nirva

How-to: Application permissions

Document version: 1.01

The permissions supported by Nirva can limit specific user access to possible operations within an application. The application procedures can check that the connected user presents the necessary access rights to allow or deny a given operation.

This document discusses only the Nirva enabled security. The Nirva integration platform relies on its own security system but can also support interfaces to external security systems. These are the Nirva security services (please refer to the Nirva documentation for more information).

The Nirva built in security is based on the “RBAC” model (for Role Based Access Control). Permissions are set in roles that in turn are assigned to the various users.

When a particular user opens up a Nirva session, his/her global permissions are stored and kept within the session context.

For more information on Nirva security, please refer to the « Security » chapter in the Nirva technical documentation

Nirva supports a number of system permissions and allows for each application and/or service the creation of new permissions. The newly created permissions can then be associated to particular roles. A set of commands are available to verify the session owner’s permissions to control access to specific functions implemented in a Nirva application.

> Application permissions are only available if security is defined at application level. Nirva Nirva can be configured fro a particular application to rely on its own security, or to rely on another application’s security or to rely on the system’s security. In the latter case, application permissions are not available.

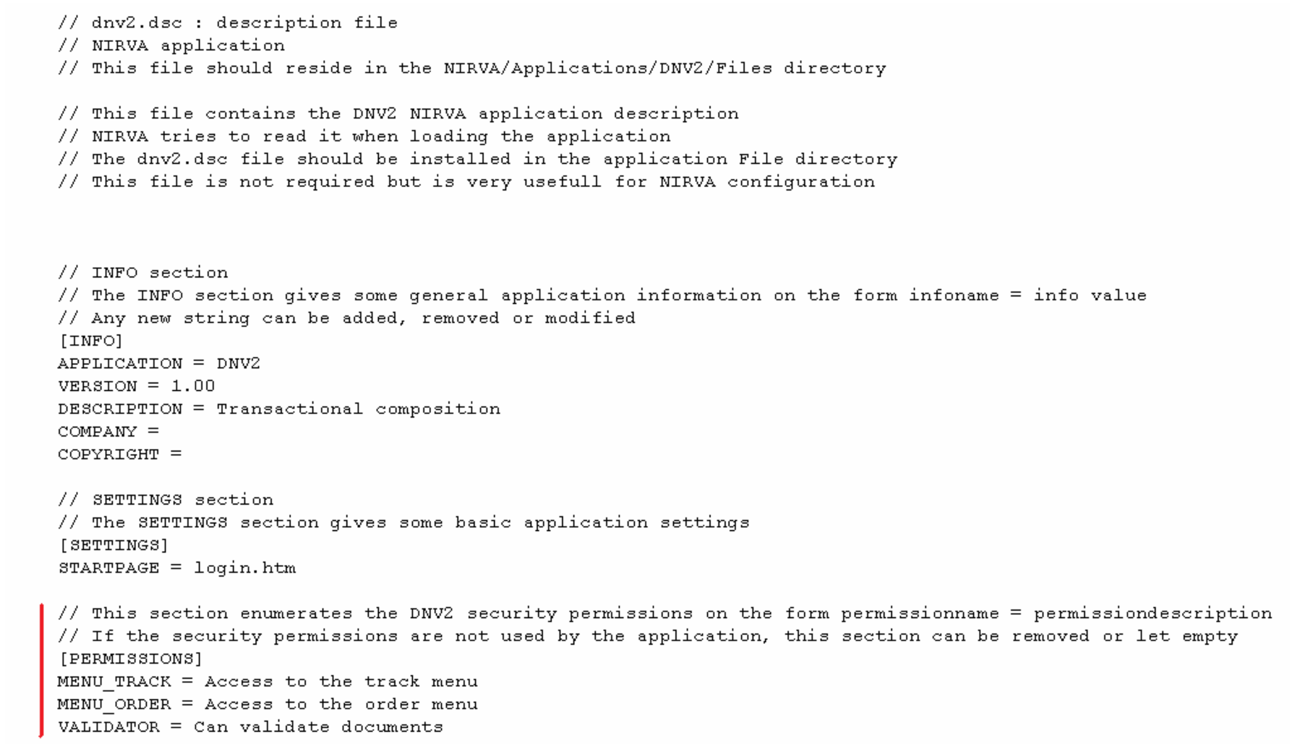
Permission definition in the “.dsc” file.

The file contains, amongst other components, the application permissions so they can be available to the administration interface and associated to roles.

The permission definitions that are needed in an application are stored in the dsc file.

The dsc file is located in the “Files” directory of a given application.

Below: a glimpse at a dsc file.



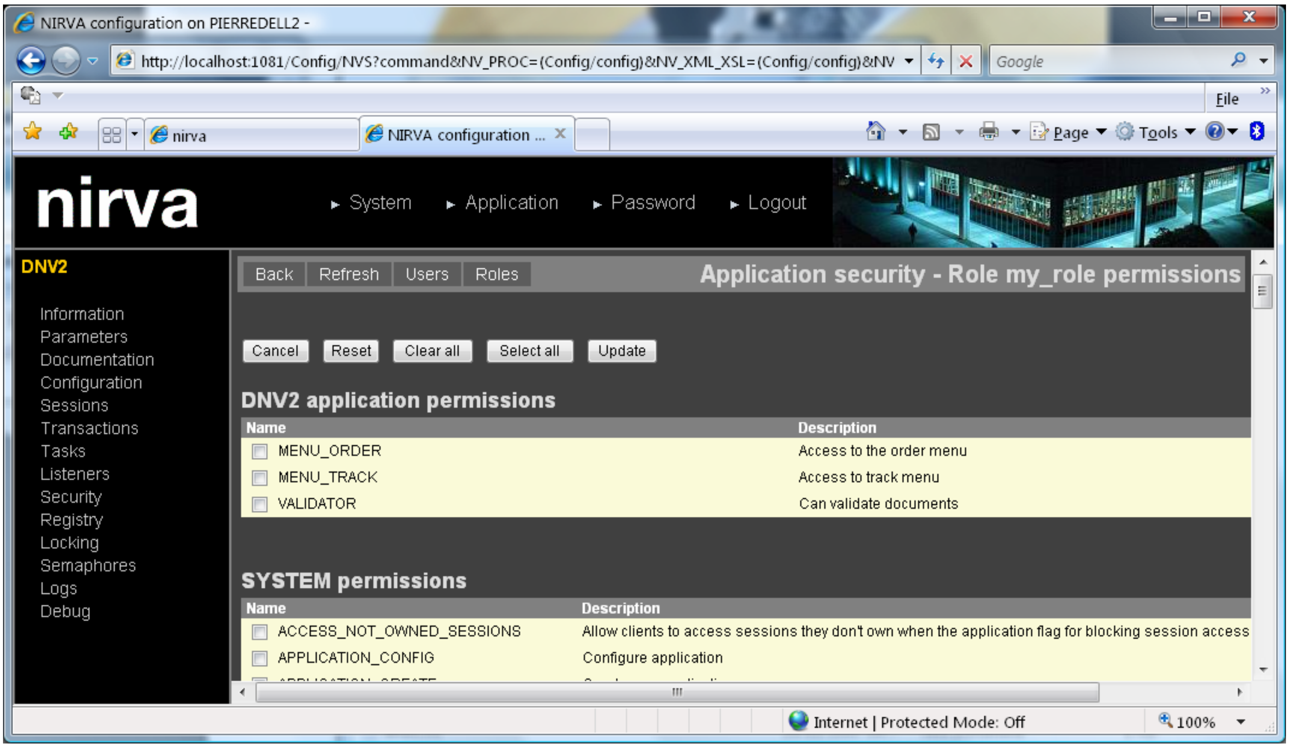
```
// dnv2.dsc : description file
// NIRVA application
// This file should reside in the NIRVA/Applications/DNV2/Files directory

// This file contains the DNV2 NIRVA application description
// NIRVA tries to read it when loading the application
// The dnv2.dsc file should be installed in the application File directory
// This file is not required but is very usefull for NIRVA configuration



// INFO section
// The INFO section gives some general application information on the form infoname = info value
// Any new string can be added, removed or modified
[INFO]
APPLICATION = DNV2
VERSION = 1.00
DESCRIPTION = Transactional composition
COMPANY =
COPYRIGHT =

// SETTINGS section
// The SETTINGS section gives some basic application settings
[SETTINGS]
STARTPAGE = login.htm

// This section enumerates the DNV2 security permissions on the form permissionname = permissiondescription
// If the security permissions are not used by the application, this section can be removed or let empty
[PERMISSIONS]
MENU_TRACK = Access to the track menu
MENU_ORDER = Access to the order menu
VALIDATOR = Can validate documents
```

New permissions can be added with a simple coupling of "Permission_name" and "Description of the permission" in the [Permissions] section, e.g.:

```
MENU_ORDER = Access to the order menu
```

A permission name must be type in all caps (all upper case) and must not contain special characters nor spaces.

Newly created permissions are then available in the Nirva configuration:



Application security - Role my_role permissions

DNV2 application permissions

Name	Description
□ MENU_ORDER	Access to the order menu
□ MENU_TRACK	Access to track menu
□ VALIDATOR	Can validate documents

SYSTEM permissions

Name	Description
□ ACCESS_NOT_OWNED_SESSIONS	Allow clients to access sessions they don't own when the application flag for blocking session access
□ APPLICATION_CONFIG	Configure application

Permission verification

The command SYSTEM:SECURITY:CHECK must be used when permission verification is need in the application procedures.

> Permissions defined in the “dsc” file of an application are the permission for this particular application. Permissions for services are declared in the “dsc” files of the services.

Any created role can receive any number of permissions by using the configuration interface. Available permissions are System level permissions, Service level permissions and Application permissions for the application to which the user is connected. In the application code itself, the permission verification command can be used to verify that the user has the correct rights for the requested operation. The result of the verification is passed back through a Boolean variable set to “TRUE” when the operation is authorised and to “FALSE” when the operation is not authorised.

Here is an example of how to use the command:

```
NV_CMD=|SECURITY:CHECK| PERMISSION=|MENU_ORDER| AUTHORIZED=|ALLOW_MENU_ORDER|
```

The AUTHORIZED parameter defines the name of a Boolean variable that is created to receive the result. In this example, a Boolean object called “ALLOW_MENU_ORDER” is created in the output container and its value indicates whether the user has the permission or not. This object can be accessed and used to select the next action, whether permission is granted or not, such as triggering an error, start another procedure, display a menu, etc.

If the AUTHORIZED parameter is not supplied in the SECURITY:CHECK command, the command returns a SYSTEM:SECURITY:105 error (operation not authorised). This is sometimes enough to limit access to a procedure, for example.

Adding permissions dynamically

Permissions are defined and stored in the dsc file and are attributed to the role through the configuration interface in Nirva.

However, it is possible to add dynamically permissions to a user’s session. This can be a permission as defined in a dsc file or can be any other type (for instance a permission defined in an external LDAP system).

This operation is only possible in the initialisation procedure of the session (session_open.nvp as the default).

```
NV_CMD=|SECURITY:ADD_SESSION_PERMISSION| PERMISSION=|MY_PERMISSION|
```

It is also possible to remove an existing permission:

```
NV_CMD=|SECURITY:REMOVE_SESSION_PERMISSION| PERMISSION=|MY_PERMISSION|
```

It is also possible to assign a complete role to a particular session. However, the role must have been previously defined in the Nirva security system:

```
NV_CMD=|SECURITY:ADD_SESSION_PERMISSION| ROLE=|MY_ROLE|
```