Getting Started with OmniVista Security

The Users and User Groups application enables you to control user access to OmniVista and to network switches. Access to OmniVista is controlled through the definition of user logins and passwords. Access to network switches is controlled through the use of security groups, which have specified levels of access to switches. All OmniVista users must be assigned to at least one security group, which defines the access rights for its members. Security groups and user logins are configured from the Users and User Groups application, and constitute one level of network security. Other levels of security are summarized in the table below.

Overview of Security Types

Security Type	Configured From
SNMP Get and Set Community Names Get and Set Community names act as read and write passwords that define whether any OmniVista user is allowed to read or write the switch's configuration information. Get and Set Community names are configurable only from the switch itself.	Switch console port or CLI command.
The "Seen By" Parameter This parameter makes individual switches visible to users in a specified OmniVista security group.	OmniVista Topology application. The Seen By parameter setting is specified in the Discovery Wizard when switches are discovered. After discovery, you can edit entries in the list of All Discovered Devices to redefine this parameter.
OmniVista Security Groups Security groups in OmniVista provide different levels of access to switches. An OmniVista user's access rights are based on the access rights of his/her assigned security group.	OmniVista Users and User Groups application.

Default Users, Groups, and Passwords

OmniVista security uses a combination of user logins and security groups to control access to OmniVista and to network switches. OmniVista is shipped with the pre-configured user logins, passwords, and security groups described below. The Users and User Groups application enables you to modify these users, passwords, and security groups, or create new ones. Note that initially the pre-configured user **admin** is the only user that has permission to change the user logins and security groups defined by the Users and User Groups application. The pre-configured users and security groups shipped with OmniVista are as follows:

User **user** in security group **Default**

> User **user** belongs to the **Default** security group and therefore has read-only access to switches that **can be seen by** the **Default** security group. The default password for this user is **switch**. User **user** can view the information for a switch, but cannot modify the information. This is because the only group right assigned to the **Default** security group is Read.

User **writer** in security group **Writers**

> User **writer** belongs to the **Writers** security group and has both read and write access to switches that **can be seen by** the **Writers** security group. The default password for this user is **switch**. User **writer** can view and modify switch information. However, user **writer** cannot use the Discovery Wizard to discover network switches and cannot manually add, delete, or modify entries in the list of All Discovered Devices also. User **writer** does not have access to the functions provided by the Audit application and the Control Panel application. This is because the only group rights assigned to the **Writers** security group are Read and Write.

User netadmin in security group Network Administrators

> User **netadmin** belongs to the **Network Administrators** security group and therefore has full administrative rights to all the switches in the network. The default password for this user is **switch**. User **netadmin** has read and write access to all the switches known to OmniVista. In addition, user **netadmin** can use the Discovery Wizard to discover network switches and can manually add, delete, or modify entries in the list of All Discovered Devices also. User **netadmin** has full access to the functions provided by the Audit , Control Panel application, and Notifications application. User **netadmin** can do everything EXCEPT edit the security groups and users defined in the Users and User Groups security application. The group rights assigned to the **Network Administrators** group are Read, Write, and Network Admin.

User **admin** in security group **Administrators**

> User **admin** belongs to the **Administrators** security group and therefore has full administrative rights to all the switches in the network -- as described above for user **netadmin** -- AND full administrative rights to edit the security groups and users defined in the Users and User Groups security application. The default password for this user is **switch**.

Selecting the Authentication Server

You can select local or remote LDAP, RADIUS, and ACE servers using the Authentication Server pane. You can configure these servers using the **Configure Servers...** button in the Authentication Server pane.

Using Security the First Time

1. Create new security groups, edit pre-configured groups, or use pre-configured groups as they are. The Groups pane enables you to add new security groups, edit existing security groups, add or remove users from existing security groups, and delete security groups. Click here for more information.

2. Create new users or edit pre-configured users. Note that all pre-configured users have the same default password, **switch**. At a minimum, it is recommended that you redefine the passwords. The Local Users pane enables you to add new users, delete users, edit existing users, add or remove users from existing security groups, and change user passwords. Click here for more information.

Sample Security Configurations

OmniVista users with Administrators or Network Administrators security rights can view and manage every switch in the network. However, selected switches can be "walled off" from users that have Writers or Default (read) security rights. The "walled off " switches can be made visible to, and manageable from, a single OmniVista security group. This is accomplished by creating a new security group and setting the **can be seen by** parameter, so that relevant switches can be seen by that security group only. (Note that, if problems arise, switches are always visible to, and can be managed by, users in the Administrators or Network Administrators security group.)

For example, first you create a security group named Marketing with Writers access rights. You also create a single user named Marketing Writer, who is the sole member of security group Marketing. The Marketing department contains five switches, and you set the **can be seen by** parameter for each switch to security group Marketing only.

The effect of this security configuration is that the five switches in the Marketing department will be visible to, and manageable by, the user Marketing Writer only. OmniVista's list of All Discovered Devices will display the five Marketing switches only when user Marketing Writer is logged in. Since the switches will not be visible in the list of All Discovered Devices when other users with Write or Read permission are logged in, they cannot be managed by other users. (Note that users with Administrators or Network Administrators security rights are an exception to this. Users with Administrators or Network Administrators security rights will always be able to see and manage the five Marketing switches.)

You could also create a second security group, perhaps named Marketing Monitor, that has read access rights only. You create a user that belongs to this security group named Marketing Reader. If you set the **can be seen by** parameter for each Marketing switch to security group Marketing Monitor and security group Marketing, user Marketing Reader will be able to view and monitor the five Marketing switches, but only user Marketing Writer will be able to configure the switches.

Creating and Managing Security Groups

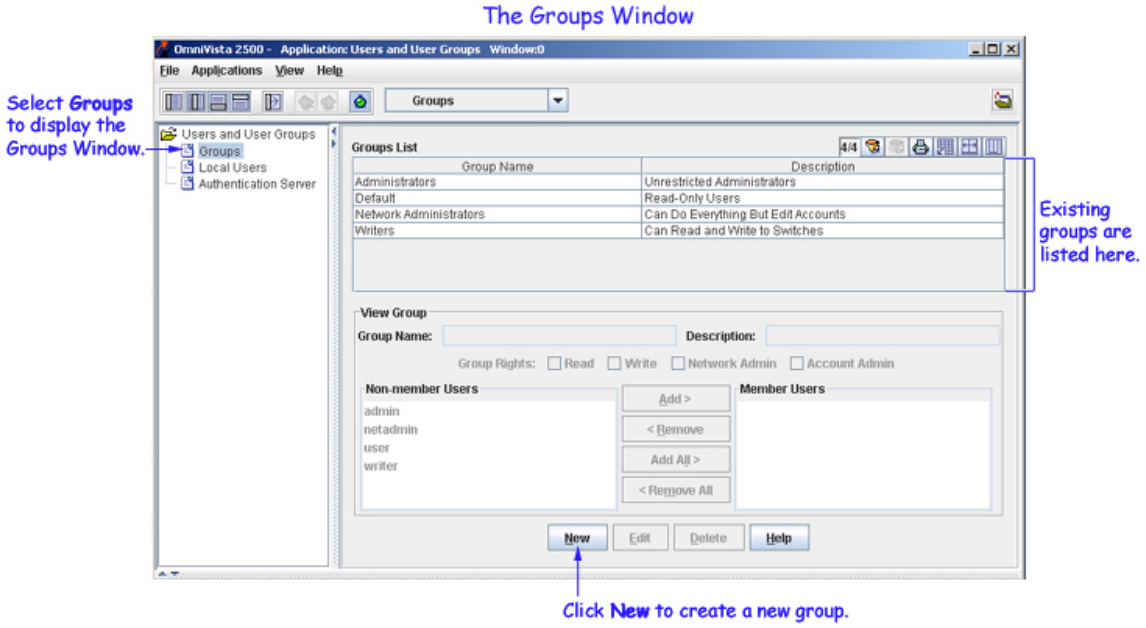
The Groups pane, shown below, enables you to add new security groups, edit existing security groups, add or remove users from existing security groups, and delete security groups. OmniVista is shipped with four pre-configured security groups, which are listed and described below.

Default group. This security group has read-only access to switches in the list of All Discovered Devices that **can be seen by** the Default security group.

Writers group. This security group has both read and write access to switches in the list of All Discovered Devices that **can be seen by** the Writers security group. However, members of the Writers security group cannot run discovery or manually add, delete, or modify entries in the list of All Discovered Devices.

Network Administrators group. This security group has full administrative access rights to all switches on the network. Members of this security group can run discovery and can manually add, delete, and modify entries in the list of All Discovered Devices. Members of the Network Administrators security group also have full read and right access to entries in the Audit Application and the Control Panel Application. Members of the network administrators security group can do everything EXCEPT edit the groups and users defined in the Users and Groups Application.

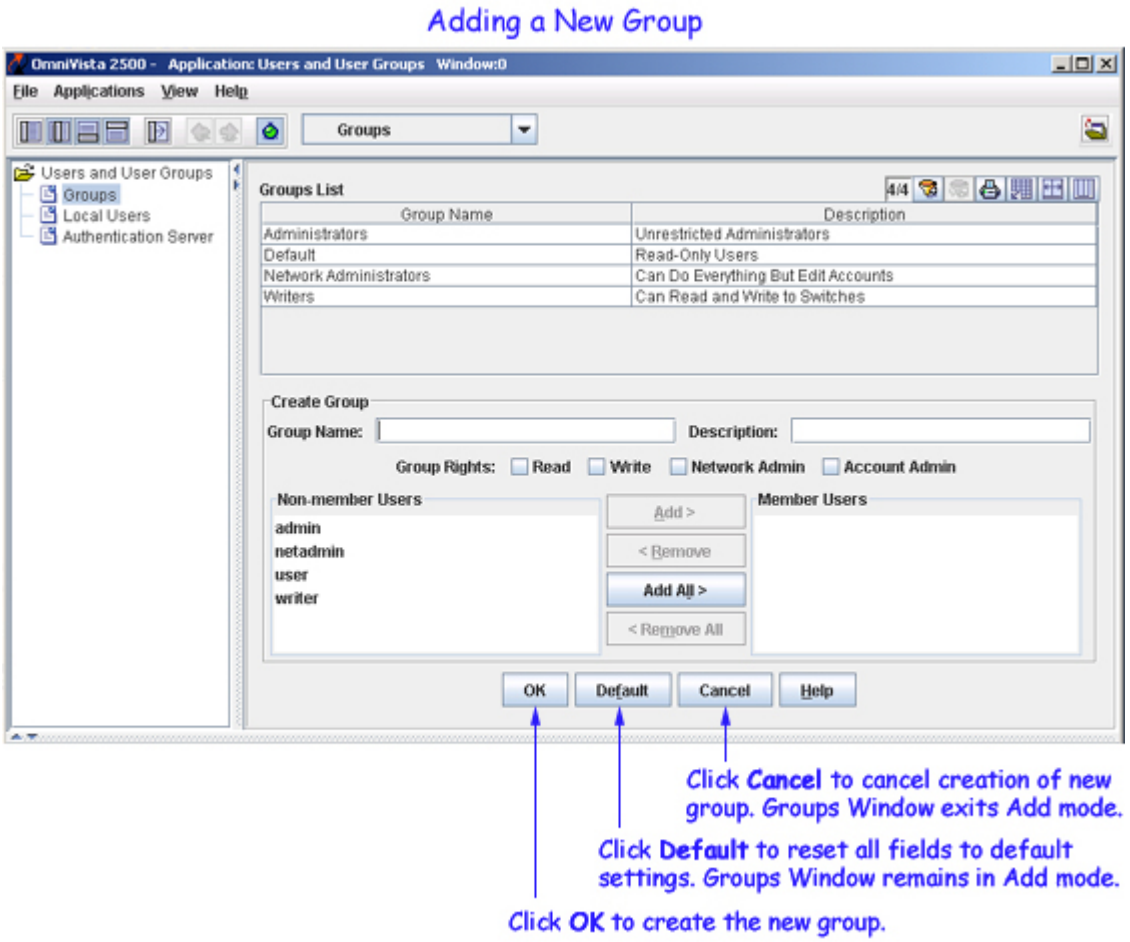
Administrators group. This security group has all administrative access rights described above for the network administrators group AND full administrative rights to edit the groups and users defined in the Users and Groups Application.



Adding a New Security Group

You can create a security group that has no member users. When you create a user, you can add them to any existing security group as a member. You can also edit a security group later to add members. Follow the steps below to add a new security group.

1. Click the **New** button, shown in the screen above. The Groups pane will enter the add mode and all fields will be activated, as shown below. Note that if you select an existing group in the Groups List and then click **New**, the fields in the Groups pane will automatically display the parameters of the selected group. You can then edit parameters as desired, to customize the new group.



2. In the **Group Name** field, enter a name for the new group.

3. In the **Description** field, enter a description of the new group.

4. Define access rights for the new group by clicking **Group Rights** check-boxes. You can click one or all of the following check-boxes:

Read checkbox

> Gives members of this security group read-only rights to switches in the list of All Discovered Devices that **can be seen by** this security group. Members of this group will be able to view switch information, but will not be able to modify the information. Members of this group will not be able to run discovery or manually add, delete, or modify entries in the list of All Discovered Devices.

Write checkbox

> Gives members of this security group both read and write access to switches in the list of All Discovered Devices that **can be seen by** this security group. Members of this group will be able to view switch information and modify the information. However, members of this group will not be able to run discovery or manually add, delete, or modify entries in the list of All Discovered Devices.

Network Admin checkbox

> Gives members of this security group read, write, and network admin access to the switches in the list of All Discovered Devices. Members of this group will be able to view switch information and modify the information. Members of this group will be able to run discovery and manually add, delete, and modify entries in the list of All Discovered Devices. Members of this group will also have full read and right access to entries in the Audit Application, the Control Panel Application, and the Notifications Application. Members of this group will be able to do everything EXCEPT edit the groups and users defined in the Users and Groups Application.

Account Admin checkbox

> Gives members of this security group all rights provided by the **Network Admin** checkbox and full rights to edit the groups and users defined in the Users and Groups Application . This is the highest level of access rights.

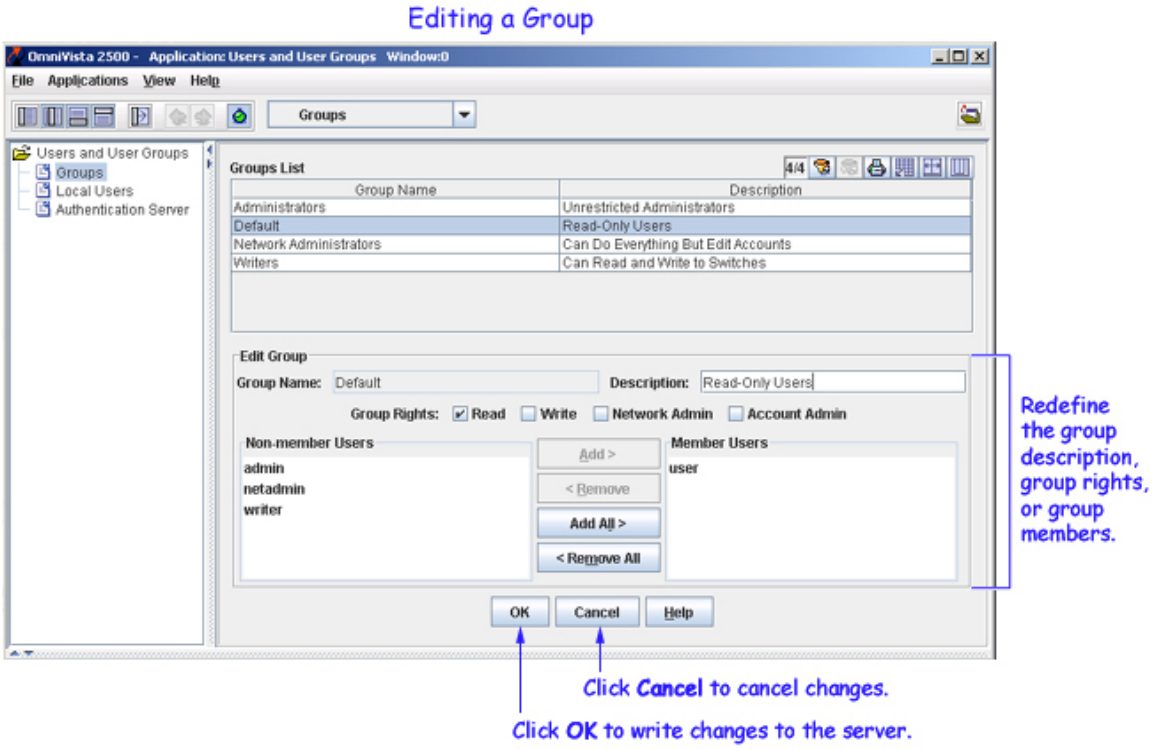
5. Add users to the new group by moving users from the **Non-Member Users** area to the **Member Users** area. All known users are listed for your selection. Note that users may belong to more than one group at a time, in which case their access rights are defined by the most privileged group to which they belong. You do not have to add users to the security group at this time. When you create a user, you can add them to any existing security group as a member. You can also edit a security group later to add members.

6. Click the **Apply** button to create the new group. Clicking the **Default** button will reset the fields in the Groups pane but leave the Groups pane in add mode. Clicking the **Cancel** button will cause the Groups pane to exit add mode.

Redefining a Security Group

Follow the steps below to redefine a security group's access rights or member users.

1. From the Groups pane, select the group in the Groups List, then click the **Edit** button. The group is placed in the edit mode.



2. Redefine the group description, the group rights, or the group members as desired. You cannot edit the group rights of the Administrators group.

3. Click the **Apply** button to write the group changes to the server. You can also click the **Cancel** button at any time to cancel your changes and exit edit mode.

Deleting a Group

To delete an existing group, go to the Groups pane, select the group in the Groups List, then click the **Delete** button. You cannot delete the Default Group or the Administrators Group.

Creating and Managing Users

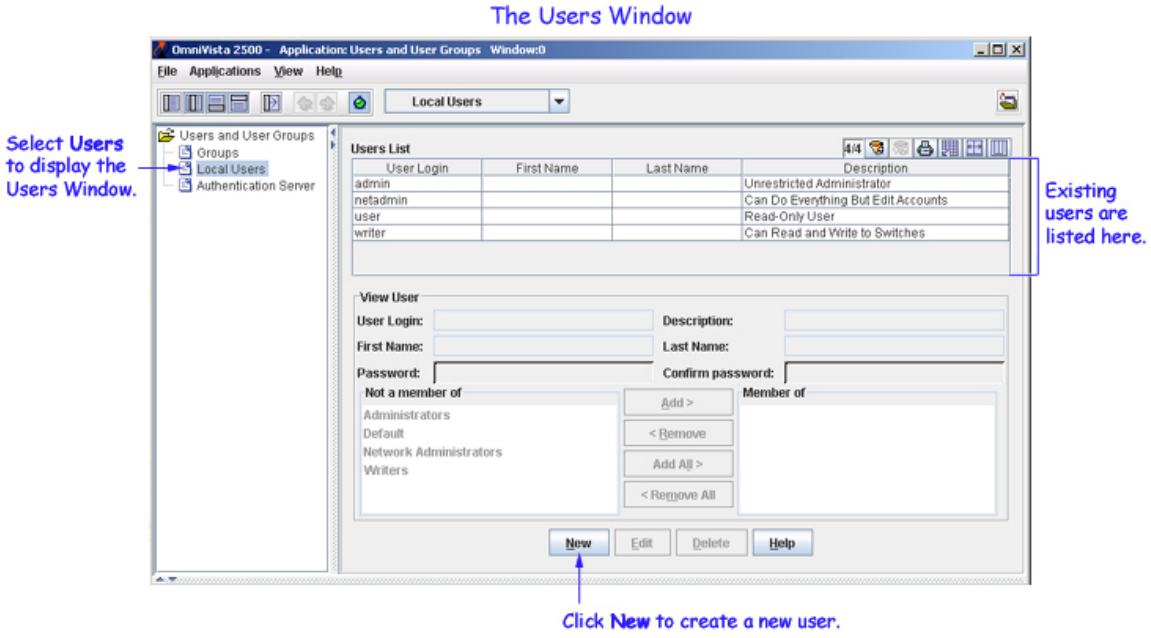
The Local Users pane, shown below, enables you to add new users, delete users, or edit existing users and change their security group assignments and passwords. Note that a user's access rights are determined by the security group in which the user is a member. OmniVista is shipped with four pre-configured users and four pre-configured security groups, which are listed and described below. The default password for all four pre-configured users is **switch**. For security reasons, it is recommended that you redefine the default passwords. The default users and their pre-configured group memberships are as follows:

user. This user belongs to the Default security group and has read-only access to switches that **can be seen by** the Default security group. The default password for this user is **switch**.

writer. This user belongs to the Writers security group and has both read and write access to switches that **can be seen by** the Writers security group. This user can view and modify switch information. The default password for this user is **switch**.

netadmin. This user belongs to the Network Administrators security group and has full administrative rights to all switches on the network. Members of this group can do everything EXCEPT edit the groups and users defined in the Users and Groups Application. The default password for this user is **switch**.

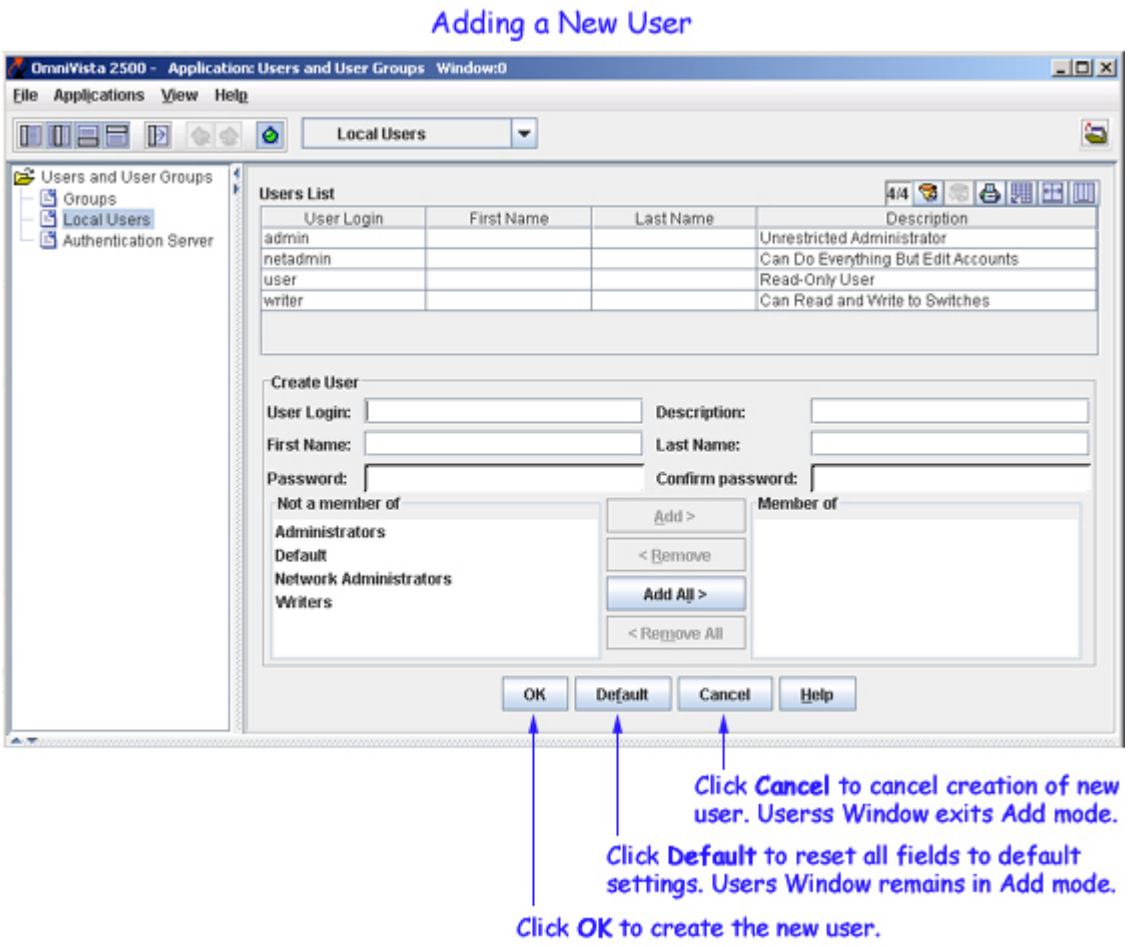
admin. This user belongs to the Administrators security group and has full administrative rights to all switches on the network AND full administrative rights to the Users and Groups Application. The default password for this user is **switch**.



Adding a New User

Follow the steps below to create a new user. When creating a new user, note that only the **User Login** field is required. All the other fields are optional. However, if no password is specified, the password will be null (that is, no password will be set). If no group membership is specified, the new user will be automatically placed into the Default security group.

1. Click the **New** button, shown in the screen above. The Local Users window enters the add mode and all fields are activated, as shown below. If you select an existing user in **Users List**, then click **New**, the fields in the **Local Users** pane will automatically display the parameters of the selected user. You can then edit parameters as desired to customize the new user.



2. In the **User Login** field, enter a login name for the new user. The user will login to OmniVista with this name.

3. In the **Description** field, enter a description of the new user for identification purposes.

4. In the **First Name** and **Last Name** fields, enter the new user's first and last names for identification purposes.

5. In the **Password** and **Confirm password** fields, enter a password for the new user. The user will use this password to login to OmniVista.

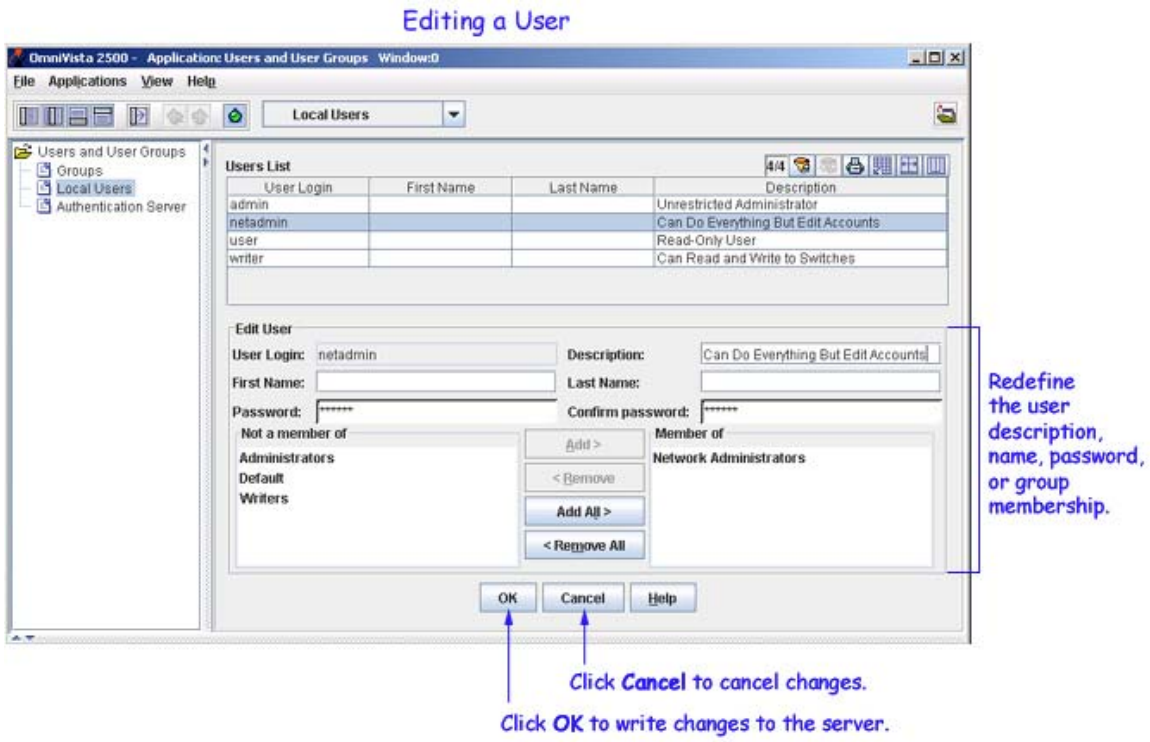
6. Add the new user to one or more security groups by moving groups from the **Not a Member of** area to the **Member Of** area. All known security groups are listed for your selection. Note that users may belong to more than one group at a time, in which case their access rights are defined by the most privileged group to which they belong.

7. Click the **Apply** button to create the new user. Clicking the **Default** button will reset the fields in the **Local Users** pane but leave the **Local Users** panel in the add mode. Clicking the **Cancel** button will cause the **Local Users** pane to exit the add mode.

Redefining a User Definition, Password, or Group Assignment

Follow the steps below to redefine a user's definition, password, or group assignment.

1. From the **Local Users** pane, select the user in **Users List**, then click the **Edit** button. The user is placed in the edit mode.



2. Redefine the user's description, name, password, or group membership. (You cannot remove user **admin** from the **Administrators** group.)

3. Click the **Apply** button to write the changes to the server. You can also click the **Cancel** button at any time to cancel your changes and exit edit mode.

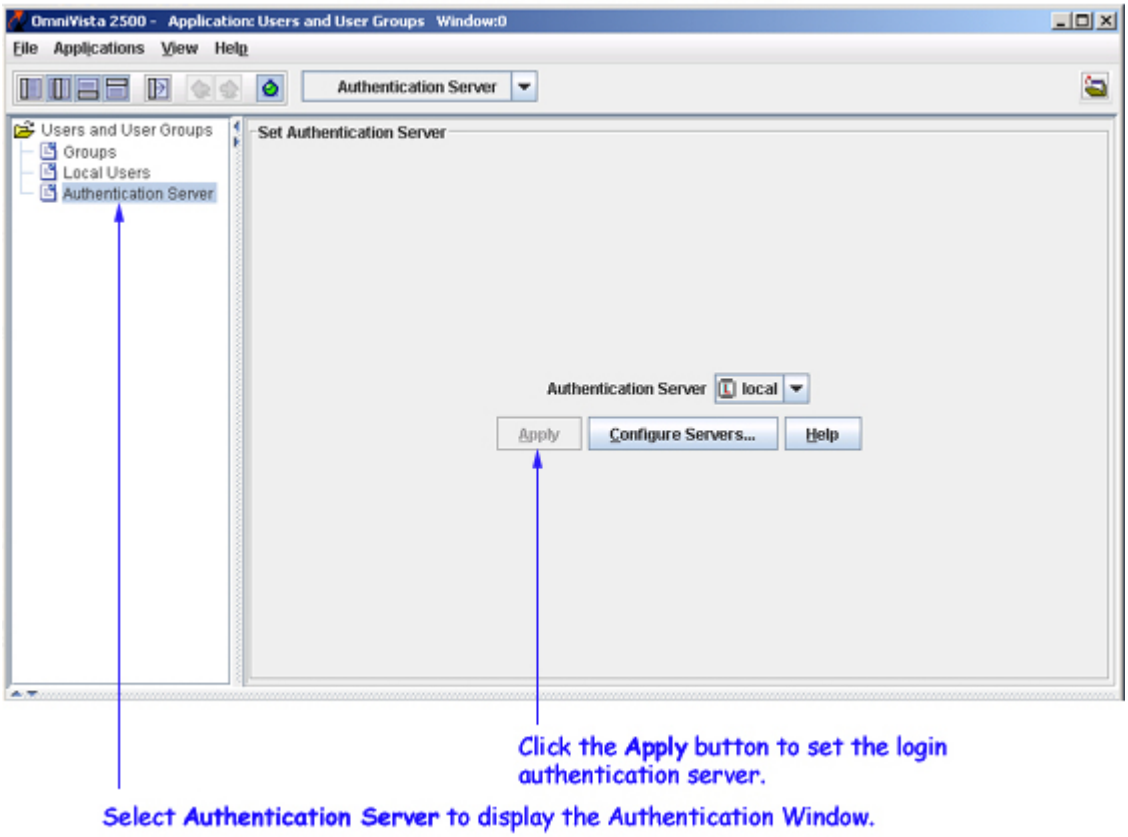
Deleting a User

To delete an existing user, go to the **Local Users** pane, select the user in **Users List**, then click the **Delete** button. (You cannot delete user **Admin**.)

Selecting the OmniVista Login Server

The Authentication Server pane, shown below, enables you to select the local login authentication server or remote RADIUS login authentication server. Prior to selecting the authentication server, you can also configure the LDAP, RADIUS, and ACE servers by clicking the **Configure Servers...** button. When you click the **Configure Servers...** button, the **Authentication Servers** application is launched.

The Authentication Server Window



Setting the Login Authentication Server

To set the login authentication server, select the local or remote authentication server from the Authentication Server drop-down list, and click the **Apply** button.

> **Note:** If a remote authentication server is selected, and that remote server and the remote backup server is not available, then the users can login from the local OmniVista server.
>
> **Note:** If the **admin** user changes the login server, the current users will remain logged in. However, if the users attempt to login/re-login, then they will be logged in using the changed login server.
>
> **Note:** Currently, only RADIUS and Local servers can be used for OmniVista login.