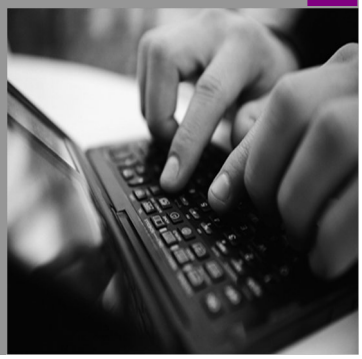
How-to Guide
SAP NetWeaver 2004



How To…
Configure Permissions for Initial Content in SAP NetWeaver Portal

Version 4.00 – February, 2013

Applicable Releases:
SAP NetWeaver 2004
(SAP NetWeaver Portal SPS 9 and higher)

Contents

Document History

Document version	Description
V 1.00	First official release of document
V 2.00	Additional permission for system administrator Addition of system administrator permissions to security zones Addition of Applications folder to section on setting portal permissions
Version 3.00	Addition of list permission documentation to appendix
Version 4.00	Content corrections

1. Introduction

SAP ships initial content for business users and administrators with the SAP NetWeaver Portal. Upon installation, the portal assigns a set of default permissions to this content to prevent unauthorized access. In EP 6.0 SP9 and higher, the initial permissions are set in a manner that authorizes “full” access for the entire portal and its initial content to the Super Admin role only.

The remaining preconfigured administration and business user roles shipped with the portal are permitted access to the out-of-the-box tools and user interfaces relevant to each role; however, access to objects within these tools is not permitted. For example, the content administrator has access to the Portal Content Studio, but the Portal Catalog is empty—the content administrator has no access to any iViews, pages, worksets, roles, or business package objects.

This guide provides recommendations and guidelines for configuring *initial permissions* to enable the preconfigured portal roles to access *initial content objects* that are relevant to each role. This guide focuses on two main areas in the portal:

- Security zones
- Portal content

The permission settings documented in this guide are intended as a set of guidelines. You need to make sure that the settings are relevant to your system landscape and configuration, and then make the necessary adjustments.

1.1 Who Can Use this Guide

Pay attention to the following to determine if the permission settings documented in this guide apply to your portal version:

- This guide is valid for all SAP NetWeaver Portal 6.0 support package versions that are based on a fresh installation of NetWeaver ’04 SR1. In NetWeaver ’04 SR1, you install EP 6.0 SP9 as the install base for the portal.

  Alternatively, you can install EP 6.0 SP9 as an upgrade from previous NetWeaver ’04 portal versions; however the EP 6.0 SP9 upgrade version is not completely supported by this guide. In this case, you may use this guide in the following manner: (i) read section *Setting Permissions to Security Zones* on page 4, and implement the changes as recommended for initial content supplied by SAP; and (ii) read section *Setting Permissions to Portal Content* on page 7, compare the settings to your content structure, and then determine for yourself which recommendations you want to apply.
- This guide is also valid for customers who are migrating from EP 5.0 SP6 or EP 6.0 SP2 to NetWeaver ’04; these migration paths both require EP 6.0 SP9 as the NetWeaver ’04 install base on the target portal.
  - **For customers migrating from EP 6.0 SP2 to NetWeaver ‘04:**

    A similar guide, but specific to EP 6.0 SP2 initial permissions, is available at http://www.sdn.sap.com/irj/scn/go/portal/prtroot/docs/library/uuid/6403e790-0201-0010-8ba2-eb0a9a30b681?QuickLink=index&overridelayout=true&5003637717394

    It is recommended you implement the recommendations described in the SP2 permissions guide as part of the migration process. If you do so, you do not need the SP9 permissions guide you are currently reading. If you have not implemented the recommendations in the SP2 permission guide, you should use the SP9 guide instead. The resulting permission configuration after using both guides is identical. Before applying the changes in this guide, make sure you first read the EP 6.0 SP2 migration guide located at http://sdn.sap.com/irj/sdn/howtoguides *SAP NetWeaver 2004 → Portal → How to Migrate from SAP Enterprise Portal 6.0 SP2 to SAP NetWeaver 2004*
  - **For customers migrating from EP 5.0 SP6 to NetWeaver ‘04:**

    Before applying the changes in this guide, make sure you first read the EP 5.0 migration guide located at http://sdn.sap.com/irj/sdn/howtoguides *SAP NetWeaver 2004 → Portal → How to Migrate from SAP Enterprise Portal 5.0 SP6 to SAP NetWeaver 2004*. The migration guide describes necessary pre- and post-migration permissions settings you need to configure on the EP 6.0 target machine. Once you have completed the migration process, you may apply the permission settings described in this guide.

- If you have modified or restructured the initial content shipped with the portal you should first compare your content to the guidelines specified in this guide, and determine for yourself which permissions need to be applied, adjusted, and rejected.
- For content that is either custom-made or supplied by SAP as supplementary content, you may use this guide only as basis for determining which permissions to assign. Then, you can assign the permissions to your own content after making the necessary adjustments.

   Note

  Permission settings in this guide for KM and Collaboration apply only if the portal installation is of usage type EP.

1.2 Prerequisites for Using this Guide

- Super Admin access to the portal.
- An in-depth understanding of the portal permission concepts (the following Concepts section specifies where you can find existing reference documentation).
- A fresh installation of EP 6.0 SP9 (or a higher support package version installed on top of NetWeaver '04 SR1). For more detailed information, see the previous section *Who Can Use this Guide*.

1.3 Concepts

For detailed documentation about the concepts used in this guide, read the "Portal Permissions" section in the portal administration documentation for SAP NetWeaver. There, you will find information about the permission inheritance model, using the Permission Editor, permission levels, security zones, and the initial permission settings shipped with the portal. Access the portal permissions documentation with the following link:

http://help.sap.com/saphelp_nw04/helpdata/en/f6/2604f005fd11d7b84200047582c9f7/frameset.htm

or navigate to *SAP Library* → *SAP NetWeaver* → *SAP NetWeaver Platform* → *SAP NetWeaver 2004* → *Application Help* → *People Integration* → *Portal* → *Administration Guide* → *System Administration* → *Permissions, Role/User Distribution, and Object Locking* → *Portal Permissions*.

1.4 Conventions Used in this Guide

The following conventions are used in this guide:

- Permissions are presented as:
  <admin permission setting>/<end-user permission setting [EU-on:EU-off]>/<[RAssigner-on:RAssigner-off]>
    - **'Administrator' permission setting:** To define this setting, choose the appropriate option in the *Administrator* drop-down list in the Permission Editor (see Figure 1).
    - **'End user' permission setting:** To define this setting, toggle the *End User* checkbox in the Permission Editor (see Figure 1). For *EU-on,* you select the checkbox, and for *EU-off,* you deselect the checkbox.
    - **'Role assigner' permission setting:** To define this setting, toggle the *Role Assigner* checkbox in the Permission Editor (see Figure 1). For *RAssigner-on,* you select the checkbox, and for *RAssigner-off,* you deselect the checkbox.

    Note that this permission setting is only available to roles and folders. If not specified, assign the value *RAssigner-off*.

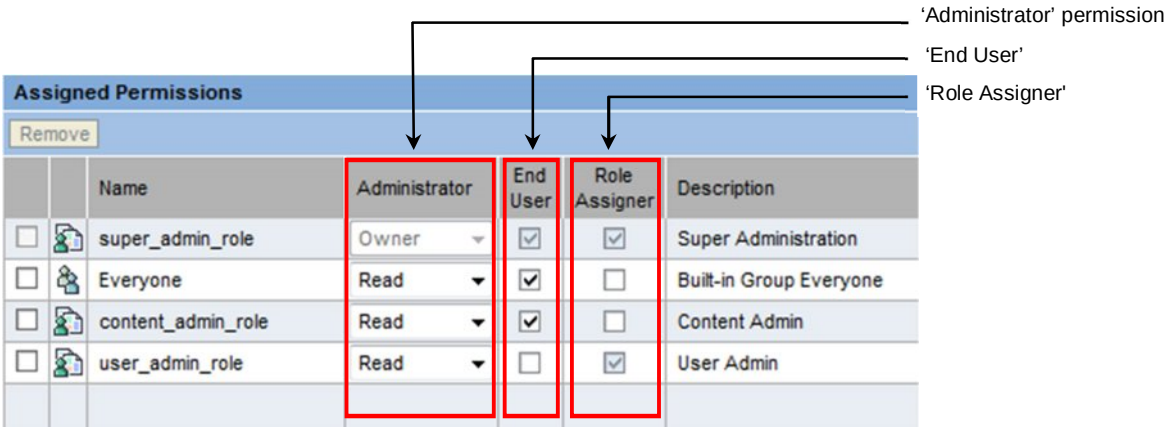


Figure 1: Permission Editor

- If a folder or object requires a number of permissions, they are provided in a list, as in the example below.
    - Folder: `Portal Content`
        - Role: **Super Admin** [Owner/EU-on/RAssigner-on]
        - Group: **Authenticated Users** [None/EU-on/RAssigner-off]
        - Role: **Content Admin** [Full Control/EU-off/RAssigner-off]

  This example specifies that you must assign the following permissions to the `Portal Content` folder:
    - Assign the *Super Admin* role with *Owner* administrator permission, enable the end-user permission, and enable the role assigner permission.
    - Assign the *Authenticated Users* group with *None* administrator permission, enable the end-user permission, and disable the role assigner permission.
    - Assign the *Content Admin* role with *Full Control* administrator permission, disable the end-user permission, and disable the role assigner permission.

2. Setting Permissions to Security Zones

Portal components and services shipped with the portal are assigned to security zones in their *portalapp.xml* file before being deployed. Upon deployment, the security zones are created in the portal with the respective components and services. The system administrator is then responsible for making the necessary adjustments, using the Permissions Editor, to verify that the appropriate roles, groups, or users are assigned to the correct security zones.

To view a security zone in the Portal Catalog, a portal administrator must have at least *Read* administrator permission assigned to that security zone. To modify permissions, an administrator requires *Owner* administrator permission in the appropriate security zones.

By default, the Super Admin role has *Owner* administrator permission to every security zone. The permission settings for the Super Admin role cannot be modified.

Prerequisites

- You have completed all installation and post-installation tasks for the Portal and KMC (Knowledge Management and Collaboration).
- The Portal Runtime (PRT) *portal.runtime.security.mode* property is set to **`production`** mode. This is required for any portal environment in which you want to implement the functionality provided by security zones.

Procedure

This section describes the recommended permissions for initial portal content in the `Security Zones` folder (in the Portal Catalog, which is accessed from the Permission Editor). Note that most of the recommended settings will already be defined in your portal after a fresh installation. If an initial permission setting is not recommended in this guide, you should remove it from the portal.

> **Important**
>
> The settings provided in this guide only cover the standard administration roles (super, content, system, user administrator) shipped with the initial portal content. As you create new custom roles or modify the preconfigured roles, you need to adjust the permission assignments to the security zones.

Component	Path in Portal Catalog	Permission Settings
`Security Zones` (root folder)	`/Security Zones`	• Role: **Super Admin** [Owner/EU-on] • Role: **System Admin** [Owner /EU-on]
Portal	`/Security Zones/sap.com/NetWeaver.Portal/no_safety`	• Role: **Super Admin** [Owner/EU-on] • Group: **Everyone** [None/EU-on] • Role: **System Admin** [Owner /EU-on]
	`/Security Zones/sap.com/NetWeaver.Portal/low_safety`	• Role: **Super Admin** [Owner/EU-on] • Group: **Authenticated Users** [None/EU-on] • Role: **System Admin** [Owner /EU-on]
	`/Security Zones/sap.com/NetWeaver.Portal/medium_safety`	• Role: **Super Admin** [Owner/EU-on] • Role: **Content Admin** [None/EU-on] • Role: **System Admin** [Owner/EU-on]
	`/Security Zones/sap.com/NetWeaver.Portal/high_safety`	• Role: **Super Admin** [Owner/EU-on] • Role: **System Admin** [Owner/EU-on]

UME	/Security Zones/sap.com/NetWeaver.UserManagement/no_safety	• Role: **Super Admin** [Owner/EU-on] • Group: **Everyone** [None/EU-on] • Role: **System Admin** [Owner/EU-on]
	/Security Zones/sap.com/NetWeaver.UserManagement/low_safety	• Role: **Super Admin** [Owner/EU-on] • Group: **Authenticated Users** [None/EU-on] • Role: **System Admin** [Owner/EU-on]
	/Security Zones/sap.com/NetWeaver.UserManagement/high_safety	• Role: **Super Admin** [Owner/EU-on] • Role: **User Admin** [None/EU-on] • Role: **System Admin** [Owner/EU-on]
EP50 [1]	/Security Zones/com.sap.portal.ep50	• Role: **Super Admin** [Owner/EU-on] • Group: **Everyone** [None/EU-on] • Role: **System Admin** [Owner/EU-on]
KM [2]	/Security Zones/sap.com/NetWeaver.KMC/low_safety	• Role: **Super Admin** [Owner/EU-on] • Group: **Everyone** [None/EU-on] • Role: **System Admin** [Owner/EU-on]
	/Security Zones/sap.com/NetWeaver.KMC/medium_safety	• Role: **Super Admin** [Owner/EU-on] • Role: **System Admin** [Owner/EU-on] • Role: **Content Admin** [None/EU-on] • Role: **KM Content Manager** [3] [None/EU-on]
	/Security Zones/sap.com/NetWeaver.KMC/high_safety	• Role: **Super Admin** [Owner/EU-on] • Role: **System Admin** [Owner/EU-on] • Role: **Content Admin** [None/EU-on]
	/Security Zones/sap.com/NetWeaver.KMC	• Role: **Super Admin** [Owner/EU-on] • Role: **System Admin** [Owner/EU-on] • Role: **Content Admin** [None/EU-on]
BI	Running the Configuration Wizard for BI-Java automatically configures permissions for BI content. (This is a post-installation task.)	

[1] Only required if you run Enterprise Portal 5.0 content in the portal.

[2] Only required if Knowledge Management (KM) is installed in the portal.

pcd:portal_content/specialist/contentmanager/ContentManager.

2.1 Long-Term Maintenance of Security Zone Permissions

After you have correctly set the initial permissions to the various security zones, as described in the previous section, the portal should be secure from any unauthorized access by direct URL.

> **Important**
>
> The settings provided in this guide only cover the standard administration roles (super, content, system, user administrator) shipped with the initial portal content. As you create new custom roles or modify the preconfigured roles, you need to adjust the permission assignments to the security zones.

If a user is denied access to a portal component due to lack of security-zone authorization, he or she will typically receive the following error notification at runtime in the portal:

Figure 2: Runtime error message indicating lack of permissions to a security zone

The name of the portal component and the relevant security zone are both listed in the error notification. If you determine that the user indeed requires permanent access to the respective portal component, assign the user access to the appropriate security zone (by role, group, or user name).

3. Setting Permissions to Portal Content

Once you have made the recommended changes to the security zone permissions, you need to reconfigure the permissions to the content stored in the Portal Content Directory (PCD). This content includes objects used by the portal, such as iViews, pages, worksets, roles, and more.

Permissions assigned to content objects also enable you to determine which templates and PAR files are available to users in the portal's content creation wizards.

By default, the Super Admin role has *Owner* administrator permission to the entire collection of content that resides in the portal. The Super Admin permission settings cannot be modified.

Prerequisites

As described in the *Prerequisites* section for security zones, you have completed all post-installation tasks.

Procedure

This section describes the recommended permissions for initial portal content in the default content folders within the Portal Catalog (using the Permission Editor). Note that most of the recommend settings will already be defined in your portal after a fresh installation. If an initial permission setting is not recommended in this guide, you should remove it from the portal.

> **Important**
>
> This guide is relevant for initial portal, KM, and Collaboration content shipped with the portal. For business packages and customer-developed content, you need to configure their permissions accordingly so that the content is available to the relevant roles, groups, and users in your organization.

The permission settings recommended in this guide adhere to the standard delegated administration concept provided with the portal. To accomplish this, the Content Admin role is assigned <*Full Control/EU-on*> permission and the System Admin role is assigned <O*wner/EU-on*> permission. This enables content administrators (in the Content Admin role) to have read/write/delete control over the entire portal content, so that they can add new content and modify existing SAP content. System administrators (in the System Admin role) are able to create, edit, copy, and delete object content, as well as modify the permissions.

In deeper Portal Catalog folders, you will remove permissions for either or both of these roles where necessary in order to separate the unique tasks of these two administration roles. One consequence of this change is that while the Content Admin role can create folders in the Portal Catalog, content administrators are unable to modify permissions in the Portal Catalog. A super administrator (in the Super Admin role) must change the folder permissions to <*Owner/EU-on*> for the Content Admin role in order to allow the content administrators to modify permissions to their content.

> **Tip**
>
> Remember that Portal Catalog folders inherit the permissions of their parent folders. If the permissions of a folder are modified in any way, the folder will cease to inherit the permissions of its parent folder. You can use the "restore inheritance" button in the Permission Editor to restore inheritance between folders.

The recommended permissions should be set as follows:

1. Set permissions to the root `Portal Content` folder.
    - Folder: `Portal Content`
        - Role: **Super Admin** [Owner/EU-on]
        - Role: **Content Admin** [Full Control/EU-on]
        - Role: **System Admin** [Owner/EU-on]
        - Group: **Everyone** [Read/EU-on]

2. Set permissions to subfolders under `Portal Content`.

   In the Portal Catalog, expand the `Portal Content` folder. Edit the permissions of each top-level folder under it.

   - Role: **Super Admin** [Owner/EU-on]
   - Role: **Content Admin** [Full Control/EU-on]
   - Role: **System Admin** [Owner/EU-on]

   Remove the *Everyone* group from each subfolder. This hides the folders from the *Page Personalization* user interface.

   Exceptions:

   - If you are running EP 5.0 content, you must not remove the *Everyone* group from the folder: `pcd:portal_content/com.sap.portal.migrated` (Migrated Content).
   - Any folder that contains content that should be available to users at runtime must have the relevant role, group or user (such as the *Everyone* or *Authenticated Users* group) assigned to it with <*None/EU-on*> permission. None of the folders delivered with the initial portal content, except for the `Standard Portal Users` folder, fall into this category (see next sub-section).

3. Set permissions to subfolders under `Content Provided by SAP`.

   In the Portal Catalog, expand `Content Provided by SAP` folder. In the following subfolders, you must reassign the *EU-on* permission to enable runtime activities for administrators using the tools.

   - Folder: `/Portal Content/Content Provided by SAP/Admin Interfaces`
     - Role: **Super Admin** [Owner/EU-on]
     - Role: **Content Admin** [Full Control/EU-on]
     - Role: **System Admin** [Owner/EU-on]
     - Role: **User Admin** [Read/EU-on]

4. Set permissions to the `Standard Portal Users` folder.

   In the Portal Catalog, expand the `Portal Users` folder and then reassign the *Everyone* group back to the `Standard Portal Users` subfolder.

   - Folder: `/Portal Content/Portal Users/Standard Portal Users`
     - Role: **Super Admin** [Owner/EU-on]
     - Role: **Content Admin** [Full Control/EU-on]
     - Role: **System Admin** [Owner/EU-on]
     - Group: **Everyone** [None/EU-on]

   This set of permissions is important for enabling certain core portal components to run in the end-user environment.

5. Set permissions to `Applications` folder.

   The Applications folder contains PAR files. If you want to expose any PAR files (and their portal components) to the *New from PAR* content creation wizard in the portal, then you must add *Read* administrator permission to the `Applications` folder.

   - Folder: `pcd:com.sap.portals.system/applications`
     - Role: **Super Admin** [Owner/EU-on]
     - Role: **Content Admin** [Read/EU-on]
     - Role: **System Admin** [Owner/EU-on]

If you want to hide certain PAR files from the content creation wizard in the portal, modify the permission of each PAR file individually.

6. Set permissions to EP 5.0 content.

   This section is only relevant if you intend to run EP 5.0 content in your EP 6.0 portal. You reassign the System Admin role and the Content Admin role so that content migration performed by these administrators is possible.

   In the Portal Catalog, expand the `/Portal Content/Migrated Content/EP 5.0` folder and set the permissions in the relevant subfolders.

   - Subfolders: `iViews, Systems`
     - Role: **Super Admin** [Owner/EU-on]
     - Role: **Content Admin** [Full Control/EU-on]
     - Role: **System Admin** [Owner/EU-on]
     - Group: **Everyone** [Read/EU-on]
   - Subfolders: `Pages, Services , Roles, Templates, Worksets`
     - Role: **Super Admin** [Owner/EU-on]
     - Role: **Content Admin** [Full Control/EU-on]
     - Role: **System Admin** [Owner/EU-on]
     - Group: **Everyone** [Read/EU-off]

7. Set permissions to KM content.

   This section is only relevant if you installed KM in your portal. The permissions enable the KM content managers to launch their iViews.

   - Folder: `/Portal Content/Content Provided by SAP/Content For Specialists/com.sap.km.ContentManager`
     - Role: **Super Admin** [Owner/EU-on]
     - Role: **KM Content Manager** [None/EU-on]
     - Role: **System Admin** [Owner/EU-on]

8. Set permissions to Collaboration content.

   This section is only relevant if you installed Collaboration in your portal.

   - Folder: `/Portal Content/Content Provided by SAP/Collaboration`
     - Role: **Super Admin** [Owner/EU-on]
     - Role: **Content Admin** [Full Control/EU-on]
     - Role: **System Admin** [Owner/EU-on]
     - Group: **Everyone** [None/EU-on]

   If you have integrated Collaboration Rooms into your portal, do the following as well:

   - Folder: `/Portal Content/com.sap.ip.collaboration`
     - Group: **Everyone** [None/EU-on]

     Note

     - The `Rooms` subfolder should inherit this permission also. This permission setting is necessary for enabling users to navigate within Collaboration-based rooms and view their content at runtime.
     - If the rooms are available to authenticated portal users only, you can add the **Authenticated Users** group with *EU-on* permission instead.

- Folder: /`Portal Content/Content Provided by SAP/Admin Content/Collaboration_Administrators`
  - Role: **Super Admin** [Owner/EU-on]
  - Role: **Content Admin** [None/EU-on]
  - Role: **System Admin** [Owner/EU-on]

Running the Configuration Wizard for BI-Java automatically configures permissions for BI content. (This is a post-installation task.)

3.1 Long-Term Maintenance of Portal Content Permissions

As noted previously, the permission settings recommended in this guide are valid only for a new EP 6.0 SP9 or higher installation. The permission settings are appropriate for content, system, and user administrators using the SAP administration roles supplied with the portal. When you create custom objects, you may need to adjust their permission settings appropriately. For example, if new roles are created to distribute and refine the capabilities of content creators, you will need to make changes to the Portal Catalog permissions.

Here are some points to take into consideration when designing new content and administration roles:

1. The permissions of a new object are inherited from its parent object or folder. For example, if you create a subfolder under the `Portal Content` folder, this new folder will allow any portal user in the *Everyone* group to see the objects contained in it (because of its *[Read/EU-on]* permission), content administrators (in the Content Admin role) will have full control (because of its *[Full Control/EU-on]* permission), and system administrators (in the System Admin role) will have *Owner* administrator permission (because of its *[Owner/EU-on]* permission).

   Folders are not the only objects that serve as container-type objects. For example, portal pages pass their permissions to the iViews contained in them. Worksets and roles also pass their permissions to the pages and iViews contained in them.
2. When you assign a user or group to a role, that user or group is automatically given access to the role and its content, regardless of the role's existing permissions. However, if some of the components in the role (such as a page or workset) call an iView outside the role hierarchy, a permission denial error will result if the user does not have *EU-on* permission to the external iView.
3. If an iView requires a system (defined in the System Landscape Editor) to access the relevant back-end application, you (or the system administrator) need to assign *EU-on* permission to the relevant users/groups/roles on the system. If not, the iView will be unable to retrieve data at runtime from the system to which the iView is pointing.

4. Appendix

Although not necessary for providing information about configuring permissions to portal initial content, the following subsections do provide information that is useful when working with portal permissions in general.

4.1 Viewing the ACL Structure in Your Portal

The Permission Editor in the portal allows you to view permissions for only a single object at a time. The portal offers an external feature that allows you to view the permission structure for many objects at a time. The output is a printable HTML form displayed in your Internet browser.

This feature is useful for viewing the overall ACL (access control list) structure in your portal and also for troubleshooting permission assignments.

The permission structure page enables you to update the automatically assigned permissions for desktops, themes, and roles, in the event that they are incorrect. (These permissions are not assigned, or visible, in the Permission Editor; they are referred to as inner ACLs.)

The HTML output page displays the following four tables:

- PCD permissions

  Shows the permissions of all PCD objects and folders that are assigned explicit permissions, not objects that inherit permissions.
- Internal permissions for desktops (com.sapportals.portal.desktop)

  Shows the inner ACLs of portal desktops.
- Internal permissions for themes (com.sapportals.portal.style)

  Shows the inner ACLs of portal themes.
- Internal permissions for roles (com.sapportals.portal.role)

  Shows the inner ACLs of portal roles.

   Note

  The output of the ACL structure is filtered according to the permission settings of the user requesting the ACL structure. The user must have at least administrator *read* permission for each object in the Portal Catalog he or she wants to view. Therefore, to view the entire ACL structure in your portal, the user requesting the ACL structure must be a super administrator or an administrator who has permission to view the entire Portal Catalog.

4.2 Updating Inner ACLs

The ability to update the *inner ACLs* of desktops, themes, and roles is a useful first step in troubleshooting in the event of runtime problems, for example:

- A role is invisible to a user who is assigned to it
- A theme appears corrupt at runtime
- The desktop is invisible to the user upon logon

These situations may occur due to missing *inner ACLs*. In this event, a button appears at the bottom of the permission structure page, *Update Inner ACL Permissions*. If you see this button, click it to update the *inner ACLs*.

Prerequisites

- At least administrator *read* permission for each object in the Portal Catalog that you want to view.
- *End-user* permission to the security zone of the following portal component:

  ```
  sap.com/NetWeaver.Portal/medium_safety/com.sap.portal.admin.acleditor/components/listPermissions
  ```

Procedure

1. Log on to the portal.
2. In the same browser session, open a new browser window.
3. Enter the following URL:

```
http://<host>:<port>/irj/servlet/prt/portal/prtroot/com.sap.portal.admin.acleditor.listPermissions
```

> **Note**
>
> Depending on the amount of data to be processed, it may take several minutes for the ACL structure to appear on the screen.

Result

The output of the ACL structure is a printable HTML form displayed in your Internet browser. The data is tabulated and displays the PCD path, permitted user/group/role, and the assigned permission setting for each item.

> **Note**
>
> In the column displaying the permission setting for each user/group/role, the *administrator* permission setting is specified first. If a user has *end-user* permission, "`(End User)`" is displayed after the *administrator* permission. If "`(End User)`" is not displayed, the user does not have *end-user* permission.

4.3 Transporting Permissions

The portal provides a standalone tool that enables you to transport content permissions from one portal to another.

When you export permissions, an XML file containing the source portal ACL structure is created. The XML contains all permissions defined in the portal, including portal content and security zones. The XML file can then be imported into any number of suitable portal installations in order to transfer the permissions.

4.4 Terminology

In this section, we use the following terms:

- **Source system:** the portal installation from which you are exporting permissions.
- **Target system:** the portal installation to which you will be importing permissions.

4.5 Workflow

The process for transporting permissions involves the following:

1. Exporting the ACL structure from a source system to an XML file. See *Exporting Permissions* on page 12.
2. Uploading the XML file to a target system. See *Importing Permissions* on page 15.

4.6 Exporting Permissions

The output of the ACL structure is filtered according to the permission settings of the user requesting the ACL structure form. Therefore, to view the entire ACL structure in your portal, the user requesting the ACL structure form must be a super administrator or an administrator who has permission to view the entire Portal Catalog.

> **Note**
>
> If you transport portal content using the Transport Package Editor, you can include permissions with the content selected for export by editing the property values of the package.

Prerequisites

- At least administrator *read* permission for each object in the Portal Catalog you want to export.
- *End-user permission* to the security zone of the following portal component:

  ```
  sap.com/NetWeaver.Portal/medium_safety/com.sap.portal.admin.acleditor/components/initialPermissionsCreator
  ```

Procedure

1. Log on to the portal.
2. In the same browser session, open a new browser window.
3. Enter the following URL:

   `http://<host>:<port>/irj/servlet/prt/portal/prtroot/com.sap.portal.admin.acleditor.initialPermissionsCreator`

> **Note**
>
> Depending on the amount of data to be processed, it may take several minutes for the XML file to be created.

Result

When the permissions have been exported, an `initialPermissions.xml` file is created on the source system in the following folder:

- **Windows:**

  `<installation drive>:\usr\sap\<Java EE instance name>\JC<instance number>\j2ee\cluster\server<server number>\apps\sap.com\irj\servlet_jsp\irj\root\portalapps\com.sap.portal.admin.acleditor`
- **UNIX:**

  `/usr/sap/<Java EE instance name>/JC<instance number>/j2ee/cluster/server<server number>/apps/sap.com/irj/servlet_jsp/irj/root/portalapps/com.sap.portal.admin.acleditor`

The XML file contains all ACL objects existing in the source system. Each ACL tag element is represented in the following format:

```
<ACL objectID="ObjectID" handlerId="ACL">
  <ACEs>
   <ACE type="[role, user, group]"
        principalID="PrincipalID"
        permission="[owner, Pcd.FullControl, Pcd.ReadWrite, Pcd.Read, NONE]"
        endUserRead="[true, false]"
        roleAssign="[true, false]"
    />
  </ACEs>
</ACL>
```

Where:

- **<ACL>** tag (Access Control List): refers to a single object, and contains a single <ACEs> tag.
  - **objectID** attribute: Specifies the ID of the PCD object.
  - **handlerId** attribute: Specifies the Generic Creator handler that processes the data in the XML; do not change this value.
- **<ACEs>** tag: groups a number of <ACE> tags that are nested in a single <ACL> tag.
- **<ACE>** tag (Access Control Entry): specifies which users, groups, or roles are assigned permissions to the object and also their respective permission levels. Each <ACE> tag refers to a single role, user, or group.
  - **type** attribute: Specifies if the user management entity being assigned permission to the object is a role, group or user.
  - **principalID** attribute: Specifies the ID of the role, group, or user being assigned permissions to the object.
  - **permission** attribute: Specifies the *administrator* permission setting. If this <ACE> attribute is not specified, its default value is **NONE**.
  - **endUserRead** attribute: Specifies the *end-user permission* setting. If this <ACE> attribute is not specified, its default value is **false**.
  - **roleAssign** attribute: Specifies the *role assigner* permission setting. If this <ACE> attribute is not specified, its default value is **false**.

    Note

    In EP 6.0 SP9, the XML formulation of the ACL structure was modified, and therefore varies in comparison to EP 6.0 SP2.

A sample XML output declaring content and permissions looks as follows:

```
<ACL objectID="pcd:portal_content" handlerId="ACL">
  <ACEs>
   <ACE type="role"
          principalID="pcd:portal_content/administrator/content_admin/content_admin_role"
          permission="Pcd.FullControl"
          endUserRead="true" />
   <ACE type="group"
          principalID="GRUP.SUPER_GROUPS_DATASOURCE.EVERYONE"
          permission="Pcd.Read"
          endUserRead="true"
          roleAssign="true" />
   <ACE type="role"
   principalID="pcd:portal_content/administrator/super_admin/super_admin_role"
          permission="owner"
          endUserRead="true"
          roleAssign="true" />
   <ACE type="role"
          principalID="pcd:portal_content/administrator/system_admin/system_admin_role"
          permission="owner"
          endUserRead="true" />
  </ACEs>
</ACL>
```

4.7 Importing Permissions

The permissions of each object defined in the XML are only processed if the object already exists in the portal; otherwise they are ignored. The import mechanism behaves as follows:

- If the XML file defines object permissions, the current ACL structure settings in the portal are replaced.
- If the XML file has no defined permissions, the ACL structure settings in the portal remain the same.

Prerequisites

- An XML file containing the ACL structure exported from a source system exists.

   Important

  The XML file does not need to be named `initialPermissions.xml`. You may rename it to any name you want, but be sure to add the `.xml` extension.
- The target portal is populated with the correct content.
- The user base in the source system and in the target system is the same.

Procedure

1. Make sure that the target system is populated with the correct content.
2. If you are working in a cluster environment, do the following:
   a. Stop all the dialog instances and server nodes in the cluster. Do not stop the central instance.
   b. Make sure that there is only one dispatcher node and one server node running on the central instance of the J2EE Engine.
3. Copy the `initialPermissions.xml` file, which you generated on the source system, to the following folder on the target system:

- **Windows:**

  ```
  <installation drive>:\usr\sap\<SAP J2EE instance name>\JC<instance
  number>\j2ee\cluster\server<server
  number>\apps\sap.com\irj\servlet_jsp\irj\root\WEB-INF\portal\system\xml\acl
  ```
- **UNIX:**

  ```
  /usr/sap/<SAP J2EE instance name>/JC<instance
  number>/j2ee/cluster/server<server
  number>/apps/sap.com/irj/servlet_jsp/irj/root/WEB-INF/portal/system/xml/acl
  ```

   Important

  In a cluster environment, you only need to copy the XML file to the central instance. The remaining server nodes and dialog instances in the cluster are updated automatically.

4. Restart the J2EE Engine on the target system. Upon restart, the ACL configuration on the target system is updated according to the specifications in the XML file.

   In a cluster environment, restart the J2EE Engine in all the cluster nodes. During the restart, the J2EE engine synchronizes all J2EE engine cluster nodes and automatically sets up the XML script on each node.

   After the content of the script has been integrated into the target system, the XML file is given the `.bak`.suffix. For example: `initialPermissions.xml.bak`.