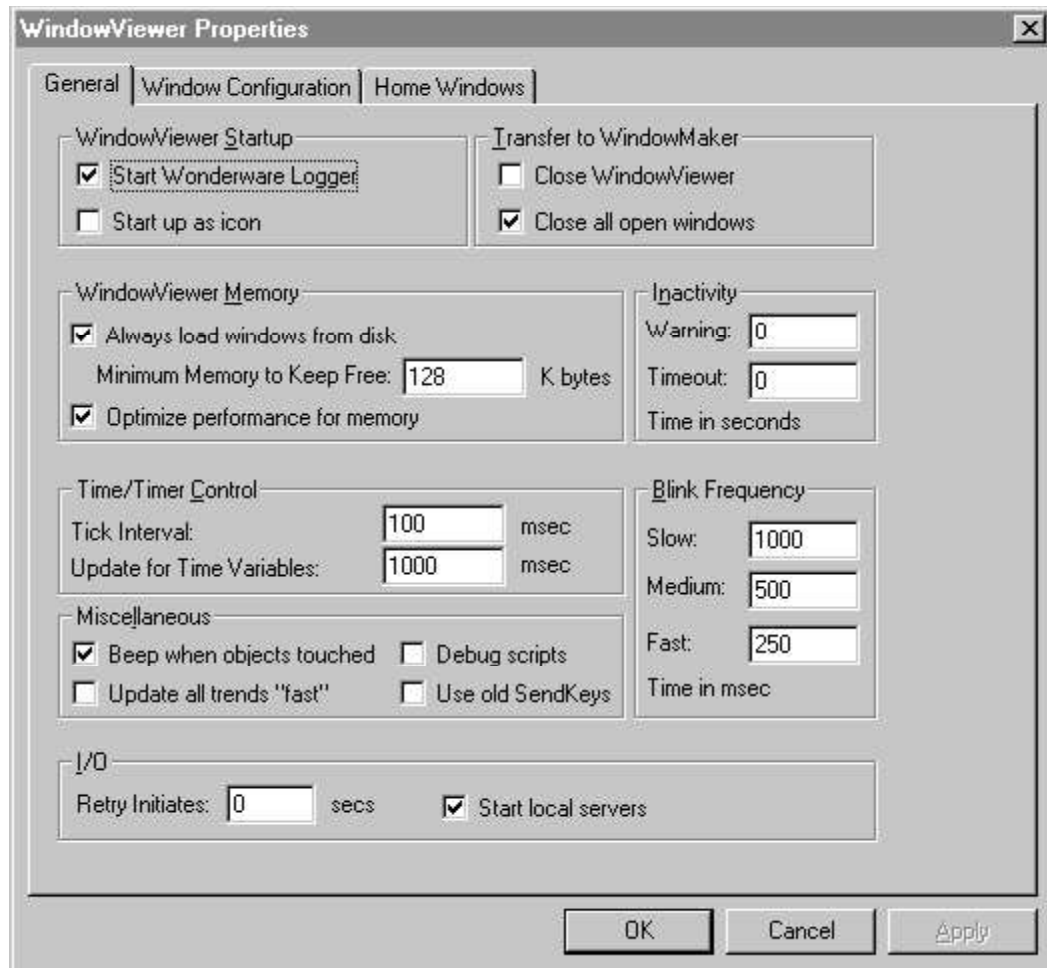
You can also configure the application to automatically log off the operator after a specified amount of time has elapsed with no activity by the operator.

## Automatically Logging Off the System

You can configure your application to automatically log off the operator when there has been no activity for a specified period of time by using the warning and time out settings.

### To configure inactivity

1. On the **Special** menu, point to **Configure** and then click **WindowViewer** or in the Application Explorer under **Configure**, double-click **WindowViewer**. The **WindowViewer Properties** dialog box appears with the **General** properties sheet active. In the Application Explorer, you can also right-click **WindowViewer** and then click **Open**.



2. In the **Warning** box, type the number of seconds that can elapse with no operator activity (mouse clicks or keystrokes) before the system discrete tagname **SInactivityWarning** is set to 1 (True). When the **Inactivity Warning** is set to zero, there will not be an inactivity warning.

**Tip** You can use **SInactivityWarning** in a Condition QuickScript to show a window warning the operator that he/she is about to be logged off the system. If the operator clicks the mouse, presses a key, or performs an action using any other pointing device before the specified time-out elapses, they are not logged off. **SInactivityWarning** and the timer are reset.

3. In the **Timeout** box, type the number of seconds that can elapse with no operator activity (mouse clicks, keystrokes, and so on) before the system discrete tagname **\$InactivityTimeout** is set to 1 (True). When **\$InactivityTimeout** is true, the system equates the logged on operator name to the reserved name "None" and sets the security tagname, **\$AccessLevel**, to 0.

---

**Tip** You can use **\$InactivityTimeout** in a Condition QuickScript to show a window telling the operator that he/she has been logged off the application.

You can use the **Timeout** feature independently of the **Warning** feature. However, the **Timeout** value must be greater than the **Warning** value for proper use of both system tagnames.

For example, set **\$InactivityWarning** to 30 and **\$InactivityTimeout** to 45. The operator will be logged off 15 seconds after the **\$InactivityWarning** variable is set to 1.

---

## Using Operating System-Based Security

In the operating system-based authentication scheme, user names can be chosen from the list of users associated with a Windows Network Domain\Workgroup. Each user name has an assigned access level that determines the user's authorization for a given activity. Since the operating system manages the passwords internally, InTouch will not store passwords.

Operating system-based security uses the InTouch script function **AddPermission** to maintain a list of users and their corresponding access levels. This list, created after the execution of the **AddPermission()** call, is written to disk. The file containing the authentication details of users will not be copied to the NAD client machines.

## Setting Up Operating System-Based Security

Operating system-based security can be selected from the Security Type menu in WindowMaker. This would typically be done when a new application is created. Typically, you will select security settings when you create a new InTouch application.

### To set operating system-based security:

1. Open a window in WindowMaker.
2. On the **Special** menu, point to **Security**, then point to **Select Security Type** and select **OS**.



## Using the Security System Tagnames

The three new security system tagnames for operating system-based security are \$OperatorDomain, \$OperatorDomainEntered and \$OperatorName. The tables below explain the functions of these new system tags and provide examples:

### \$OperatorDomain

Category	Security
Usage	If operating system-based security is selected and an operator has successfully logged on, the \$OperatorDomain tag will contain the domain or machine name that was specified at log on. If ArchestrA security is selected a user is logged on, the \$OperatorDomain will contain "ArchestrA." If InTouch security is selected, the \$OperatorDomain tag contains the string "InTouch." If "None" is selected, it is an empty string "".
Remarks	N/A
Data Type	String
Example(s)	<code>\$Operator = "john";</code> <code>\$OperatorDomain="CORPORATE_HQ";</code>
See Also	<b>\$Operator</b>

### \$OperatorDomainEntered

Category	Security
Usage	Whenever the \$PasswordEntered tag changes, a log on is attempted internally without any GUI being displayed. The log on attempt uses the \$*Entered tags as input user name and the string value of \$OperatorDomainEntered as the domain name (used only if the current mode is operating system-based security). If the security mode is not operating system-based, this tag is ignored.
Remarks	N/A
Data Type	String
Example(s)	<code>\$OperatorEntered="john";</code> <code>\$OperatorDomainEntered="Corporate_hq"</code> <code>\$PasswordEntered="password";</code>
See Also	<b>\$Operator</b>

## \$OperatorName

<b>Category</b>	<b>Security</b>
<b>Usage</b>	The \$OperatorName tag will contain the full legal name of the operator if operating system-based or ArchestrA authentication is used and someone has logged on and has not logged off. Otherwise, the tag will contain the name of the user logged on (same contents as the \$Operator tag).
<b>Remarks</b>	N/A
<b>Data Type</b>	String
<b>Example(s)</b>	<code>\$Operator = "john"; \$OperatorName = "John Smith";</code>
<b>See Also</b>	<b>\$Operator</b>

## \$VerifiedUserName

	Contains the verified user's full name if the call to InvisibleVerifyCredentials() is successful and if the security mode is set to operating system-based or ArchestrA AppServer-based security. If the call fails, then the above system tag will be set to null.
<b>Category</b>	security
<b>Usage</b>	<b>\$VerifiedUserName</b>
<b>Remarks</b>	Whenever the above system tag changes (meaning whenever InvisibleVerifyCredentials is called), an event will be generated and the column "Value" will contain the verified user's full name if the call was successful. The column "Value" will contain null if the call failed. The column Name will contain the value "\$VerifiedUserFullName."
<b>Data Type</b>	String
<b>Valid Values</b>	<b>A User's full Name</b>
<b>Example(s)</b>	Tag = InvisibleVerifyCrdenentials( "john","password", "Plant_Floor"). If the call is successful, the \$VerifiedUserName is set to "John Smith" and an Operator Event is generated. The name column indicates in the event \$VerifiedUserName and the value column is set to "John Smith." If the above call is not successful, \$VerifiedUserName and the value column in the event are set to "". Every time the above script function is called, the \$VerifiedUserName is set to the corresponding user's full name or to null.
<b>See Also</b>	<b>InvisibleVerifyCredentials(); \$OperatorName, \$Operator</b>

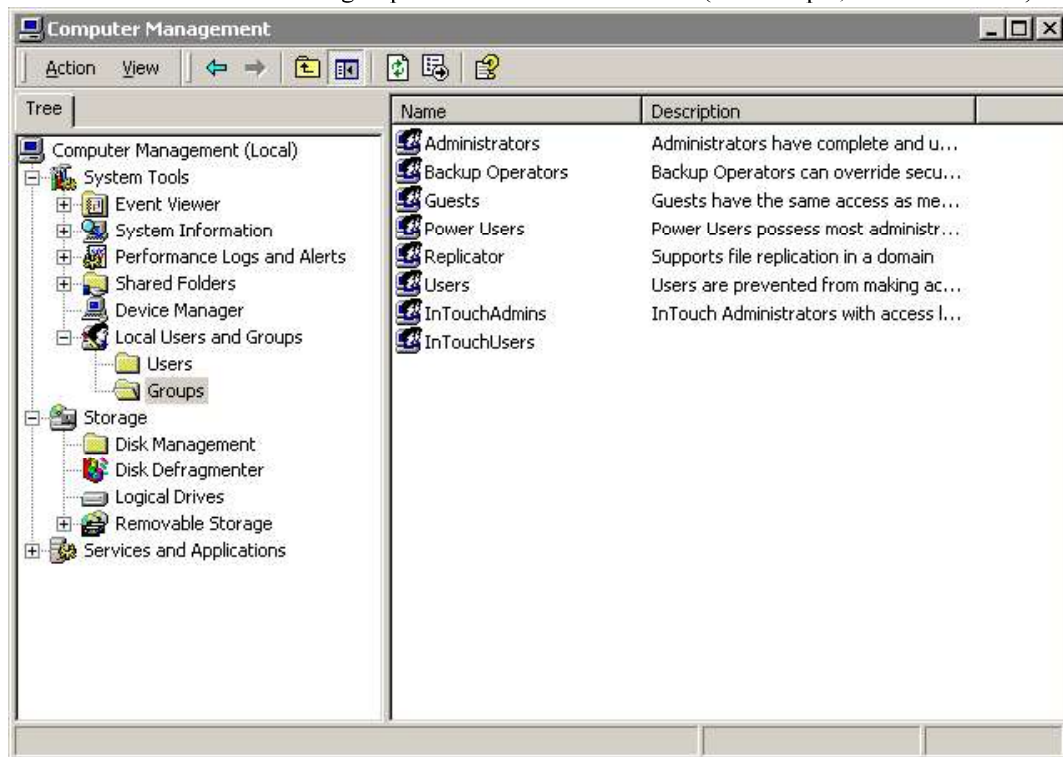
## Setting Up User Groups

Operating system-based security uses a list of authorized Windows user groups. Users will create user groups either on the local computer or a domain server. The administrator must associate Windows users to groups by adding them to specific groups. In WindowMaker, the application developer must use the script function AddPermission() to set up a list of groups with the desired access levels for each group. AddPermission() will typically be called on application start-up so that view recognizes all the authorized user groups when a user is ready to log on. You must be logged on as a local administrator

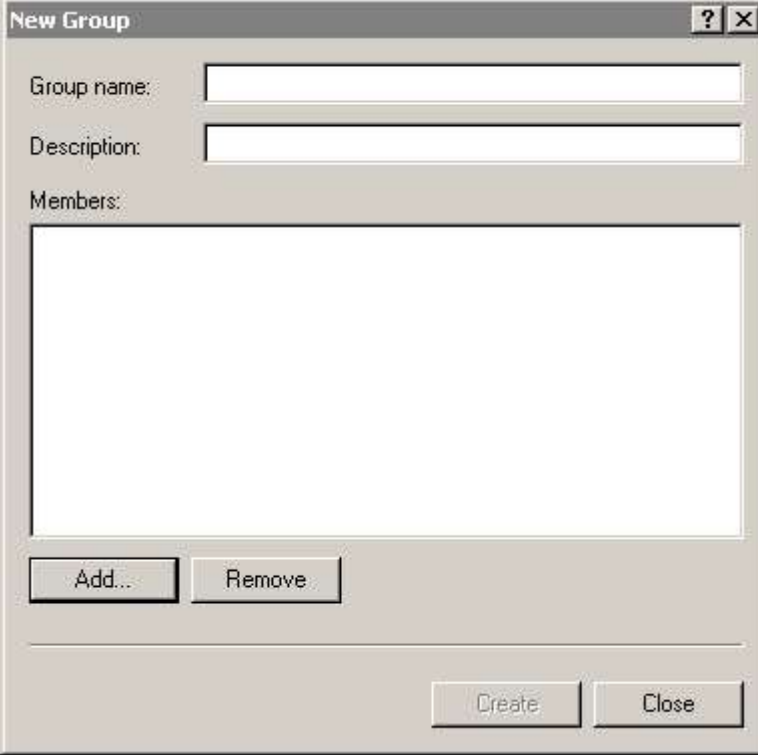
or have local administrator rights to set up and administrator group on a local computer.

### To set up an administrator group on a local computer and add users

1. On the **Start** menu, click **Settings**, then click **Control Panel**.
2. Double-click the **Administrative Tools** icon, then double-click the **Computer Management** icon. The Computer Management window appears.
3. In the operating system's Computer Management window, create a new user group for InTouch administrators (for example, InTouchAdmins).



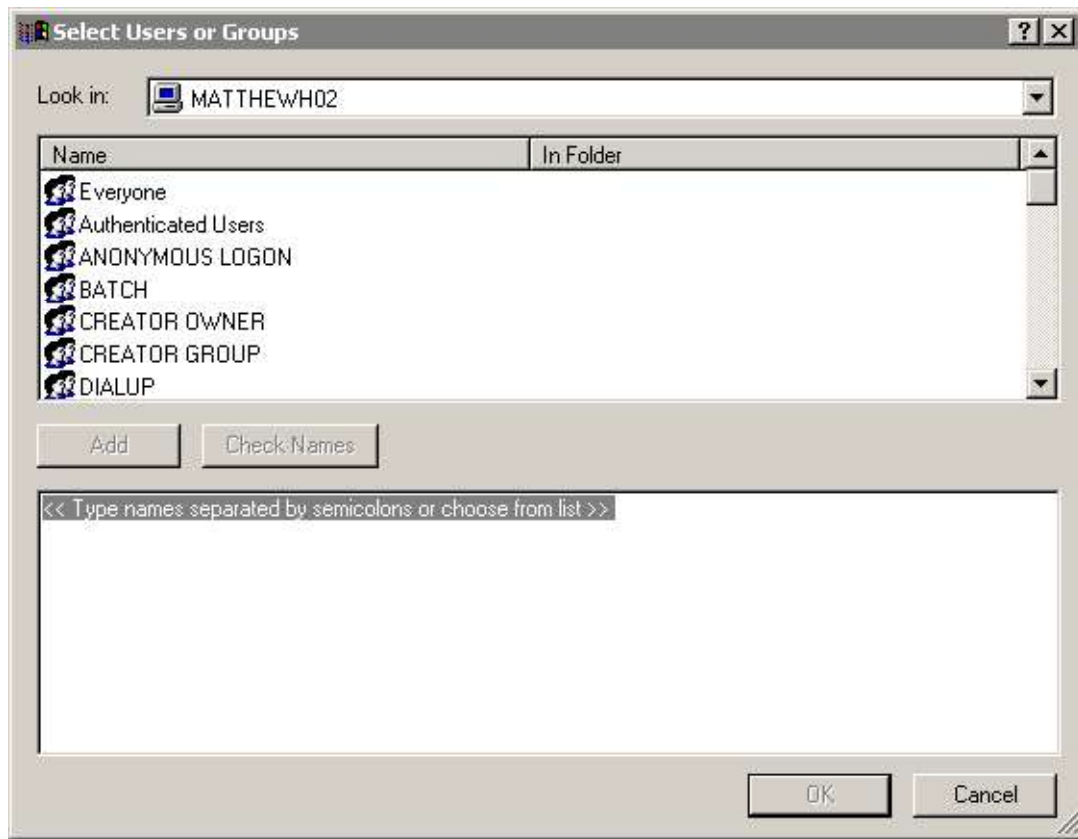
4. From the **Action** menu, click **New Group** or right-click in the right pane of the column management screen and click **New Group** on the shortcut menu. The **New Group** dialog box appears.



The image shows a 'New Group' dialog box with a title bar containing a question mark and a close button. The dialog has three input fields: 'Group name:', 'Description:', and 'Members:'. The 'Members:' field is a large empty box. Below the 'Members:' field are two buttons: 'Add...' and 'Remove'. At the bottom right of the dialog are two buttons: 'Create' and 'Close'.

5. In the **Group Name** box, type a name for your group, then type a description, if desired, in the **Description** box.

6. Click **Add**. The **Select Users or Groups** window appears.



7. Click the name of the member to add, then click **Add**.

---

**Tip** To add multiple members, hold down the CTRL key and click additional member names, then click **Add**.

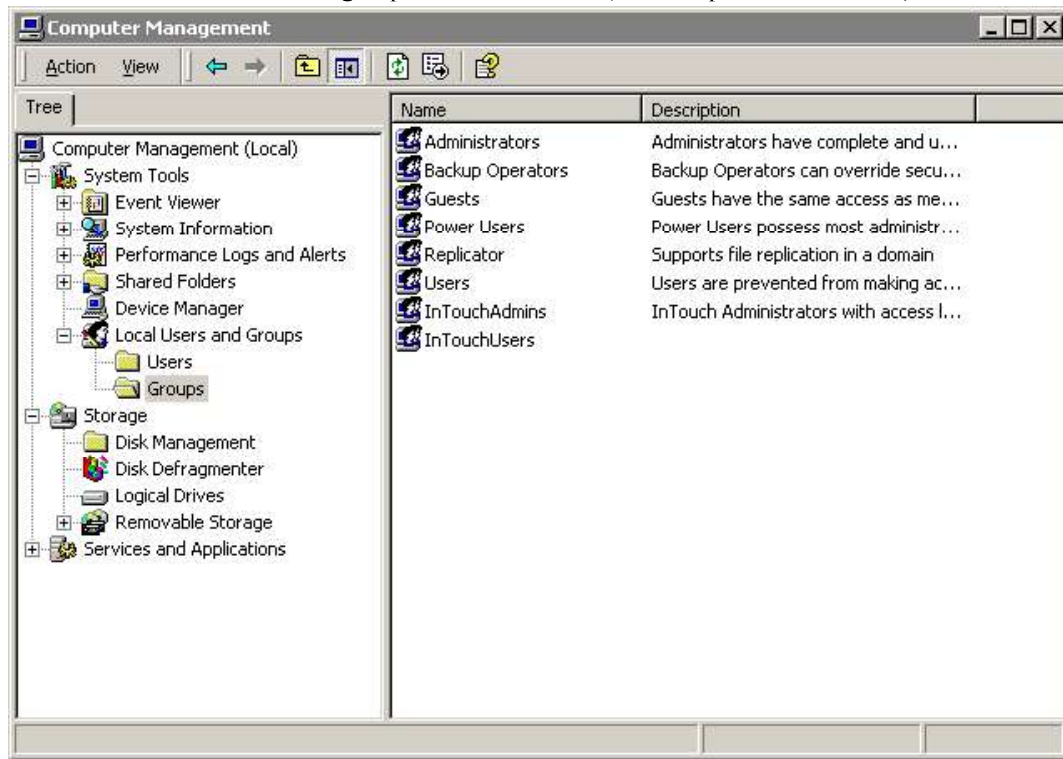
---

8. Click **OK**.

#### **To set up a user group on a local computer and add users**

1. On the **Start** menu, click **Settings**, then click **Control Panel**.
2. Double-click the **Administrative Tools** icon, then double-click the **Computer Management** icon. The Computer Management window appears.

3. In the operating system's **Computer Management** window, create a new user group for InTouch users (for example, InTouchUsers).



4. From the **Action** menu, click **New Group** or right-click in the right pane of the column management window and click **New Group** on the shortcut menu. The **New Group** dialog box appears.
5. In the **Group Name** box, type a name for your group, then type a description, if desired, in the Description box.
6. Click **Add**. The **Select Users or Groups** window appears.
7. Click the name of the member to add, then click **Add**.

---

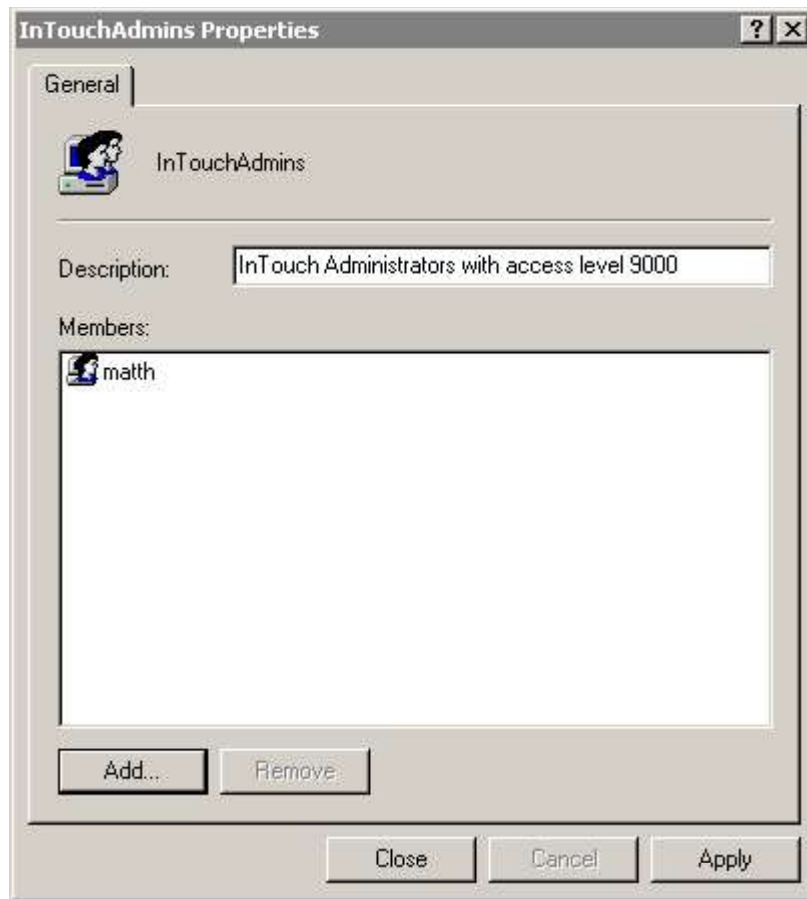
**Tip** To add multiple members, hold down the CTRL key and click additional member names, then click **Add**.

---

8. Click **OK**.

**To add users to an existing group**

1. Double-click the group name to view the group properties dialog box. The group's **Properties** dialog box appears.



2. Click **Add** to add users. The **Select Users or Groups** window appears.
3. Click the name of the member to add, then click **Add**.

---

**Tip** To add multiple members, hold down the CTRL key and click additional member names, then click **Add**.

---

4. Click **OK**.

For more information on creating user groups, see your Windows operating system documentation.

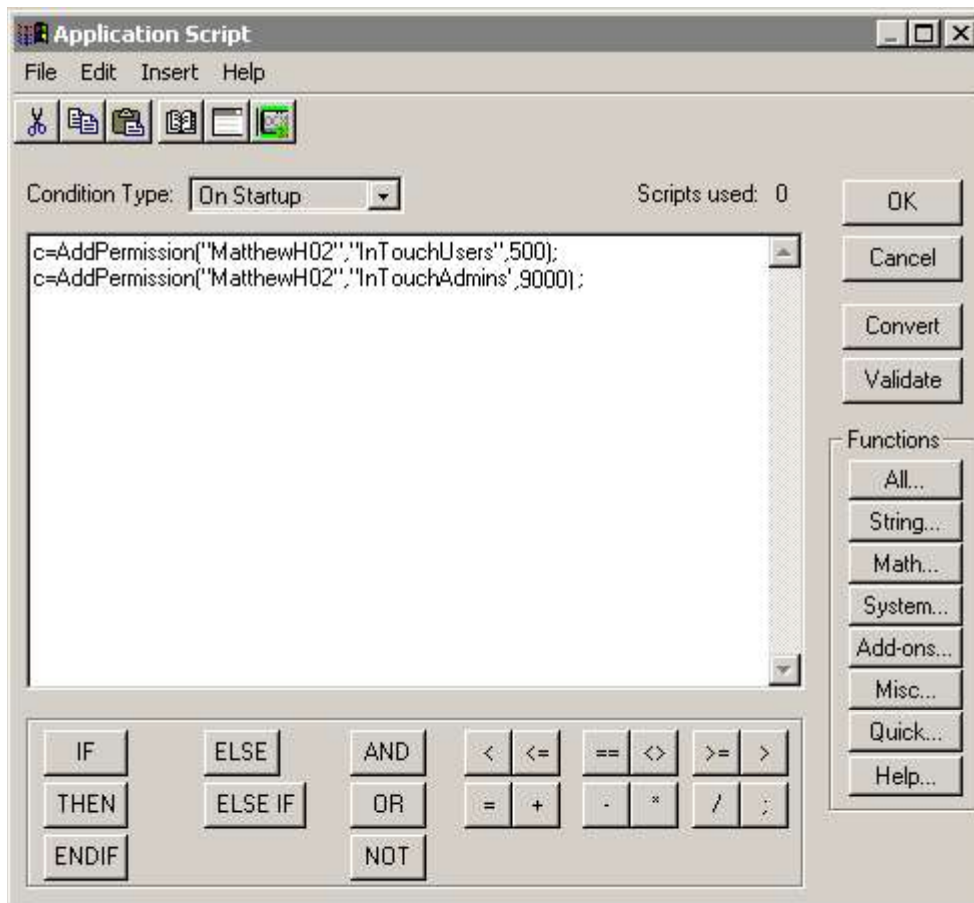
Once you configure the InTouch Application to utilize the operating system Authentication and internal InTouch Authorization, the **Change Password**, **LogOn**, **Configure Users** and **LogOff** options on the **Special...Security** menu will be unavailable.

## Setting Up Access Levels for Groups in WindowMaker

The final step in setting up operating system-based security for InTouch is to set up access levels for groups in WindowMaker. In WindowMaker, AddPermission() is used to setup a list of groups with the desired access level.

### To set up access levels for groups

1. Start WindowMaker.
2. On the **Special** menu, point to **Scripts** and click **Application Scripts**.
3. In the **Condition Type** list, click **On Startup**.
4. Using AddPermission(), enter the group names and corresponding access levels. The required and default arguments for AddPermission() are operating system or Domain, Group and Access level.



5. Click **OK**.



## InTouch Operating System Security Functions

The operating system-based authentication scheme inherits enforcement of some account policies from the operating system, while other policies are enforced within InTouch. Password policies such as maximum and minimum password age and minimum password length are enforced by the operating system. User names used during installation act as a part of the operating system. The Windows domain must be set up with the desired account policies in order to enforce these standards. InTouch enforces the inactivity time-out.

## Logging on to an Operating System-Secured Application

When a user logs on to an InTouch application, a dialog box appears requiring user name, password and domain or local computer name. The Domain/User Name combination is passed on to the operating system to authenticate the account. An attempt is made to log on with or without enabling the operating system cache. If the user cannot be logged on without the cache (due to a network outage, for example), but the user was previously authenticated with the cache enabled, then the user's full name and access level is obtained from the local InTouch cache. If all of the security checks are cleared successfully, the user is considered to be logged on to InTouch and the relevant data structures (for example, \$Operator) are updated. Otherwise, an appropriate error message is displayed.

---

**Note** If the operator has never logged on successfully before and the domain is unavailable, the log on will fail.

---

## Using ArcestrA-Based Security

When you configure a node to use ArcestrA security, InTouch invokes methods and dialog boxes from AppServer for configuring users and for Logins/Logoff. Users are configured on the AppServer Galaxy node. For more information, see the AppServer documentation.

## About ArcestrA Authentication and Authorization

The ArcestrA Security system is designed to allow the system administrators to easily define the users of the system and assign the operations they are allowed to perform. The security permissions are defined in terms of the operations the users can perform using these UI tools. The basic approach consists of the following steps:

1. Define the security model.
2. Organize the automation objects according to the security model for protection.
3. Define the users according to the security model.

The system administrator defines the system users by creating corresponding user profiles. He/she then defines their roles (a user can have more than one role) by selecting from a list of user roles predefined in the security model.

InTouchView users are normally authenticated by means of password based log-in. An install time option is provided to use the Windows log-in for authentication. This of-course requires that the user be defined in the Windows operating system.

A user authentication utility is also provided as an ActiveX control that can be used by third parties to develop client applications for ArchestrA with support for ArchestrA security.

## Setting Up ArchestrA-Based Security

After the administrator has defined user profiles for users of the InTouch or InTouchView application, the administrator can set up ArchestrA

### To set ArchestrA-based security:

1. Open a window in WindowMaker.
2. On the **Special** menu, point to **Security**, then point to **Select Security Type** and select **ArchestrA**.

---

**Note** Once you configure the InTouch application to use ArchestrA authentication and authorization, the **Change Password**, **LogOn**, **Configure Users** and **LogOff** options on the **Special...Security** menu will be unavailable.

---

## InTouch ArchestrA Security Functions

The ArchestrA security system is a global function that applies to every object in the Galaxy Database. It is a relationship-based system between users and the objects and functions of the Galaxy. This system is based on security roles (configuration, system administration, and runtime permissions) and security groups, which determine a particular security role's runtime permissions on an object-level basis. Configuration of the security system is done in the GalaxyObject's editor and applied to every object through its own editor.

## Logging on to an ArchestrA-Secured Application

Users typically log on and log off of an ArchestrA-secured InTouch application by entering a valid user name and password.

If your system has been configured with open security, the log in credentials of the default user are used and you are not prompted to log in. The following procedure assumes your system has been configured for authentication mode security.

### To log on, do the following:

1. Launch the ArchestrA-secured InTouch application. A log in dialog box is displayed.

2. Type a valid user name and password. If the system cannot authenticate you, you will be prompted again to log on.

After the system authenticates your log in data, access to all future operations is granted based on your associated roles/permissions in the Security Model.

## Creating a Custom Security Log on Window

If the **Special** menu will not be displayed in WindowViewer, you can create a custom logon window that the operator uses to log on to the application.

### To create a custom log on window

- Link the **\$OperatorEntered**, **\$PasswordEntered** and **\$OperatorDomainEntered** system tagnames to user input objects or use them in a QuickScript to set the "User Name," "Password," and Domain Name (these are internal message type tagnames that are intended for write operation only.) The **\$OperatorDomainEntered** is required only if the security mode is operating system-based. Otherwise, this tag will be ignored. If the security mode is operating system-based and the **\$OperatorDomainEntered** is null, it is treated as pointing to local machine.

For example:

```
Set the User Name string into ->$OperatorEntered
```

```
Set the User Domain Name string into ->  
$OperatorDomainEntered
```

```
Set the User Password string into ->$PasswordEntered
```

Unlike **\$OperatorEntered** and **\$PasswordEntered**, a change in the value of **\$OperatorDomainEntered** does not trigger a log on.

If the entries are valid, the **\$AccessLevel** and **\$Operator** internal tagnames are set to their predefined values (configured in the security user list).

Also, when you are not displaying the **Special** menu in WindowViewer, you can link a **User Input - Discrete** button to the **\$ChangePassword** tagname to show the **Change Password** dialog box and allow the operator to change his/her password. When the operator clicks the button, the value of the **\$ChangePassword** tagname is set to 1 and the **Change Password** dialog box appears. When the operator closes the dialog box, the system resets the value to 0. (This is a system discrete tagname intended for write operation only.)

You can also link a **User Input - Discrete** button to the **\$ConfigureUsers** tagname to allow an authorized operator with an access level of equal to or greater than 9000 to access the **Configure Users** dialog box to edit the security user name list. When the operator clicks the button, the value of the **\$ConfigureUsers** tagname is set to 1 and the **Configure Users** dialog box appears. When the operator closes the dialog box, the system resets the value to 0. (This is a system discrete tagname intended for write operation only.)

## Security and Alarms

When an InTouch alarm provider is configured to use either operating system or ArchestrA authentication and an alarm occurs, the alarm display object will contain the full name of the operator in the operator column, assuming the operator is logged on. For example if a user is registered in the PLANT\_FLOOR domain with a UserID of JohnS and a full name of John Smith, the operator column will contain John Smith. If the alarm is subsequently ACKed, and the node performing the ACK is set to use operating system or ArchestrA security, the operator column will be updated to show the full name of the ACK operator. Otherwise the alarm display object will show a computer name concatenated with whatever is in the \$Operator tag

### Full Name Expansion in Alarm Records

InTouch security can provide an operator's full name on alarm acknowledgements. This is also possible on records pertaining to alarm detection. In most organizations, a Login ID is not a person's full name, but rather an abbreviation or role classification.

When operating system authentication is chosen at provider and consumer InTouch nodes:

- The alarm display object will display full names when alarms are generated and when acknowledgements are performed.
- The alarm print object will print full names when alarms are generated and when acknowledgements are performed.
- The Alarm DB Logger will record domain name, login userID, and full user name with each alarm record for both operator and AckOperator fields. This will allow for unique identification even if an organization has two employees with identical full names.
- The domain name and login userID will be concatenated to the existing operator name field when alarm and ack packets are sent on the network.

## InTouch Security Script Functions

InTouch features new security related script functions. The new functions are described in the section below.

### InvisibleVerifyCredentials()

	Checks to verify the credentials of the given user without logging the user on to InTouch.	
<b>Category</b>	<b>security</b>	
<b>Syntax</b>	AnalogTag=InvisibleVerifyCredentials( "UserId", "Password", "Domain" );	
	<b>Parameter</b>	<b>Description</b>
	UserId	Windows operating system user account name that is part of local machine, workgroup or domain.

<b>Remarks</b>	If the supplied combination of user, password and domain are valid then the corresponding access level associated with the user is returned as an integer, in all other cases -1 is returned. This call does not change the currently logged on user. The domain field is only valid for the operating system-based security mode. If ArchestrA security mode is in use and if ArchestrA security is in turn using operating system-based security, the UserId should contain the fully qualified user name with domain name or computer name.
<b>Example(s)</b>	<code>AnalogTag=InvisibleVerifyCredentials( "john", "Password", "corporate_hq" );</code>
<b>See Also</b>	<b>PostLogonDialog(), AttemptInvisibleLogon(), IsAssignedRole(), QueryGroupMembership(), AddPermission().</b>

## PostLogonDialog()

	Brings up the InTouch Logon Dialog and returns TRUE.	
<b>Category</b>	<b>security</b>	
<b>Syntax</b>	<code>DiscreteTag=PostLogonDialog();</code>	
	<b>Parameter</b>	<b>Description</b>
	N/A	N/A
<b>Remarks</b>	Brings up the InTouch Logon Dialog and returns TRUE.	
<b>Example(s)</b>	<code>DiscreteTag=PostLogonDialog();</code>	
<b>See Also</b>	<b>InvisibleVerifyCredentials(), AttemptInvisibleLogon(), IsAssignedRole(), QueryGroupMembership(), AddPermission().</b>	

## AttemptInvisibleLogon()

	Attempts to logon to InTouch using the supplied credentials.	
<b>Category</b>	<b>security</b>	
<b>Syntax</b>	<code>DiscreteTag=AttemptInvisibleLogon( "UserId", "Password", "Domain" );</code>	
	<b>Parameter</b>	<b>Description</b>
	UserId	A valid user account name.
	Password	Password of the user.
	Domain	Name of the local machine, workgroup or domain to which the user belongs. This column applies only if the current security type is operating system-based.
	DiscreteTag	Return value: returns TRUE if authentication is successful. Otherwise, it returns FALSE.

<b>Remarks</b>	An attempt is made to logon to InTouch using the supplied credentials (Domain is ignored if the security mode is not operating system-based). If the logon attempt succeeds, then TRUE is returned and the system tags \$OperatorDomain, \$OperatorName, \$AccessLevel and \$Operator are updated accordingly. If the Logon attempt fails, then FALSE is returned and the currently logged on user (if any) continues to be the current user. The domain field is only valid for the operating system-based security mode. If ArchestrA security mode is in use and if ArchestrA security is in turn using operating system-based security, the UserId should contain the fully qualified user name with domain name or computer name.
<b>Example(s)</b>	<pre>AnalogTag=AttemptInvisibleLogon( "john", "Password", "corporate_hq" ); \\ security is operating system-based AnalogTag=AttemptInvisibleLogon( "john", "Password", "" ); \\ security is either InTouch or ArchestrA-based.</pre>
<b>See Also</b>	<b>PostLogonDialog(), InvisibleVerifyCredentials(), IsAssignedRole(), QueryGroupMembership(), AddPermission().</b>

## IsAssignedRole()

<b>Category</b>	<b>security</b>	
<b>Syntax</b>	DiscreteTag=IsAssignedRole( "RoleName" );	
	<b>Parameter</b>	<b>Description</b>
	RoleName	The role associated with a AppServer user.
<b>Remarks</b>	Valid for ArchestrA security mode only and applies to the currently logged on user. If a user is currently logged on and if he has the role RoleName assigned to him in Galaxy IDE, then a TRUE is returned. In all other cases a FALSE is returned.	
<b>Example(s)</b>	DiscreteTag=IsAssignedRole( "Administrator" );	
<b>See Also</b>	<b>AttemptInvisibleLogon(), PostLogonDialog(), InvisibleVerifyCredentials(), QueryGroupMembership(), AddPermission().</b>	

## QueryGroupMembership()

<b>Category</b>	<b>security</b>	
<b>Syntax</b>	DiscreteTag=QueryGroupMembership( "Domain", "Group" );	
	<b>Parameter</b>	<b>Description</b>
	Domain	Name of the domain or local machine in which the group is located
	Group	Name of the domain or local machine in which the group is located.

<b>Remarks</b>	Valid for operating system security mode only and applies to the currently logged on user. If a user is currently logged on and if he part of the group Group which is located on the domain Domain then a TRUE is returned and in all other cases a FALSE is returned. QueryGroupMembership will work with InTouch OS security and with InTouch ArchestrA security only when the ArchestrA security is set to OS Group based security
<b>Example(s)</b>	<code>DiscreteTag=QueryGroupMembership( "corporate_hq", "InTouchAdmins" ); DiscreteTag=QueryGroupMembership( "JohnS01", "InTouchUsers" );</code>
<b>See Also</b>	<b>BOOL PostLogonDialog(), InvisibleVerifyCredentials(), BOOL IsAssignedRole(), AttemptInvisibleLogon(), AddPermission().</b>

## AddPermission()

	Attempts to reach the account Account located on domain Domain	
<b>Category</b>	<b>security</b>	
<b>Syntax</b>	<code>DiscreteTag=AddPermission( "Domain", "Group", AccessLevel );</code>	
	<b>Parameter</b>	<b>Description</b>
	Domain	Name of the domain or local machine in which the group is located.
	Group	Windows user group.
	AccessLevel	InTouch AccessLevel that is associated with the given group
<b>Remarks</b>	Valid for operating system security mode only. An attempt is made to reach the account Account located on domain Domain. If successful, a TRUE is returned and the access level AccessLevel is assigned to the account in the internal records in InTouch for use during authorization when a user logs on. In all other cases, a FALSE is returned.	
<b>Example(s)</b>	<code>DiscreteTag=AddPermission( "corporate_hq", "InTouchAdmins", 9000);DiscreteTag=AddPermission( "johns01", "InTouchUsers", 5000);</code>	
<b>See Also</b>	<b>PostLogonDialog(), InvisibleVerifyCredentials(), IsAssignedRole(), AttemptInvisibleLogon(), QueryGroupMembership().</b>	

## ChangePassword()

	Displays the <b>Change Password</b> dialog box allowing the logged on operator to change his/her password.	
<b>Category</b>	<b>security</b>	
<b>Syntax</b>	<code>[Result=]ChangePassword();</code>	
	<b>Parameter</b>	<b>Description</b>
	[Result]	Returns one of the following integer values:
		0 = Cancel was pressed.
		1 = OK was pressed.

<b>Remarks</b>	If using touch screen applications, there is an option to use the alphanumeric keyboard.
<b>Example(s)</b>	<code>Errmsg=ChangePassword();</code>
	This QuickScript, if placed on a button or called based on a Condition or Data Change QuickScript, will open a dialog box (with optional keyboard) prompting the user to enter the current password, the new password and verification of the new password.



## Logoff()

	Logs the user off of InTouch.	
<b>Category</b>	<b>security</b>	
<b>Syntax</b>	<code>DiscreteTag = LogOff();</code>	
	<b>Parameter</b>	<b>Description</b>
	N/A	
<b>Remarks</b>	Logs off the currently logged on user and sets the current user status to the default none operator.	
<b>Example(s)</b>	<code>DiscreteTag = LogOff();</code>	
<b>See Also</b>	<b>PostLogonDialog(), InvisibleVerifyCredentials(), IsAssignedRole(), AttemptInvisibleLogon(), QueryGroupMembership(), AddPermission().</b>	

## InTouch Security System Tags

### \$OperatorName

<b>Category</b>	<b>Security</b>
<b>Usage</b>	The \$OperatorName tag will contain the full name of the operator if operating system-based or ArchestrA authentication is used and someone has logged on and has not logged off. Otherwise, the tag will contain the name of the user logged on (same contents as the \$Operator tag).
<b>Remarks</b>	N/A
<b>Data Type</b>	String
<b>Example(s)</b>	<code>\$Operator = "john";</code> <code>\$OperatorName = "John Smith";</code>
<b>See Also</b>	<b>\$Operator</b>

### \$OperatorDomain

<b>Category</b>	<b>Security</b>
<b>Usage</b>	If operating system-based security is selected and an operator has successfully logged on, the \$OperatorDomain tag will contain the domain or machine name that was specified at log on. If ArchestrA security is selected a user is logged on, the \$OperatorDomain will contain "ArchestrA." If InTouch security is selected, the \$OperatorDomain tag contains the string "InTouch." If "None" is selected, it is a empty string "".
<b>Remarks</b>	N/A
<b>Data Type</b>	String
<b>Example(s)</b>	<code>\$Operator = "john";</code> <code>\$OperatorDomain="CORPORATE_HQ";</code>
<b>See Also</b>	<b>\$Operator</b>

## \$OperatorDomainEntered

Category	Security
Usage	Whenever the \$PasswordEntered tag changes, a log on is attempted internally without any GUI being displayed. The log on attempt uses the \$*Entered tags as input user name and the string value of \$OperatorDomainEntered as the domain name (used only if the current mode is operating system-based security). If the security mode is not operating system-based, this tag is ignored.
Remarks	N/A
Data Type	String
Example(s)	<code>\$OperatorEntered="john"; \$OperatorDomainEntered="Corporate_HQ"; \$PasswordEntered="password"; \</code>
See Also	<b>\$Operator</b>