



Part 2.

Managing Access to nVista Projects



Accounts, Users and Groups

In nVista, accounts, users and groups are used to organize and manage access to published projects. Here's how it works: your nVista administrator can create one or more nVista **accounts**. Each account has its own set of nVista projects as well as a list of **users** who are authorized to log into that account. Within each account, each authorized user can also be given specific access rights for each of the projects in that account. To avoid the inconvenience of assigning project-specific access rights one user at a time, you can create **groups** of users within an account. When you assign an access permission to a group, each user within that group will automatically receive that permission level.

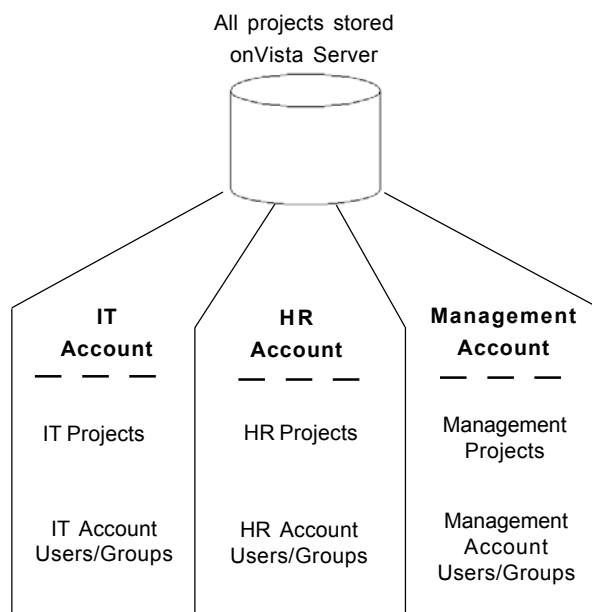
Accounts

An account holds a collection of nVista projects and is associated with a list of authorized users. Each time a user logs into nVista, he or she must choose an account to log in to. Once logged in, the user will only see the nVista projects in that account. To see projects in other accounts, that user must log out, choose a different account, and log back in. In that sense, there is a “wall” between nVista accounts.

When creating your organization's nVista accounts, you should think about which groups of people will need to see which types of nVista projects. You may, for example, have an “IT” account that contains projects depicting network data, an “Administrative” account with projects depicting workflows, a “Management” account with sensitive financial information, and so on. But because you can also control access to projects on a per-user basis within a single account, you could also choose to have just one nVista account for an entire organization.

Choices you make about accounts can be changed at any time. However, as time goes by, you are likely to accumulate a lot of users, groups and projects within each account. The longer you use nVista, the more time consuming it will be to alter your organization's nVista account structure.

Note: Accounts may be created, modified or deleted only by your nVista administrator.



Each nVista account has its own group of projects and users

Users

Each account has users. These are individuals who are authorized to log in to the account and who have some degree of access to the nVista projects in the account. While an authorized user can always log into an account, that user's access to particular projects (or portions of projects) may still be limited by using nVista's access permissions.

Example: Your organization has an nVista account called "IT", which contains network diagrams. You make John, a junior network administrator, a "user" in the IT account, so that he can see the network diagrams for troubleshooting purposes. Your organization is considering opening a new office and creates an nVista project that contains a proposed network design for that office. The project is published to the IT account so that other IT personnel can see and comment on it, but it contains sensitive information about implementation costs and personnel projections. You can set the permissions for that project so that John will not see it in the IT account's project list even though he continues to be able to log in to the IT account.

Groups

Groups are simply collections of users in an account. Groups are useful for setting access permissions within an account quickly.

Example: In the same example above, say your organization has six junior network administrators and you want to limit their access to the project with sensitive financial information. Instead of setting permissions separately for each of the six, you can simply create a group called “Junior IT” that contains those six individuals. When you set project permissions for that group, each of those individuals will automatically “inherit” those permissions. If you like, you can still set permissions for each member of that group individually.

Who Your Users and Groups Should Be

Here’s an approach to use in deciding who your users and groups should be for a given account.

Note: It’s very easy to create, modify or delete users and groups, so it’s not worth agonizing over who your users and groups should be. Try something. If it’s not perfect, it will be easy to change.

Defining Your Users

You can’t create groups until you have users, so choose users first. Think about who in your organization would likely need access to the projects in the account. If it’s an IT account, each member of your IT team should probably be a user. Don’t forget management representatives. If you have an ongoing relationship with a hardware vendor or outside design team, you may want to include them too. If it’s an account that will hold information about business processes, like new-employee intake, you’ll need to make members of the HR team users, not to mention benefits personnel and someone from the payroll office.

Defining Your Groups

Once you've got your users identified, you'll want to put them into logical groups. The key here is to decide what combinations of users will typically share the same access rights to projects. You don't need to decide yet what those access rights will be, only that they'll be the same for everyone in the group. For example, all users in upper management will likely have the same access to projects, so they'd make a good group. The same goes for all members of the design team, all junior network technicians, and so on.

Note: Individual group members can always be assigned access rights to a project that are different than their inherited group rights. A user can also be a member of more than one group. For information on how nVista deals with the conflicting access rights that could result, see Permissions, later in this section.

The Role of the Account Administrator

One or more users in an nVista account can be given administrator rights. Just as a network administrator has the right to add authorized users to your organization's network, the administrator(s) in each nVista account can add, modify or delete users or groups for that account.

Each time you create a new account, you are required to identify a single, first user. This user is automatically given account administrator rights. That first user can then log into the account to create more users and groups.

Account administrators also have the power to create additional user administrators or change an existing user into an administrator. There is no upper limit to the number of administrators an account can have. However, an account must always have at least one administrator.

Note: Be careful not to create too many administrators in a given account. If you give a lot of people the right to create, delete and modify users and groups, it can become difficult to manage the account's users.

Creating\Modifying\Deleting Accounts

Accounts can only be created, modified or deleted by your company's nVista administrator. For more information about creating new accounts or your organization's existing nVista account structure, contact your administrator.

Creating New Users

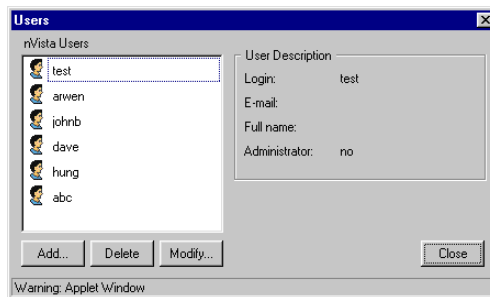
If you have administrator rights in an account, you can create new users.

To create a new user:

1. Log into nVista.
2. Click the **Admin** button on the nVista Toolbar.

Note: You must have administrative rights in your account to create, modify or delete users or groups. If the Admin button on the nVista toolbar is "grayed out," then you do not have administrative rights and you will not be able to perform the following actions.

3. Click **Users...** You will see a dialog box like the one shown below.



4. Click **Add...**
5. Fill in the information about the new user. Check the **Administrator** box if you want this new user to have account administrator privileges.



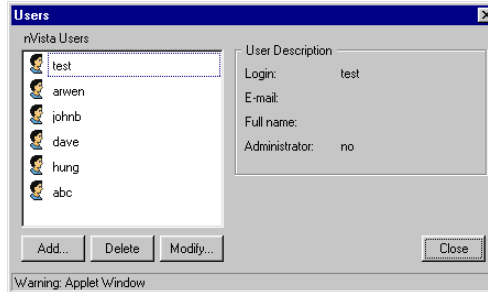
6. To set a password for this new user, click **Set Password...**
When you're done, click **OK** in each box.

Modifying User Properties

If you have administrator rights in an account, you can modify a user's properties. That includes changing a user's log in and/or password, name, e-mail address or administrator privileges.

To modify the properties of an existing user:

1. Log into nVista.
2. Click **Admin** on the nVista toolbar.
3. Select **Users...**



4. Highlight a user name and click **Modify. . .**
5. Make the desired changes to the user properties and click **OK**.

Deleting Users

If you have administrative rights in an account, you can delete users from that account. To delete a user:

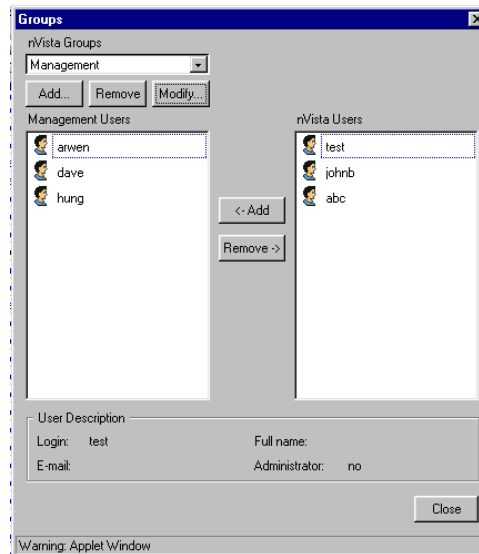
1. Log into nVista.
2. Click **Admin** on the nVista toolbar.
3. Select **Users. . .**
4. Select a user name and click **Delete**.

Creating Groups

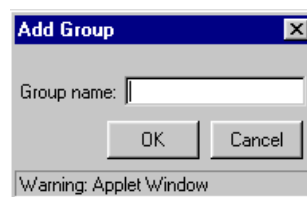
If you have administrative rights in an account, you can create or modify groups. To do that:

1. Log into nVista.
2. Click the **Admin** button on the nVista toolbar.

3. Select **Groups ...**
4. Click **Add ...** in the upper left portion of the window



5. You will be prompted to enter a name for your new group, as shown below. Name the group and click **OK**.



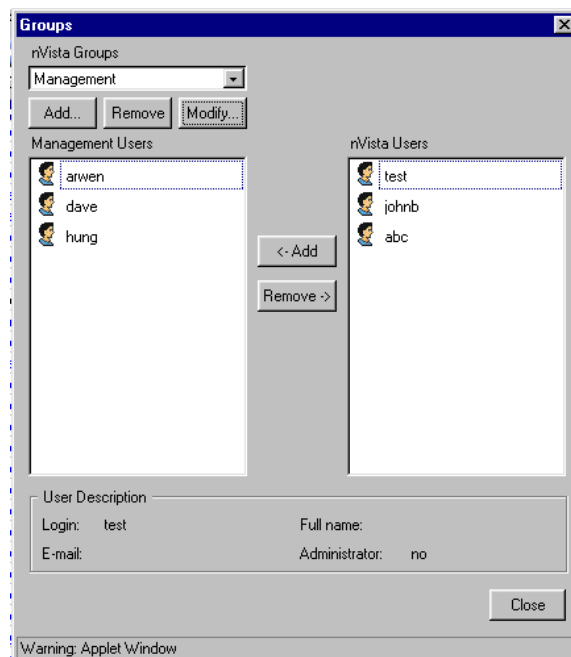
6. All of the account's users are listed in a column on the right. For each user that you would like to add to the new group, select the user and move him or her into the column on the left by using the **Add** button. To remove a user from the group, use the **Remove** button.
7. When you're done, click **Close**.

Modifying Groups

If you have administrative rights in an account, you can modify a group's name or composition.

To modify a group name:

1. Log into nVista.
2. Click the **Admin** button on the nVista toolbar.
3. Select **Groups ...**
4. Select the group you want to modify from the pull down at the upper left of the dialog box.



5. Click **Modify...**



6. Modify the group's name as desired and click **OK**.

To modify a group's composition:

1. Log into nVista.
2. Click the **Admin** button on the nVista toolbar.
3. Select **Groups...**
4. Select the group you want to modify from the pull down at the upper left of the dialog box as shown below.
5. All of the account's users are listed in a column on the right. For each user that you would like to add to the new group, select the user and move him or her into the column on the left by using the **Add** button. To remove a user from the group, use the **Remove** button.
6. When you're finished, click **Close**.

Permissions

What are nVista Permissions?

By default, all of the users in an account have some level of access to that account's nVista projects. One way to refine project access is by assigning custom permission rights to individual projects on a user-by-user basis. Permission rights range from no access at all to the ability to edit project data and delete or overwrite projects. Permissions can be set so that a given user/group has the same access right across an entire project or different rights for different portions of the project.

nVista's Permissions defined

nVista allows you to select one of five different access levels, for all or part of a project, as follows:

No Access – User can see diagram name in Hierarchy Browser, but will not be able to view the diagram.

Note: If a user is given "No Access" to an entire project, that project name will not even appear in the project list when the user logs into the account.

Read - User can open a read-only version of a diagram. Read only includes the ability to see diagrams as well as the data associated with diagram objects.

Annotate – User can place comments on or graphically mark up diagrams, but cannot change underlying diagram data.

Edit Data – User can change underlying project data.

Delete Annotations - User can delete annotations created by other users.

Project Administrator – User can delete or overwrite entire projects and can set or modify access permissions for the project.

Note: nVista access permissions are cumulative. Each higher permission level includes all of the rights of the levels below it.

The Role of the Project Administrator

For each project in an nVista account, there must be at least one person with the power to delete or overwrite the project as well as set the project permissions for the other users and groups in the account. That person is the Project Administrator. By default, whenever a person publishes a netViz project to nVista, that person is automatically designated the Project Administrator for the project. After the project is published, that Project Administrator can modify the access rights to that project for all of the account's users. Among other things, the Project Administrator can create additional Project Administrators.

Note: Because Project Administrators can delete projects and change user permissions, it is best not to have more than one or two Project Administrators for any nVista project.

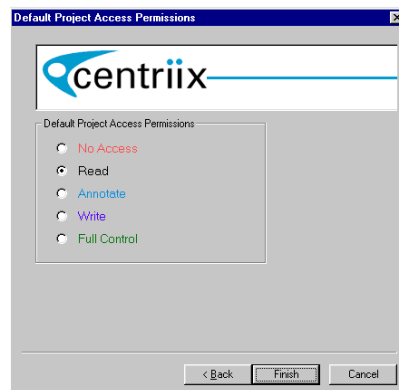
How to Set/Modify Permissions

Each time a netViz project is published to nVista, the project's publisher will be asked to choose an initial access permission for all the users and groups in the account that the project is being published to. After a project is published, anyone with Project Administrator rights can change those access permissions.

At the Time of Publishing

When a project's author publishes to nVista, he or she will be prompted to pick an initial permission level for the project, as shown below. This is the permission that will be given for the entire project to every user and group in the project's

account. At this stage, it is best to err on the side of providing less access. Once the project is published, it's easy to provide more access to the users and groups who need it.

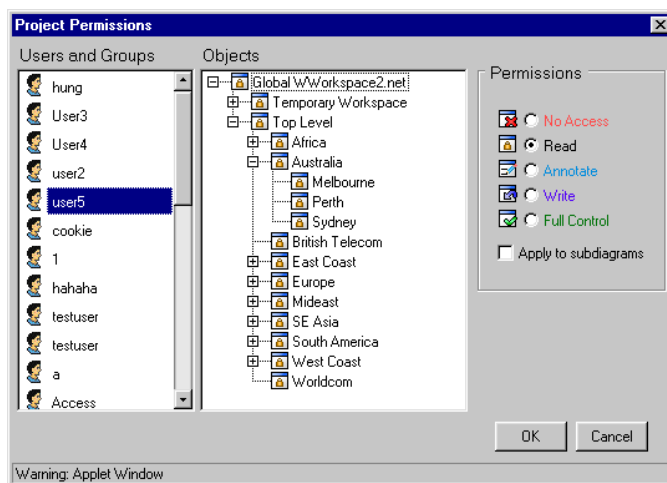


Note: When the project is published, the person who published it will automatically be given Project Administrator rights.

After a Project is Published

Anyone with Project Administrator rights can change the access permissions to a project after it's been published. Here's how:

1. Log into nVista.
2. Select the project from the list by clicking it.
3. Click **Permissions**. The window on the left shows all of the users and groups in the selected account. The window on the right shows the levels of the selected project.



Note: You can expand levels and sublevels by clicking on the “+” sign to the left of the diagram name.

5. Select a user or group from the window on the left. The window on the right will show that user’s current access permissions for each project level. To change an access permission, select the desired project level and choose a new permission.

Note: To automatically apply your changes to all of a branch’s subdiagrams, check the “Apply to Subdiagrams” box. If you set permissions without checking that box, your changes will only be applied to the specific diagrams you select.

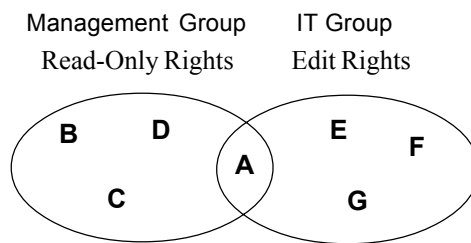
The top line in the window on the right shows the project’s name. If you select that line and set an access permission, the permission you select will automatically be applied to *all* project levels. Keep in mind, this will override all existing access permissions.

Note: If you set a user permission to “No Access” for an entire project, the project name will not even appear on the project list when that user logs into the account. If you set a user permission to “No Access” for only a portion of the project, the user will be able to open the project and all of the diagram names will appear in the Hierarchy Browser, but the user will not be able to view the diagrams set to No Access.

Conflicting Permissions Among Users/Groups

At times a given user can have conflicting permissions for a project because of that user’s group membership. Say, for example, that A belongs to the Management Group and to the IT Group, and the Project Administrator gives Read access to one group and Annotate access to the other. Which access right should A have? nVista uses the following logic to resolve such permission conflicts:

If a person is a member of multiple groups that have different access levels, that person will get the highest access level available, as shown below:



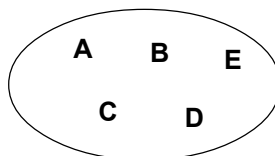
As a member of both the Management Group and the IT Group, User A will have the higher access, in this case, “Edit” rights.

If a person is a member of a group that has access to a project, but that person is given a different access level as an individual, that person will get the access level assigned to him/her as an individual.

User A
Read-Only rights

IT Group
Edit rights

A



Even though User A is a member of the IT group, she will have the read-only rights that were assigned to her as an individual.

In the event of a conflict, the precedence nVista gives to a user's permission settings for a given project is as follows:

Permission set for that individual user.

If user belongs to multiple groups, the highest permission among those groups.

If user belongs to a single group, that group's permission.

Default permission (i.e. the permission assigned at the time of publishing).

Highest



Lowest