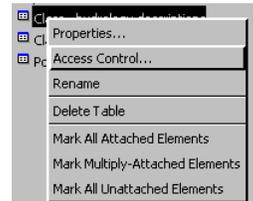
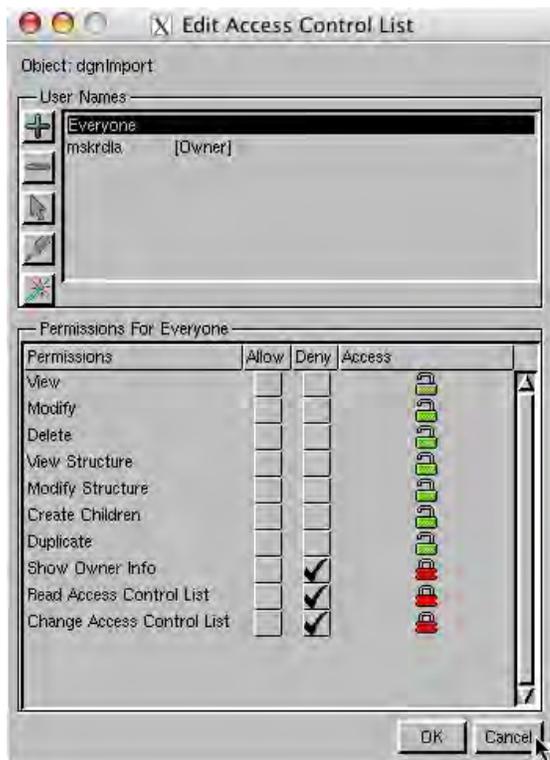


System

Access Control Lists

 In enterprise situations where many people are involved, you may want to restrict who has permission to view and who has permission to change geospatial data or the information in database fields. With or without an enterprise environment, you may have developed a custom product using the TNT SDK and want to control how others can manipulate the data distributed with it. Such management issues are handled by credentials and access control lists. Credentials are established by user name and password. An access control list determines the necessary credentials to access the contents of a Project File, object, or subobject in a variety of ways, which include viewing, modifying, deleting, viewing database structure, modifying database structure, creating subobjects (children), and copying. You can even control who has access to individual database tables and database fields. Thus, a specific user may be unable to view some fields in a table, be allowed to view but not change certain fields, and be able to view and change others. The access control list also determines who can see owner information for the file/object and who can read and change the access control list.

Access control is set up in the Project File Maintenance process. For database tables and fields, access control can also be set up anywhere the database has been selected for viewing. When you click on the Edit Access Control icon or select Access Control from the right mouse button



menu for a table, you are prompted for your user name and password. If the file, object, or subobject does not already have an access control list at that level, you become the owner by default. There are two sets of default permissions: one for the owner and the other for “everyone.” Everyone is all people not specifically named in the list. The owner always has permission to see owner information and read and change the access control list. These three permissions are off by default for “everyone” but can be turned on. When Show Owner Info is allowed for the current user, the information entered in the Edit Owner Information window is included with the other information shown about the file or object when you click on the Info button in Project File Maintenance.

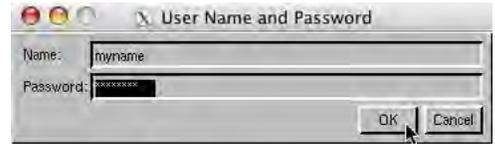
There are three access permission states indicated by check boxes: allow, deny, and ambiguous (neither box is checked). When permissions are ambiguous for an individual user, the permissions set for “everyone” are checked. If permissions are still ambiguous, the permissions for the parent object are checked up to the file level. For example, if no permissions are set for a database field (specific user and everyone), the permissions for the table are checked, and if these are not set, then the permissions for the database are checked followed by permissions for the vector. If permissions are still ambiguous, the permissions for the file are checked. If these permissions are also am-

biguous, the action is allowed. The color of the locks to the right of the permissions check boxes indicates whether an option is allowed for both explicit and ambiguous settings. Some permission combinations are nonsensical, such as allowing modification but not viewing at the same level. However, allowing modification of a database table without permission to view the vector it is under may be useful.

Access control is optional and need not be used unless you want to restrict access to your data in situations such as noted above. Access control lists can be viewed by all TNTmips users, but the ability to edit access control lists must be requested from MicroImages. If you do not have this option, the OK button is never active.

When a file with an access control list at any level is selected for any process, the user is prompted for name and password just as when editing an access control list. If a file with an access control list was the last selected file for a process, you will be prompted for name and password before you select anything.

Access Control in SML and SDK. You can pass or require credentials (user name and password) to control what data is accessed and where it is written in custom scripts and in custom processes you develop using TNTmips' SDK. If credentials are passed, any person running the script or process has the access of the user specified in the script. If credentials are not passed and are required, the open and create functions will prompt for user name and password. There is also a function to prevent this dialog from opening if credentials are not passed and the script tries to access an object or file that requires credentials.



A simple script that opens a raster using credentials and reports the raster type in the Console window is shown below.

```
class RASTER R;  
class RVC_CREDENTIALS credentials;  
credentials.Set("myname", "password");  
OpenRaster(R, "E:/test/credtesting/creds.rvc", "_24BIT_BGR", credentials);  
typ$ = R.$Info.Type; "print(typ$);
```

If this line is omitted, the script will prompt for user name and password if needed when run.

When credentials are passed and a file/object is created by a process developed with the SDK or a script, the user named becomes the owner of the file. Additional permissions are set as described on the other side of this page. The function called DisableCredentialsPopup() is used to prevent the User Name and Password prompt from opening when credentials are not passed. A script that uses this function will fail with an error (user does not have permission to complete the operation) without first prompting for credentials when a file/object is used that has restrictive permissions set. This error is the same error received when the credentials entered or passed will not provide access to the file/object.

