Inova Solutions
A Geomant Company

# LightLink Security Manager User Guide

Inova Solutions
A Geomant Company

# LightLink Security Manager

## User Guide

July 26, 2018


971 2nd ST S.E.
Charlottesville, VA 22902
434.817.8000

www.inovasolutions.com

Inova Solutions
A Geomant Company

# Table of Contents

# 1. Introduction to Security Manager in Inova LightLink

Inova LightLink® Security Manager assigns access privileges to the Inova LightLink supervisor and client applications (LightLink Administrator, System Manager, Message Editor, Bitmap Editor, Marquee, DataLink, TaskLink, and Security Manager). Security Manager also assigns access privileges to the output channels and devices configured in the Inova LightLink system.

The LightLink Security Manager application is installed with the LightLink Middleware (refer to the *LightLink Middleware Installation Guide* for more information) and as such is available only on LightLink Middleware hosts.

Because LightLink Security Manager connects directly to the LightLink database, users running Security Manager must have LightLink database permissions commensurate with the LightLink Middleware processes. Using the default settings for the LightLink database ensures that users running LightLink Security Manager have the correct permissions.

With Security Manager you can:

- Manage Inova LightLink Users with a combination of network login accounts and domain groups and Inova LightLink Security Groups.
- Create Inova LightLink Security Groups and subgroups.
- Attach user and user group privileges (profiles) to users and user groups.
- Assign or deny groups and users the Access Rights to existing output channels, display groups, and devices.
- Assign to LightLink Security Groups Default Profiles that will apply to their member users.

All Inova LightLink users and domain groups are members of Inova LightLink Security Groups. An individual Windows user account or domain group can be a member of only one LightLink Security Group.

In order to properly resolve domain groups into their respective users when those users initiate a client login, the network domain privileges of the Log On account configured for the Inova Application Launcher service must be equivalent to those of the user running Security Manager while configuring LightLink Security. Both must be able to access all of the domains whose domain groups will be included in LightLink Security.

 

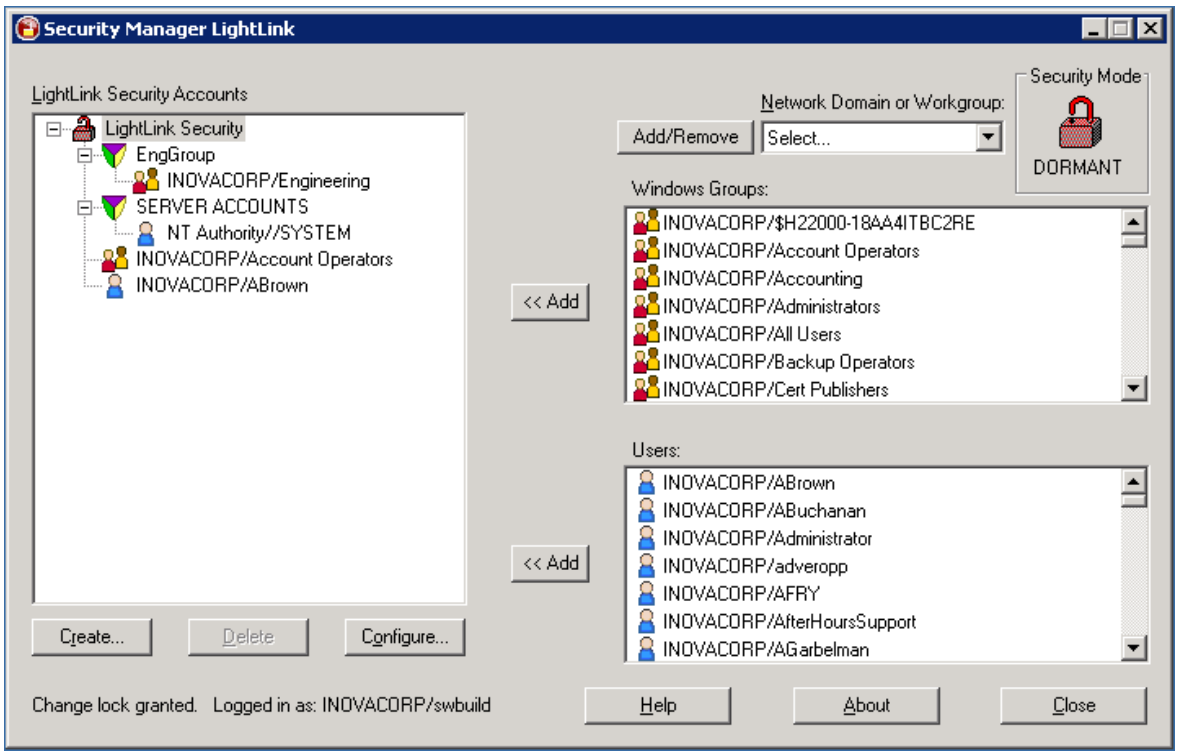


**Figure 1**

All Inova LightLink client applications validate the user as a legitimate Windows user and retrieve the profile for that user. When LightLink Security is active, if the user is not a member of an Inova LightLink Security Group, the client application will not launch when accessed by that user. Inova LightLink must be running to launch Security Manager.

Figure 1 shows the main window of the Security Manager application. The Inova LightLink Security tree at the left displays all the current Inova LightLink Security Groups, and the network login IDs of the members within each Inova LightLink Security Group. Also in the main window are the following features:

- The ***Security Mode*** is shown at the right top of your screen.
- The ***Create*** button allows you to add a LightLink Security Group with a new name. The group name so created cannot contain the \ " / [ ] : | < > + = ; , ? * @ characters, which are also disallowed in Windows NT user names.
- Once a group or user is added then they can be configured by selecting the ***Configure*** button or deleted by selecting the ***Delete*** button.
- The ***Help*** button gives you additional information about using Security Manager.
- The ***About*** button gives you the details about Security Manager.

 

- The ***Close*** button closes your session with Security Manager.

## 1.1. Accessing Security Manager

Security Manager can be launched through one of the following methods:

- Start > All Programs > Inova Solutions > LightLink Middleware > Security Manager
- Inova Quick Launch > Tools > Security Manager
- Administrator > Tools > Security Manager
- Administrator > Security Manager  icon

When LightLink security is active, the user account launching the Security Manager application will be validated against the user and domain group list of the LightLink™ Security Groups. If the launching user ID, either individually or as a member of a specified domain group, is not in one of the Inova LightLink Security Groups with access privileges, the Security Manager application will display a message to that effect and will shut down. When LightLink security is dormant, this check is not made.

When the main screen appears, the Inova LightLink Security tree displays the current Inova LightLink Security Groups and the network login IDs and domain groups currently configured within Inova LightLink Security.

## 1.2. Active and Dormant Modes

LightLink Security Manager allows you to control which users and groups have access to the system components and what they will be permitted to do. Security Manager will also provide access to application profiles for personal settings for client and supervisor applications based on a user's network logon ID and group membership.

The LightLink System has two security modes: **active** and **dormant**. You can tell which mode LightLink Security is operating under by looking at the Security Mode icon in the Security Manager application window (Figure 2). The settings for access privileges only take effect when LightLink Security is in Active Mode.

> ***Note:*** *LightLink applications only check on their startup, so that if any applications are already running when Security is set to Active Mode, they won't enforce the access privileges settings until they are restarted.*

In Figure 2, Security Manager is shown in dormant mode. In dormant mode, Security Manager will supply totally permissive security information to the LightLink applications without regard to the permissions information stored in

 

the security database. In Dormant Mode the default application profiles are still adhered to by the LightLink applications.

To change the security mode, use the Security Key application available from Inova Technical Support.

> ***Note:*** *Before you activate LightLink Security, be sure to make yourself a member of an Inova LightLink Security Group with privileges to run Security Manager and make changes.*


**Figure 2**

 

# 2. Managing Security Groups for Inova LightLink Security

## 2.1. Creating a Security Group

The following details how to create security groups for Inova LightLink Security.

1. In Security Manager, select the LightLink Security node (Figure 3) or the existing group to which you would like to add a new LightLink Security group.

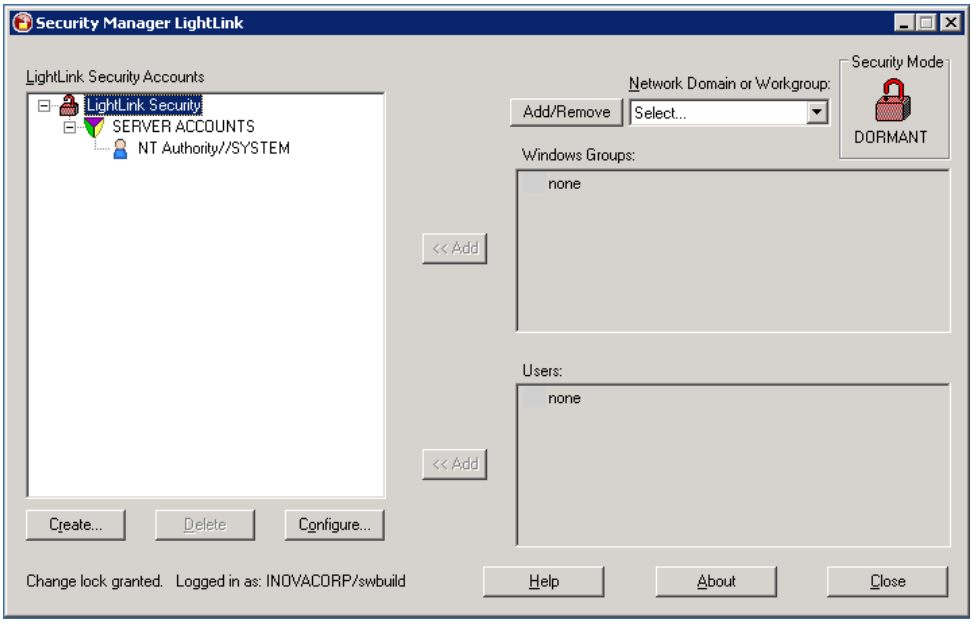


**Figure 3**

2. Click *Create*. The Security Group dialog appears.
3. Enter the name of the Security Group you want to create and click *OK*.

The new security group appears on the screen.

The Server Accounts LightLink Security Group is created automatically when you install Inova LightLink. It includes the Windows "local system account" on the LightLink Middleware host when the software was installed. The Server Accounts group cannot be modified or deleted; you cannot modify the Server Accounts member list.

## 2.2. Deleting from a Security Group

The following steps detail how to delete a user or domain group from a security group in Inova LightLink Security Manager.

1. Locate the Inova LightLink Security Group you wish to modify.

 

2. Select the User network login ID in the Inova LightLink Security Tree.
3. Click *Delete* to delete the selected user from the Inova LightLink Security Group. The Security Manager Delete dialog appears.
4. Click *Yes* to delete the user or domain group from the Inova LightLink Security Group.

## 2.3. Adding to a Security Group

The following steps detail how to add to a Security Group in Inova LightLink Security Manager.

1. In the Security Manager LightLink Security Accounts tree, select the LightLink Security Group to which you would like to add members (see Figure 4).

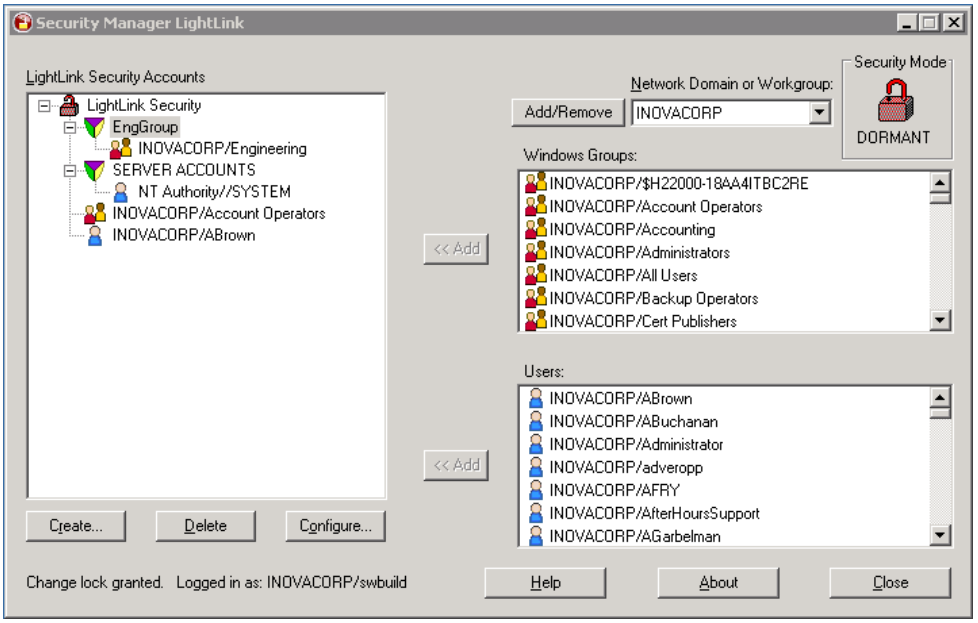


**Figure 4**

2. From the Network Domain or Workgroup drop down menu in Security Manager, select the Windows Domain from which you want to add Windows users or groups. Use the Add/Remove Domain button to specify alternate Windows Domains from which to add users and groups.

   When a Windows Domain is selected, Security Manager populates the Windows Groups and Users panels with the members of that Domain, given that the user running Security Manager has privileges to view those entities.

 

3. From either the Windows Group or the Users panel, select the Windows group or user you want to add and select the corresponding *Add* button.

   The Windows group or user will be added to the LightLink Security Group selected in the Inova LightLink Security Accounts tree (Figure 4).

   ***Note:*** *User groups created on the local machine cannot be added to LightLink Security.*

### 2.3.1. Load only groups from the specified domain

Security Manager may not be able to load users for large organizations with many Active Directory users. There is a feature that allows you to load only the Windows Domain Groups, without loading any users from that Windows Domain. To enable this feature, create a file named *security_man.ini* in the LightLink Server folder with these contents:

```
[uisettings]
loadusers=false
```

### 2.3.2. Load specific domain/usernames

If the desired Windows Domain is not showing in the Network Domain dropdown menu, you can add one or more users y choosing the *Add Users…* option from the drop-down menu in Security Manager and then specifying each individual user's Domain/Username in the provided dialog; this option does not allow one to add Windows Domain Groups in the same way.

## 2.4. Deleting an Inova LightLink Security Group

The following details how to delete a security group from Security Manager in Inova LightLink.

1. Locate the Inova LightLink Security Group you want to delete.
2. Select the Inova LightLink Security Group.
3. Click *Delete* to delete the selected Inova LightLink Security Group. The *Security Manager* delete confirmation dialog appears.
4. Confirm your choice and click *Yes* to delete the Inova LightLink Security Group or click No to leave it.

 

# 3. Changing Passwords

Passwords can only be changed at the network login/password level. Inova LightLink Security Manager does not store or allow the modification of user passwords. Inova LightLink obtains user and domain assignments from Windows and attaches profile information to determine Inova LightLink system privileges and security.

 

# 4. Configuring Privileges

When an Inova Solutions LightLink Security Group, subgroup, or individual user is selected in the Security Manager dialog, clicking the *Configure* button will invoke the Configure dialog for the selected node. The Configure dialog contains a Privileges tab, an Access Rights tab, and for Security Groups only, a Default Profiles tab.

You can use the Privileges tab to manage privileges for Marquee, DataLink, TaskLink, LightLink Administrator, Configuration Editor, Message Editor, Security Manager, and System Manager.

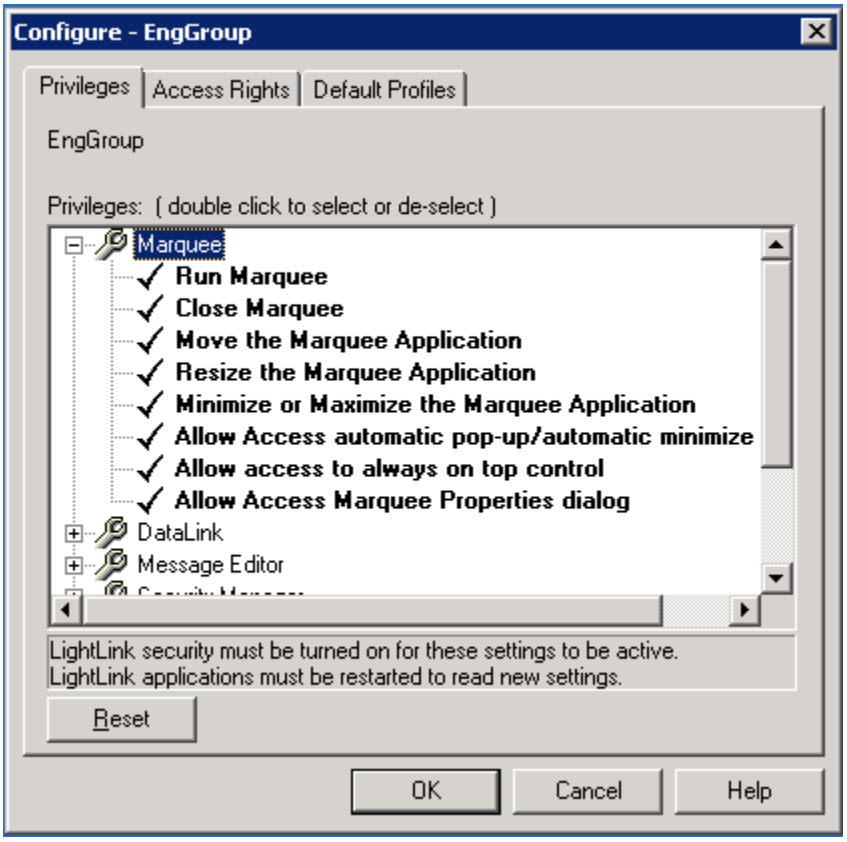


**Figure 5**

Refer to Figure 5 for a sample configuration dialog with the Privileges tab. Within each privilege, you can select or de-select it by double clicking on it. The checkmark shows it enabled and the "X" shows it disabled. Once you have made your changes, click *OK* to complete the configuration changes or *Cancel* to return to the previous screen and settings.

 

When an Inova LightLink group is selected and the Configure dialog invoked, the *Reset* button on each property page will return the content of that page to the settings inherited from the parent Inova LightLink group to which it belongs.

## 4.1. Privileges for Individuals

In the special case where a user's individual privileges are changed to be different from the Inova LightLink group privileges and then the group privileges are changed to be the same as the individual privileges, the user's override will NOT be supplanted by the group privilege setting unless the user's settings are saved again. If the group privileges are returned to their original state without any edits on the user's privileges, the override for the individual user will remain in effect.

EXAMPLE 1: The group privileges do not permit members to close the Marquee application. Someone changes the privilege for a particular user in that Inova LightLink group to permit that user to close Marquee. Later, the group privilege is changed to permit all of the group's members to close Marquee. Yet again, at a later time, someone else changes the group privilege back to prevent the group's members from closing Marquee. Provided that the user's privileges have not been edited and saved during this group privilege changing, the particular user whose privilege was overridden to permit closing Marquee will still have that privilege.

EXAMPLE 2: The group privileges do not permit members to close Marquee. Someone changes the privilege for a particular user in that Inova LightLink group to permit that user to close Marquee. Later, the group privilege is changed to permit all of the group's members to close Marquee. The privileges for the user are then edited to change another privilege. When the user's privileges are saved, the Security Manager realizes that the user's privilege on closing Marquee is the same as the parent group, so the user's setting for closing Marquee reverts to inheriting the parent group's setting.

Yet again, at a later time, someone else changes the group privilege back to prevent the group's members from closing Marquee. The user set of privileges will now inherit the group's setting on closing Marquee and will not permit the user to close Marquee.

## 4.2. Setting Privileges

To access and set the privilege options, double click to expand the desired application. A checkmark by an option indicates that the user has that option; a red "X" indicates that node does not have that option. You can modify the privileges by double-clicking on each option to add or remove the checkmark. Refer to Table 1 for more information about privilege options.

 

| LightLink Application | Privilege Options |
|---|---|
| **Marquee** | • Close Marquee<br>• Access automatic pop-up/automatic minimize control<br>• Access to always on top control<br>• Minimize or Maximize the Marquee Application<br>• Move the Marquee Application<br>• Access Marquee Properties dialog (Selecting this option gives you permission to display and make changes to the Properties dialog.)<br>• Resize the Marquee Application<br>• Run Marquee |
| **DataLink** | • Access to AlwaysOnTop control<br>• Access to Automatic Pop-up control<br>• Close DataLink<br>• Edit DataLink Views<br>• Minimize the DataLink Application (Selecting this option gives the user permission to minimize the DataLink application to an icon on the taskbar.)<br>• Move the DataLink Application (Selecting this option gives the user permission to move DataLink and reposition it on the desktop.)<br>• Resize the DataLink Application<br>• Run DataLink |
| **Message Editor** | • Send a modified message (Selecting this option gives the user permission to edit existing Message Editor messages and resend them to the system.)<br>• Send a message |
| **Security Manager** | • Add or Delete groups or users (Selecting this option gives the user permission to add or delete groups or users from any Inova LightLink Security Group.)<br>• Edit group profiles<br>• Edit user profiles<br>• Run Security Manager<br>• View group profiles<br>• View user profiles |
| **System Manager** | • Browse Externally-defined devices such as email addresses (Selecting this option gives the user permission to access non-Inova LightLink resources such as corporate email directories.0<br>• Cancel messages<br>• Create/Modify virtual displays (Selecting this option gives the user permission to create or modify virtual displays, which are regions of an existing Display that can be addressed separately.) |

 

| | |
|---|---|
| | • Create/Modify a display group<br>• Run System Manager<br>• Deactivate/Return to schedule a message |
| **LightLink Administrator** | • Edit LightLink configuration (Selecting this option gives the user permission to obtain "Config Permission". Without this privilege, the user cannot make any changes to the Inova LightLink System using the Inova LightLink Administrator application.)<br>• Run LightLink Administrator<br>• Start and Stop services (Selecting this option gives permission to start and stop components via the Inova LightLink Administrator.)<br>• Start and Stop all LightLink Software (Selecting this option gives permission to invoke the Start all Inova LightLink Software and the Stop all Inova LightLink Software options via Inova LightLink Administrator.) |
| **Configuration Editor** | • Run Configuration Editor. |
| **TaskLink** | • Close TaskLink<br>• Access Preferences Dialog<br>• Enable Always on Top<br>• Move TaskLink Application<br>• Enable Resize Application<br>• Run TaskLink |

**Table 1**

 

# 5. Configuring Access Rights

LightLink security is set to allow LightLink users access to all output channels, output devices, and display groups by default (for example, to send messages or view status). If desired, LightLink Security can be activated and users can be denied access to specific output channels and display groups. During LightLink Middleware installation, an option is provided to deny access by default, whereby when LightLink Security is Active users must be granted explicit access to output channels, output devices, or display groups in order to interact with them. When LightLink Security is Dormant, the default access settings of "allow" and "deny" have no effect – all LightLink users have access to all destinations.

The discussion that following discussion assumes that LightLink was installed with the default access set to "allow". A similar, yet opposite set of steps is required when the default access is set to "deny".

## 5.1. Access Rights for Security Manager

By setting access rights on output channels and display groups for Inova LightLink Security Groups, the System Administrator can restrict the ability of the group members to see various output channels and display groups.

In Figure 6, the Sales Inova LightLink Security group may access all output channels and display groups. The Inova LightLink Service group may access both Sales and Service output channels and display groups. The Inova LightLink Tech Support group may access only the Tech Support output channels and displays groups.

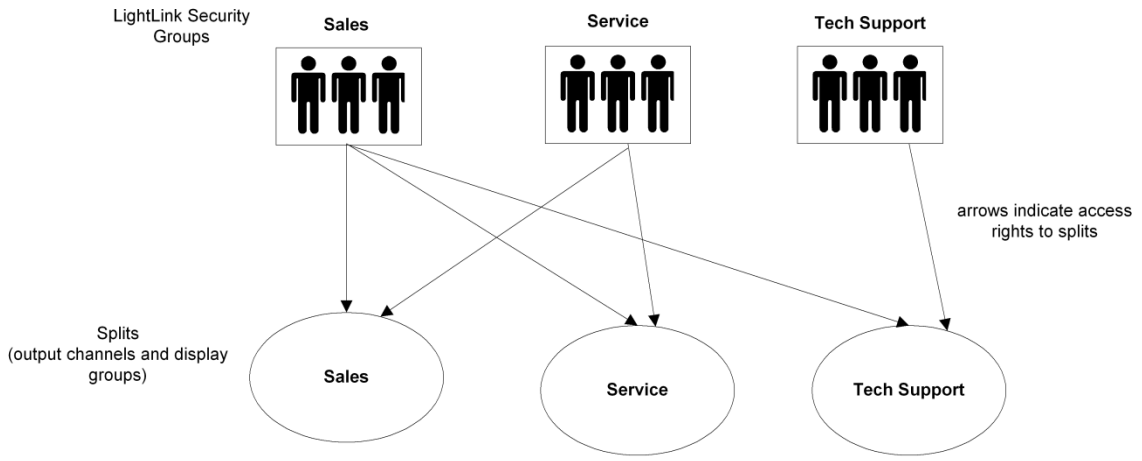


**Figure 6**

 

By defining the set of displays and display groups for individual Inova Solutions LightLink users, those users can be restricted to making modifications to only that set of output channels or display groups as indicated in Figure 7.

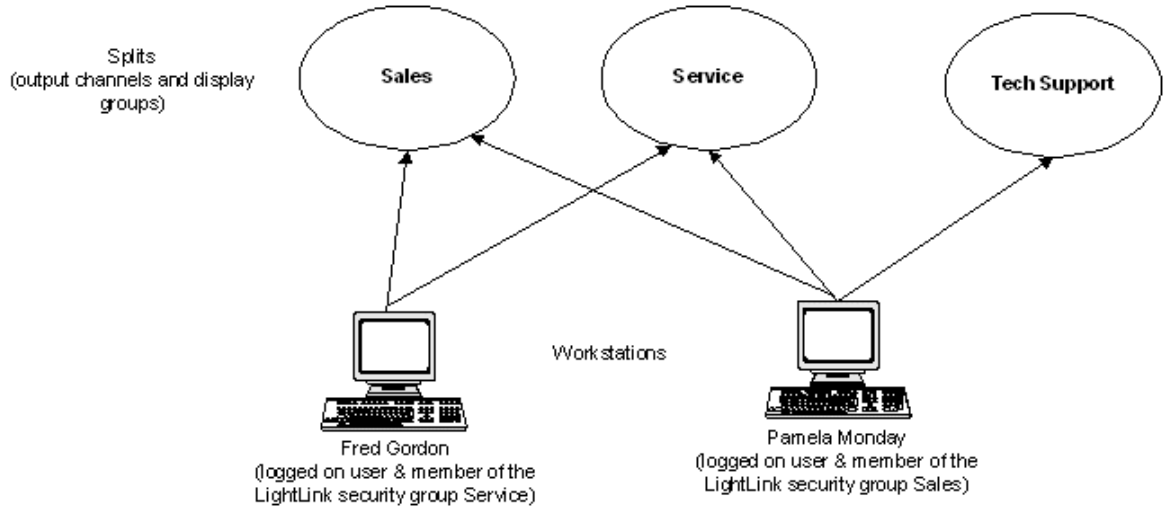


**Figure 7**

Fred Gordon, a member of Service inherits the Service access rights and can access the Sales and Service channels, display groups, and devices. Pamela Monday, a member of Sales, can access all channels, display groups, and devices.

## 5.2. Configuring Access Rights

The Access Rights tab is available on the Configure dialog; refer to Figure 8 . The Access Granted window permits the System Administrator to add and remove configured output channels, display groups from the set of devices a user or group member is prohibited from accessing. Any devices to which a user or group is not explicitly denied access will be accessible.

For Inova LightLink, the only access right available is visibility. Denying visibility to an output channel or display group will effectively deny modification to that device. The Inherited Access Denied window displays the entities to which the user is denied access by virtue of being a member of a group for which those entities are denied access.

 

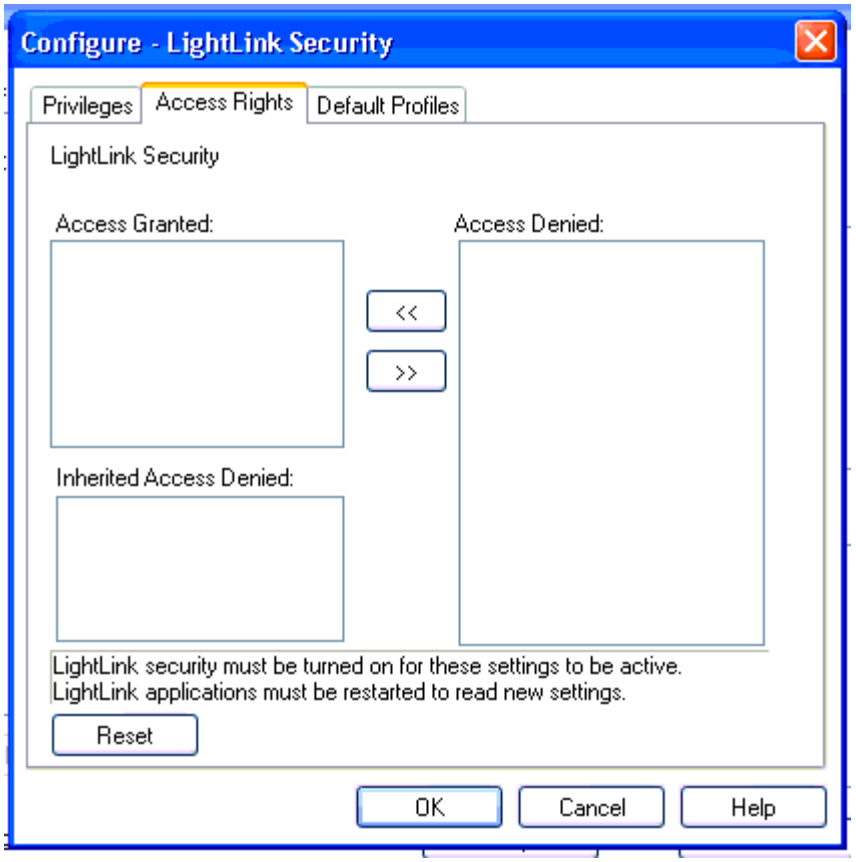


**Figure 8**

*Clicking the Reset button will return the Access Rights for the group to that of the parent group, or in the case above to that of the default, access granted to all groups and devices.*

## 5.3. Restricting Access to Displays and Devices

### 5.3.1. Inheritance

The privileges, access rights, and application profiles set for any Inova LightLink Security Group apply to all the subgroups and members that it contains. The privileges and access rights set for an individual group member apply only to that group member.

The privileges and access rights set for any windows group apply to any users that belong to that windows group. Any given privilege or access right set on an individual user will override the setting of the subgroup to which he belongs. Any given privilege, access right, or application profile set for a group will override the setting of the Inova Solutions LightLink Security Group to which that subgroup belongs.

 

### 5.3.2. The Reset Button

When an Inova LightLink group is selected and the Configure dialog invoked, the Reset button on each property page will return the content of that page to the settings inherited from the parent Inova LightLink group to which it belongs.

When a member node is selected and the Configure dialog invoked, the Reset button will return the member's settings to those inherited from the group to which that member belongs.

When the top “Inova LightLink Security Groups” node is selected and the Configure dialog is invoked, the Reset button will return the settings to enable all privileges or access rights on the respective tab or, in the case of the Default Profiles Tab, to the set of default profiles for the selected application at installation time.

A confirmation prompt is displayed before any content on a tab is reset.

 

# 6. Configuring Default Profiles

## 6.1. Default Profiles Tab

The Default Profiles tab of the Configure dialog is only enabled when a Security Group has been selected. The following steps detail how to configure the Default Profiles for the LightLink applications.

***Note**: Inova Solutions recommends changing these settings only in consultation with Inova Technical Support.*

1. Select a Security Group from the LightLink Security Accounts pane.
2. Select Configure. The Configure - LightLink Security dialog appears; click on the Default Profiles tab (Figure 9).

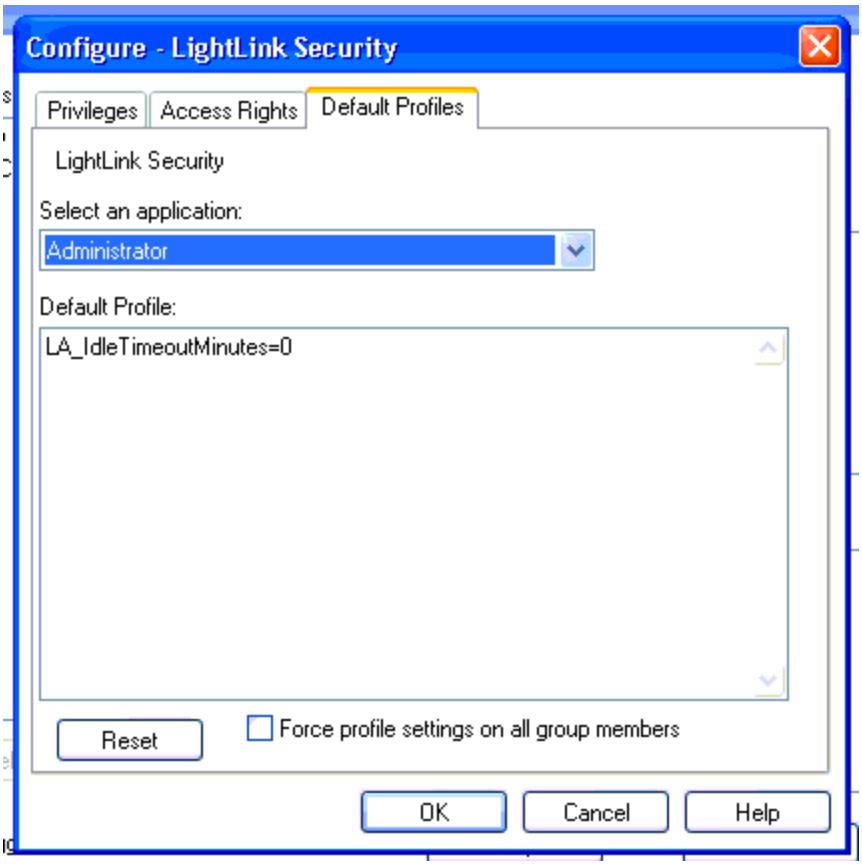


**Figure 9**

3. Complete the following Default Profiles for Configuring LightLink Security:

 

- **Select an application** - To configure the default profile settings for a LightLink application, click the arrow icon for the application drop down menu and select the desired application.
- **Default Profile** - This **is** the current set of profile settings for the selected application. Change the value for each setting you wish to change.
- **Reset** - This option resets the currently selected properties to those of the parent security group, or to those of the installation defaults if the top-level node is selected. The confirmation dialogs presented when one clicks the Reset button describe the actions that will be taken.
- **Force profile settings on all group members** - When this is checked, it forces the default profile **settings** on all group members. The users in that Inova LightLink Security Group will have the default profile settings of each LightLink application be those of their group rather than the profile settings saved the last time they used each application.

4. Click *OK* to accept your configuration.

## 6.2. Default Properties for System Manager

There are several default settings in System Manager that are configured through Security Manager. Only the name/value pairs of the settings are discussed here. All settings are saved back to the profile when System Manager is closed by the user. However, if the checkbox entitled, "Force profile settings on all group members" has been checked, then the default settings for the group of which the user is a member will be applied the next time the user starts the application.

### 6.2.1. System Manager Default Profile Settings

The System Manager default profile settings include both System Manager and Fast Text settings.

- **FT_BGColor –** Shows default background color for Fast Text messages. This is set to the last background color used in a sent Fast Text message. The format of the setting is hexadecimal with a hash mark as the first character. For example, #ff00ff indicates the RGB value for bright pink. If the hash mark is missing, the value will be interpreted as a decimal value and will be ignored. If the value is not in the proper format, a log entry in System Manager will be issued indicating the error.

 

- **FT_FGColor –** Shows default foreground color for Fast Text messages. This is set to the last background color used in a sent Fast Text message. Same format as for FT_BGColor; see the description above for the format.
- **FT_FontName –** Displays default font used for Fast Text messages.
- **FT_Bold –** Displays default setting for the bold font attribute check box. 1 = bold, 0 = normal.
- **FT_Italic –** Displays default setting for the italics font attribute check box. 1 = italicized, 0 = normal.
- **FT_Enabled** - Indicates whether Fast Text should be available in System Manager. 1 = enabled, 0 = disabled.
- **SM_LoadTestEnabled** - reserved.
- **SM_ShowMigration** - Indicates whether the Message Migration menu items should be displayed. 1 = yes, 0 = no.
- **SM_IdleTimeoutMinutes** - Indicates that System Manager should shut down after the specified number of minutes if no activity is detected. 0 = no timeout.
- **SM_RefreshEnabled** - Indicates whether the View > Refresh Overall Status menu option is presented; 1 = yes, 0 = no. SM_RefreshEnabled works on the current selection in the LightLink tree, clearing the Overall Status panel and refreshing it with current messages and their statuses.
- **SM_SummaryThreshold** - Indicates how many message/display pairs define the point at which the Overall Status pane starts displaying in Summary Mode. In large systems with many messages, System Manager performance can degrade at the top-most nodes (System root node and Display Group root nose). Instead of showing all messages in the system, it will simply show how many there are. To see actual messages the user will have to select a channels, display groups or displays. 5 messages sent to 10 displays is 50 message/display pairs.

 