How to Use the Security Zones in NetWeaver '04 SPS09

Release 648

ADDON.EP_PCT_BP_MIGRATION

Copyright

Icons in Body Text

Icon	Meaning
	Caution
	Example
	Note
	Recommendation
	Syntax

Additional icons are used in SAP Library documentation to help you identify different types of information at a glance. For more information, see *Help on Help* → *General Information Classes and Information Classes for Business Information Warehouse* on the first page of any version of *SAP Library*.

Typographic Conventions

Type Style	Description
Example text	Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options. Cross-references to other documentation.
Example text	Emphasized words or phrases in body text, graphic titles, and table titles.
EXAMPLE TEXT	Technical names of system objects. These include report names, program names, transaction codes, table names, and key concepts of a programming language when they are surrounded by body text, for example, SELECT and INCLUDE.
`Example text`	Output on the screen. This includes file and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools.
Example text	Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.
<Example text>	Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.
`EXAMPLE TEXT`	Keys on the keyboard, for example, `F2` or `ENTER`.

How to Use the Security Zones in NetWeaver ’04 SPS09

Implementation Considerations

The security concept of security zones was introduced with SAP Enterprise Portal 6.0 SP2 and extended with the following functions for NetWeaver ’04 SPS09 and NetWeaver ’04 SR1:

- Permissions are now checked for every access to components and services through the security zone (until this was done only for direct access to components, but not for access to iViews).
- In the portal catalog, the security zone structures are automatically completed with the name of the portal application and the name of the component or service, based on *Vendor*, *SecurityArea*, and *SafetyLevel*.
- Security zones are created for each PAR file. If no security zones are defined in the PAR file, the system generates standard security zones in the portal catalog (known as undefined security zones).

  Security zones are only a part of the security concept that SAP provides. Nevertheless it is important to configure the security zones, because otherwise considerable problems can occur, for example, that users without permission use the URLs to access iViews containing confidential data.

Features

This how-to guide is divided into two sections and is aimed at the following audiences:

- Portal administrators who are upgrading from a release earlier than NetWeaver ’04 SPS09 or using content that the customer has developed to NetWeaver ’04 SPS09 or NetWeaver ’04 SR1.
- Developers who want to implement security zones in portal content to use the extended security zone concept in NetWeaver ’04 SPS09.

Requirements

- You can implement the security zones concept only if your business package contains PAR files (the security zones are physically stored in the PAR files).
- To understand this guide, you require basic knowledge about security zones. In the SAP Library, you can find the documentation on security zones at *SAP NetWeaver* → *People Integration* → *Portal* → *Administration Guide* → *System Administration* → *Permissions, Role/User Distribution, and Object Locking* → *Portal Permissions* → *Security Zones*.

How-To Guide for Administrators

Use

The target audience for this how-to guide is portal administrators who are upgrading from a release earlier than NetWeaver ’04 SPS09 or using content that the customer has developed to NetWeaver ’04 SPS09 or NetWeaver ’04 SR1.

Establishing the Type of the Existing Security Zone Structures

Check which security zone structures your content contains.

1. In the portal, choose *System Administration* → *Permissions* → *Portal Permissions*. The Permissions Editor appears.
2. In the portal catalog, choose the *Security Zones* area.
3. Check which security zone structures are contained in the business packages you are using.

   The following types are possible:

   - Security zone structures that were introduced with SAP Enterprise Portal 6.0 SP2 (EP6 SP2)

     You can recognize these structures by the fact that they start with *com.sap.*, whereas the structures from NetWeaver ’04 SPS9 start with *sap.com*.

     Example of a structure from EP6 SP2: com.sap.portal/high_safety

   - Security zone structures that were introduced with the extended concept in NetWeaver ’04 SPS09

     These structures are composed as follows:

     {Vendor}/{SecurityArea}/{SafetyLevel}/{PortalApplicationName}/components/{ComponentName} for components

     {Vendor}/{SecurityArea}/{SafetyLevel}/{PortalApplicationName}/services/{ServiceName}
     for services

     Example:
     sap.com/NetWeaver.Portal/high_safety/com.sap.portal.prt.cache/components/DBTest

   - Compatible structures

     These structures can contain any syntax separated by a slash (/); however, they are generally structured like the security zone structures in NetWeaver ’04 SPS09. Development creates these structures if a business package is intended not only for use on NetWeaver’04 SPS09, but also for one or more earlier releases.

   In rare cases, you may also find mixed structures in your business package.

   In SAP Note 786946, you can find a list of business package with details of the security zones that they contain.

Updating Security Zones

1. For each business package that you are using, use the following graphic to identify the starting point:

The system landscape is upgraded to NetWeaver ‘04 SPS09

→ NetWeaver’04 SPS09 contains the extended security zones concept

Business packages used to date	Are you planning to update the business package?	Case assignment
EP 6.0-based packages without security zones	Yes	See case 1
	No	See case 2
EP 6.0-based packages with security zones from releases earlier than NetWeaver’04 SPS09	Yes	See case 1
	No	See case 3
EP 5.0-based packages (“migrated content“)	Yes	See case 4
	No	See case 4

Graphic 1: Case differentiation for upgrading to automatically generated security zones in NetWeaver ’04 SPS09

For your own content, see case five.

2. Work through the steps necessary for your case.

Case 1: During the upgrade to NetWeaver ’04 SPS9, you import a business package support package.

- You have not used security zones to date (that is, no security zones were defined in the PAR files):

  If the security zones are defined according to the extended concept in the business package (BP) support package (or compatible structures have been created), you only have to assign access control lists (ACLs) in the portal catalog.

- You have already used security zones (that is, security zones were defined in the PAR files):

  If the business package contains new PAR files, you can find the security zone structure for NetWeaver ’04 SPS09 alongside the security zone structure for EP6 SP2 in the portal catalog.

  Assign ACLs to the structures for NetWeaver ’04 SPS09.

If you want to avoid having mixed structures in the portal catalog, you can convert the structures in the PAR files from EP6 SP2 to compatible structures.

Case 2: You are using content without security zones.

1. Import the business package again. Because no security zones are defined in the PAR files, undefined security zone structures appear in the portal catalog.

   Example:
   UndefinedVendorID/UndefinedSecurityArea/UndefinedSafetyLevel/UndefinedPortalApplicationName/components/UndefinedComponentName

2. Use the security zone browser to check which components and services are contained in the UndefinedSafetyLevel and decide which users or ACLs you want to assign permissions to.

3. In the portal catalog, assign ACLs to the security zones.

In undefined security zone structures, you cannot identify what content they are related to and which component they originate from. To use the extended security zone concept, SAP recommends importing a more recent support package that contains security zones in the PAR files.

Case 3: You are using content with security zones from EP6 SP2 and do not import a BP support package containing the structures for the extended security zone concept.

The security zone structure has changed in NetWeaver ’04 SPS09, but you can continue to use the security zones from EP6 SP2.

No activities are required.

Case 4: You are using content based on SAP Enterprise Portal 5.0 (EP 5.0).

To identify the type of content you are using, look for the following characteristics:

- EP5.0 business package (migrated) "50.x" -> *.pkg file
- EP5.0 business package (migrated) "60.1" -> *.pkg file
- EP6.0 business package "60.x" -> *.epa or *.sca file

During the upgrade to NetWeaver ‘04 with at least SPS09, the system generates default security zones, which appear as follows:
com.sap.portal.ep50

In the portal catalog, assign ACLs to the security zones.

SAP recommends assigning generous permissions for the ACLs for these security zones, because EP6.0 continues to support the *AuthRequirement* property from EP 5.0. This property is used additionally to check whether a user has access rights for a component.

Case 5: You have developed your own content.

- You have already used security zones (that is, security zones were defined in the PAR files):

  The security zone structure has changed in NetWeaver ’04 SPS09, but you can continue to use your existing security zone structures.

  No activities are required.

  When you import new content, you can find the security zone structures for NetWeaver ’04 SPS09 alongside the security zone structures for EP6 SP2 in the portal catalog.

  If you want to avoid having mixed structures in the portal catalog, you can convert the structures in the PAR files from EP6 SP2 to compatible structures.

- You have not used security zones:

  In the PAR files for your content, define security zones and then import the content again. In the portal catalog, assign ACLs to the security zones.

  For information about implementing security zones in the PAR files, see the how-to guide for developers.

In the standard system, the security zones function is always activated. Nevertheless, you can also activate an additional security check.

For more information about this, see the documentation at *SAP NetWeaver* → *People Integration* → *Portal* → *Administration Guide* → *System Administration* → *Permissions, Role/User Distribution, and Object Locking* → *Portal Permissions* → *Security Zones*, section *Controlling Portal Component Access through iViews*.

How-To Guide for Developers

Use

The target audience for this guide is developers who want to implement security zones in portal content.

Checking PAR Files for Security Zones

Check your PAR files for security zones. The following starting points are possible:

- No security zones have been stored in the PAR files to date.
- Security zones that conform to the structure used in SAP Enterprise Portal 6.0 SP2 have been stored in the PAR files.

  You can recognize these structures by the fact that they start with *com.sap.*, whereas the structures from NetWeaver ’04 SPS9 start with *sap.com*.

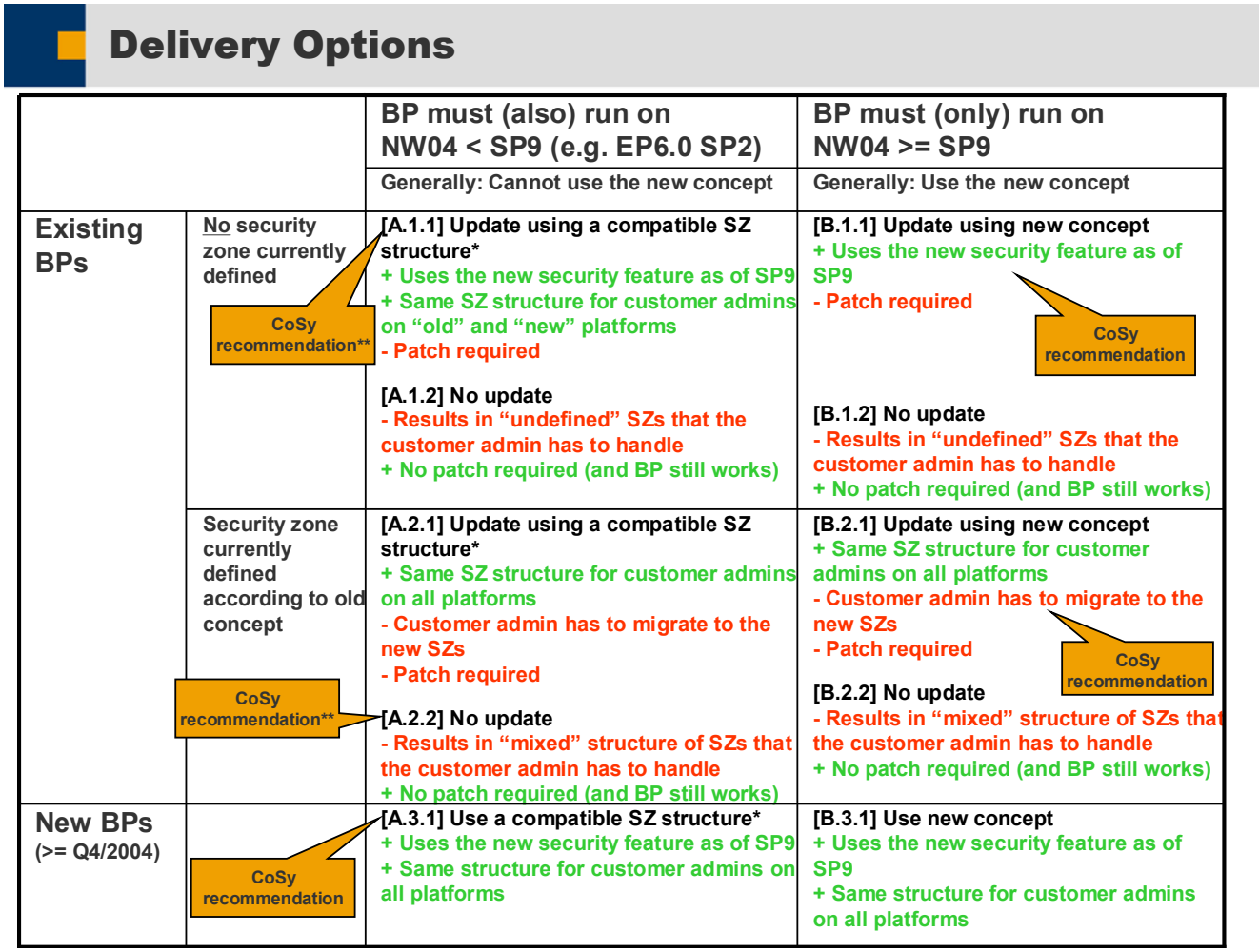
  Example of a structure from EP6 SP2: *com.sap.portal/high_safety*
- Some PAR files contain security zone structures, others do not.

Planning the Creation of Security Zones

In order to be able to implement security zones in portal content, you must have created security zone structures in all PAR files.

To use the extended security zone concept, you can create either the new structures as in NetWeaver ’04 SPS09 or compatible structures that ensure backwards compatibility.

The following graphic helps you to decide which structures you should create:



Graphic 2: Recommendations for which security zone structures you should store in the PAR file

**: Depends on the “mix” within the portal content

1. Use graphic two to decide whether you want to continue using existing security zone structures from EP6 SP2 or create new or compatible structures. In doing this, distinguish between the following:
   - Whether the content runs only on NetWeaver ’04 SPS09

     → In this case, create the structures based on the extended concept in NetWeaver ’04 SPS09.
   - Whether the content also runs on releases earlier than NetWeaver ’04 SPS09

→ In this case, create compatible structures.

The structures from EP6 SP2 also work with NetWeaver ’04 SPS09. Therefore, you can leave these structures unchanged. However, if you also create new structures, you should bear in mind that the portal content then contains a mixture of structures. To avoid this, you can convert the structures from EP6 SP2 to compatible structures.

Creating Security Zones

Create new structures according to the following examples:

1. Structures from NetWeaver ’04 SPS09:

   In the PAR file, create the *VendorID*, *Security Area*, and *Safety Level*. The *Portal Application Name* and *Component Name* or *Service Name* are generated automatically in the portal catalog.

   In the portal catalog, the structure then appears as follows:

   {Vendor}/{SecurityArea}/{SafetyLevel}/{PortalApplicationName}/

   components/{ComponentName} for components

   {Vendor}/{SecurityArea}/{SafetyLevel}/{PortalApplicationName}/

   services/{ServiceName} for services

   Example: sap.com/NetWeaver.Portal/high_safety/com.sap.portal.prt.cache/

   components/DBTest

2. Compatible structures

   These structures can contain any syntax separated by a slash (/). However, SAP recommends structuring them exactly like the security zone structures in NetWeaver ’04 SPS09 (see a), so that the structures have a uniform appearance.

   Because *Portal Application Name* and *Component Name* or *Service Name* are not generated automatically in releases earlier than NetWeaver ’04 SPS09, you should store these details in the PAR file as well if you want them to appear in the portal catalog.

   If you convert existing security zones structures in the PAR file and change the security level while doing this, the ACLs have to be reassigned later in the content catalog.