



**How-to Guide
SAP NetWeaver '04s**

How To... setup NWDI Permissions and Roles

Version 1.20 – November 2006

**Applicable Releases:
SAP NetWeaver '04
SAP NetWeaver 2004s**

© Copyright 2006 SAP AG. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

Microsoft, Windows, Outlook, and PowerPoint are registered trademarks of Microsoft Corporation.

IBM, DB2, DB2 Universal Database, OS/2, Parallel Sysplex, MVS/ESA, AIX, S/390, AS/400, OS/390, OS/400, iSeries, pSeries, xSeries, zSeries, z/OS, AFP, Intelligent Miner, WebSphere, Netfinity, Tivoli, and Informix are trademarks or registered trademarks of IBM Corporation in the United States and/or other countries.

Oracle is a registered trademark of Oracle Corporation.

UNIX, X/Open, OSF/1, and Motif are registered trademarks of the Open Group.

Citrix, ICA, Program Neighborhood, MetaFrame, WinFrame, VideoFrame, and MultiWin are trademarks or registered trademarks of Citrix Systems, Inc.

HTML, XML, XHTML and W3C are trademarks or registered trademarks of W3C[®], World Wide Web Consortium, Massachusetts Institute of Technology.

Java is a registered trademark of Sun Microsystems, Inc.

JavaScript is a registered trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.

MaxDB is a trademark of MySQL AB, Sweden.

SAP, R/3, mySAP, mySAP.com, xApps, xApp, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world. All other product and service names mentioned are the trademarks of their respective companies. Data

contained in this document serves informational purposes only. National product specifications may vary.

These materials are subject to change without notice. These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

These materials are provided "as is" without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. SAP shall not be liable for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials.

SAP does not warrant the accuracy or completeness of the information, text, graphics, links or other items contained within these materials. SAP has no control over the information that you may access through the use of hot links contained in these materials and does not endorse your use of third party web pages nor provide any warranty whatsoever relating to third party web pages.

SAP NetWeaver "How-to" Guides are intended to simplify the product implementation. While specific product features and procedures typically are explained in a practical business context, it is not implied that those features and procedures are the only approach in solving a specific business problem using SAP NetWeaver. Should you wish to receive additional information, clarification or support, please refer to SAP Consulting.

Any software coding and/or code lines /strings ("Code") included in this documentation are only examples and are not intended to be used in a productive system environment. The Code is only intended better explain and visualize the syntax and phrasing rules of certain coding. SAP does not warrant the correctness and completeness of the Code given herein, and SAP shall not be liable for errors or damages caused by the usage of the Code, except if such damages were caused by SAP intentionally or grossly negligent.

1	Scenario.....	2
2	Introduction.....	3
3	Technical mapping.....	7
3.1	UME Actions.....	7
3.2	J2EE Security Roles.....	9
3.3	DTR Permissions.....	9
3.4	Track-specific Authorizations.....	12
4	The Step By Step Solution.....	13
4.1	Check and edit UME settings.....	13
4.2	Set J2EE Security Roles.....	16
4.3	Check and edit DTR Permissions.....	17

1 Scenario

The SAP NetWeaver Development Infrastructure¹ serves as base for realising a comprehensive software development process, comprising development of several components, activating components for shared usage, up to consolidation, testing and deployment.

- All development objects (sources, table definitions, Web Dynpro definitions etc.) are stored and versioned in the Design Time Repository (DTR)
- Central builds and the resulting archives are provided by the Component Build Service (CBS)
- The Name Server is the naming authority ensuring unique names (e.g. for development components (DCs), database tables, Java packages etc.)
- The Change Management Service (CMS) is providing software logistic functionality and is controlling the development landscape
- The SAP NetWeaver Developer Studio (NWDS) is installed on the developer desktop and provides an integrated development environment for development using NWDI

Compare help.sap.com, for a short description of the development steps using NWDI:
<http://help.sap.com> → Documentation → SAP NetWeaver → SAP NetWeaver 2004s → English → SAP Library

- SAP NetWeaver Library
- Administrator's Guide
- Technical Operations Manual for SAP NetWeaver
- Administration of SAP NetWeaver Systems
- AS Java (Application Server for Java)
- Software Logistics
- Development Infrastructure (DI)
- SAP NetWeaver Development Infrastructure
- Development Scenarios with the NWDI

The intention of this guide is to show a sample how you can expand the initial security configuration of the NWDI, which is done by the template installer during the setup phase, to adapt it to your business needs. With the installation of the usage type DI (Development Infrastructure) and the post-installation step using the DI template with the Template Installer, the NWDI is ready to use with a preconfigured track, users, groups and roles. This guide introduces additional logical roles involved for NWDI based software development, describes the tasks covered by each role and explains the needed permissions. Help is given to check and if necessary to adopt the various user, group and roles settings to your specific installation.

¹ For this official name, two abbreviations are currently in use: JDI (Java Development Infrastructure) and NWDI (NetWeaver Development Infrastructure). Therefore you can find both abbreviations in parallel.

2 Introduction

Assume your team wants to extend a Product by a new feature. The initial installation of NWDI and basic configuration steps are supposed to have been done already. For implementing the new product feature, a single CMS Track has to pass through. Figure 1 illustrates the activities and attached systems of a CMS Track.

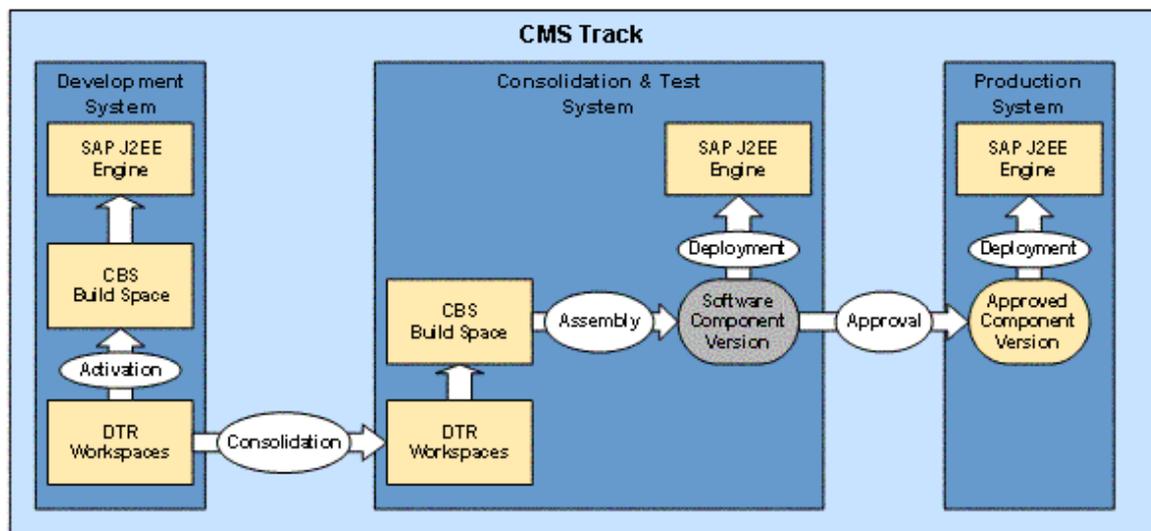


Figure 1 CMS track structure.

During development, five major roles have to be occupied:

- **Software Architect**
As a result of designing the software architecture he defines the Product version, included Software Components to be developed, required Software Components and their dependencies. He uses mainly the System Landscape Directory.
- **Landscape Administrator**
He sets up the initial environment for developing a Product, comprising name reservations, Track definitions and Development Configurations. The Landscape Configurator part of CMS is used for these purposes.
- **Transport Manager**
He is responsible for transporting the according deliveries between the logical systems that built up the track. In our scenario, he would start with importing the necessary sources and archives in the Development System. Later on, he imports the Development Components in the Consolidation and Test System. Besides this, he is responsible for assembling components to the new Product version. The Transport Studio of CMS is his preferred tool.
- **Member of Development Team**
Based on the imported Development Configuration, team members create and implement Development Components (DCs) as part of the changeable Software Components of the Product or change existing ones. Typically developers pass the steps Design → Implementation → (Unit) Testing for each Development Component in a local environment. Then they activate their changes in order to make them useable for further development steps. Builds and deployments in a central development environment ensure an ongoing integration of all changes made by development team members. When the feature is implemented and

tested in the Development System, the corresponding Development Components are released for import in the Consolidation system. The NetWeaver Developer Studio is the developer's main tool for these tasks.

- **Quality Manager**

The quality manager assures that the new product conforms to the requested quality standards. He is responsible for Product consolidation and for final approval before product delivery. For approval of the product shipment the Transport Studio of CMS is used.

Figure 2 assigns the mentioned roles to the process steps while passing a CMS Track.

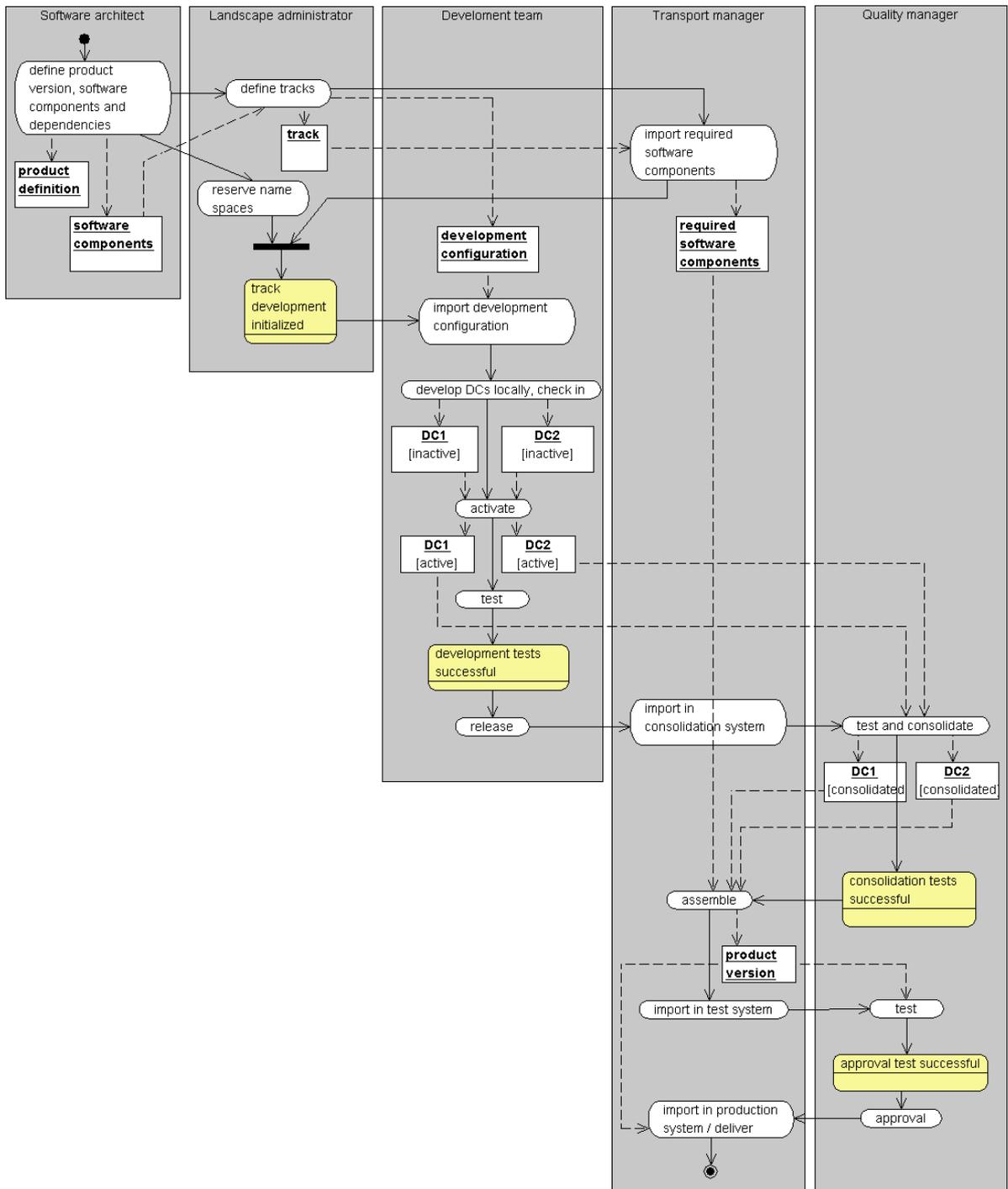


Figure 2 Java Software Lifecycle Management with the SAP NWDI

The following table describes the tasks for each identified role in more detail. Please note: The column “Involved systems” summarizes all systems that are called directly as well as implicitly while processing the tasks. In accordance, the column “needed privileges” lists privileges needed not only by the role itself but also needed by internal system users (e.g. service users like NWDI_CMSADM).

NWDI Role	Tasks	Involved systems	Needed privileges
Administrator	initial setup & maintenance of CMS Domain data ² , Rescue User	CMS → Landscape Configurator	(write Domain data in CMS)
Software Architect	define Product version, Software Components and dependencies	SLD → Software Catalog	write into the “Software Catalog” in SLD
Landscape Administrator	define Tracks	CMS → Landscape Configurator	read, write track information in CMS
	define Track authority	CMS → Track Authority	assign permissions in CMS
	reserve Namespaces	SLD → Name Reservation	read, write Namespaces in SLD
Development Team	import Development Configuration	NWDS, SLD, CMS	read SLD and CMS data
	synchronize sources	NWDS, DTR	read sources from DTR
	synchronize required archives	NWDS, CBS	read archives from CBS
	create and check in Development Components	NWDS, DTR	write, check in to DTR, write name reservation to SLD
	build / deploy /test locally	NWDS, local J2EE Engine	administration of local engine
	activate	NWDS, DTR, CBS	create build requests

² Note: Using the template installer will pre-configure the Domain ID, which cannot be changed afterwards.

	test	CMS, central development system	access to development runtime system
	release	NWDS, CMS	Create, release requests
Transport Manager	Access to file system of CMS server	CMS → Transport Studio	import in CMS systems
	Access to SAP Service Marketplace		
	Check-in and import required SCs into Development System		
	import into Consolidation System		
	Assemble Software Component version		
	import into Test System import into Production System		
Quality Manager	tests in Test System	appropriate test tool	Administration
	test	CMS, central Development System	access to development runtime system
	Release	NWDS, CMS	create release requests

Table 1 Involved systems and necessary privileges

3 Technical mapping

The NWDI roles and their privileges described in Table 1 must be mapped to technical permission settings on several levels (UME Actions, J2EE Security Roles, DTR ACLs and Track-specific ACLs). The following paragraphs give an overview of the settings that have to be done. Chapter 4 gives a step by step solution for doing it.

Detailed information to the technical mappings can be found in <http://help.sap.com>: → Documentation → SAP NetWeaver → SAP NetWeaver 2004s → English → SAP Library

- SAP NetWeaver Library
- Administrator's Guide
- Technical Operations Manual for SAP NetWeaver
- Administration of SAP NetWeaver Systems
- AS Java (Application Server for Java)
- Software Logistics
- Development Infrastructure (DI)
- SAP NetWeaver Development Infrastructure
- Configuring the NWDI User Management

Note: Please keep in mind that this guide is based on a single-server installation (all NWDI components and SLD on a single server). If the NWDI components or the SLD are distributed on multiple servers a central user administration (CUA) is recommended. Otherwise you need to setup the same credentials (same user with the same password) with the appropriate permissions on all systems.

Note: The following permission settings are always based on UME Groups. Depending on whether an SAP system, LDAP or database is used as user store, users and UME Groups respectively SAP Roles must be created in different ways. For a detailed description please see

<http://help.sap.com>: → Documentation → SAP NetWeaver → SAP NetWeaver 2004s → English → SAP Library

- SAP NetWeaver Library
- SAP NetWeaver Security Guide
- User Administration and Authentication
- Integration of User Management in Your System Landscape

3.1 UME Actions

The permission concept of CBS, CMS and SLD is based on UME Actions that need to be mapped to UME Roles. This has to be done using the Web-based User Management Engine Administration Console (<http://<server>:<port>/useradmin>) that is part of the SAP J2EE Engine.

Table 2 summarizes the mapping of identified NWDI Roles to necessary users and their assigned UME Groups, UME Roles and UME Actions.

NWDI Role	User	UME Group	UME Role	UME Actions
Administrator	NWDI_ADM (default user)	NWDI .Administrators	NWDI .Administrator	CBS.Administrator CMS.Administrate LcrInstanceWriterAll
Member of development team	(default: NWDI_DEV)	NWDI .Developers	NWDI .Developer	CBS.Developer (CBS.XDeveloper) CMS.Display CMS.ExportOwn (CMS.ExportForeign) LcrInstanceWriterNR
Software Architect		NWDI .Architects	NWDI .Architect	CBS.Guest CMS.Display LcrInstanceWriterCR
Landscape Configurator		NWDI .Configurators	NWDI .Configurator	CMS.ConfigureDomain CMS.CreateTrack CMS.Display CMS.ModifyTrack CMS.UserAdmin LcrInstanceWriterLD LcrInstanceWriterNR
Transport Manager		NWDI .Operators	NWDI .Operator	CBS.Administrator CMS.CriticalFunctions CMS.Display CMS.Transport
Quality Manager		NWDI .QManagers	NWDI .QManagers	CBS.Guest CMS.Approve CMS.Display
CMSAdmin (technical user used by CMS)	NWDI_CMSADM (default user)	NWDI .CMSAdmins	NWDI .CMSAdmin	CBS.Administrator LcrInstanceWriterLD LcrInstanceWriterNR

Table 2 Necessary users, UME Groups, Roles and Actions for NWDI

For the standard workflow, your named users are mapped to the necessary Groups as needed. Besides this, there are two technical users that are used for special purposes only; they are not mapped to named users.³

The NWDI_ADM user has all privileges and therefore can perform all tasks in the NWDI. He is intended to be used for the initial setup of the NWDI and as an emergency user. For your regular development cycle, you should not use the NWDI_ADM user to ensure traceability. Instead the usage of dedicated admin users belonging to group NWDI.Administrators enables you to decouple the J2EE Administrator user from the applications itself. Furthermore dedicated admin users can be used for delegated administration of Tracks (see chapter 3.4).

Another unnamed user which is required is the NWDI_CMSADM. This user is not assigned to a real person, but intended to be used only internally by the CMS. He can perform all actions in the DTR, CBS, and SLD that are required to configure the NWDI and operate the CMS. He is also used for intra-component communication between CBS, DTR and SLD.

³ If you used the Template Installer for the configuration of the NWDI, these users are already created and assigned to the necessary groups. The settings should be checked either.

3.2 J2EE Security Roles

For the SLD, it is also necessary to set permissions enabled through J2EE Security Roles. This has to be done in the Visual Administrator Tool. The permissions have to be assigned for the application “sap.com/com.sap.lcr*sld”.

Table 4 shows the settings for the J2EE Security Roles.

UME Group	Security Role
NWDI.Administrators	LcrInstanceWriterAll
NWDI.Architects	LcrInstanceWriterCR
NWDI.CMSAdmins	LcrInstanceWriterLD LcrInstanceWriterNR
NWDI.Configurators	LcrInstanceWriterNR LcrInstanceWriterLD
NWDI.Developers	LcrInstanceWriterNR

Table 3 Necessary Java Security Role settings for SLD.

For an easier assignment, Table 4 shows the settings per security role.

Security Role	UME Group
LcrInstanceWriterNR	NWDI.Developers NWDI.Configurators NWDI.CMSAdmins
LcrInstanceWriterAll	NWDI.Administrators
LcrInstanceWriterCR	NWDI.Architects
LcrInstanceWriterLD	NWDI.Configurators NWDI.CMSAdmins

Table 4 Necessary Java Security Role settings for SLD.

3.3 DTR Permissions

The DTR permission concept based on ACLs (Access Control Lists) determine which privileges a principal has with respect to a certain resource. Principals are users and groups. DTR files, folders and workspaces are resources. Privileges include read and write access to DTR, check in, and several administration privileges. To set DTR permissions, the DTR admin plugin of the SAP NetWeaver Developer Studio is used.

For details about the DTR authorization, please refer to <http://help.sap.com>

- SAP NetWeaver Library
 - Administrator’s Guide
 - Technical Operations Manual for SAP NetWeaver
 - Administration of SAP NetWeaver Systems
 - AS Java (Application Server for Java)
 - Software Logistics
 - Development Infrastructure (DI)
 - SAP NetWeaver Development Infrastructure
 - Configuring the NWDI User Management
 - User Authentication and User Authorization in the DTR

Please be aware that you may lock out the user you use to manage permissions, since permissions are stored as versioned files in the DTR. If this occurs, please refer to the

section “User Management Steps after Installation → Editing the Emergency User” in the “Configuring the NWDI User Management” section of the online documentation.

Table 5 summarizes the permission settings for DTR.

Principal	Type	Resource	Right	Privilege
NWDI.Administrators	Group	/	grant	All privileges
		/sysconfig		
		/system-tools →/administration		
		/ws/system		
NWDI.CMSAdmins	Group	/	grant	All privileges
		/ws/system		
NWDI.Configurator	Group	/ws/system	grant	Access, Read, Write, CheckIn
		/act	grant	Read, Write
		/wr	Grant	Read, Write
NWDI.Developers	Group	/	grant	Access, Read
		/act	grant	Write, CheckIn
		/vh	grant	Write
		/wr	grant	Write
		/ws	grant	Write, CheckIn
		/vcr	grant	Write

Table 5 DTR permissions for using NWDI

To make the assignment easier, **Table 6** shows the privileges per resource.

Resource	Inherit	Principal	Type	Right	Privileges
/ws/system	Ignore	NWDI.Administrators	Group	grant	All
		NWDI.CMSAdmins	Group	grant	All
		NWDI.Configurator	Group	grant	Access, Read, Write, CheckIn
/system-tools →/administration	Ignore	NWDI.Administrators	Group	grant	All
/sysconfig	Ignore	NWDI.Administrators	Group	grant	All
/act	Yes	NWDI.Developers	Group	grant	Write, CheckIn
		NWDI.Configurators	Group	Grant	Read, Write
/vcr	Yes	NWDI.Developers	Group	grant	Write
/vh	Yes	NWDI.Developers	Group	grant	Write
/wr	Yes	NWDI.Developers	Group	grant	Write
		NWDI.Configurators	Group	grant	Read, Write
/ws	Yes	NWDI.Developers	Group	grant	Write, CheckIn
/	Yes	NWDI.Developers	Group	grant	Access, Read
		NWDI.Administrators NWDI.CMSAdmins	Group	grant	All

Table 6 DTR permissions by resource

Note: In order to grant permissions on Track level, you should grant the privileges “write” and “checkIn” on all inactive Workspaces belonging to this Track. The pattern for the inactive Workspaces is “/ws/<Trackname>/<SC-name>/<CMS-system>/inactive/”.

It is useful to create a UME Group for each Track and grant the permissions to the group instead of single users.

This can also be used to prevent developers from accidentally working on the CONS Development Configuration.

3.4 Track-specific Authorizations

In NetWeaver 2004s and with NetWeaver'04 SPS15, it is possible to specify NWDI permissions per CMS track. By assigning authorizations to tracks you define areas of responsibilities for Administrators or Quality Managers.

Note: To restrict access on the DTR workspaces for developers, please use the DTR ACLs to control the permissions there. With CMS authorizations, it is only possible to control transports of Change Request, but not the access to a development configuration.

The track-specific authorizations can be assigned using a separate UI that is started by using the URL: **http://<host>:<port>/webdynpro/dispatcher/sap.com/tc~SL~CMS~tsawebui/CmsTrackAuthority**

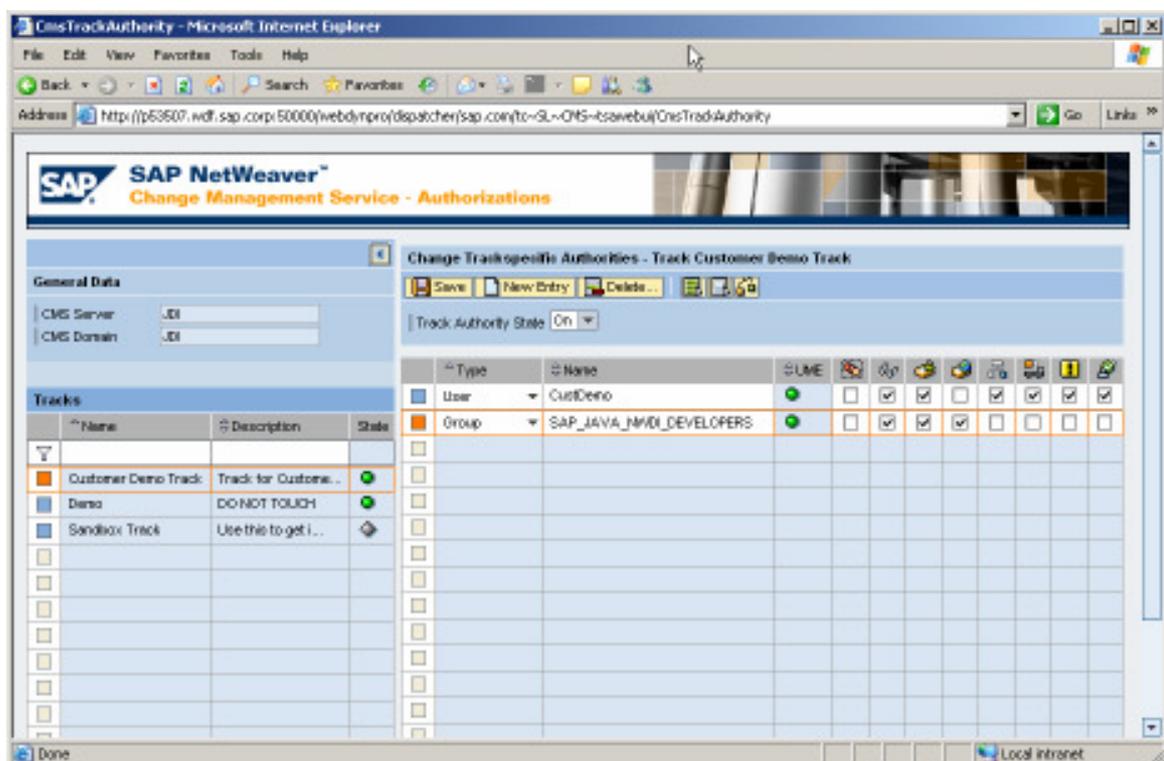


Figure 3: CMS Track Authority Web UI

For detailed information, please refer to the online documentation on <http://help.sap.com>:
→ Documentation → SAP NetWeaver → SAP NetWeaver 2004s → English → SAP Library

- SAP NetWeaver Library
- Administrator's Guide
- Technical Operations Manual for SAP NetWeaver
- Administration of SAP NetWeaver Systems
- AS Java (Application Server for Java)
- Software Logistics
- Development Infrastructure (DI)
- SAP NetWeaver Development Infrastructure
- Configuring the NWDI User Management
- Authorizations in Change Management Service
- Track-specific Authorizations

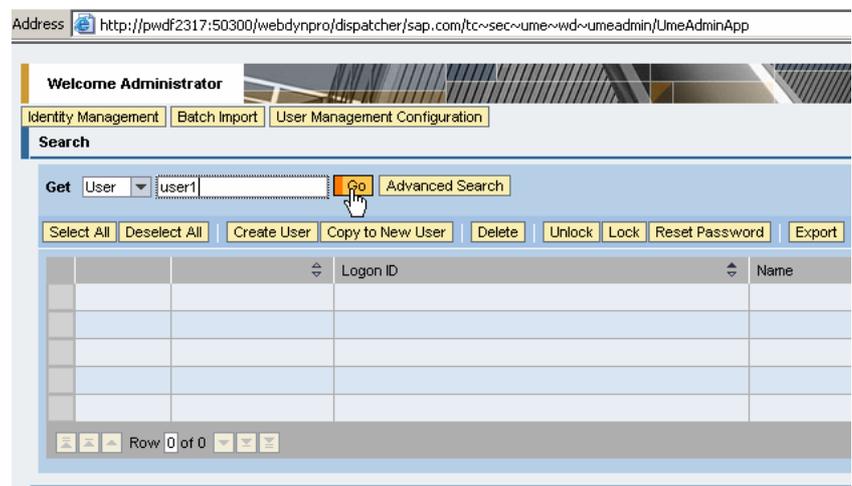
4 The Step By Step Solution

This chapter gives instructions to check and if necessary to create the settings described above, based on an NWDI installed on a single server using the UME as user and group store.⁴ For distributed installations or the usage of a central user and/or group administration, you have to adopt the steps to your needs.

4.1 Check and edit UME settings

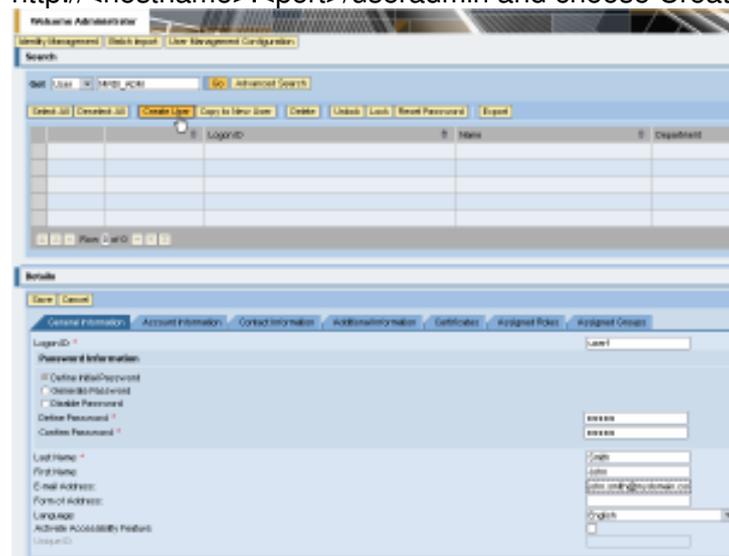
1. Search for existing users

Log in to the UME User Administration GUI <http://<hostname>:<port>/useradmin> and enter the userid. Choose *Go* to start the search.



2. Create new users

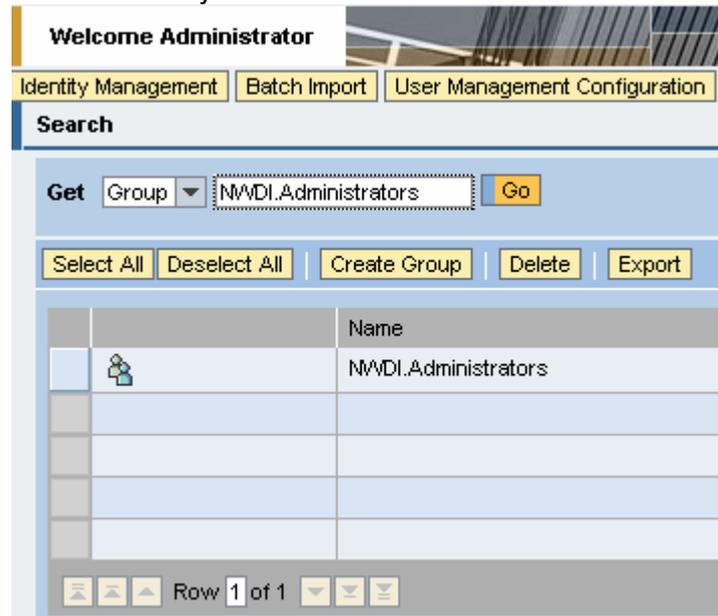
Log in to UME User Administration GUI <http://<hostname>:<port>/useradmin> and choose *Create User*.



⁴ The configuration shown applies for SAP NetWeaver 2004s. The user interface for SAP NetWeaver' 04 looks different.

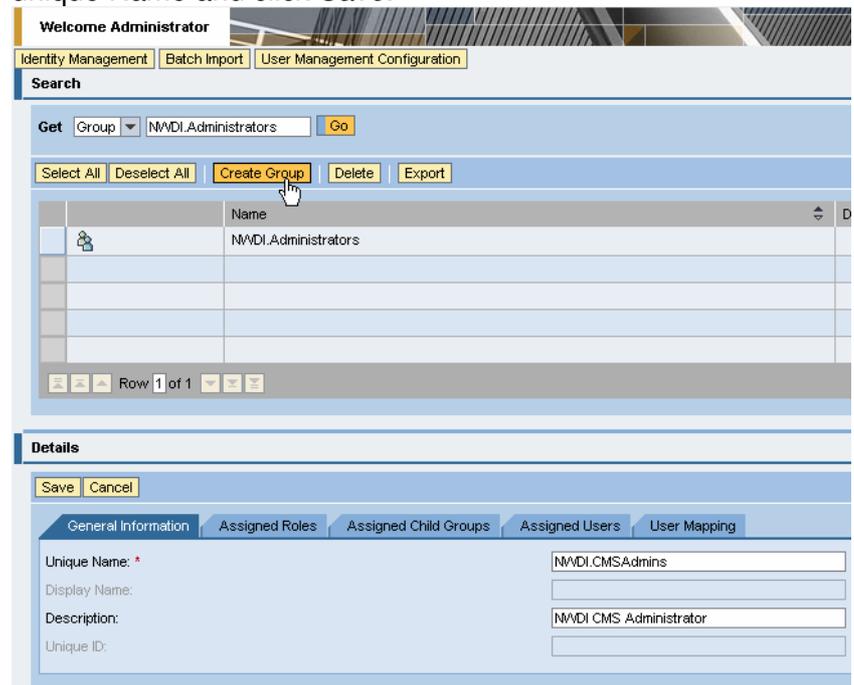
3. Search for existing groups

Log in to UME User Administration GUI
<http://<hostname>:<port>/useradmin> and select *Group* from the list box. Enter your search criteria and choose *Go*.

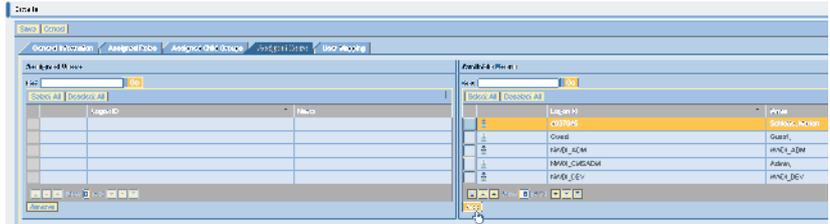


4. Create new group and assign users

Log in to UME User Administration GUI
<http://<hostname>:<port>/useradmin>, select *Group*, enter a unique Name and click *Save*.



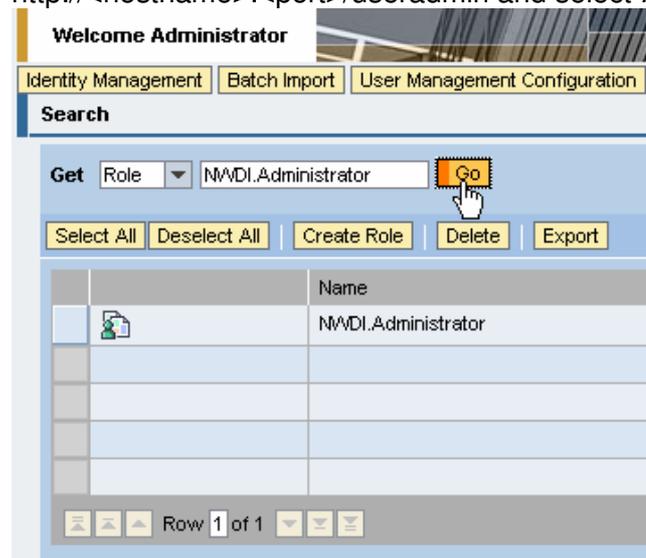
After creating a group, you can assign users by clicking the *Assigned Users* tab.



On the right side click the *Go* button to get a list of all available users. Select one and choose *Add*. Finish with *Save*.

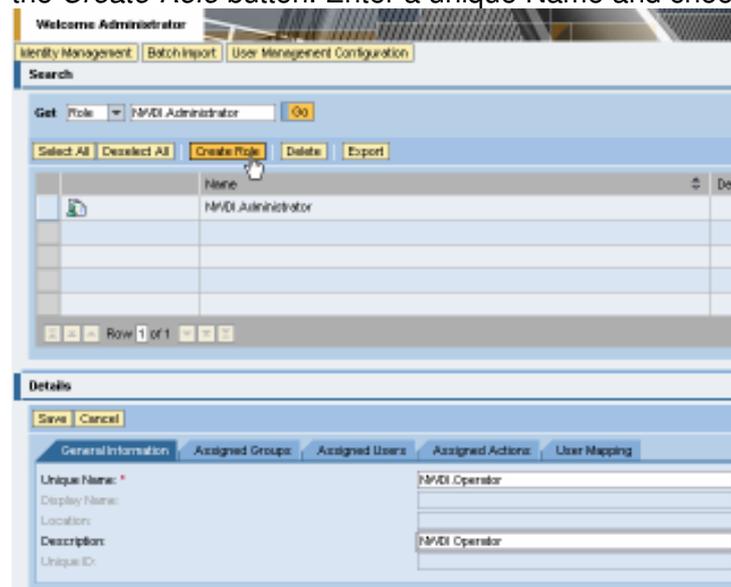
5. Search for existing roles

Log in to UME User Administration GUI
<http://<hostname>:<port>/useradmin> and select *Role*.



6. Create new role and assign group and actions

Log in to UME User Administration GUI
<http://<hostname>:<port>/useradmin> and choose *Roles*. Click the *Create Role* button. Enter a unique Name and choose *Save*.

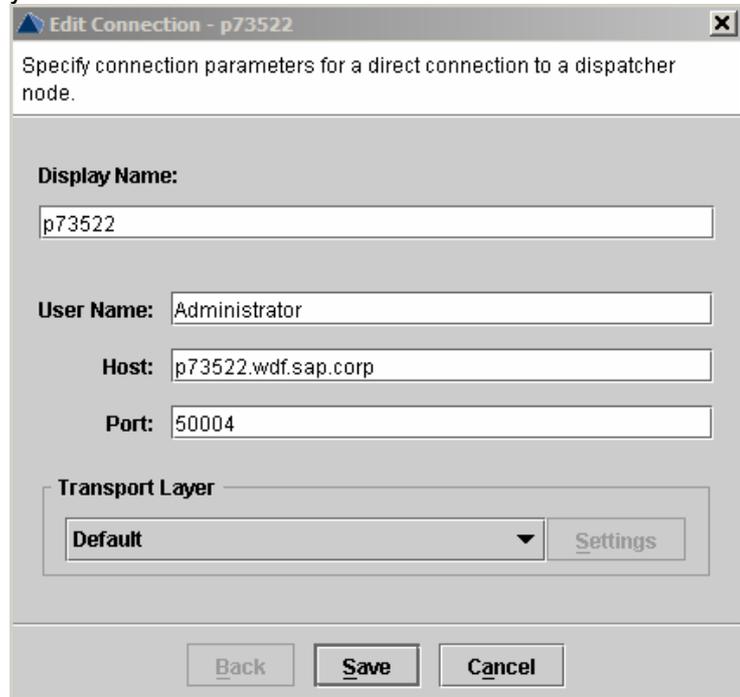


To assign groups choose the *Assigned Groups* tab. The same applies for assigning Actions via the *Assigned Actions* tab. Proceed as described in step 4.

4.2 Set J2EE Security Roles

7. Start J2EE Engine Visual Administrator

Go to the Web AS installation directory and start <Web AS install directory>\<SID>\JC<instancenr>\j2ee\admin\go.bat. Choose *Connect* → *Login* → *New* and specify a connection to your Web AS.



Specify connection parameters for a direct connection to a dispatcher node.

Display Name:
p73522

User Name: Administrator

Host: p73522.wdf.sap.corp

Port: 50004

Transport Layer
Default Settings

Back Save Cancel

Use the new connection to login.

8. Check and edit Java security roles.

On the left side, choose *Server* → *Services* → *Security Provider*. Search the component of interest; this is `sap.com\com.sap.lcr*sld` in our case (see Figure 4). Then click on the tab “Security Roles” and choose the security role you want to assign, e.g. `LcrInstanceWriterNR`. Search for the user or group, that should be assigned, e.g. `NWDI.Developers`. Choose Add and Save.

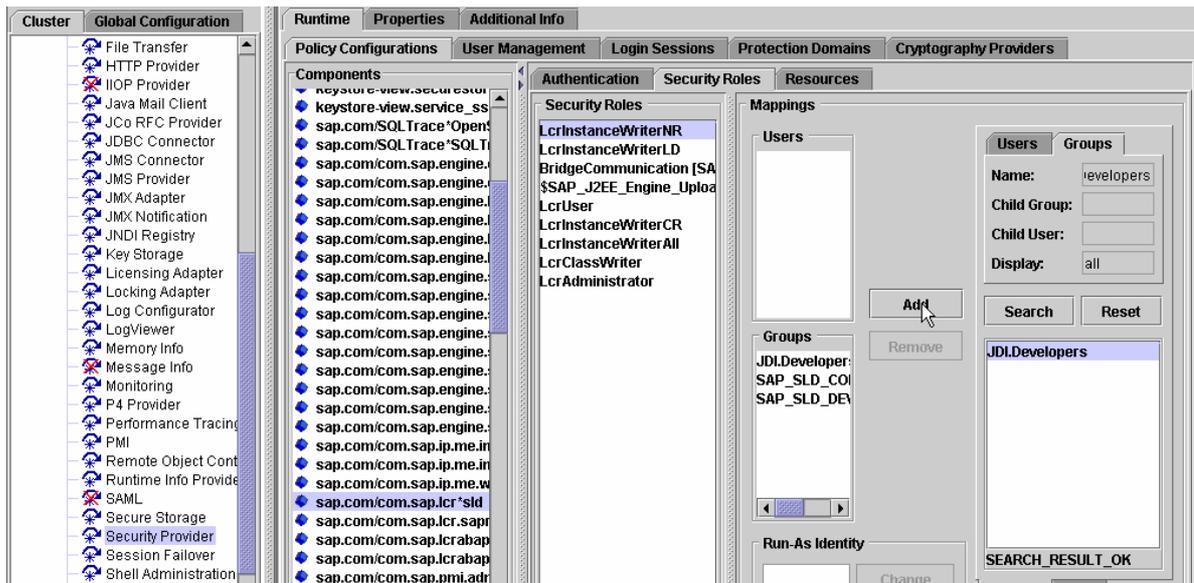


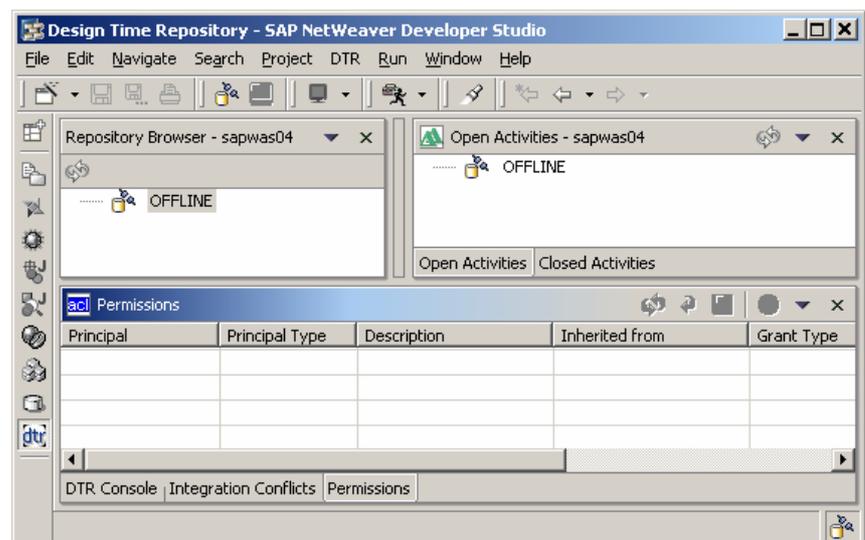
Figure 4 Assign security roles using the Visual Administrator

4.3 Check and edit DTR Permissions

9. Activate DTR plugin

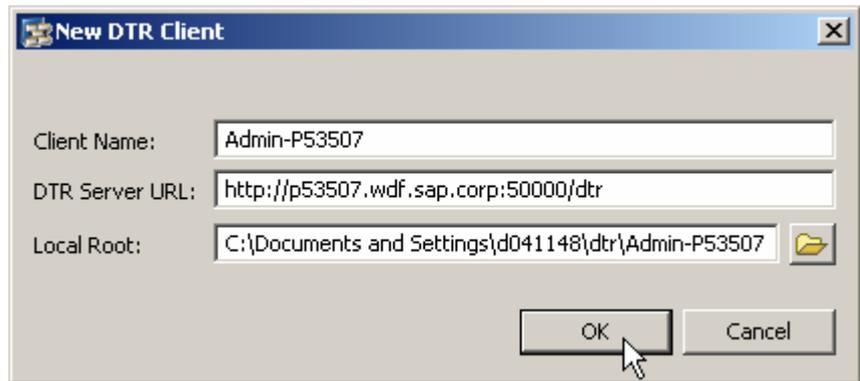
For managing DTR permissions (authorization) you need the DTR admin plugin of the SAP NetWeaver Developer Studio. Make sure that the plugin is active: If necessary, rename the plugin.xml.disabled file in the <SAPDEVSTUDIOHOME> \eclipse\plugins\com.tssap.dtr.client.eclipse.admin\ to plugin.xml.

Open the DTR perspective in NetWeaver Developer Studio (*Window* → *Open Perspective* → *Design Time Repository*)



10. Create DTR client and log in.

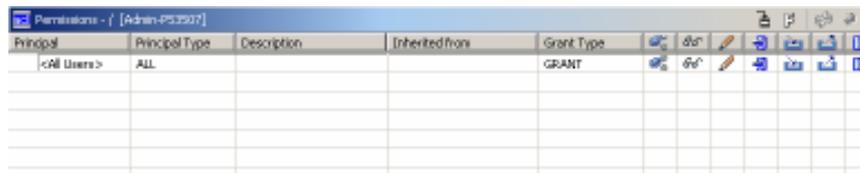
A DTR client represents a connection to a certain DTR server. In order to create a DTR client, use the DTR perspective. This is done using the context menu of item "OFFLINE" in the Repository Browser → "Create Client". Enter the necessary data for your DTR.



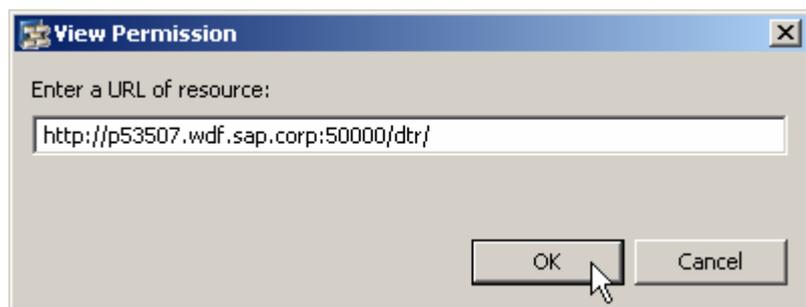
After that, you should be able to connect to the DTR, using the same context menu. Problems may occur if you already have created already another client. Check which client is selected for login (click *DTR* → *Select Client*). In order to change the login name, please close and re-open the NetWeaver Developer Studio.

11. Connect to a specific resource

In order to manage the permissions for a resource, click the context menu of repository browser and choose *View Permissions* from the title bar of the Permissions view, choose *Menu* and select the URL using *View Permissions for URL...*



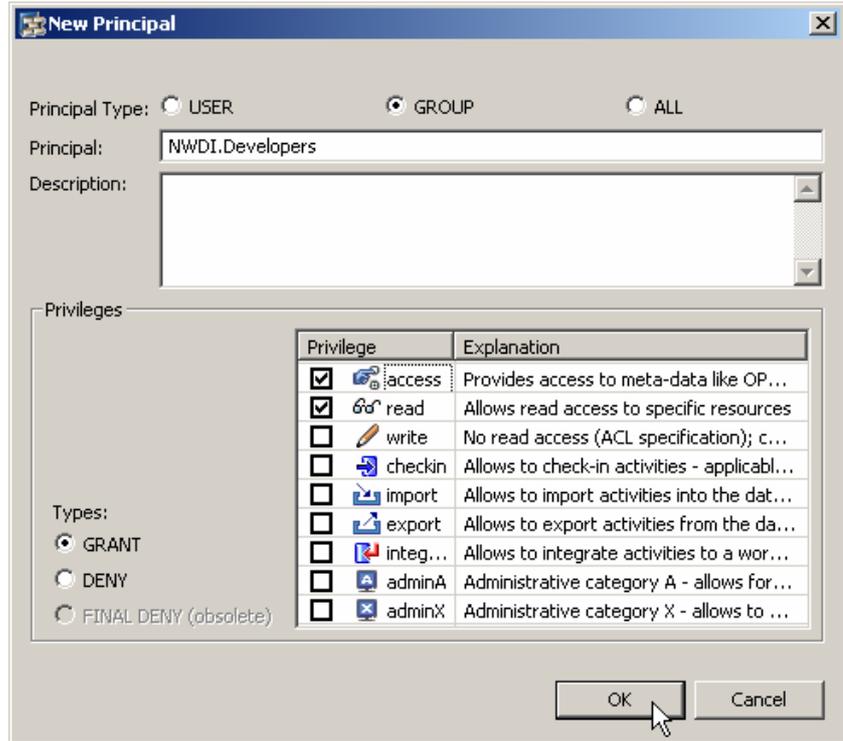
Enter the URL of the resource you want to edit, e.g. `http://<dtrhost>:<port>/dtr` for root.



12. Grant permissions to a resource

To edit permissions of an existing principal, right-click on the principal and choose “Edit principal”. For a new principal, choose “Add principal”.

Type in the desired principal (group or user name) and choose the necessary type. Then select the privileges and the privilege type.

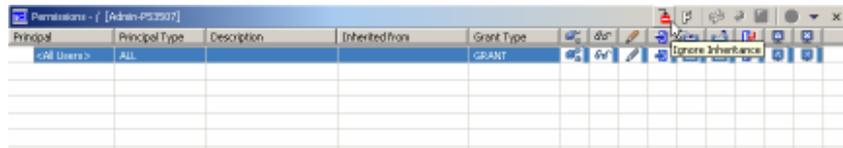


Press OK to confirm the principal.

13. Setting the “Ignore inheritance” flag

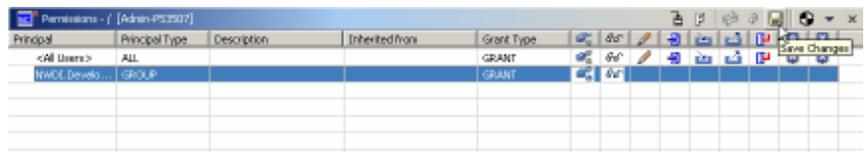
For some resources you should break the inheritance by setting the “Ignore inheritance” flag.

Use the “Ignore inheritance” button in the top bar of the permissions view to set this flag for the selected resource.



14. Save the settings for the folder

When you are finished with all configuration steps for this resource, save the entries by pressing the “Save Changes” button on the top bar of the permissions view.

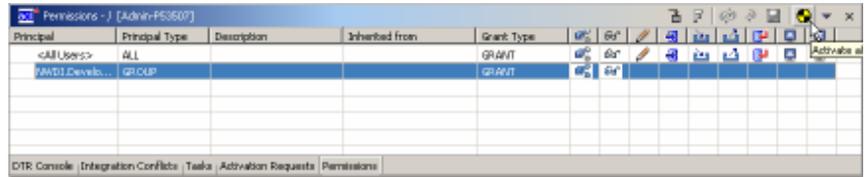


15. Repeat steps 11 to 14 for all resources

Repeat the steps for all resources you want to set permissions to.

16. Activate your changes

When you are finished with your configuration steps, activate the settings in the DTR. You do this via pressing the Activation button in the top bar of the permissions view.



It might take a few minutes until the changes take effect. Alternatively you can open a browser window using the URL <http://<DTR server>:<port>/dtr/sysconfig/support/AclRefresh> and choose "Refresh".

<http://service.sap.com/nw2004s-howtoguides>