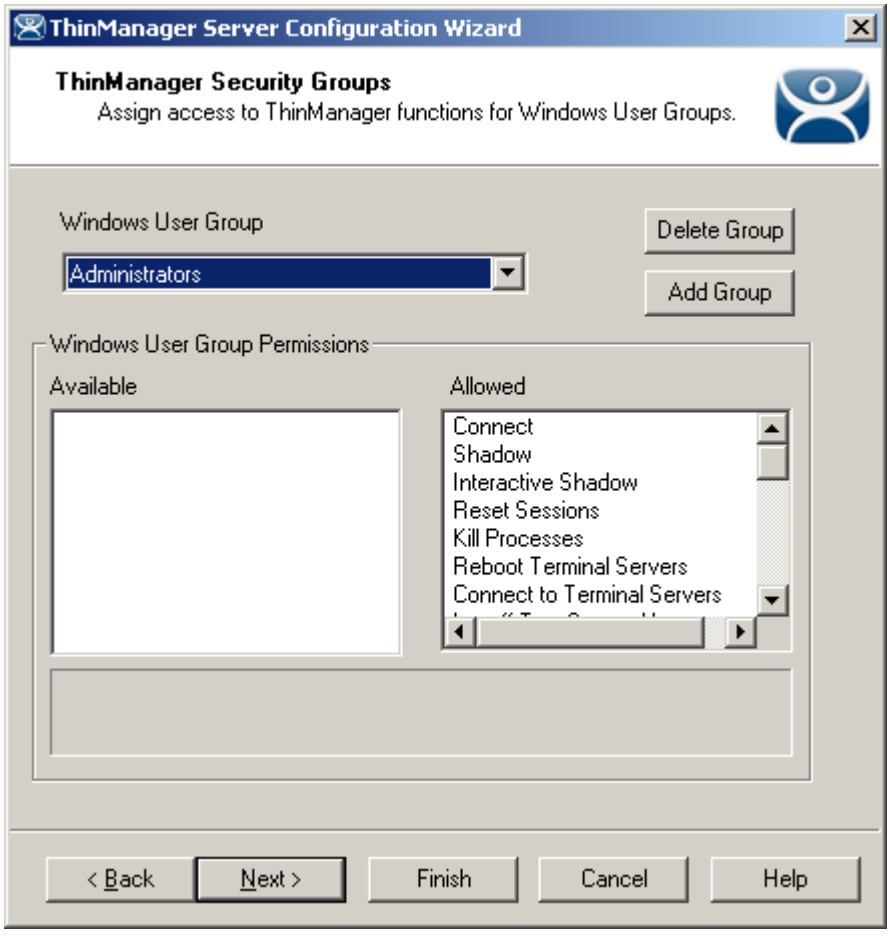
24 ThinManager Security

24.1 ThinManager Security Groups

Access to ThinManager can be assigned to Windows User Groups on the **ThinManager Security Groups** page.



ThinManager Security Groups

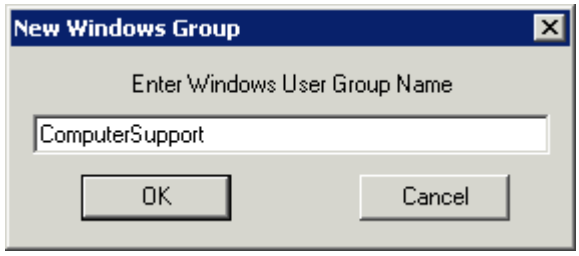
ThinManager allows different levels of access and functionality based on standard Windows groups.

Standard Windows Groups can be created in the Computer Management console and given different privileges in ThinManager.

ThinManager comes with privileges pre-defined for six groups:

- **Administrators -** The Microsoft defined Administrator group is given all privileges by default in ThinManager. This may be denied by unselecting the various **Windows User Group Permissions.**
- **ThinManager Administrators** have full permission to do anything within ThinManager including the power to logoff sessions, kill processes, send messages, restart terminals, calibrate touch screens, change terminal configurations, update firmware, update the TermCap, and restore configurations. Administrators and members of ThinManager Administrators can shadow terminals and interactively control the terminal session. **These privileges may not be removed** and will be grayed out**.**
- **ThinManager Interactive Shadow Users** - Members of this group may shadow a terminal interactively.
- **ThinManager Power Users** can logoff sessions, kill processes, send messages, restart terminals, and calibrate touch screens. They cannot change terminal configurations, update firmware, update the TermCap, and restore configurations. ThinManager Power Users can shadow terminals from within ThinManager but cannot interact with the session.
- **ThinManager Shadow Users** - Members of this group may shadow a terminal but not interactively.
- **ThinManager Users** can view only. They cannot logoff sessions, kill processes, send messages, restart terminals, or calibrate touch screens. ThinManager Users cannot shadow a terminal.

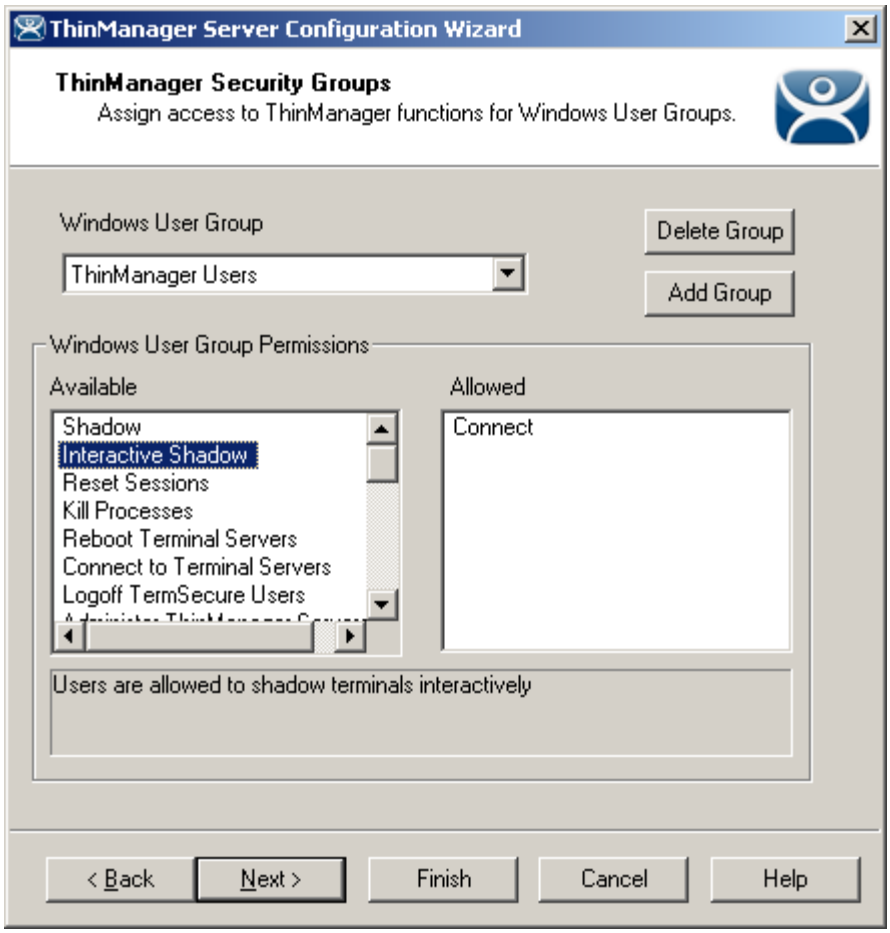
Additional **Windows User Groups** can be configured by selecting the ***Add Group*** button to launch the **New Windows Group** window.



New Window User Group Window

Adding a Windows Group name in the field of the New Window Group window and selecting the ***OK*** button will add the Windows User Group to the drop-down list.

Note: This doesn't create the user group on any servers. This just adds the name of an existing group to the list that ThinManager is maintaining.

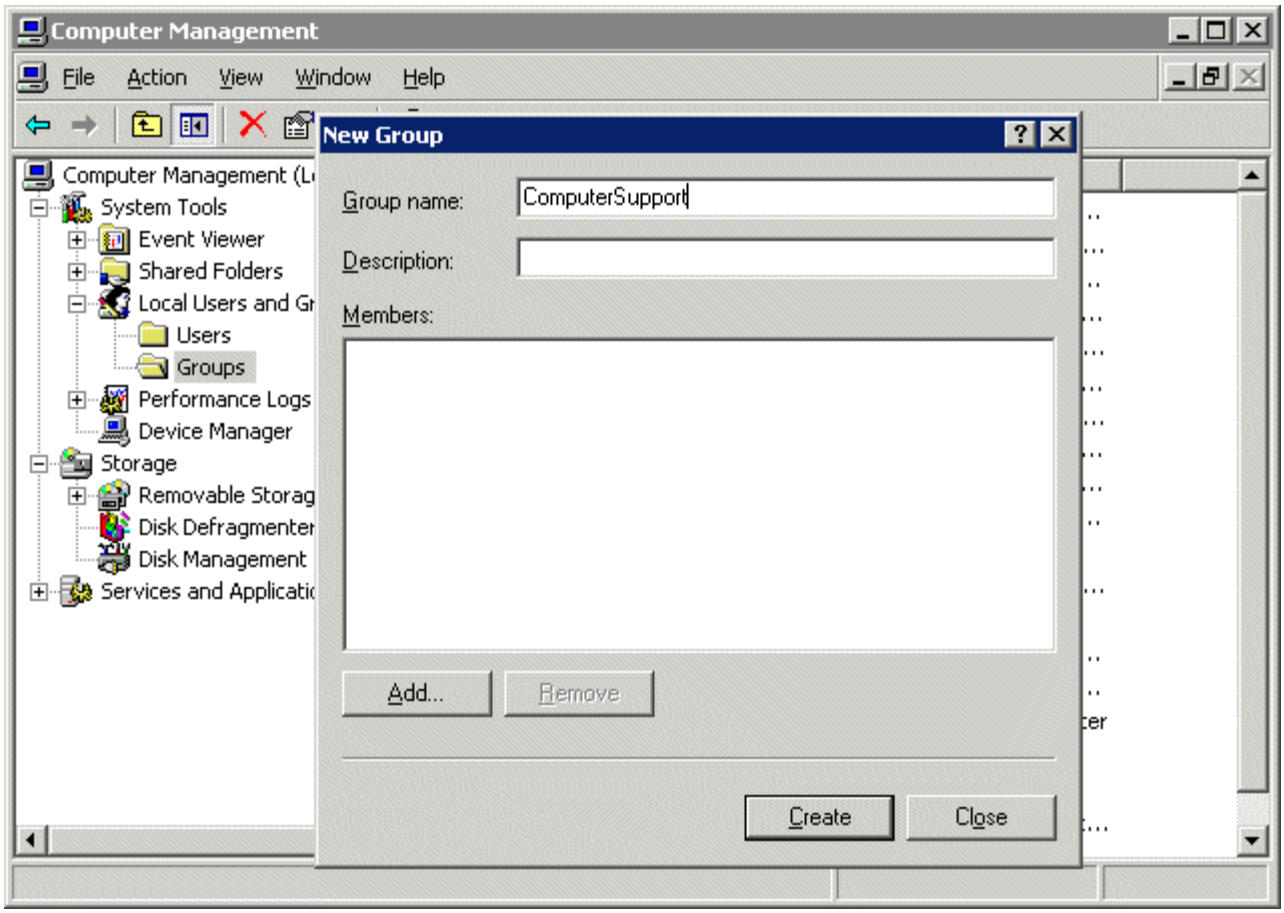


New ThinManager Security Group

Select the group from the **Windows Users Group** drop-down. Choose the permissions you want to grant to the group by double clicking on the function in the Available Windows User Group Permissions list. Members of the Windows User Group will have the selected permissions the next time they login.

Although ThinManager has Windows User Groups pre-configured with privileges, these groups have not been created on the terminal servers.

To Create A Windows User Group Open the **Computer Management Console** by selecting ***Start > Settings > Control Panel > Administrative Tools > Computer Management***.



Created ThinManager Security Groups

Highlight **Groups** in the tree and select ***Action > New Group***.

Name the group and select the ***Create*** button.

Add **Users** to the Windows User Group.

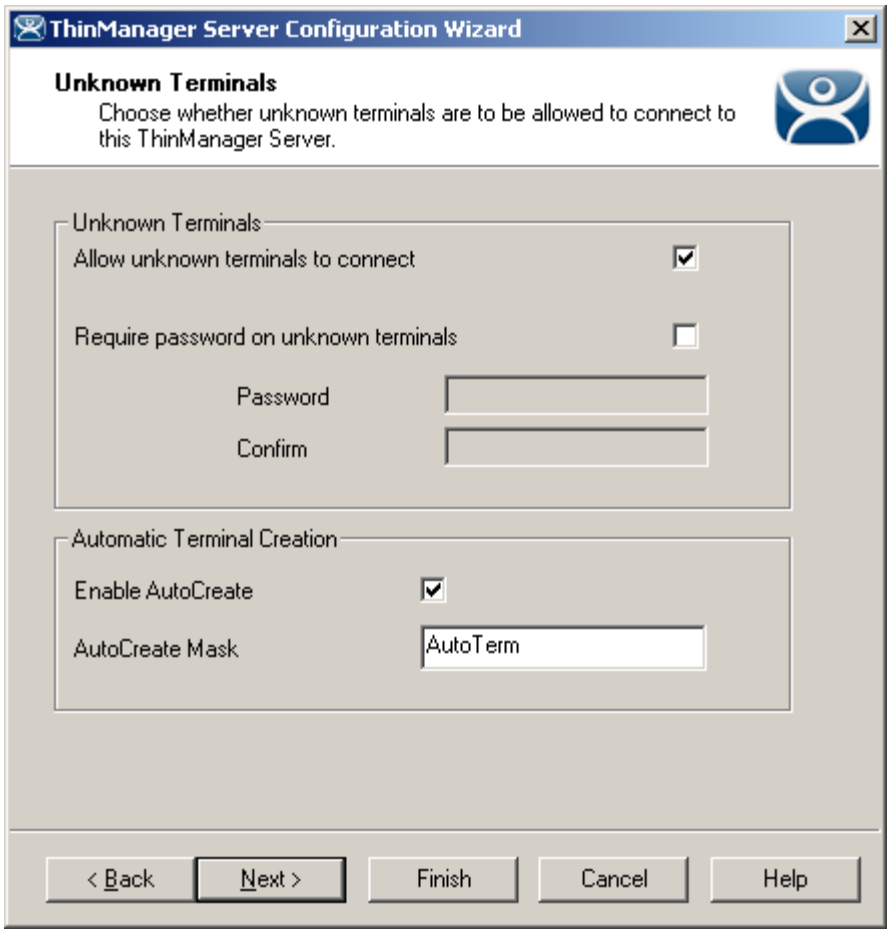
Members of the Windows User Group will have the selected permissions the next time they login.

If groups are not created, members of the standard Windows Administrator group have full privileges in ThinManager while members of the standard Windows User group will be denied access.

Note: The **thinserver** service will need to be stopped and restarted and the users will need to re-login for the changes to take effect.

24.2ThinManager Server Security

ThinManager has a number of security settings for the ThinManager Server. Open the **ThinManager Server Configuration Wizard** by right clicking on the ThinManager Server in the tree and selecting ***Modify***, or highlight the ThinManager Server and select ***Edit > Modify*** from the menu.

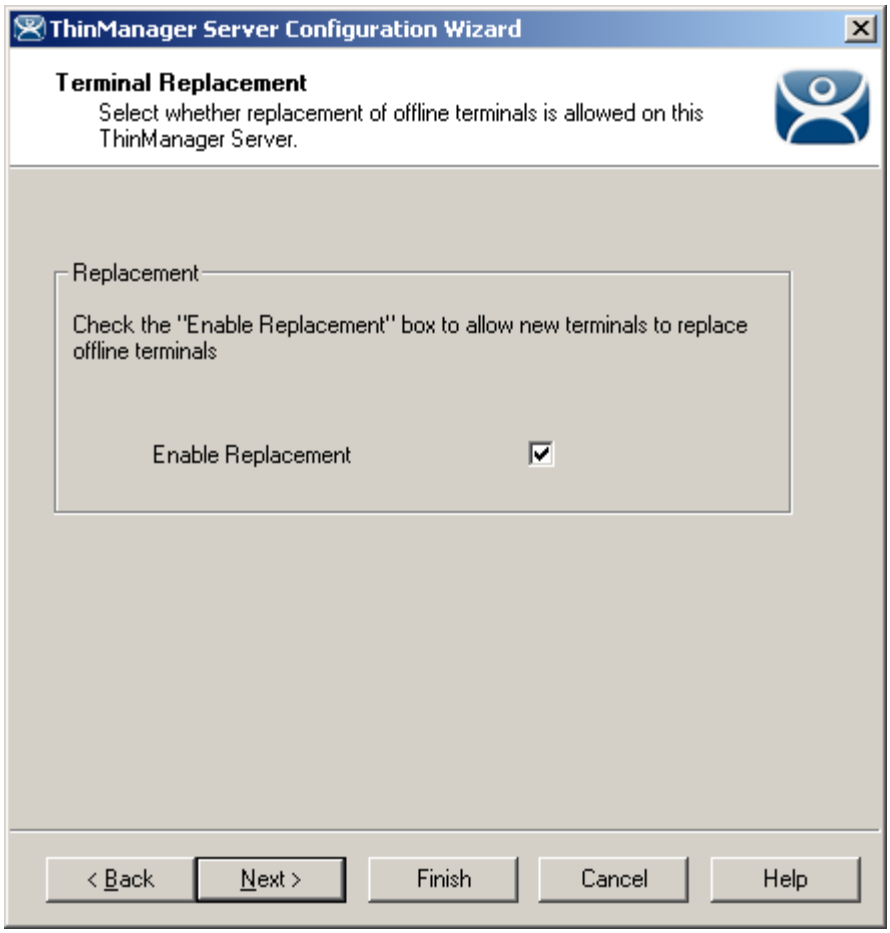


ThinManager Server Configuration Wizard

The second page of the wizard has two settings related to security:

- ***Allow unknown terminals to connect*** - This, when unchecked, will prevent any new terminals connecting to the system.
- ***Require passwords on unknown terminals*** - This checkbox, if checked, allows new terminals to be added, but only if the installer has the password.

Note: The use of this password setting in ThinManager is an effective way to limit hardware addition to authorized users. DO NOT use the password setting in the BIOS of the hardware. Forgetting the BIOS password can make the unit inoperable.



Terminal Replacement

On the **Terminal Replacement** page of the **ThinManager Server Configuration Wizard** is the ***Enable replacement*** checkbox. This allows failed terminals to be replaced. If this is unchecked, terminals can still be added, but only by using the ***Create New Terminal*** process.

This is a global setting that affects all terminals connected to this ThinManager Server. The ***Enable replacement*** checkbox is also found on the **Terminal Configuration Wizard** of each terminal and the **Terminal Group Configuration Wizard** of each Terminal Group so that the setting can be applied to individual terminals and Terminal Groups.

24.2.1 Windows Security

The ACP ThinManager system delivers a Windows 2000/2003/2008 desktop to each thin client by default. Each thin client has full access to the server resources, as if it is the server. However, just because the thin client has the ability to have full access to the server resources doesn't mean that the user should be granted full access to the server. To prevent unauthorized changes to the server, it is recommended that each user profile have security policies applied through the System Policy Editor to limit access to the needed functions. Windows 2000/2003/2008 Security procedures are discussed in the Windows on-line help and in many books and articles.

Administrators usually require that each user login to a terminal with their personal account and have the Microsoft policy determine the user's access rights.

Note: Task Manager has a feature that allows the launching of applications. If using an Initial Application, access to Task Manager should be denied in the security policy or with the Key Block Module to prevent a user from launching unauthorized programs.