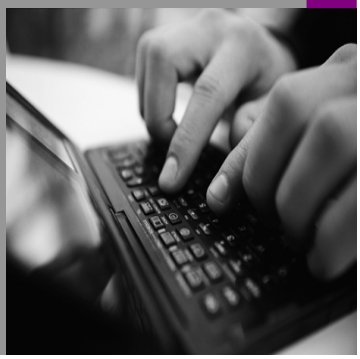
How-to Guide
SAP NetWeaver '04



How To... Set Up and Configure a Global Portal Environment with Syndicated Content

Version 1.20 – June 2005

Applicable Releases:
SAP NetWeaver '04
(SAP Enterprise Portal 6.0 SP2 and higher)

Contents

1 Overview

1.1 Purpose

The large business enterprises of today are global—serving employees, customers, and an IT infrastructure that is dispersed in numerous geographical locations worldwide. SAP offers an enterprise portal-based solution that is able to share, integrate and display multi-lingual information located in applications and persistence layers all over the world, so that portal clients at any geographical location can access this information. The solution enables live and direct access to global applications without the need to deploy replication and synchronization mechanisms for content repositories.

> **Important:**
>
> The solution is currently supported on a project-basis only. Customers must first contact their SAP representative to determine if their requirements can be met before implementing it.

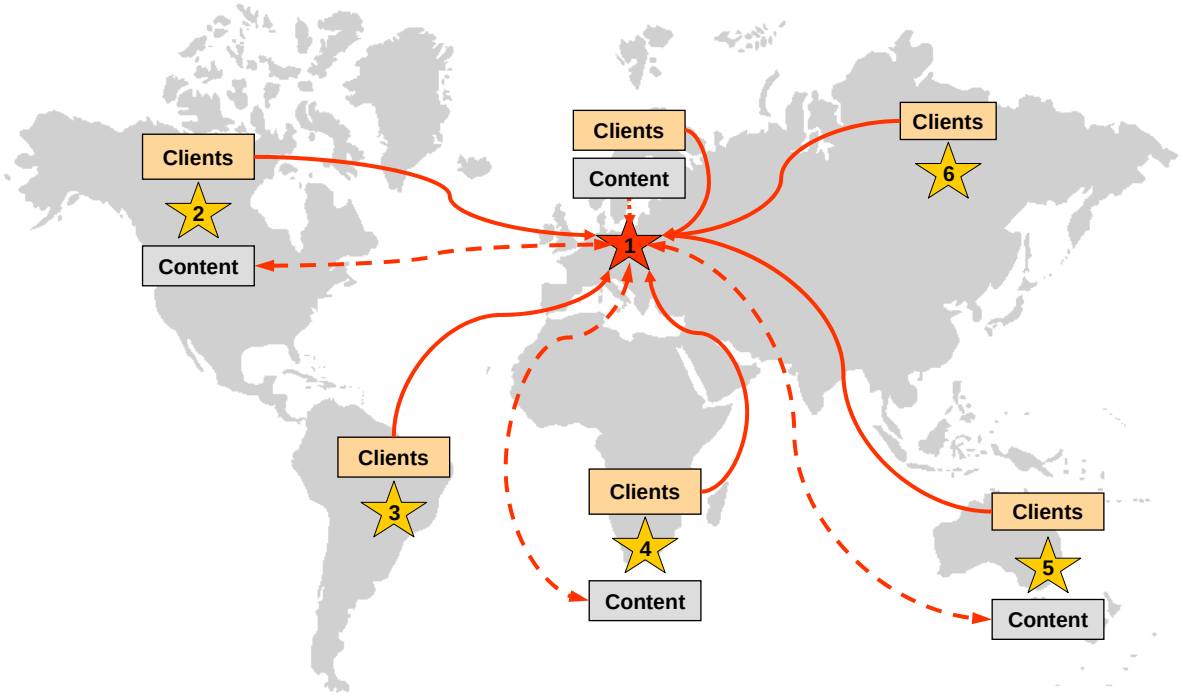
A global portal network reduces total cost of ownership (TCO) while increasing the autonomy of business units. Sharing content between sites when back-end systems are distributed worldwide improves overall performance, and decreases bandwidth usage.
SAP Enterprise Portal drives SAP's current global portal solution. The portal provides the framework, tools, and services for setting up a global portal network supporting "syndicated" content. This type of global network comprises a single centralized portal and any number of remote sites (remote content providers) spread worldwide. The main portal publishes its own local content, and also remote content originating from other sites within the network. This configuration enables the central portal to optimally retrieve up-to-date data from remote back-end systems, regardless of their geographical location, and offer it to any portal user worldwide.

> **Note:**
>
> The syndicated content solution is intended as preliminary step of a complete solution that will ultimately offer "federated" content sharing in a global portal network that comprises multiple autonomic portal installations distributed worldwide. The portals share content, users, and administration tasks in any direction, thereby functioning together as a single seamless portal network.

A global portal network is more than just sharing content; SAP Enterprise Portal includes other functionalities and technologies that further support global enterprises:

- Multi-language user interface support
- Delegated administration for setting up different administrator groups (for example: user, content, and system administrators) as well as a sub-administrator groups (for example: local and regional administrators)
- User-, group-, role- and company-specific branding
- Single sign-on to all back-end systems, including SAP and non-SAP systems
- Tools to guarantee high availability (such as clustering, backup and restore) and high performance (such as caching)
- Security

SAP's global portal solution is based on Web services and the Web Services for Remote Portals (WSRP) standard. SAP Enterprise Portal uses WSRP to exchange information between remote sites. WSRP enables content and applications to be shared in a manner that does not require manual adaptations to consuming applications. To further increase performance issues, third-party performance-enhancing software, such as caching managers and proxies, can be utilized. This document introduces the concepts behind SAP's current global portal solution of syndicated content, and describes in detail the requirements and procedures to implement it.



Example: Distribution of sites in a global portal network with syndicated content. Clients worldwide access the main portal (site 1) to log on to the portal. Content offered by the main portal is based on local applications and also remote applications originating from remote sites (sites 2, 4, and 5) worldwide.

1.2 Scenario Description

The Global Portal Network

From a content and application perspective, the global portal scenario enables portal end users to access information and conduct transactions with applications that are hosted in different geographical locations.

A global portal network in the current SAP solution consists of a central autonomous portal (referred to as the **main portal**) and any number of **remote content provider** sites located worldwide (see following figure). The main portal publishes and exposes its own content and data applications, as well as content from remote content providers. Typically, a remote content provider site collects and compiles iView data from back-end systems that are in close geographical proximity to it, and transfers fully rendered markup data (HTML, XML etc.) back to the main portal for delivery to end users at run time. Since the time consuming process of iView data rendition is performed at run time solely by a remote site and not the main portal, the global portal infrastructure improves overall performance and decreases bandwidth usage of the network between the main portal and the location of the remote back-end systems.

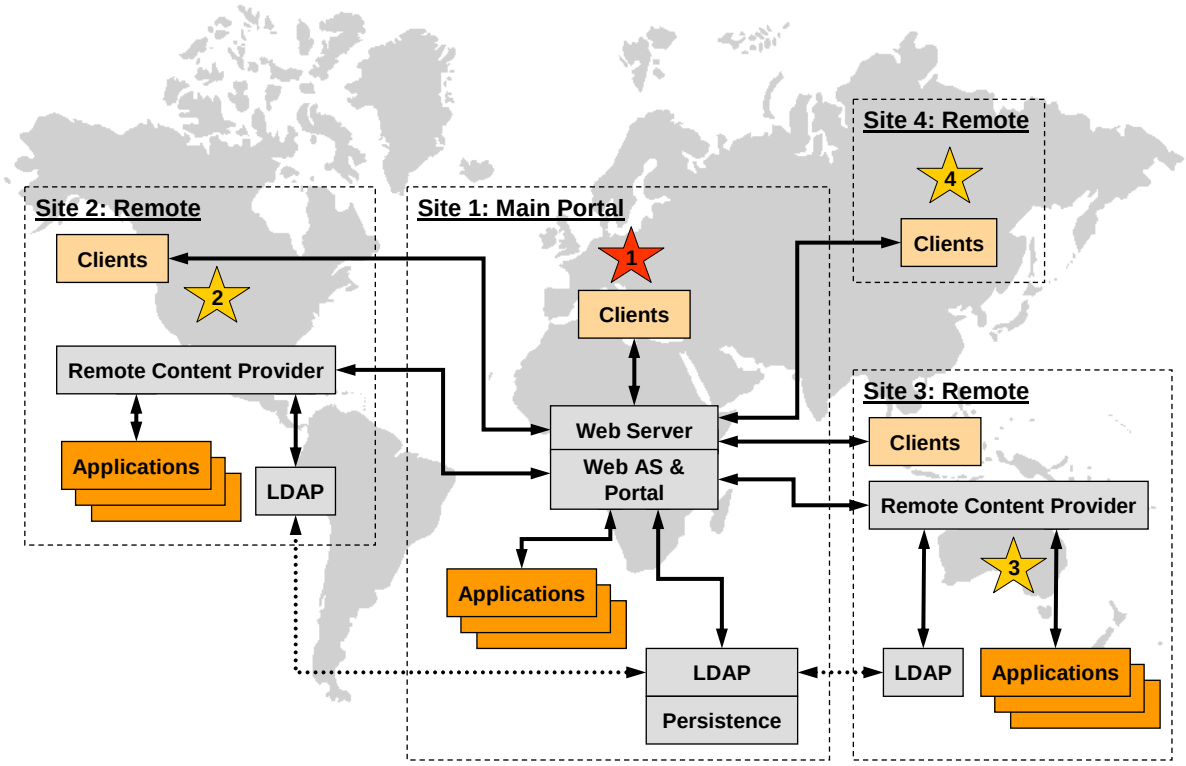
In the most basic scenario, the main portal site is a full SAP Enterprise Portal installation that serves as an access point for all portal users in the global network, regardless of their geographical location. The remote content provider sites are also SAP Enterprise Portal installations, but they do not run as functional portals; they merely exist to serve the main portal by sharing their content with it in a unidirectional manner. In this scenario, remote content provider sites do not interact with one another; they react only with the main portal. Typically, any remote back-end system or application that provides data for iViews on the main portal is physically located in close proximity to the remote content provider.

In the basic scenario described above, the main portal is the only single point of user access and a remote content provider only publishes content for the main portal. The basic scenario can however be extended to more complex ones, for example:

- Two or more main portals in the global portal network which share content from one or more remote content providers; in other words, a remote content provider can serve more than one main portal.
- Two or more portal which exist independently, but also serve as remote content providers for other main portals in the global portal network; in other words, each portal installation can have a dual purpose acting as both a main portal and a remote content provider.

> Note:
>
> This document assumes you are implementing the basic scenario. Nevertheless, the concepts and procedures described within apply to more complex scenarios. You may need to adjust them slightly, where needed.

Content sharing is performed at the level of the "iView" only. The main portal hosts proxy iViews (referred to as **proxy-to-remote iViews**), which dispatch requests (including execution, editing, and personalization) to the actual content-based iViews (commonly referred to as **remote iViews**) that reside on the remote content provider. Since iView sharing may limit the desire to share an application or a hierarchical structure – such as a workset, role, or business package – the portal provides a content conversion tool that can overcome this limitation.



Example: Site distribution for a global portal network offering a syndicated content scenario. The main portal (site 1) is based in Central Europe. It has its own local content and applications, but also consumes content produced by remote content provider sites located in North America (site 2) and Australia (site 3). The portal clients (end users) in this global enterprise are dispersed worldwide in Central Europe, North America, Australia, and Russia (site 4), but all use the main portal site as their central point of access. The local and syndicated content is available to all clients on a need-to-have basis, depending on access authorization and role assignment. In this scenario, the user store of the LDAP at site 1 is replicated to site 2 and 3.

User Management

The basic assumption is that the main portal and remote content providers share the same user persistence store. This is possible through the various scenarios, such as:

- using a single user directory (the directory to which the main portal and remote content providers are connected)

- using replications of the same user directory (installed on each site in the network)
- using multiple user directories exposed as single user base (through the use of third-party software)

Before content is shared, the system administrator must create trust between the main portal and remote content provider sites. Trust enables all users to be recognized on a remote content provider site through the main portal. Without trust, all users on the main portal would be recognized as anonymous users on the remote content provider sites; it would not be possible to define user mapping for remote systems nor would it be possible for content administrators to gain access to remote content in the iView Wizard.
End users can perform user mapping on the remote content provider from the main portal by using a dedicated remote user-mapping tool in the portal.

Global Portal Administration Tools and Services

Portal administrators generally administer the main portal and any remote content provider using the standard administration tools. Remote content on a remote content provider can be distributed according to the standard delegated administration model, in the same manner as performed with local content on the main portal.
In addition, new services and tools have been added in the portal to fully support the implementation of SAP Enterprise Portal 6.0 in a global portal network. These include:

- A tool for defining the connection between the main portal and remote content providers.
- A tool enabling automated conversion of local iViews on the main portal to proxy-to-remote iViews, which reference remote iViews on a remote content provider site.
- A specialized iView wizard on the main portal that enables the viewing of the Portal Catalog of a remote content provider, to choose remote iViews, and generate proxy-to-remote iViews that reference them.
- A WSRP service that facilitates content sharing through the use of predefined standards and application interfaces.

The global portal tools are contained in a new portal administrative area, which is accessible in the top-level navigation under:

- *System Administration* → *Global Portal*
- *Content Administration* → *Portal Content*

1.3 Prerequisites

Expertise Level

This document requires prior knowledge and high-level expertise using SAP Enterprise Portal 6.0, including areas in user-, content- and system administration.

Additional Documentation

Procedures that require the use of portal tools specific to the global portal scenario are described in detail in this document. Although certain general portal-related procedures are detailed in this document as well, most are not. In such cases, references will be given to the relevant section in the *SAP Enterprise Portal 6.0 Administrator Guide* or *End User Guide*.
These guides are available on the SAP Help Portal at **`http://help.sap.com`** → *SAP NetWeaver* → *SAP Enterprise Portal*. Note that references to specific chapters in these guides are liable to change in future versions.

1.4 Features

1.4.1 Remote iViews and Proxy-to-Remote iViews

In the current global portal solution, the main focus is on **iViews**. iViews on the main portal and remote sites work in couplets at run time and design time to retrieve live content from remote applications and to deliver it to clients through the main portal.
The iViews involved are referred to as either a *remote iView* or a *proxy-to-remote iView*, depending on their location:

iView Type	Description
Remote iView	A remote iView is an iView residing on a remote content provider. A remote content provider is typically situated in the same geographical location as the back-end system or application (the information source) on which the iView is based. At run time, the remote iView is responsible for interfacing directly with the information source, retrieving the necessary data, and rendering the data for display. The rendered data is then transferred as markup to its corresponding proxy-to-remote iView on the main portal, to be delivered to portal end users.
Proxy-to-remote iView	A proxy-to-remote iView is an iView residing on the main portal. The proxy-to-remote iView references a remote iView that resides on a remote content provider site through another transparent iView called an *intermediary iView* (see description that follows). At design time, the proxy-to-remote iView is the entity that is assigned to portal end users through role-based assignment. At run time, the proxy-to-remote iView triggers its corresponding remote iView on a remote content provider, obtains rendered markup data from it, and displays it as-is in an iView on the end user's portal desktop.

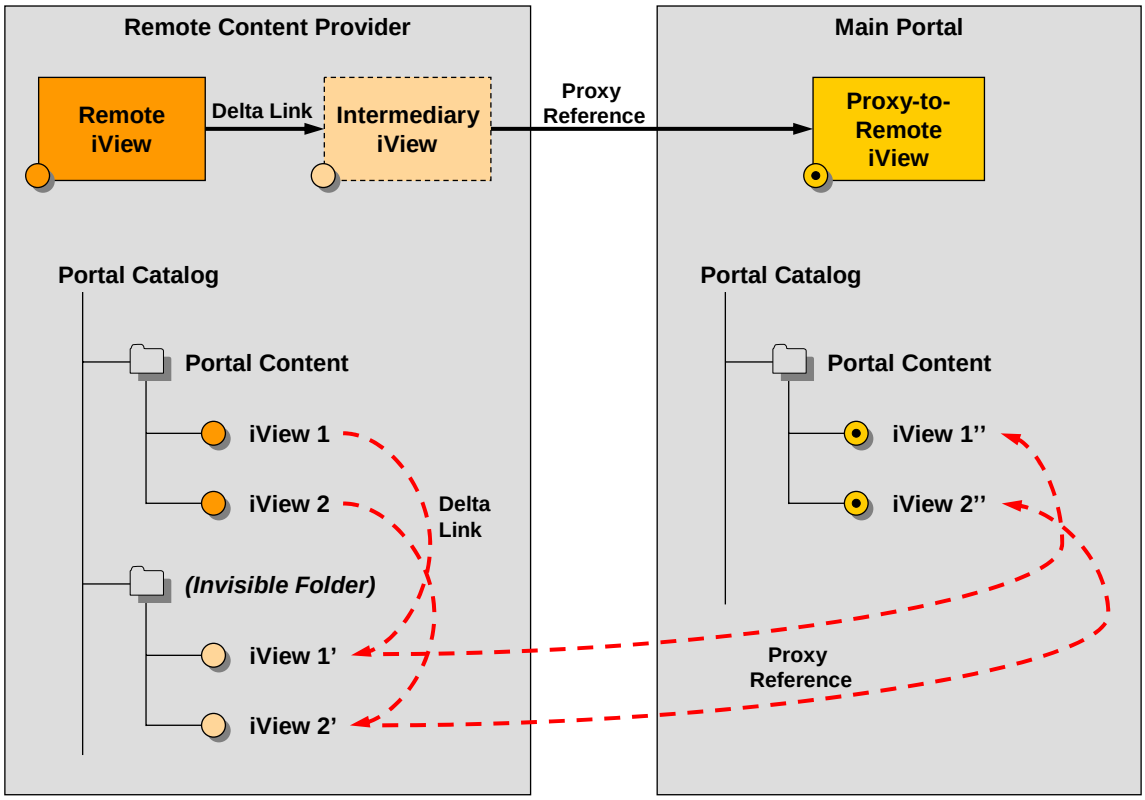
A proxy-to-remote iView is a second-generation descendant to its corresponding remote iView. When you create a proxy-to-remote iView on the main portal, the following occurs (see also following figure):

1. An **intermediary iView** is automatically generated on the remote content provider in a transparent folder. The intermediary iView is related to the remote iView through a *delta link*.

   Note:

   Intermediary iViews are a technical necessity for the implementation of syndicated content. For example, they store personalized properties performed by end users. Intermediary iViews exist in the PCD, but are completely transparent in the Portal Catalog and thus cannot be modified.

2. A new **proxy-to-remote iView** is then generated on the main portal, based on the remote iView. This iView is related to the intermediary iView through a link type known as a *proxy reference*. The proxy-to-remote iView is a reference to the intermediary iView, but it also has its own set of metadata that is not inherited from the intermediary iView.



Delta link and proxy reference relationship between remote iView (on a remote content provider) and corresponding proxy-to-remote iView (on the main portal)

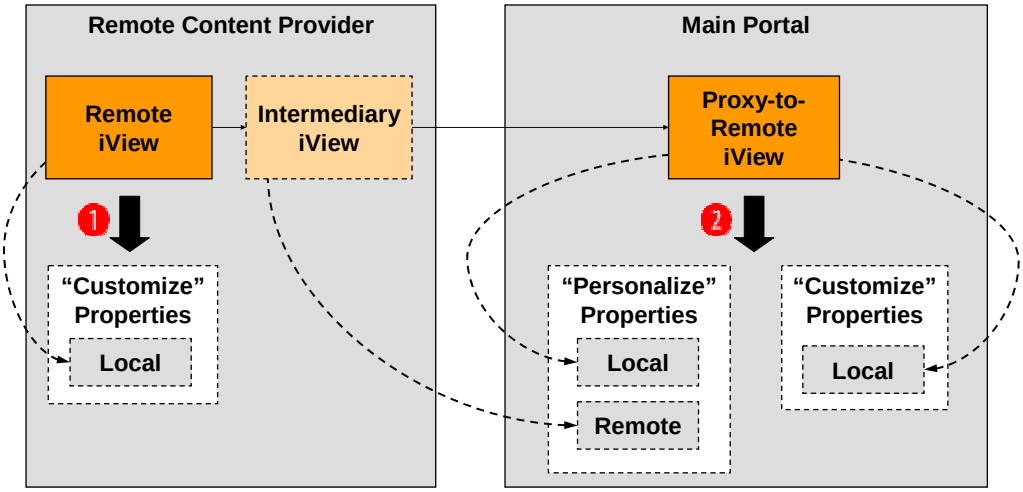
Proxy-to-remote iViews on the main portal are accessible from the Portal Catalog in the Portal Content Studio. They are a type of semantic iView object, and are handled just like other standard portal objects. For example, you may edit them, add them to pages and roles, cut and paste them, and assign permissions. Note that when a content administrator edits a proxy-to-remote iView, the properties of the remote iView are not displayed; only the local metadata of the proxy-to-remote iView is editable. Remote iViews must be maintained directly on their respective remote content provider.

You can create proxy-to-remote iViews on the main portal as “templates”, if needed. Additional iViews can then be created on the main portal from this template.

1.4.2 Customization and Personalization of iView Properties

At design time, content administrators can *customize* proxy-to-remote iViews on the main portal only and remote iViews on a remote content provider only. At run time on the other hand, end users can *personalize* both proxy-to-remote iViews and remote iViews through the main portal only.

Content administrators must understand the distribution of properties to determine which iView to edit at design time; either the proxy-to-remote on the main portal or the remote iView on the remote content provider. The following figure illustrates the distribution of properties between remote iViews and proxy-to-remote iViews (a detailed description follows):



Distribution of properties in remote iViews and proxy-to-remote iViews: (1) remote iViews edited (customized) by a content administrator on a remote content provider provide access to its local properties only; (2) proxy-to-remote iViews edited (customized) by a content administrator on the main portal provide access to the local properties of the proxy-to-remote iView only, but if "personalized" by an end user at run time, both local and remote properties are available.

Customization of Properties by Content Administrators

Before a content administrator customizes an iView, he or she must understand which properties can be customized in a remote iView and its corresponding proxy-to-remote iView.

When editing a **proxy-to-remote iView** on the main portal, note the following:

- The properties displayed are specific to the proxy-to remote iView object only.

  These properties are mostly general properties, such as the iView name, ID, description, and appearance characteristics (display height, tray type etc.). They do not include properties that define the connectivity to the back-end system or application upon which the iView is based (for example, the URL address in a URL iView). To access those properties, you need to edit the remote iView directly on the remote content provider.
- Any specialized editors required by certain iViews, such as the URL iView Editor for URL iViews, are not available. To access a specialized editor, you need to edit the remote iView directly on the remote content provider.

See also "Editing Proxy-to-Remote iViews" on page 24.

When editing a **remote iView** on a remote content provider, note the following:

- The properties displayed in the Property Editor are specific to the remote iView only.

  You will notice certain properties (for example, iView height and tray type) that also exist in the iView's corresponding proxy-to-remote iView. When customizing the properties of a remote iView, you should only do so for the connection-specific properties; these are usually properties that define the connectivity to the back-end system or application upon which the iView is based (for example, the URL address in a URL iView). The remaining set of properties should only be customized in the proxy-to-remote iView on the main portal.

For example, the iView height is defined as 100 pixels on both the proxy-to-remote iView and remote iView. If you modify the iView height to 350 pixels on the remote iView, the proxy-to-remote iView will remain 100 pixels.

- Any specialized editor (if the iView type requires one) is also displayed alongside the Property Editor.

For more information, see “Editing Remote iViews” on page 15.

Personalization of Properties by End Users

The iViews delivered to end users at run time are proxy-to-remote iViews. However, when an end-user chooses to personalize such an iView, he or she receives two sets of properties:

- Local properties: these are the properties that are specific to the proxy-to-remote iView.
- Remote properties: these are the properties that are specific to the remote iView.

It is the task of the content administrator at design time to define which properties, on both the proxy-to-remote iView and remote iView entities, are personalizable by end users. For more information, see “Preparing Remote iView Properties for End-User Personalization” on page 16 and “Preparing Proxy-to-Remote iView Properties for End-User Personalization” on page 25. For information on end-user personalization of properties, see “Personalizing Proxy-to-Remote iViews at Run Time (by End Users)” on page 27.

1.4.3 WSRP Standard

Web Services for Remote Portals (WSRP) defines a standard for interactive, presentation-oriented web services with a common, well-defined interface and protocol for processing user interactions and providing presentation fragments suitable for aggregation by portals. For further information, visit `http://www.oasis-open.org/`.

Although currently not fully compliant with the WSRP standard, the global portal solution makes extensive use of WSRP APIs for the following:

- Publishing portal content
- Providing the consumer portal (main portal in this case) with the rendered HTML representation of a remote iView from the producer (a remote content provider in this case)
- Enabling the portal client to interact with a remote iView as if it was deployed locally

For developers, the services provided in the PRT Eclipse Toolkit allow for rapid updates of the WSRP service implementation in the portal, when needed.

1.5 Limitations

For known limitations, see **SAP Note 852071**.

2 Workflow

To set up a global portal with syndicated content, perform the following procedure. Authorized user-, content- and system administrators of the portal typically perform these tasks.

1. Install the portal software on the main portal and remote content provider sites. See “Installing the Software” on page 12.

   After installation, make sure the main portal is fully operational, and that you are able to create and run local content on each main portal and remote content provider separately (without yet sharing content).
2. Set up the same user persistence store on the main portal and all remote content provider sites by deploying either of the following:
   - A single user directory to which the main portal and remote content providers are connected
   - Replications of the same user directory installed on each site in the network

3. Configure each **remote content provider** site as follows:
    a. Make sure the remote content provider is in active mode.
    b. Create systems on the remote content provider to enable connectivity to the back-end applications.
    c. Create the iViews that will be referenced from the main portal.
    d. Assign portal permissions to the iViews to allow the content administrator on the main portal to access them.
    e. Set up user mapping for secure data sources, if needed.
    f. Test the iViews on the remote content provider site.
    g. Prepare the iView properties for end user personalization (this can be done at a later stage).

    Detailed instructions for the above steps are described in "Remote Content Provider – Configuration and Administration" in pages 13-16.
4. Configure the **main portal** as follows:
    a. Create connections to any number of remote content providers, and define aliases for them.
    b. Set up trust between the main portal and each remote content provider site.
    c. Create proxy-to-remote iViews on the main portal using either the specialized iView Wizard or content conversion tool, or both.
    d. Fine-tune the proxy-to-remote iView properties.
    e. Prepare the proxy-to-remote iView properties for end-user personalization.
    f. Assign the proxy-to-remote iViews to end users through page and role assignments.
    g. Test the proxy-to-remote iViews on main portal.

    Detailed instructions of the above steps are described in "Main Portal – Configuration and Administration" in pages 16-26.

3 Installing the Software

Procedure

Install SAP Enterprise Portal 6.0 on the main portal and on each remote content provider in your global portal network. Although the installation of the core portal software on a remote content provider is identical to that of the main portal, its functionality differs considerably.
For instructions on installing the portal, see the SAP Enterprise Portal 6.0 Installation Guide located on SAP Service Marketplace at **`http://service.sap.com/ep60`** → *Documentation & More* → *Installation*.

Requirements

LDAP	The main portal and all remote content providers must use the same LDAP. If it is technically impossible to connect a remote content provider over the network to the central LDAP of the main portal, then it is possible to connect the remote content provider to a local LDAP that contains the same users (and user IDs) as the central LDAP. The trust you will set up later between the main portal and remote sites will allow seamless authentication across sites (see "Creating Trust between the Main Portal and a Remote Content Provider" on page 19).
Portal versioning	The main portal and all remote content providers must be running the same portal version, including support package (SP), patch, and hotfix level. The current solution requires EP 6.0 SP2 or SP3.

4 Remote Content Provider – Configuration and Administration

A **remote content provider** is a site in the global portal network that exposes its content for publication on the main portal. The remote back-end applications that provide data for iViews on the main portal are physically located in close geographical proximity to the remote content provider.

Although a remote content provider is a SAP Enterprise Portal installation, it does not function as a regular portal. Its sole function is to enable connectivity to the back-end system (data source) and provide iView data to the main portal installation. It is thus also referred to as a *producer* (which is parallel to WSRP terminology).

The iViews that reside on the remote content provider are known as **remote iViews**. These iViews connect directly to back-end applications and transfer fully rendered markup data to the main portal for publication. Each remote iView is referenced from the main portal by its own corresponding iView, known as a **proxy-to-remote iView**.

In the sub-sections that follow, we discuss the necessary tasks administrators need to perform on the remote content provider to setup and configure a global portal environment with syndicated content.

For a summary of the complete procedural workflow on the main portal and remote content provider sites, see “Workflow” on page 11.

4.1 Activating a Remote Content Provider

Before the main portal can connect to a remote content provider and gain access to its shared content, the system administrator must activate the remote portal installation. When a remote content provider site is in active mode, the Web service configuration that handles the WSRP protocol is enabled, thus enabling sites to communicate.

Prerequisites

- Access to the Service Configuration tool on the remote content provider (by default, it is assigned to the standard System Administrator role)

Procedure

1. In the portal of the remote content provider, navigate to *System Administration* → *System Configuration* → *Service Configuration*.
2. In the Portal Catalog, choose one of the following services, depending on the support package (SP) version your SAP Enterprise Portal:

SP	Service
SP2	*Applications* → **`com.sap.portal.ivs.global`** → *Services* → *Producer*
SP3	*Applications* → **`com.sap.portal.ivs.global`** → *Services* → *AutoGenProducer*

3. Right-click the relevant service, and choose *Edit* from the context menu that appears. The Property Editor opens.
4. To activate the remote content provider, set the *Enable Global Portal* property to **`True`**. Note this is the default setting.

   To deactivate the remote content provider at any time, set the *Enable Global Portal* property to **`False`**.
5. Save the service to apply your changes.
6. Restart the Java application server.

4.2 Creating System Objects

The system landscape in the portal environment is a collection of system objects representing back-end applications in your organization. Systems act as a gateway for portal iViews to connect to these applications and retrieve data from their information repositories. In the global portal environment, systems must be defined and maintained on the remote content provider sites where the back-end applications are located.

The system landscape of each remote content provider is not accessible from the main portal in the administrative environment. Nevertheless, the main portal *does* expose systems on remote content providers in the run time user mapping tool, which enables end users to enter their user mapping credentials for remote iViews (through their corresponding proxy-to-remote iViews on the main portal).

For more information on system landscapes, see the *SAP Enterprise Portal 6.0 Administration Guide* → *Portal Platform* → *System Administration* → *System Landscape*.

4.3 Creating Remote iViews

The content administrator is responsible for creating iViews on the remote content provider using the standard and customized iView wizards and editors in the Portal Content Studio.

For more information on remote iViews and their relation to proxy-to-remote iViews, see “Remote iViews and Proxy-to-Remote iViews” on page 8.

For more information on creating iViews in the portal, see the *SAP Enterprise Portal 6.0 Administration Guide* → *Portal Platform* → *Content Administration* → *iViews* → *Creating iViews*.

4.4 Setting Permissions to Remote iViews

An administrator on the remote content provider must assign the appropriate portal permissions to iViews that will be consumed by the main portal. iViews must have at least *read* (administrator) permission for a content administrator on the main portal. If an iView is not granted access permissions to a content administrator on the main portal, the administrator will be unable to create the necessary proxy-to-remote iViews.

The global portal solution with syndicated content requires that the main portal and any remote content provider use the same LDAP, meaning that the same users reside on both local and remote sites. Trust relations must be set up between sites (see “Creating Trust between the Main Portal and a Remote Content Provider” on page 19). Thus, all folders and objects on remote sites, to which a user has permissions, will be available in the main portal with the same permissions.

> **Note:**
>
> It is the task of the system administrator to assign end user permissions to the remote iViews on the remote content provider so that they are available at run time. End user permissions must also be enabled on their corresponding iViews on the main portal.

Prerequisites

- Authorization to define content permissions on the remote content portal (*owner* permission)
- Access to any one of the following portal tools that allow assignment of portal permissions:
  - Portal Content Studio (by default, assigned to the standard Content Administrator role)
  - central Permission Editor (by default, assigned to the standard System Administrator role)

Procedure

For more information on portal permissions and how to use the Permission Editor, see *SAP Enterprise Portal Administration Guide* → *Portal Platform* → *System Administration* → *Portal Permissions*.

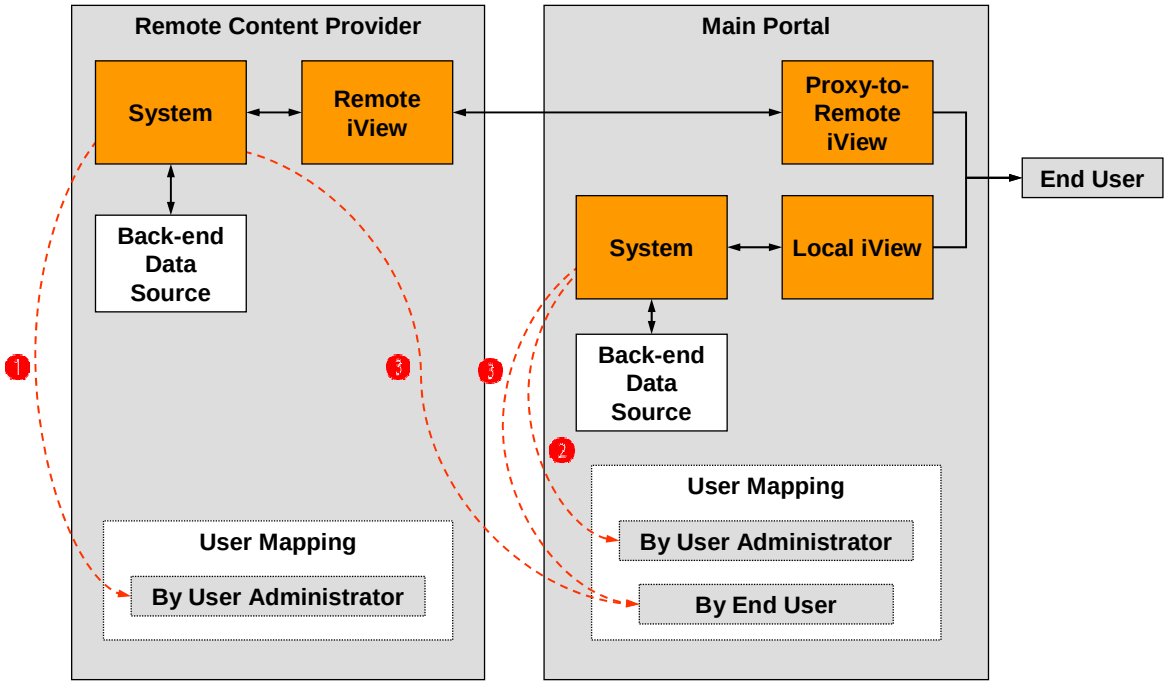
4.5 Setting Up User Mapping

Mapping of logon credentials for users (such as user name and password) to secured data sources enables single sign-on. With single sign-on, users are not prompted for logon information every time an iView retrieves data from a secure source at run time.

User mapping is performed by providing logon data per data source from the portal. The system administrator responsible for configuring the necessary systems in the portal must define for each system if a user administrator, end user, or both perform the user mapping for each system object. The delegation of tasks depends on the nature of the data source. For more information, see *SAP Enterprise Portal 6.0 Administration Guide → Portal Platform → User Administration → User Mapping*.

If the user administrator is responsible for setting up the user mapping, this must be done directly on the remote content provider. User mapping can be assigned on the level of single users, groups, or entire roles, using the *User Administration → User Mapping* interface in the portal. User administrators cannot set up user mapping on the main portal because the systems on which the remote iViews are based are not exposed on the main portal.

If end users are responsible for setting up their own user mapping, this is performed on the main portal, even though the system is located on the remote content provider. End users must use the *Personalization → User Mapping (Remote iViews)* interface on the portal to perform user mapping for remote systems. For more information, see “Mapping User Information to Remote Content (by End Users)” on page 28.



Site distribution of user mapping assignment tasks by user administrators and end users for local and remote systems: (1) user mapping by user administrators on remote systems can only be performed on the remote content provider; (2) user mapping by user administrators on local systems is performed from the main portal, and; (3) user mapping by end users on local and remote systems is performed from the main portal.

4.6 Editing Remote iViews

Content administrators can edit iViews on the remote content provider as needed, using the Portal Content Studio.

Remote iViews on the remote content provider can be modified before or after they are referenced as proxy-to-remote iViews on the main portal. Since proxy-to-remote iViews on the

main portal are merely pointers to their corresponding remote iViews on a remote content provider, any modifications (such as changes to property values) that are made to iViews on the remote content provider are applied immediately on the main portal, except for local properties specific to proxy-to-remote iViews, which are not overwritten.
For more information, see *SAP Enterprise Portal 6.0 Administration Guide → Portal Platform → Content Administration → Portal Content Studio*.

4.7 Preparing Remote iView Properties for End-User Personalization

The content administrator needs to define which properties in each remote iView will be available to the end user for personalization at run time.
This is done in the Property Editor in the Portal Content Studio on a remote content provider. For each property, one of the following settings may be defined:

- *Hidden:* The property is not displayed when the object is personalized.
- *Read-Only:* The property and its value are displayed when the object is personalized, but the end user cannot personalize the property.
- *Read/Write:* The property and its value are displayed when the object is personalized. The end user can personalize the property value.

For more information on using the Property Editor, see the *SAP Enterprise Portal Administration Guide → Portal Platform → Content Administration → Portal Content Studio → Property Editor*.

4.8 Testing the iViews

Each remote iView must be thoroughly tested by the content administrator before it can be assigned to the portal content hierarchy. Afterwards, it serves as the basis for generating the proxy-to-remote iView on the main portal.

4.9 Assigning Remote iViews to Pages, Worksets and Roles

Once the content administrator has generated, configured, and tested the iViews on the remote content provider, they need to be assigned to a higher content hierarchy (portal pages, worksets, and roles) on the main portal in order to deliver them to portal end users.
This can be done in the following ways:

- On the main portal, generate proxy-to-remote iViews based on standalone remote iViews located on a remote content provider. Then, also on the main portal, assign the proxy-to-remote iViews to local portal pages, worksets, and roles, as needed.

  For more information, see “Creating Proxy-to-Remote iViews using the iView Wizard” on page 22.
- On the remote content provider, first assign the standalone iViews to local portal pages, worksets, or roles, as needed. Create a transport package that includes the necessary content hierarchy and import the package on the main portal. Then, use the Local-to-Remote Conversion tool on the main portal to automatically replace the local iViews from the package with proxy-to-remote iViews.

  For more information, see “Creating Proxy-to-Remote iViews using the Local to Remote Conversion Tool” on page 22.

See also “Integrating Proxy-to-Remote iViews as Content on the Main Portal” on page 25.

5 Main Portal – Configuration and Administration

The **main portal** is the central portal installation site in a global portal network. It handles all administrative aspects of the portal and content delivery to end users at run time. The main portal may contain local iViews, but in the context of a global portal scenario, it also contains proxy-to-

remote iViews that reference iViews on remote content provider sites. Therefore, the main portal is also referred to as a *consumer* (which is parallel to WSRP terminology).
The global portal tools are contained in a new portal administrative area, which is located under *System Administration* → *Global Portal* in the top-level navigation.
This section describes the necessary tasks performed by portal administrators on the main portal to setup and configure a global portal environment with syndicated content. It assumes that the relevant remote content providers have already been set up, as described in "Remote Content Provider – Configuration and Administration" in pages 13-16.

5.1 Connecting to a Remote Content Provider from the Main Portal

Before the main portal can begin using content shared by a remote content provider, the system administrator on the main portal must define which remote content providers it can connect to. A connection can only be made once the remote content provider has been activated as a producer (see "Activating a Remote Content Provider" on page 13).
The sub-sections that follow describe the necessary steps needed to define and maintain a connection from the main portal to a remote content provider:

1. Creating a connection from the main portal to a remote content provider
2. Defining an alias for the remote content provider on the main portal
3. Creating trust between the main portal and a remote content provider

5.1.1 Creating a Connection to a Remote Content Provider

The main portal provides a wizard that enables a system administrator to add active remote content providers. When a remote content provider is defined in the main portal, it is represented as a semantic object in the Portal Content Directory (PCD). The object holds all the properties required for the main portal to connect to the remote content provider. The object is accessible from the Portal Catalog, and it can be maintained like any other object in the PCD; for example, it can be edited, deleted, and have portal permissions assigned to it.

Prerequisites

- Authorization to create remote content provider objects in the Portal Catalog

Procedure

1. On the main portal, navigate to *System Administration* → *Global Portal* → *Remote Content Providers*.
2. In the Portal Catalog, right-click a folder, and choose *New* > *Remote Content Provider* from the context menu. The Remote Content Provider Wizard is displayed.
3. In the *General Properties* step, enter the correct information for all the available fields in order to define the basic properties of the remote content:
   - `Remote Content Provider Name`
   - `Remote Content Provider ID`
   - `Remote Content Provider ID Prefix`
   - `Master Language`
   - `Description`
4. Click *Next*.
5. Click *Finish*. An object reflecting the selected remote content provider is created in the Portal Catalog.
6. In the Portal Catalog, right-click the remote content provider you just created, and choose *Edit* > *Remote Content Provider* from the context menu that appears. The properties of the remote content provider objects are displayed.

7. In the Property Editor, define the following properties. Note that the properties are located in the *Remote Content Provider* category.

Property	Description
Connection Protocol	Choose either *HTTP* or *HTTPS,* depending on the connection protocol you prefer. Note that portal sites themselves most be appropriately configured to support a HTTPS connection. This setting alone does not define the connection protocol between sites.
Consumer Name	Specifies the unique ID of the main portal. The main portal and remote content provider use this value to assist in locating iViews in the global portal network. **Important:** You may modify this value before you create proxy-to-remote iViews through this remote content provider; however, once you have created iViews you must NOT modify the value.
Group Name	Currently, this property is not utilized by any interfaces or mechanisms in the portal; you may therefore disregard it. You can, however, use it to enter a group name to which you want the remote content provider to belong. For example: Asia, North America, and Australasia.
Host Name	The portal address of the remote content provider site. For example: **`goofy.sap.corp`**.
Port	Enter the port number of the remote content provider site.

For more information on using the Property Editor, see the *SAP Enterprise Portal Administration Guide*.

8. Save your changes.

Note:

Once a remote content provider has been defined on the main portal, it must be assigned at least one alias. See “Defining an Alias for a Remote Content Provider” on page 18.

5.1.2 Defining an Alias for a Remote Content Provider

A remote content provider defined on the main portal must be assigned at least one alias. Note that the following user interfaces use aliases to identify the remote content providers you define on the main portal:

- Proxy-to-remote iView Wizard
- Local-to-Remote Conversion tool
- User Mapping (end-user personalization)

Prerequisites

- Authorization to edit remote content provider objects in the Portal Catalog

Procedure

1. On the main portal, navigate to *System Administrator* → Global Portal → *Remote Content Providers*.

Tip:

If the remote content provider object is already open in editing mode, choose *Remote Portal Aliases* in the object editor toolbar. Then skip directly to step 4.

2. In the Portal Catalog, navigate to the remote content provider object.
3. Right-click the remote content provider object, and choose *Edit* > *Remote Portal Aliases* (or *Edit* and then choose *Remote Portal Aliases* in the object editor toolbar). The aliases currently defined for the remote content provider are displayed in the *Defined Aliases* list.

4. In the editor, do any of the following as necessary:

Action	Description
Add an alias	In the *Alias* box, enter the name of the alias, and click *Add*. The new alias will be added to the *Defined Aliases* list.
Delete an alias	Choose an alias in the *Defined Aliases* list, and click *Remove*.
Rename an alias	Choose an alias in the *Defined Aliases* list, and click *Rename*. Then modifies the existing name in the *Defined Aliases* list area. **Important:** Do NOT change the alias of a remote content provider once you have created proxy-to-remote iViews based on that site. This will prevent the existing proxy-to-remote iViews from being able to retrieve data from their back-end application.

5. Click *Save* to apply your changes.

5.1.3 Editing a Connection (Remote Content Provider Object)

Once you have created a connection to a remote content provider from the main portal, it exists as an object in the Portal Catalog. As with other object types in the Portal Catalog, you may perform certain maintenance actions on a remote content provider object, such as:

- Copy, cut, and paste
- Edit objects
- Edit aliases
- Edit permissions
- Delete objects

To perform these actions, right-click the remote content provider object in the Portal Catalog, and choose the relevant option from the context menu.

5.1.4 Creating Trust between the Main Portal and a Remote Content Provider

Trust must be established between the main portal and all remote content providers in order for them to communicate and share content. This section describes how to establish the trust relationship.

Note that there is no need to set up trust between remote content provider sites since they do not collaborate with each other directly.

Prerequisites

- Log on to the main portal as a System Administrator.
- The clocks for the main portal and remote content provider are synchronized.

  If the clocks of the main portal and remote content provider are not synchronized, then the remote content provider (the ticket-accepting system) may receive a logon ticket from the main portal (the ticket-issuing system) that is not yet valid, which causes an error.

  Note:

  The authentication mechanism for logon ticket defines a tolerance time period to compensate for unsynchronized clocks of the accepting and ticket-issuing systems. The default time tolerance is 3 minutes.

Procedure

Step 1: Download “verify.der” File

In the first phase of setting up trust between the main portal and a remote content provider, you must download a `verify.der` file from the main portal.

1. On the main portal, navigate to *System Administration* → *System Configuration* → *Keystore Administration*.
2. In the *Content* tab, click *Download verify.der File*.
3. Browse to the folder in which you want to save the file, and save it with a ZIP extension.
4. Open the ZIP file and extract the `verify.der` file.

If you have more than one main portal in your network, perform these instructions again to download a `verify.der` file from each portal.

Step 2: Import "verify.der" File

In the second phase of setting up trust between the main portal and a remote content provider, you must import the `verify.der` file you downloaded from the main portal to the remote content provider.

1. In the portal on the remote content provider, navigate to *System Administration* → *System Configuration* → *Keystore Administration*.
2. In the *Import Trusted Certificate* tab, click *Browse*.
3. Choose the *verify.der* file you downloaded from the main portal.
4. In the *Alias* field, specify a name for the key you are uploading for easy identification of the site it refers to.
5. Click *Upload*.
6. Open the *Content* tab and make sure that the key is listed in the keystore list.
7. Restart the servers on the main portal and remote content providers.

   Note:

   If you are running NW '04 SP Stack 5 and higher, you do not need to restart the server now. You can do so after completing "Step 3: Trust Configuration in Visual Administrator" described in the following section.

If you have more than one remote content provider in your network, repeat these steps on each remote content provider to import the `verify.der` file.
If you have more than one main portal in your network, perform these instructions again to import the `verify.der` file you download from each main portal. Each site in the global portal network must have a unique keystore name (alias) per remote content provider.

Step 3: Trust Configuration

To complete the process of setting up trust between the main portal and a remote content provider, you must configure the `ticket` component in the Visual Administrator on the remote content provider.

Note:

This step is only necessary from NW '04 SP Stack 5 and higher.

1. On the remote content provider, open the Visual Administrator tool.
2. Navigate to *Server Node* → *Services* → *Security Provider*.
3. In the right-hand pane, navigate to the *Runtime* → *Policy Configuration* tab.
4. In the *Components* list, choose the `ticket` component.
5. In the Authentication tab, choose the following login module:
   `com.sap.security.core.server.jaas.EvaluateTicketLoginModule`
6. Click *Modify*. The *Edit Logon Module* screen is displayed.

7. In the *Edit Logon Module* screen, create the following parameters in the *Options* table.

Parameter Name	Value
`trusteddn1`	Enter the distinguished name of the certificate owner. You can obtain this value as follows: 1. In the portal on the remote content provider, navigate to *System Administration* → *System Configuration* → *Keystore Administration*. 2. In the *Content* tab, choose the alias of the main portal in the drop-down list. 3. Copy the value of the `DN of Owner` property.
`trustediss1`	Enter the distinguished name of the certificate issuer. You can obtain this value as follows: 1. In the portal on the remote content provider, navigate to *System Administration* → *System Configuration* → *Keystore Administration*. 2. In the *Content* tab, choose the alias of the main portal in the drop-down list. 3. Copy the value of the `DN of Issuer` property.
`trustedsys1`	Enter the system ID and client ID of the main portal, in the format: **`<System_ID>,<client_ID>`** . Separate the values with a comma (,). • `System ID`: Specifies the 3-letter ID defined during the installation of the main portal. • `Client ID`: Specifies the client ID. Since you are connecting to a J2EE-based system, always enter **`000`**. For details, see SAP Note 721815. For example: **`GP1,000`**

If you have more than one main portal in your network, define additional parameters in the login module to represent each main portal by incrementing the suffix in the parameter name. For example: **`trusteddn2`**, **`trustediss2`**, **`trustedsys2`**, and so on.

8. Restart the server on the remote content provider.

If you have more than one remote content provider in your network, repeat these steps on each remote content provider.

5.2 Creating Proxy-to-Remote iViews on the Main Portal

After you have added the remote content providers to the main portal, you may begin the process of creating **proxy-to-remote iViews** on the main portal.
SAP Enterprise Portal provides two approaches for creating proxy-to-remote iViews on the main portal. Although the two approaches differ considerably, they are merely alternative means to generating the same proxy content. You can use either approach exclusively or use them both, whichever is convenient.

- **Proxy-to-Remote iView Wizard:** With the use of a dedicated iView template, the iView Wizard lets you navigate the Portal Catalog of a remote content provider from the main portal, and then choose the remote iViews you want referenced as proxy-to-remote iViews on the main portal. For more information, see “Creating Proxy-to-Remote iViews using the iView Wizard” on page 22.
- **Local-to-Remote (iView) Conversion Tool:** This tool enables you to convert local iViews already residing on the main portal to proxy-to-remote iViews. This is accomplished by comparing mirrored pieces of the Portal Catalog on the main portal with a selected remote content provider. For more information, see “Creating Proxy-to-Remote iViews using the Local to Remote Conversion Tool” on page 22.

For detailed information on the syndicated iView model, see “Remote iViews and Proxy-to-Remote iViews” on page 8.

5.2.1 Creating Proxy-to-Remote iViews using the iView Wizard

This procedure describes how to use the iView Wizard to create proxy-to-remote iViews on the main portal. The wizard enables you to view the Portal Catalog of a selected remote content provider, and then choose the remote iViews you want referenced via proxy-to-remote iViews on the main portal.

Prerequisites

- The necessary remote iViews have been generated on the remote content provider sites.
- You have at least *read* administrator permissions to the remote iViews on the remote content provider sites.
- You have at least *read/write* administrator permissions to the Portal Catalog folder on the main portal in which you intend to create the proxy-to-remote iViews.

Procedure

1. On the main portal, navigate to *Content Administration* → *Portal Content*. The Portal Content Studio is displayed.
2. Right-click a folder, and choose *New* → *iView*. The iView Wizard is displayed.
3. In the *Template Selection* window, choose *Proxy-to-Remote iView*.
4. Click *Next*.
5. In the *Remote Content Provider* window, choose a remote content provider. The list displays the default alias of each remote content provider that has been added to the main portal.
6. Click *Next*.
7. In the *Remote iView Selection* window, choose the iViews from which you want to create proxy-to-remote iViews. Do so as follows:
    a. In the *iViews on Remote Content Provider* pane, navigate the Portal Catalog of the selected remote content provider and highlight the appropriate iViews.

       Note that the iViews you see are those for which you have been assigned at least *read* administration permission.
    b. Click *Add*. The iViews you selected are listed in the *Selected iViews* pane.

       To remove selected iViews, choose them in the *Selected iViews* pane, and click *Remove*.
    c. When you have completed selecting all the iViews you want, click *Next*.
8. In the *Summary* window, review the remote iViews you have selected. If you want to modify your selection, click *Back* and make the necessary changes in the appropriate window.
9. Click *Finish* to generate the proxy-to-remote iViews that reference the remote iViews you selected.

Result

Proxy-to-remote iViews are created in the folder you chose before initiating the wizard. Intermediary iViews are also created on the remote content site; they connect between each remote iView and its corresponding proxy-to-remote iView on the main portal. The default property values of the proxy-to-remote iViews are copied from their corresponding remote iViews. See “Notes on Local Properties in Proxy-to-Remote iViews” on page 24.

5.2.2 Creating Proxy-to-Remote iViews using the Local to Remote Conversion Tool

This procedure describes how to use the Local to Remote Conversion tool to convert *local iViews* already residing on the main portal to proxy-to-remote iViews. Note that the current global portal solution supports the syndication of iViews only; other object types, such as roles, worksets, and pages are not yet supported.

The content conversion tool operates as follows (instructions on using it follow):

1. You define which remote content provider you would like the tool to analyze.
2. The tool then compares local iViews on the main portal with remote iViews on the selected remote content provider, and lists which *local iViews* on the main portal have the same iView ID and full PCD path.

Note:

- The content analysis performed by the tool is *recursive* from the folder you have selected in the Portal Catalog onwards, which means sub-folders are included.
- The Portal Catalog folder structure of the area you are comparing on the main portal must match the folder structure of the remote content provider in an *absolute* manner. In other words, for a match to occur, the entire PCD path of each matching object must be identical.

3. You choose which matching local iViews on the main portal you want to replace with proxy-to-remote iViews.

   Note:

   You will only see the local iViews for which you have administration *read* permission.

4. The conversion tool first creates intermediary iViews on the remote content site and then converts the local iViews on the main portal to proxy-to-remote iViews (which reference their corresponding remote iView through the respective intermediary iViews).

Example

The content conversion tool enables mass content conversion. It is useful when you have a business package set up on the remote content provider, and the iViews you want to convert are already integrated into roles, worksets, and portal pages. To support this scenario, you would first create a transport package (including roles, worksets, pages, and iViews, for example) on the remote content provider or use an existing business package, and then transport it into the main portal. Make sure that the business package on the main portal is uploaded to the same Portal Catalog folder as that of the remote content provider. After the business package has been generated on the main portal, you can use the content conversion tool to replace the local iViews in the business package with proxy-to-remote iViews.

Prerequisites

You must install the content identically on both the main portal and the remote content provider site.

Procedure

1. On the main portal, navigate to *System Administrator* → *Global Portal* → *Local to Remote Conversion*. The Local to Remote Conversion tool is displayed.
2. Right-click a folder, and choose *New* → *Convert*.
3. In the *Select Remote Content Provider* window, choose the remote content provider you want analyzed for duplicate remote iView content. The list displays the default alias assigned to each remote content provider added to the main portal.
4. Click *Next*.
5. In the *Select iViews to Convert* window, you see a list of local iViews on the main portal that match remote iViews on the selected remote content provider. Choose the local iViews that you want converted to proxy-to-remote iViews.
6. Click *Next*.
7. In the *Summary* window, review the local iViews you have selected for conversion. To modify your selection, click *Back* and make the necessary changes in the appropriate windows.
8. Click *Finish* to initiate the conversion of the selected iViews on the main portal to proxy-to-remote iViews. Depending on the number of iViews that need to be converted and the complexity of the tree, this procedure may take several minutes.

Result

When the conversion process has finished, you will receive a report stating which local iViews were successfully converted to proxy-to-remote iViews.
Since the proxy-to-remote iViews are already part of a local content hierarchy (portal pages, worksets, and roles), no further configuration to the content should be necessary on the main portal. Once the roles are assigned to users, the iViews should function immediately. Make sure

that the initial values of the local properties in each proxy-to-remote iView are copied from their corresponding remote iView. See “Notes on Local Properties in Proxy-to-Remote iViews” on page 24.

5.2.3 Notes on Local Properties in Proxy-to-Remote iViews

Whether you have created proxy-to-remote iViews using either the wizard or the conversion tool, a number of local properties are defined in each proxy-to-remote iView. The list below shows the most important local properties assigned to proxy-to-remote iViews. These local properties always override their parallel remote properties in corresponding remote iViews. The initial value of each local property is taken from its parallel remote property at the time the proxy-to-remote iView is created.

- `iView Name`
- `iView ID`
- `Description`
- `Cache Level`
- `Fixed Height (Pixels)`
- `Height Type`
- `Isolation Mode`
- `Help URL (if exists).`
- `Show 'Open in New Window' Option`
- `Show 'Help' Option`
- `Show 'Personalize' Option`
- `Show 'Refresh' Option`
- `Show 'Remove' Option`
- `Show Name`
- `Show Tray`
- `Tray Type`
- `Cache Validity Period (msecs)`
- `iView width` (if exists)
- `Width Type` (if exists)
- `Authentication Scheme`

5.2.4 Editing Proxy-to-Remote iViews

Proxy-to-remote iViews on the main portal can be customized (edited) by content administrators in the Portal Content Studio, just as other local iViews are.
Only the local properties (see previous section) of the proxy-to-remote iView – and not the corresponding remote iView – are displayed and editable. Customized properties are stored locally with the proxy-to-remote iView on the main portal. For further information, see “Customization and Personalization of iView Properties” on page 10.
Note that customization of proxy-to-remote iViews by administrators at design time should not be confused with personalization of proxy-to-remote iViews by end users at run time. See the previous reference for more information.

Prerequisites

- You must have the appropriate portal permissions to edit an iView.

Procedure

1. On the main portal, navigate to *Content Administration* → *Content*. The Portal Content Studio is displayed.
2. In the Portal Catalog, browse to the iView you want to edit.
3. Right-click the iView, and choose *Edit* → *Object* from the context menu. The Property Editor is displayed, listing the local properties of the proxy-to-remote iView.

   Alternatively, choose a secondary editor from the *Edit* option in the context menu, to modify other aspects of the iView, such as permissions or object-based navigation settings.
4. Perform the necessary changes.
5. Click *Save* to apply your changes.

5.2.5 Preparing Proxy-to-Remote iView Properties for End-User Personalization

When end users personalize proxy-to-remote iViews at run time, they receive two sets of properties they can personalize: (i) the local properties of the proxy-to-remote iView, and; (ii) the local properties of the remote iView. You need to define which properties of each iView (in both proxy-to-remote iView and corresponding remote iView) are personalizable by end users. You may specify if a property is hidden, read-only, or read-write.
This section describes how to define the end-user personalization mode of *local* properties in the proxy-to-remote iView.

> **Note:**
>
> Make sure that the properties of the corresponding remote iView on the remote content provider are also appropriately configured for end user personalization. The procedure described below is identical for the properties in remote iViews. For more details, see “Preparing Remote iView Properties for End-User Personalization” on page 16.

Procedure

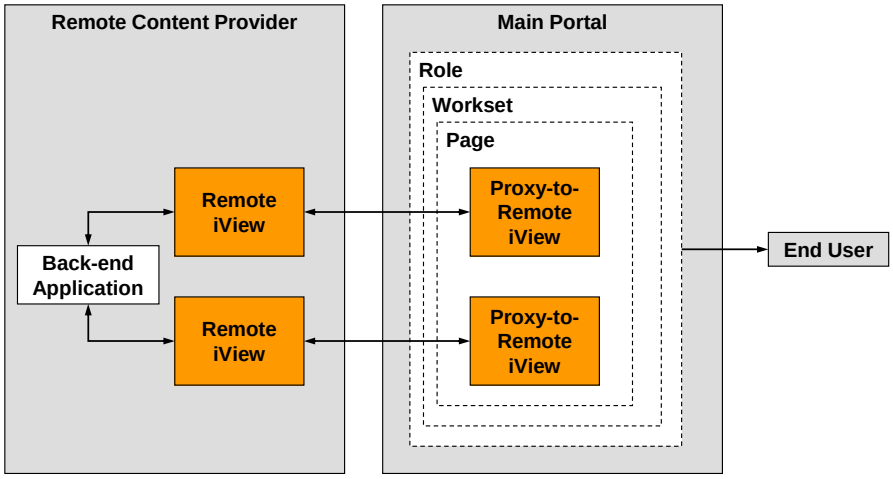
For information on using the Property Editor, see the *SAP Enterprise Portal Administration Guide* → *Portal Platform* → *Content Administration* → *Portal Content Studio* → *Property Editor*.

5.2.6 Integrating Proxy-to-Remote iViews as Content on the Main Portal

Once you have generated the necessary proxy-to-remote iViews, you may begin the task of integrating the proxy-to-remote iViews into a higher content hierarchy of portal pages, worksets, and roles in order to deliver the content to portal end users. Note that if your proxy-to-remote iViews are already assigned to role-based content on the main portal (and you most probably used the Local-to-Remote Conversion tool to convert local iViews to proxy-to-remote iViews), you may skip this section.

> **Important:**
>
> When adding a proxy-to-remote iView, add it as a delta link only; do not add the iView as a copy. For example, in the Page Editor, use the *Add iView to Page* → *Delta Link* action.

The following figure illustrates the typical distribution of iViews, pages, worksets, and roles in the current global portal solution supporting syndicated content. The remote iView is closest to the back-end data application on the remote content provider, while its corresponding proxy-to-remote iView is situated on the main portal and is embedded in a local portal page, which is in turn assigned to a local workset and role.



Typical distribution of iViews, pages, worksets, and roles on the main portal and a remote content provider site

Note that to test the initial content retrieval by a remote iView from its back-end data application and its run-time operation, you may assign remote iViews on the remote content provider to local roles, worksets, and portal pages. However, from a run-time perspective in a global portal environment, the proxy-to-remote iView must be assigned to its own local content. In any case, proxy-to-remote iViews reference only standalone objects in the Portal Catalog (embedded objects are not visible in the Portal Catalog and therefore cannot be selected in the Proxy-to-Remote iView Wizard); standalone objects themselves are not embedded into roles, worksets, and pages. For example, when you embed an iView into a portal page, a delta link iView is automatically generated from the standalone object, and the delta link object is the instance that is embedded into the portal page.
For detailed information on using the necessary portal tools for integrating iViews into portal pages, worksets, and roles, refer to the relevant sections in *SAP Enterprise Portal 6.0 Administration Guide → Portal Platform → Content Administration*.

5.2.7 Notes on Caching

The current global portal solution does not offer a solution-specific caching mechanism to improve performance. You may enable your portal to use the standard caching mechanism of SAP Enterprise Portal or integrate third-party cache management software that effectively supports caching of SAP Enterprise Portal content“
When a user runs any proxy-to-remote iView from the main portal, it triggers its corresponding remote iView to run on the remote portal. If the proxy-to-remote iView is saved in cache on the main portal, the content comes from this cache; otherwise, the request is received from the remote content provider. If the iView is available on the remote portal cache, it comes from there.
Note that the only valid iView cache settings are those defined in the proxy-to-remote iViews, and not those in their corresponding remote iViews. This allows the content administrator to manage the cache settings in one location only: on the main portal. The cache setting in intermediary iViews on the remote content provider is set to *none*, and cannot be modified.

5.2.8 Notes on User Mapping

Since system objects for back-end applications are defined on remote content provider sites, and not on the main portal, a user administrator must perform any necessary user mapping for users, groups, or roles in an organization directly on the remote content provider. See “Setting Up User Mapping” on page 15.

6 End User Tasks

Whether the portal running in your organization is a standard standalone portal or one belonging to a global portal network, end users generally should not notice any difference in the day-to-day run-time operation of the portal. Syndicated iViews display content just as local iViews do. The underlying connectivity for proxy-to-remote iViews is almost completely transparent to end users. The minor differences, which will be apparent to end users when comparing local and remote iViews, are as follows (these are described in more detail in the following sections):

- Proxy-to-remote iViews offer two sets of properties to personalize: local and remote.
- Proxy-to-remote iViews require users to define user mapping for single sign-on in a different user interface.

Note that remote iViews do not necessarily display in the look and display of the portal theme selected by an end user in his or her portal personalization preferences. Since remote iViews are

rendered on a remote content provider site, the default theme assigned to the user on that site is applied.

6.1 Personalizing Proxy-to-Remote iViews at Run Time (by End Users)

Typically, end users should not be able to differentiate between proxy-to-remote iViews and local iViews by just viewing them on their portal desktop. However, when an end user chooses to personalize a proxy-to-remote iView, he or she will notice two differences (as opposed to local iViews) in the user interface of the *Personalization* dialog box:

- A message at the top of the dialog box informs the end user that the iView delivers content from a remote content provider.
- An additional drop-down list, labeled *Properties to Display*, is available.

Note that it is the task of the content administrator to define the availability and level of personalization of each property per iView. For more information, see “Preparing Remote iView Properties for End-User Personalization” on page 16 and “Preparing Proxy-to-Remote iView Properties for End-User Personalization” on page 25.

Procedure

1. Click the iView option menu icon in the iView title and from the menu choose *Personalize*. The *Personalization* dialog box appears.
2. In the *Properties to Display* drop-down list, choose either of the following to toggle the display of properties:
    - *Local:* display the local properties of the proxy-to-remote iView
    - *Remote:* displays the remote properties of the corresponding remote iView
3. Modify the properties you want to personalize, as required.
4. Click *Save All Changes*.

6.2 Mapping User Information to Remote Content (by End Users)

To access and retrieve data from a secure data source through syndicated content in a global portal environment, end users can map logon information (such as user name and password), just as they can with standard local iViews. However, since the iViews actually run on the remote content provider and the systems they are based on do not exist on the main portal, end users must map themselves using an additional mapping tool on the main portal, which is designed specifically for remote content.

User mapping enables single sign-on, which permits end users to provide logon data per secured data source from which the portal retrieves information so that end users are not prompted for logon information every time an iView retrieves data from a secure source.

> **Note:**
>
> Alternatively, portal administrators can predefine user mapping for their end users by doing so directly on the remote content provider site. See “Setting Up User Mapping” on page 15. It is the task of the system administrator to decide, for each system, whether an administrator, end user, or both is able to set the user mapping.

Prerequisites

- The content administrator has given you mapping permission to the target system.
- Your organization has set up a global portal environment with syndicated content.

Procedure

1. In the portal header area, click *Personalize*. A separate window opens and the list of portal preferences you can personalize appears in the navigation panel.
2. Choose *User Mapping (Remote Content)*.

   > **Note:**
   >
   > The standard *User Mapping* option is used to map logon information for local systems. Your portal administrator should be able to provide you with specific information relating to your organization’s system landscape.
3. In the *Remote Content Provider* drop-down list, select the name of the relevant content provider for which you want to enter your user logon credentials.
4. From the *System* drop-down list, select the target system.
5. In the *User* and *Password* fields, enter the system logon definitions. If you are not defined as a user for a system, enter the user name and password of a defined user; you will be mapped to the logon ID of that user.
6. Click *Save* to apply your changes.

   To undo your changes before you have saved them, or to remove the current user and password, click *Clear*.
7. Click *Close* to return to close the window and to the portal.

7 Testing

After setting up your global portal network, you should perform the following steps to test its basic functionality:

1. Create and expose a remote iView on the remote content provider.
2. Create a proxy-to-remote iView on the main portal pointing to the remote iView on the remote content provider.
3. Test the data connectivity between iViews.
4. Test the user mapping functionality on the proxy-to-remote iView.
5. Check functionality that relates to user management and portal permissions.
6. Edit proxy-to-remote iViews.
7. Edit the remote iView and test the proxy-to-remote iView for updates.
8. Test user personalization of the proxy-to-remote iView.

http://www.sdn.sap.com/irj/sdn/howtoguides