SAP NetWeaver '04

Security Guide

Portal Platform Security Guide

Document Version 1.00 – April 29, 2004

SAP AG
Neurottstraße 16
69190 Walldorf
Germany
T +49/18 05/34 34 24
F +49/18 05/34 34 20
www.sap.com

Disclaimer

Some components of this product are based on Java™. Any code change in these components may cause unpredictable and severe malfunctions and is therefore expressively prohibited, as is any decompilation of these components.

Any Java™ Source Code delivered with this product is only to be used by SAP's Support Services and may not be modified or altered in any way.

Documentation in the SAP Service Marketplace

You can find this documentation at the following Internet address:
`service.sap.com/securityguide`

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*.

Icons

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*.

Contents

Portal Platform Security Guide

SAP Enterprise Portal offers users a single point of access to all applications, information, and services needed to accomplish their daily tasks. Links to back-end and legacy applications, self-service applications, company intranet services, and Internet services are all readily available in the user's portal. Because the borders between company intranets and the Internet are blurring, comprehensive security is vital to protect the company's business.

In this guide you will find the following security-related topics:

- The section on authentication [Page 6] describes how authentication is handled in the portal and how to configure the portal for anonymous access.
- Authorizations [Page 24] provides an overview of the authorization concepts in the portal and points you to where you can find more details.
- The following section outlines the different variants of Single Sign-On [Page 25] available in the portal and describes how to set up these variants.
- Finally the section on secure communications [Page 42] provides an overview of the communication channels used in a typical SAP Enterprise Portal installation. It also covers Secure Sockets Layer (SSL) communication with an LDAP directory.

See also SAP Note 702684 for updates to this guide.

1 Authentication

Authentication provides a way of verifying the user's identity before he or she is granted access to the portal. Once the user has been authenticated, he or she is issued a SAP logon ticket that allows him or her to access all the applications, information and services in SAP Enterprise Portal using Single Sign-On. Since many of these applications may contain sensitive data, it is imperative that the user in question can be identified and this identity authenticated.

The process of authentication is based on each user having a unique set of credentials for gaining access. For example, with user ID and password authentication, the authentication server compares a user's authentication credentials with other user credentials stored in a data repository. If the credentials match, the user is granted access to the Enterprise Portal. Otherwise, the authentication fails and portal access is denied.

In the portal, authentication is defined using authentication schemes [Page 7] which are assigned to iViews. Users log on to the portal with a specific authentication scheme and this is stored in the user's logon ticket. If a user needs to access an iView which requires a stronger authentication scheme, he or she must re-authenticate as specified by the stronger authentication scheme.

The portal offers the following authentication mechanisms:

- Authentication with user ID and Password
  - Form-based logon (default authentication method)
  - Basic Authentication
- Authentication with X.509 client certificates [Page 16]
- Windows authentication [Page 18]

In addition, it is possible to configure the portal for anonymous access [Page 19].

To log on to the portal, users must enter the full URL in the browser including the fully qualified domain name, otherwise the browser will not get the correct SAP logon ticket. If the portal is running in the intranet only, you can configure your Web server to change a host name to a full URL.

1.1 Authentication Schemes

Definition

An authentication scheme is a definition of what is required for an authentication process. This includes:

- Type of information used to compute user's identity. For example, user ID and password, client certificate, and so on.
- How user data is checked. For example, against an LDAP directory or an SAP System.
- Validity of user logon, that is, the amount of time after which a user has to log on again.
- Priority, allowing authentication schemas to be ordered.

Use

Authentication schemes allow you to enforce different authentication mechanisms for different content. Each iView is assigned an authentication scheme and only users that have logged on successfully with that authentication scheme or one with a higher priority can access the iView.

In addition, authentication schemes enable pluggable authentication. You can easily ‘plug in’ additional authentication schemes into the portal using modules that adhere to the *Java Authentication and Authorization Service* (JAAS) standard.

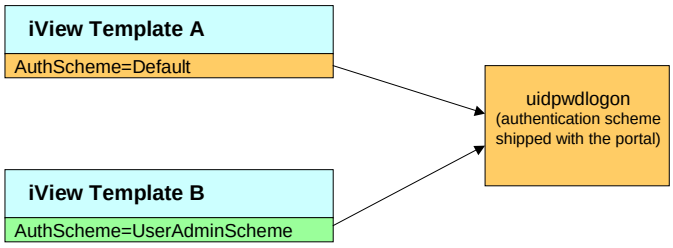
Integration

SAP Enterprise Portal is shipped with a set of authentication schemes [Page 15]. Each shipped iView template is assigned a reference to an authentication scheme. Initially all references to authentication schemes point to the same authentication scheme (Default). If you have special authentication requirements, you can define custom authentication schemes and then change the configuration of the portal so that the references point to your custom authentication schemes. This allows you to change the authentication schemes without having to modify the iViews or iView templates.

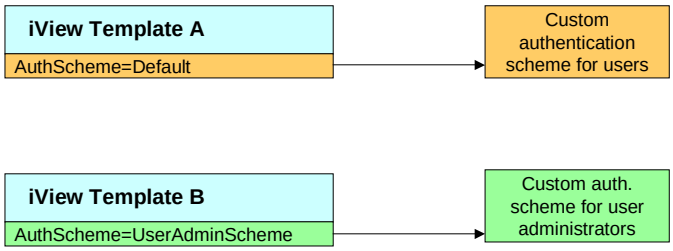
1 Authentication

The following diagram illustrates this concept:

Initial Configuration of Portal



(Optional) Custom Configuration of Portal



For details on changing the references to authentication schemes, see Defining References to Authentication Schemes [Page 12].

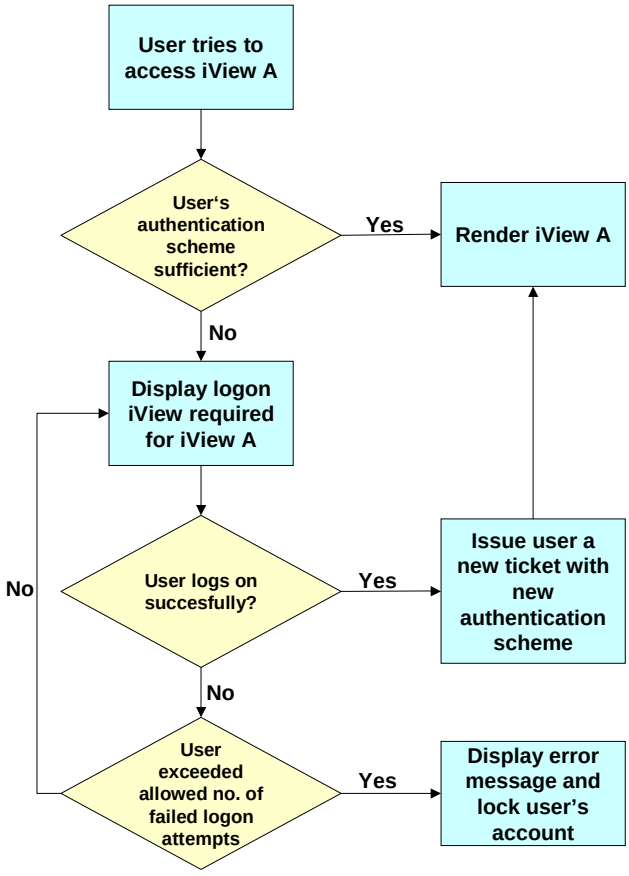
For details on defining new authentication schemes, see Defining an Authentication Scheme [Page 10].

1.1.1 What Happens When a User Logs on to the Portal

When users launch SAP Enterprise Portal, they are required to log on with the authentication scheme that corresponds to the iViews on the first displayed page. If the users satisfy the authentication requirements for the authentication scheme, this information is stored in their logon ticket. If users try to access an iView that requires a ‘stronger’ authentication scheme, the users will have to re-authenticate themselves and will be issued a new logon ticket with the new authentication scheme in it.

For example: The authentication scheme in which users are logged on with a client certificate has a higher priority than an authentication scheme in which users are logged on with user ID and password. This means that users logged on with a client certificate can access all iViews that require an authentication scheme in which users are logged on with user ID and password.
If a user that is logged on with user ID and password tries to access an iView that requires authentication with a client certificate the user will have to re-authenticate and provide a client certificate.

The following diagram illustrates the flow of authentication.



SAP Enterprise Portal is shipped with a set of default authentication schemes. In addition, you can define you own authentication schemes to suit your company’s individual requirements.

1.1.2 Defining an Authentication Scheme

Use

You can define custom authentication schemes if your specific requirements are not covered by the authentication schemes shipped with the portal. You define authentication schemes in the file authschemes.xml [Page 59].

Procedure

Open the file authschemes.xml [Page 59] for modifying as described in Changing the authschemes.xml File [Page 14].

Here is an example of the contents of this file:

```
<document>

    <authschemes>
        <!--  authschemes, the name of the node is used -->
        <authscheme name="uidpwdlogon">
            <!-- multiple login modules can be defined -->
            <authentication-template>
                ticket
            </authentication-template>
            <priority>20</priority>
            <!-- the frontendtype TARGET_FORWARD = 0 -->
            <!-- TARGET_REDIRECT = 1, TARGET_JAVAIVIEW = 2 -->
            <frontendtype>2</frontendtype>
            <!-- target object -->
            <frontendtarget>com.sap.portal.runtime.logon.certlogon
             </frontendtarget>
        </authscheme>


        <authscheme name="certlogon">
            <authentication-template>
                client_cert
            </authentication-template>
            <priority>21</priority>
            <frontendtype>2</frontendtype>
            <frontendtarget>com.sap.portal.runtime.logon.certlogon
             </frontendtarget>
        </authscheme>
        …
    </authschemes>

    <!--  References for Authentication Schemes -->

    <!--  this section must be after authschemes -->
```

```
    <authscheme-refs>
        <authscheme-ref name="default">
            <authscheme>uidpwdlogon</authscheme>
        </authscheme-ref>

        <authscheme-ref name="UserAdminScheme">
            <authscheme>uidpwdlogon</authscheme>
        </authscheme-ref>
    </authscheme-refs>

</document>
```

To define an authentication scheme (`authscheme`), you need to provide the following information:

- Login module stack
- Priority
- Frontend type
- Frontend target

These are described in more detail below.

Authentication Template

In the `<authentication-template>` tag, you define which login module stack in the J2EE Engine controls authentication. The login module stack of the J2EE Engine defines the list of login modules and their control flags (Required, Requisite, Sufficient, Optional) and is defined in the J2EE Engine Visual Administrator. You do not define the logon modules in the `authschemes.xml` file.

For more information on defining login module stacks in the Visual Administrator, see Authentication on J2EE Engine [SAP Library] and Managing Authentication Modules [SAP Library].

For example, you have defined a login module stack called `certlogon` in the Security Provider service in the Visual Administrator. You want to create an authentication scheme that uses this login module stack. To do this, you add the following excerpt to the `authschemes.xml` file.

```
   <authscheme name="myauthscheme">
       <!-- multiple login modules can be defined -->
       <authentication-template>
         certlogon
       </authentication-template>
       <priority>20</priority>
       <!-- the frontendtype TARGET_FORWARD = 0,
            TARGET_REDIRECT = 1, TARGET_JAVAIVIEW = 2
         -->
       <frontendtype>2</frontendtype>
       <!-- target object -->
       <frontendtarget>com.mycompany.certlogonapp
        </frontendtarget>
   </authscheme>
```

Priority

The priority of an authentication must be a positive integer.

```
<priority>20</priority>
```

The higher the integer, the higher the priority of the authentication scheme. Each iView is assigned an authentication scheme and only users that have logged on successfully with that authentication scheme or one with the same or a higher priority can access the iView.

For example, an authentication scheme that requires the user to authenticate using user ID and password has a priority of 10. An authentication scheme that requires the user to authenticate using a client certificate has a priority of 20. If a user has authenticated himself with a client certificate (priority 20) and then tries to access an iView that requires authentication with user ID and password (priority 10) he will not need to re-authenticate himself.

We strongly recommend that if you have two or more authentication schemes that use the login module stack, all these authentication schemes must have the same priority.

Frontend type

In the Enterprise Portal the frontend type must always be 2.

Frontend target

The frontend target defines which iView is to be launched when a user's session does not satisfy the required authentication scheme. Whereas the login module defines how the user is authenticated, the frontend target defines the user interaction that needs to take place to gather the required information.

In addition you may want to define a reference to an authentication scheme. For details, see Defining References to Authentication Schemes [Page 12].

When you are finished editing `authschemes.xml`, save the file and proceed as described in Changing the authschemes.xml File [Page 14].

Result

You have defined a custom authentication scheme and can assign it to iView templates or iViews. For details, see Assigning an Authentication Scheme to an iView [Page 13].

1.1.3 Defining References to Authentication Schemes

Use

A reference to an authentication scheme is a 'pointer' to an authentication scheme. All iViews templates shipped with SAP Enterprise Portal have a property that contains a reference to an authentication scheme. By changing what the reference points to (that is, by modifying a reference to an authentication scheme), you can change the authentication scheme for a whole set of iViews and iView templates without having to change the property in each individual iView or iView template.

Procedure

Open the file authschemes.xml [Page 59] for modifying as described in Changing the authschemes.xml File [Page 14].

The first part of this file contains a list of authentication schemes. At the end of the file you can define references to authentication schemes. The following is an example:

```
<!--  References for Authentication Schemes,
    this section must be after authschemes -->
<authscheme-refs>
    <authscheme-ref name="default">
        <authscheme>uidpwdlogon</authscheme>
    </authscheme-ref>
</authscheme-refs>
```

In the above example, the reference `default` points to the authentication scheme called `uidpwdlogon` that is defined in the same file. All iView templates that are assigned to the authentication scheme reference `default` require the `uidpwdlogon` authentication scheme. By changing `uidpwdlogon` to `basicauthentication`, for example, all the iView templates that are assigned to `default` now require the `basicauthentication` authentication scheme.

When you are finished editing `authschemes.xml`, save the file and proceed as described in Changing the authschemes.xml File [Page 14].

1.1.4 Assigning an Authentication Scheme to an iView

Use

All iViews shipped with SAP Enterprise Portal have an authentication scheme assigned to them. You can change this authentication scheme in the properties of the iView.

Procedure

Use one of the following procedures to assign an authentication scheme to an iView.

Assigning an authentication scheme to an iView or iView template

1. In the portal, choose *Content Administration* → *Portal Content*.

   The Portal Content Studio is displayed.

2. In the Portal Catalog on the left, navigate to the iView that you want to change.
3. Click on the iView with the secondary mouse button and choose *Edit* → *Object*.

   The property editor of the iView is opened in the editing area on the right.

4. In the *Property Category* listbox, choose *Advanced*.

5. Change the *Authentication Scheme* property to either:
   - the name of an authentication scheme
   - a reference to an authentication scheme

   The default value for this property is *default*.
6. Save your changes.

Assigning an authentication scheme to a portal component before uploading it into the portal

1. In the configuration section of the `portalapp.xml` file of the portal component, set the property `AuthScheme` to either
   - the name of an authentication scheme
   - a reference to an authentication scheme

   The following is an example of how to define the authentication scheme in a portalapp.xml file.

```
<component-profile>
    <property name="ForcedRequestCountry" value="">
        <property name="personalization" value="none"/>
    </property>
    <property name="ForcedRequestLanguage" value="en">
        <property name="personalization" value="none"/>
    </property>
    <property name="AuthScheme" value="basicauthentication"/>
</component-profile>
```

2. Save the file.
3. Upload the portal component into the portal.

1.1.5 Changing the authschemes.xml File

Use

You can change the `authschemes.xml` file using the Config Tool of SAP Web Application Server Java. When you edit the file, you should download the file to a local directory, edit it, and when uploading the edited file, create a new node in the configuration tree for it. In this way you do not loose the original version of the file.

Prerequisites

All dispatcher and server nodes in the cluster are shut down.

Procedure

1. Start the Config Tool by executing `<SAPJ2EEEngine_installation>\j2ee\configtool\configtool.bat`.
2. Choose the symbol for *Switch to configuration editor mode*.
3. In the tree, navigate to *cluster_data* → *server* → *persistent* → *com.sap.security.core.ume.service*.
4. To switch to edit mode, choose  (*Switch between view and edit mode*).
5. In the tree, select *authschemes.xml* and choose  (*Show the details of the selected node*).
6. Choose *Download* and save the file to a local directory.
7. Edit the file locally.
8. Create a new node in the configuration tree for the edited file as follows:
   a. Select the node *com.sap.security.core.ume.service*.
   b. Choose the symbol for *Create a node below the selected node* ().
   c. Select the type *File-entry*.
   d. Choose *Upload* and select the file from your local directory.
   e. Enter the name for the entry, for example, **`authschemes_productive.xml`**. By default, the name of the uploaded file is used.
   f. Choose *Create*.
   g. Choose *Close window*.

   The new node appears in the configuration tree.

   For UME to use the new file, you have to change the value of the property `login.authschemes.definition.file` to the name of the new authschemes file. Change the property as described in Editing UME Properties [SAP Library].
9. Restart the nodes in the cluster for the changes to take effect.

1.1.6 Authentication Schemes Shipped with SAP Enterprise Portal

The following authentication schemes are shipped with SAP Enterprise Portal:

Name	Description	Login Module Stack	Referenced by
uidpwdlogon	Requires form-based logon with user ID and password.	ticket	default, UserAdminScheme
certlogon	Requires authentication using client certificates.	client_cert	
basicauthentication	Uses the Basic Authentication feature of the HTTP protocol.	ticket	
header	Allows authentication using external Web access management products.	header	
anonymous	Provides a very basic form of anonymous logon. A logon ticket is **not** issued.		

1.2 Authentication Using Client Certificates

Use

If you require a high level of security, you can use certificate-based authentication through the Secure Sockets Layer (SSL) protocol in your Enterprise Portal. The actual authentication takes place through the SSL protocol between Web browser and Web server, during the so-called SSL handshake. SSL authentication and X.509 certificates use Internet standard technology that provides a higher level of security and eliminates the need for passwords altogether.

Certificate-based authentication provides a high level of security for applications with highly sensitive company data. However, it also requires the company to invest in a public key infrastructure (PKI).

Optionally, users' client certificates can be stored as an attribute of the user on the LDAP directory. To configure this, you must map the relevant attributes. For more information, see Attribute Mapping for Client Certificates [SAP Library].

If users do not have a client certificate in their user data, the portal maps client certificates to portal users. The first time users log on with a client certificate, they must enter their user ID and password. The portal uses this information to map the certificate. Alternatively, administrators can map certificates to a user.

The authentication scheme *certlogon* allows for authentication with client certificates. For more information, see Authentication Schemes [Page 7] and Authentication Schemes Shipped with SAP Enterprise Portal [Page 15].

Prerequisites

- Users have obtained valid X.509 client certificates as part of a public key infrastructure (PKI) and have imported them into their Web browsers.

  The role of the PKI is to verify the identity of certificate owners and to issue, validate, renew, and revoke certificates. If you use X.509 client certificates for authentication, then you need access to a PKI. You can either establish your own PKI or you can rely on a Trust Center for these tasks.

- If users client certificates are stored in the LDAP directory, you have performed the required configuration. For more information, see Attribute Mapping for Client Certificates [SAP Library].

- The browser and portal Web server are configured to communicate using SSL. See the Web server documentation for detailed instructions.

  If you are using the Web server functions of the SAP J2EE Engine, you can find instructions in the document Configuring the Use of SSL on the SAP J2EE Engine [Page 59].

- The portal Web server is configured to trust the Certification Authority (CA) that issued the user certificates. See the Web server documentation for detailed instructions.

  If you are using the Web server functions of the SAP J2EE Engine, you can find instructions in the document Configuring the Use of Client Certificates for Authentication [Page 59].

- The portal Web server is configured to accept client certificates. See the Web server documentation for detailed instructions.

  If you are using the Web server functions of the SAP J2EE Engine, you can find instructions in the document Configuring the Use of Client Certificates for Authentication [Page 59].

Activities

- In user management properties, make sure that the property `ume.logon.allow_cert` is set to TRUE.

  `For more information on setting user management properties, see` UME Properties [SAP Library].

- Each user's client certificate must be mapped to his portal user ID. There are two options for this. Either the administrator maps users' certificates to portal user IDs, or each user maps his or her certificate the first time he or she logs on to the portal that has been set up for certificates. For more information on mapping certificates, see *Enterprise Portal Administrator Guide* → *Portal* → *User Administration* → *User Management Administration Console* → Mapping Client Certificates to Users [SAP Library].

Result

Users log on to the portal using https.

When a user accesses an iView that requires certificate logon (the authentication scheme of the iView is `certlogon`), the browser must present a certificate to authenticate the user. If the presented certificate has not been mapped to a user yet, the user will be prompted for user ID and password. After the user enters user ID and password, the certificate is mapped to that user. The Portal Server authenticates the user and issues an SAP logon ticket to the user. The next time the user logs on with a certificate, he or she will no longer need to enter user ID and password.

1 Authentication

1.3 Windows Authentication

Use

In Windows authentication, authentication of users is delegated to the operating system. You can use the following Windows authentication methods:

Basic Authentication: This authentication mechanism is based on the Basic Authentication feature of the HTTP protocol. The portal user enters his or her existing Windows user name and password into the browser dialog box. The Windows Domain Controller then authenticates the user. This mechanism is typically deployed when the enterprise portal is accessible from the extranet. With this authentication method, the password is transmitted unencrypted, so you should ensure that all connections use SSL.

If you are using basic authentication, we strongly recommended that you set up the browser and portal Web server to communicate using Secure Sockets Layer (SSL). Otherwise users' credentials will be transmitted in clear text.

Integrated Windows authentication (previously known as NT Challenge/ Response): If the enterprise portal is implemented as an intranet portal only, a previously successful logon to the Windows operating system can be reused for automatically logging the user on to the portal. This authentication mechanism is based on Windows security. The user is not required to reenter his Windows authentication credentials again. But in order for this to work, the client must use a Microsoft Internet Explorer browser and be within the same Windows domain as the Web server of the portal.

1.4 Anonymous Logon

Use

Anonymous logon allows users to access the portal in anonymous mode, without providing any form of authentication. For example, if your company sets up an external portal that is accessible through the Internet, you can make anonymous content available to anyone who wants to visit the portal. Using self-registration, visitors can then register themselves as portal users.

Restrictions

Currently SAP Knowledge Management objects do not support anonymous logon.

Integration

Modes of Anonymous Logon

SAP Enterprise Portal provides two forms of anonymous logon:

- **Anonymous logon with named anonymous users (default configuration)**

  This form of anonymous logon uses 'named' anonymous users, which are users that exist either in the user data store or as service users. These users are automatically assigned to the group *Anonymous Users*. You can assign roles containing anonymous content to the users individually or to the group *Anonymous Users*.

- **Simple anonymous logon**

  With this form of anonymous logon there is no physical user in the data store, so, for example, you cannot assign a role containing anonymous content to an anonymous user. As there is no user, a logon ticket is **not** issued.

  If you use simple anonymous logon, there is no current user. This means that personalization functions such as modifying the user's profile are not available.

For anonymous logon the following SAP User Management Engine (UME) properties are relevant:

Property	Value	Description
`ume.logon.anonymous_user.mode`	`1` = Anonymous logon with named anonymous users is used. (Default value) `0` = Simple anonymous logon is used.	Defines which mode of anonymous logon is to be used.
`ume.login.guest_user.uniqueids`	Comma-separated list of user IDs. The default value is `anonymous`.	Only required if `ume.logon.anonymous_user.mode=1`. Defines which users are the named anonymous users. These users automatically belong to the default group *Anonymous Users*.  The administrator has to create these anonymous users in the user data store
`ume.login.guest_user.defaultid` (Optional)	`<no_value>` = The first user in the list for `ume.login.guest_user.uniqueids` is used. `<User ID>`	Defines which anonymous user is used for anonymous logon if the parameter `j_user` in the portal URL is empty.

For more information on how to set these properties, see Editing UME Properties [SAP Library] in the Administration Guide for SAP Web Application Server Java.

With the following example values, the users `anon1`, `anon2`, and `anon3` are defined as anonymous users and, if no user is specified in the portal URL, `anon2` is used for anonymous access to the portal.

Property	Value
`ume.login.anonymous_user.mode`	`1`
`ume.login.guest_user.uniqueids`	`anon1,anon2,anon3`
`ume.login.guest_user.defaultid`	`anon2`

The authentication scheme `anonymous` is shipped with SAP Enterprise Portal to support anonymous logon. See also Authentication Schemes Shipped with SAP Enterprise Portal [Page 15].

Activities

You can define anonymous logon at iView level or at portal level.

- For an example of setting up the **complete portal** for anonymous logon with named anonymous users, see Configuring Anonymous Logon with Named Anonymous Users [Page 21].
- Alternatively you can define an **individual iView** as anonymous content by setting the value of the iView parameter *Authentication Scheme* to `anonymous`. See Assigning an Authentication Scheme to an iView [Page 13]. Users can launch an anonymous iView using the direct URL for that iView without having to provide authentication.

For example, users can call up the self-registration iView directly using the following URL:
`http://<server>:<port>/irj/servlet/prt/portal/prtroot/usermanagementadmin.SelfReg`

1.4.1 Configuring Anonymous Logon with Named Anonymous Users

Use

This procedure describes how to configure the portal for anonymous logon with named anonymous users and using `anonymous` as the authentication scheme. The anonymous users are not issued with a SAP logon ticket.

By setting up anonymous logon with one or more named anonymous users, you can assign roles containing anonymous content to the named anonymous users. You can either assign the roles to the users individually or to the group *Anonymous Users*. If you define more than one anonymous user, you can assign different roles to the different anonymous users and set up different URLs to the portal, allowing you to control the anonymous content that portal users see.

Prerequisites

Check that the user management properties are correctly set

To set up the portal for anonymous logon, the user management properties should be set as follows:

```
ume.logon.anonymous_user.mode=1
ume.login.guest_user.uniqueids=<list_of_anonymous_users>
```

```
ume.logon.anonymous_user.mode=1
ume.login.guest_user.uniqueids=anon1,anon2,anon3
```

Procedure

Create named anonymous users

1. Create the anonymous users that you defined in `ume.login.guest_user.uniqueids`.

   For example, create users with the user IDs `anon1`, `anon2`, and `anon3`.

   After you restart the Java application server, these users are automatically in the *Anonymous Users* group.

Create anonymous content

2. Create a role in which, for all pages and iViews, *Authentication Scheme* is set to `anonymous`.

   By default iViews and pages that are part of the framework page, such as navigation iViews and the framework page itself, are defined as anonymous content, however, if you have created your own versions of these, you must ensure that they are set to the authentication scheme `anonymous`.

   For more information on creating roles, see *Portal Administration Guide → Portal Platform → Content Administration.*

As this role will be available to anonymous users, you should ensure that it does not contain sensitive content, for example administration functions.

Assign anonymous content to anonymous users

3. Assign the anonymous role you created to one of the anonymous users or to the *Anonymous Users* group.

Create a copy of PortalLauncher iView and set its authentication scheme to anonymous

4. Choose *Content Administration* → *Portal Content*.

   The Portal Content Studio appears.

5. In the Portal Content Studio, choose *New from Portal Archive* → *iView*.
6. In the iView Wizard, choose *com.sap.portal.navigation.portallauncher* and continue through the wizard.

   When the wizard is completed, the Property Editor is displayed.

7. In the Property Editor, change the *Authentication Scheme* to `anonymous`.
8. Save your changes.
9. Make a note of the ID of your anonymous PortalLauncher iView.

   For example:
   `pcd:portal_content/myFolder/iViews/com.sap.AnonPortallauncher`

Redirect the portal to the copy of the PortalLAuncher iView

When a user starts the portal using the URL `<server>:<port>/irj`, the URL is redirected to the PortalLauncher iView. You have to change the redirect so that the portal is redirected to the copy of PortalLauncher you just created.

10. On the file server, open the following file:

    ```
    SAP_J2EEngine6.20\cluster\server\services\servlet_jsp\work\jspTemp
    \irj\root\index.html
    ```

    This file contains the following line:

    ```
    <body
    onload="location.replace('servlet/prt/portal/prtroot/com.sap.porta
    l.navigation.portallauncher.default' +
    document.location.search)"></body>
    ```

11. Change this line to the following:

    ```
    <body onload="location.replace('servlet/prt/portal/prtroot/
    <ID_of_anonymous_PortalLauncher>' +
    document.location.search)"></body>
    ```

    For example, if the ID of your anonymous PortalLauncher iView is `pcd:portal_content/myFolder/iViews/com.sap.AnonPortallauncher`, change the line to the following:

    ```
    <body
    onload="location.replace('servlet/prt/portal/prtroot/pcd!3aportal_content!2fmyFolder!2fiViews!2fcom.sap.AnonPortallauncher' + document.location.search)"></body>
    ```

12. Restart the java application server.

Result

When users launch the portal, they are logged on as the first user in the list of anonymous users (in this example, `anon1`). They do not have to provide any form of authentication, unless one of the pages or iViews in the role assigned to the anonymous user is not set to `anonymous`. In this case, a logon screen appears in the page or iView.

A log on link appears in the header area. When the user clicks on this link, the form-based logon screen appears giving users the option to register as portal users.

Possible Variations

Use a specific named anonymous user for anonymous logon

The URLs to access the portal can optionally contain a `j_user` parameter that specifies the user to be used for anonymous logon.

In the following example, the portal is accessed with the anonymous user `anon2`:
`http://<server>:<port>/irj/index.html?j_user=anon2`

2 Authorizations

Authorizations define which objects users can access and which actions they can perform. The portal has an authorization concept that is implemented using permissions, security zones, UME actions, and the *AuthRequirement* property. These are described in more detail below.

- **Permissions**: permissions for all Portal Content Directory (PCD) objects. Portal permissions define portal user access rights to portal objects in the PCD and are based on access control list (ACL) methodology. Essentially, every portal object can be assigned directly to an individual user or collectively to groups of users through user groups and roles. Portal content objects for which you can set permissions are folders (Portal Catalog folders, not role folders), iViews, pages, layouts, roles, worksets, packages, and systems. When any portal user accesses a portal tool that displays portal objects stored in the PCD, those objects are filtered according to the user's access permissions. If a user is permitted to access a portal object, the permission level set for the user defines which actions and operations the user can perform on that object. Permissions also define which objects are available to end users in a runtime portal environment.

  The default permissions assigned to portal objects after installation of the portal only provide a minimum level of security. Before you deploy a test or production portal, we strongly recommend that you carefully plan the reassignment of the default portal permissions to prevent access to the entire PCD by all users. This includes the standard content shipped with the portal and the higher safety levels in the portal security zones.

  For more information on permissions, see *SAP Library* → *SAP NetWeaver* → *People Integration* → *Portal* → *Administration Guide* → *System Administration* → Portal Permissions [SAP Library].

- **Security Zones**: permissions for portal components. A means of implementing an additional layer of security to portal components and services which are accessed by a

URL. Access is controlled by means of progressive safety levels and portal permissions which are assigned to authorized users. Security zones are defined in portal components at the development phase. Portal applications that are not assigned to a security zone can only be accessed via an iView, not a direct URL. Therefore, it is only necessary to define a security zone for portal applications that are not launched via iViews. Information on defining security zones at the code level in portal components is provided in detail in the Portal Development Kit (PDK) documentation, which is available on the iViewStudio at www.iviewstudio.com.

For more information on security zones, see *SAP Library → SAP NetWeaver → People Integration → Portal → Administration Guide → System Administration → Portal Permissions →* Security Zones [SAP Library].

- **UME Actions**: the User Management Engine (UME) equivalent of portal permissions. The User Management Engine verifies that users have the appropriate UME actions assigned to them before granting them access to UME iViews and functions. All other portal services do not use UME actions.

  For more information on security zones, see *SAP Library → SAP NetWeaver → People Integration → Portal → Administration Guide → User Administration →* UME Actions in the Portal [SAP Library].

- **AuthRequirement property**: This is a master iView property used in EP 5.0 that defines which users are authorized to access a master iView or Java iViews derived from a master iView. For backward compatibility with iViews developed for EP 5.0, EP 6.0 supports this property.

  For details on the *AuthRequirement* property, see *SAP Enterprise Portal 5.0 Administration Guide → iViews → Master iViews → Master iView Properties → Portal Component Properties*.

In the portal, roles are only indirectly linked to authorization. Portal roles group together the portal content required by users with a certain role in the company. In addition, the role structure defines the navigation structure that a user sees in the portal. Users and groups assigned to a role inherit the permissions of the role. By default this is end user permission.

3 Single Sign-On

Single Sign-On (SSO) is a key feature of the Enterprise Portal that eases user interaction with the many component systems available to the user in a portal environment. Once the user is authenticated to the enterprise portal, he or she can use the portal to access external applications. With SSO in the Enterprise Portal, the user can access different systems and applications without having to repeatedly enter his or her user information for authentication.

The Enterprise Portal SSO mechanism is available in two variants depending on security requirements and the supported external applications:

- SSO with SAP logon tickets
- SSO with user ID and password

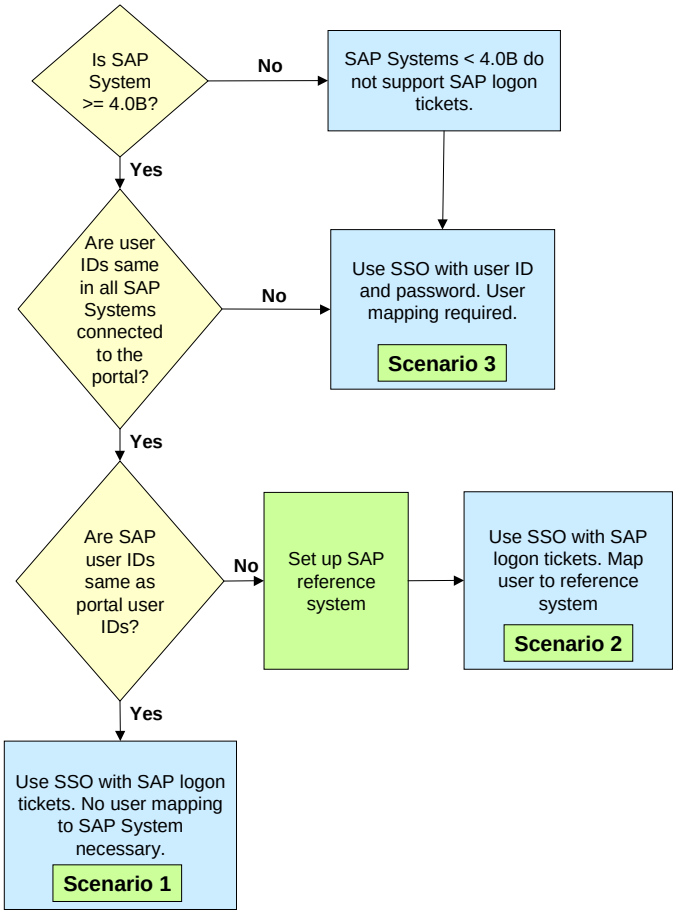
Both variants eliminate the need for repeated logons to individual applications after the initial authentication at the enterprise portal. Whereas SSO with SAP logon tickets is based on a secure ticketing mechanism, SSO with user ID and password forwards the user's logon data (user ID and password) to the systems that a user wants to call.

3.1 Single Sign-On to SAP Systems

3 Single Sign-On

This section summarizes the different scenarios for Single Sign-On to SAP Systems. Which method of Single Sign-On (SSO) you use with a SAP System depends on various parameters, such as the release of the system. There are different prerequisites, for example, users must have the same user ID in all SAP Systems that are accessed via SSO with SAP logon tickets.

The following diagram helps you find out which method of Single Sign-On to use with a specific SAP System.



Scenario 1: Single Sign-On using SAP logon tickets without user mapping

Users must have the same user IDs in all SAP systems that are accessed via SSO with SAP logon tickets. If the SAP user IDs are the same as the portal user IDs, user mapping is not required. You need to perform the following steps:

1. Configure Portal Server for SSO with SAP Logon Tickets [Page 30]
2. Configure SAP Systems to Accept and Verify SAP Logon Tickets [Page 31]

Scenario 2: Single Sign-On using SAP logon tickets with user mapping

If users have different users IDs in the SAP Systems than in the portal, you must define a SAP reference system and map each user's user ID to their user ID in the reference system. You must perform the following steps:

1. Define an SAP Reference System for User Data [Page 27]
2. Configure Portal Server for SSO with SAP Logon Tickets [Page 30]
3. Configure SAP Systems to Accept and Verify SAP Logon Tickets [Page 31]
4. Each user must map his or her user ID to his or her user ID in the SAP Reference System as described in *Enterprise Portal Administration Guide → Portal → User Administration → User Mapping → Mapping Users: User Enters Own Data*.

Scenario 3: Single Sign-On using user ID and password with user mapping

There are two cases where you would use this method of Single Sign-On:

- The SAP System has release 3.1I.
- Users have a different user ID in the SAP System in question than in the reference SAP System used for logon tickets.

You must perform the following step: Configuring SSO with User ID and Password to SAP Systems [Page 40].

3.1.1 Defining an SAP Reference System for User Data

Use

When you use SAP logon tickets for Single Sign-On to SAP Systems, users must have the same user IDs in all SAP Systems that are configured to use SAP logon tickets. If the SAP user IDs are different to the portal user IDs, you must define an SAP reference system. Users then map their portal user ID to the user ID in the SAP reference system.

The mapped user ID is included in the SAP logon ticket and enables Single Sign-On using logon tickets to all SAP Systems in which the user has the same user ID.

Prerequisites

Users have the same ID in all SAP component systems that are configured to use logon tickets for Single Sign-On. Passwords do not have to be identical.

Procedure

Define a system object for the reference system

1. If the system you wish to use as SAP reference system has not yet been defined as a system in the portal, define it as described in *Enterprise Portal Administration Guide → Portal → System Administration → System Landscape → System Landscape Editor → Creating a System Landscape Object*.
2. Ensure that a system alias has been defined for the system. If it does not have a system alias, it will not appear in the user mapping tool.
3. If required, also set the user mapping properties. For details, see *Enterprise Portal Administration Guide → Portal Platform → User Administration → User Mapping → System Properties for User Mapping*.
4. Save your changes.

Define the reference system in the user management configuration tool

5. In the user management configuration tool, choose *Security Settings*.

   For more information on the user management configuration tool, see *Enterprise Portal Administration Guide → Portal Platform → System Administration → User Management Configuration → User Management Configuration Tool.*.
6. In *R/3 Reference System*, enter the system alias of the above system.
7. Restart the Java application server.

Result

When users start the user mapping function, one of the component systems that they can select is the SAP reference system. They can map their portal user ID to their user ID in this reference system. The user mapping function connects to the SAP reference system using the user ID and password to verify that the password entered by the user is correct.

The next time the user logs on to the portal, the portal generates an SAP logon ticket for the user that contains both his or her portal user ID and mapped user ID.

3.2 Single Sign-On with SAP Logon Tickets

Purpose

SAP logon tickets represent the user credentials. The Portal Server issues a logon ticket to a user after successful initial authentication. The logon ticket itself is stored as a cookie on the client and is sent with each request of that client. It can then be used by external applications such as SAP systems to authenticate the portal user to those external applications without any further user logons being required.

SAP logon tickets contain information about the authenticated user. They do not contain any passwords. Specifically, logon tickets contain the following items:

- Portal user ID and one mapped user ID for external applications
- Authentication scheme
- Validity period
- Information identifying the issuing system
- Digital signature

Technically, SSO with SAP logon tickets works as follows:

1. The first time the Portal Server is started, it generates a cryptographic key pair. The private part of this key is used for ticket generation (for the digital signature).
2. Once the user has been successfully authenticated in the portal, the Portal Server issues a logon ticket to the user. This logon ticket is stored as a non-persistent cookie in the browser on the client.
3. Each time the user tries to access an external system from the portal, the Portal Server sends the logon ticket with the request to the external system.
4. The external system checks that the logon ticket is valid by verifying the digital signature of the Portal Server. It uses the public key contained in the digital certificate of the Portal Server to verify this.
5. If the logon ticket is valid, the external system extracts the user ID for that system from the logon ticket.
6. The user is logged on to the external system without having to enter his or her user ID and password.

The Portal Server issues a SAP logon ticket for the Internet domain or a sub-domain of the Portal Server only.

Process Flow

To allow Single Sign-On using SAP logon tickets between the portal and its component systems you must perform the following steps:

1. Configure the Portal Server to allow Single Sign-On with SAP logon tickets. This step is optional, as by default the portal is configured for SAP logon tickets.
2. Configure the component systems to accept and verify SAP logon tickets.

3.2.1 Configuring Portal Server for SSO with SAP Logon Tickets

Use

In the default mode, the Portal Server creates and digitally signs SAP logon tickets for users, therefore you do not need to make any settings. However there are some settings that you need to make in particular cases. These are described below.

Procedure

Configure the lifetime of the SAP logon ticket

You set the lifetime of the SAP logon ticket in the user management configuration tool. For details, see *Enterprise Portal Administration Guide → Portal → System Administration → User Management Configuration → User Management Configuration Tool*.

Map portal user IDs to user IDs in other systems

If users' portal user IDs are different to their user IDs in the component systems, the administrator or user must map the portal user ID to the user ID in the other systems. For details, see *Enterprise Portal Administration Guide → Portal → User Administration → User Mapping*.

If you have several SAP component systems in your portal landscape, and the SAP users have not been synchronized with the portal users, you define a reference system for user data and map the portal users to the users in this system. For more information, see Defining an SAP Reference System for User Data [Page 27].

SAP Systems only: Set logon method to SAP logon tickets in portal system landscape

For each SAP System that you wish to access with SAP logon tickets, do the following:

1. Open the system for property editing as described in *Enterprise Portal Administration Guide → Portal → System Administration → System Landscape → System Landscape Editor → Editing System Properties*.
2. Set the value of the property *Logon Method* to *SAPLOGONTICKET*.
3. Save your changes.

3.2.2 Configuring Component Systems for SSO with SAP Logon Tickets

When a user calls an external application, his or her logon ticket is passed on to the appropriate application or information system where it is checked to see if it is valid. In order to work with SAP logon tickets, the external application has to perform three tasks as follows:

1. The external system has to make sure that a trusted Portal Server has issued the ticket.
2. The digital signature in the ticket of the Portal Server needs to be verified. The first two steps require the digital certificate of the issuing Portal Server.
3. If the ticket is valid, the appropriate user ID contained in it has to be extracted.

This verification procedure is standard in SAP systems. For information on how to configure SAP Systems, see Configuring SAP Systems to Accept and Verify SAP Logon Tickets [Page 31].

Configuring SAP Systems to Accept and Verify SAP Logon Tickets

Use

The Portal Server digitally signs SAP logon tickets as it issues them to the portal users. SAP Systems need to accept the tickets and verify the Portal Server's digital signature. The following information is important for the SAP System to be able to accept and verify SAP logon tickets:

- The SAP System should only accept SAP logon tickets issued from their designated Portal Server. Therefore, the identity of the Portal Server needs to be entered in the SAP System's SSO access control list (ACL).
- The SAP System needs to be able to verify the Portal Server's digital signature. The Portal Server has a self-signed certificate, therefore the SAP System needs access to the Portal Server's public-key information, which needs to be entered in the SAP System's certificate list.

Prerequisites

- The SAP System has Release 4.0B or higher. SAP logon tickets are not supported in releases lower than 4.0B.
- For SAP Systems with Release less than 6.20, the Enterprise Portal Plug-In that corresponds to the Enterprise Portal release must be installed in the SAP System. SAP Systems based on SAP Web Application 6.20 or higher do not require the Plug-In.
- The required kernel patches have been applied to R/3 Systems prior to Release 4.6C. For more information, see the section on implementing new kernels for the SAP Application Server in SAP Note 177895. Note that after applying the kernel patches, you may need to patch the operating system of the R/3 System so that the new kernel works.

- Users must have the same user IDs in all SAP Systems that are accessed via Single Sign-On with SAP logon tickets. If the SAP user IDs are different to the portal user IDs, you must define a SAP reference system. See Defining an SAP Reference System for User Data [Page 27].
- The SAP Security Library is installed on all of the system's application servers. For best practices, we recommend installing the most recent version of the library, which is available on the `sapserv<x>` under `/general/misc/security/SAPSECU/<platform>`.
- You have configured the Portal Server for Single Sign-On with logon tickets. See Configuring Portal Server for SSO with SAP Logon Tickets [Page 30].

Procedure

In SAP systems with Release 4.6C or higher you can use transaction STRUSTSSO2 to complete the first 2 steps of the following procedure. This is described in Using Transaction STRUSTSSO2 in SAP System >= 4.6C [Page 33].

Add Portal Server to ACL of component system

The Portal Server is identified by system ID, client, and the name in the certificate. You must enter these details in the access control list of the component system as follows.

1. In the component system, maintain table *TWPSSO2ACL* with transaction *SM30*.
2. Create a new entry for the Portal Server by choosing *New entries*.
3. Enter the portal's system ID and client. By default, the portal's system ID is the common name (CN) of the Distinguished Name entered during installation of the portal. The default client is 000.

   If necessary, you can change these default values by changing the properties `login.ticket_issuer` and `login.ticket_client` respectively in user management properties.
4. Enter the following values for *Subject name*, *Issuer name*, and *Serial number*.

Field	Value
Subject name	Distinguished name (DN) of owner of portal server certificate. This is the DN that was entered during installation of the portal. For example: `CN=EP6, OU=Portal Installation, OU=Enterprise Portal, O=SAP Trust Community, C=DE`
Issuer name	Distinguished name of issuer of portal server certificate. If the portal is using a self-signed certificate, this is the same as the above entry.
Serial number	00

You can look up the subject name, issuer name, and serial number of the portal server certificate in the Keystore Administration [Page 41] tool.

5. Save your entries.

Import public-key certificate of Portal Server to component system's certificate list

This procedure is release-specific.

- If the SAP component system is based on Release 4.6C or higher, follow the procedure detailed in Importing Portal Certificate into SAP System >= 4.6C [Page 35].
- If the SAP component system is based on Release 4.0B to 4.6B, follow the procedure detailed in Importing Portal Certificate into SAP System < 4.6C [Page 37]

Set profile parameters

On all of the component system's application servers:

1. Set the profile parameters `login/accept_sso2_ticket` = 1 and `login/create_sso2_ticket` = 0 in every instance profile.
2. For Releases 4.0 and 4.5, also set the profile parameter `SAPSECULIB` to the location (path and file name) of the SAP Security Library.

Set ITS service parameters

On each of the ITS servers of the SAP component system, in the global service file `global.srvc` , set the following parameters:

Set the Parameter	To the Value	Comment
~login	(space)	
~password	(space)	
~mysapcomusesso2cookie	1	Enables the user to log on to the system using an existing SAP logon ticket.

Result

The SAP component systems are able to accept SAP logon tickets and verify the Portal Server's digital signature when they receive a logon ticket from a user.

Using Transaction STRUSTSSO2 in SAP System >= 4.6C

Procedure

Download public-key certificate of Portal Server

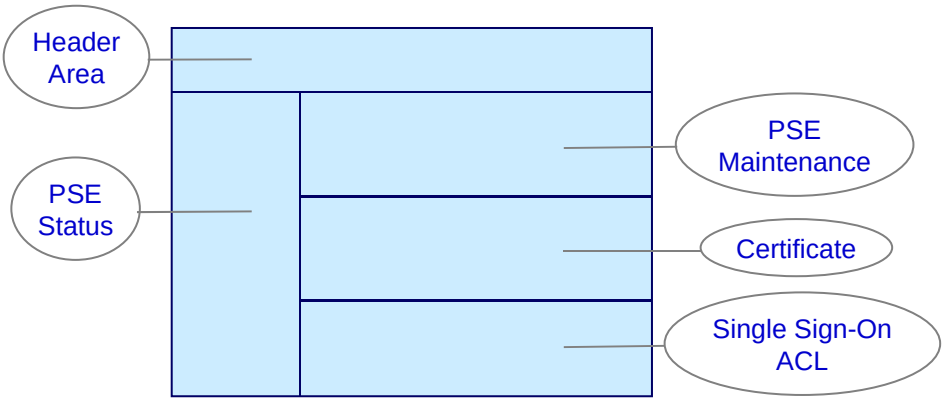
Use the Keystore Administration [Page 41] tool to download the `verify.der` file from the portal.

Import public-key certificate of Portal Server to component system's certificate list and add Portal Server to ACL of component system

Both of these steps can be performed with transaction *STRUSTSSO2*, which is an extended version of transaction *STRUST*. For detailed documentation on transaction *STRUST*, see the Web Application Server documentation under *Security* → *Trust Manager.*

1. In the SAP System, start transaction *STRUSTSSO2*.

   A screen with the following layout appears.



   The **PSE status** frame on the left displays the PSEs that are defined for the system.

   The **PSE maintenance** section on the top right displays the PSE information for the PSE selected in the PSE status frame.

   Below that, the **certificate** section displays certificate information for a certificate that you have selected or imported.

   The **Single Sign-On ACL** section on the bottom right displays the entries in the ACL of the system.

   Note that the layout of the transaction will vary slightly, depending on the release of the SAP System.

2. In the PSE status frame on the left, choose the *system* PSE.
3. In the certificate section, choose *Import Certificate*.

   The *Import Certificate* screen appears.

4. Choose the *File* tab.
5. In the *File path* field, enter the path of the portal's verify.der [Page 59] file.
6. Set the file format to *DER coded* and confirm.

7. In the Trust Manager, choose *Add to PSE*.
8. Choose *Add to ACL*, to add the Portal Server to the ACL list.
9. In the dialog box that appears, enter the portal's system ID and client. By default, the portal's system ID is the common name (CN) of the Distinguished Name entered during installation of the portal. The default client is 000.

   If necessary, you can change these default values by changing the properties `login.ticket_issuer` and `login.ticket_client` respectively in user management properties.

   The other values are taken from the certificate.
10. Save your entry.
11. Do not forget to set profile parameters and ITS service parameters as described in Configuring SAP Systems to Accept and Verify SAP Logon Tickets [Page 31].

Result

The SAP component systems are able to accept SAP logon tickets and verify the Portal Server's digital signature when they receive a logon ticket from a user.

Importing Portal Certificate into SAP System >= 4.6C

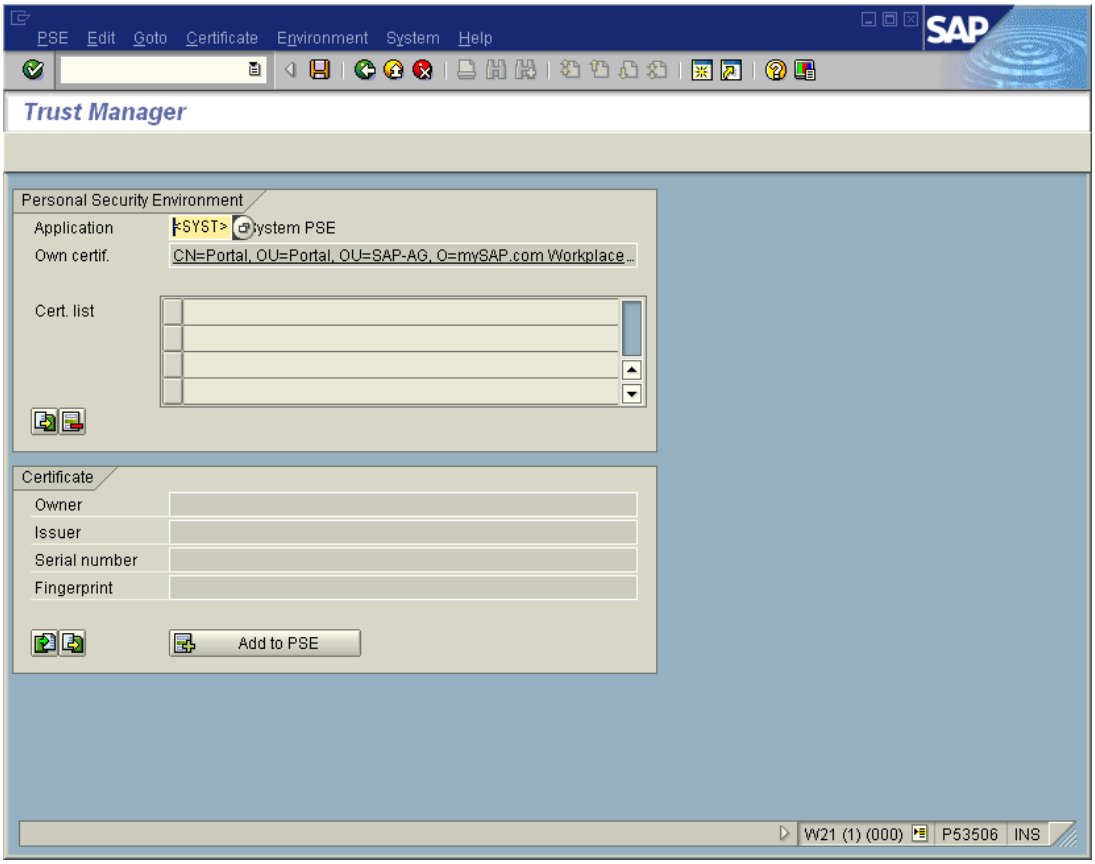
Prerequisites

You have downloaded the public-key certificate of the portal server (`verify.pse` file). Use the Keystore Administration [Page 41] tool for this.

Procedure

1. In the component system, start transaction STRUST.

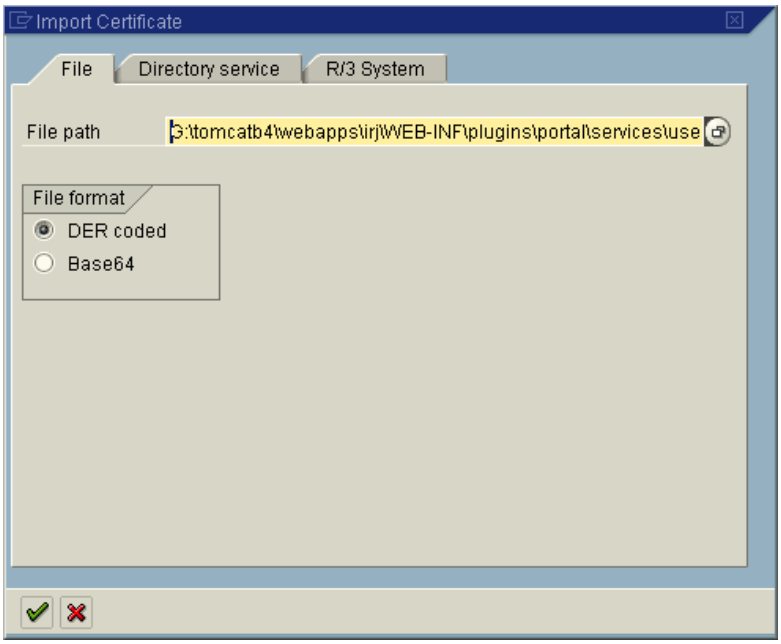
   The following screen appears.



This screen displays a list of the certificates contained in the PSE of the component system.

2. In the certificate group box, choose *Import Certificate*.

   The *Import Certificate* screen appears.



3. Choose the *File* tab.

4. In the *File path* field, enter the path of the portal's verify.der [Page 59] file.
5. Set the file format to DER coded and confirm.
6. In the Trust Manager, choose *Add to PSE*.
7. Save the new certificate list.

The new certificate list is automatically replicated to all application servers in the system. You do not have to import the portal certificate onto each application server separately.

Importing Portal Certificate into SAP System < 4.6C

Check whether there is a file `DIR_PROFILE\SAPSSO2.pse` in the profile directory of the component system. (*DIR_PROFILE* is a profile parameter).

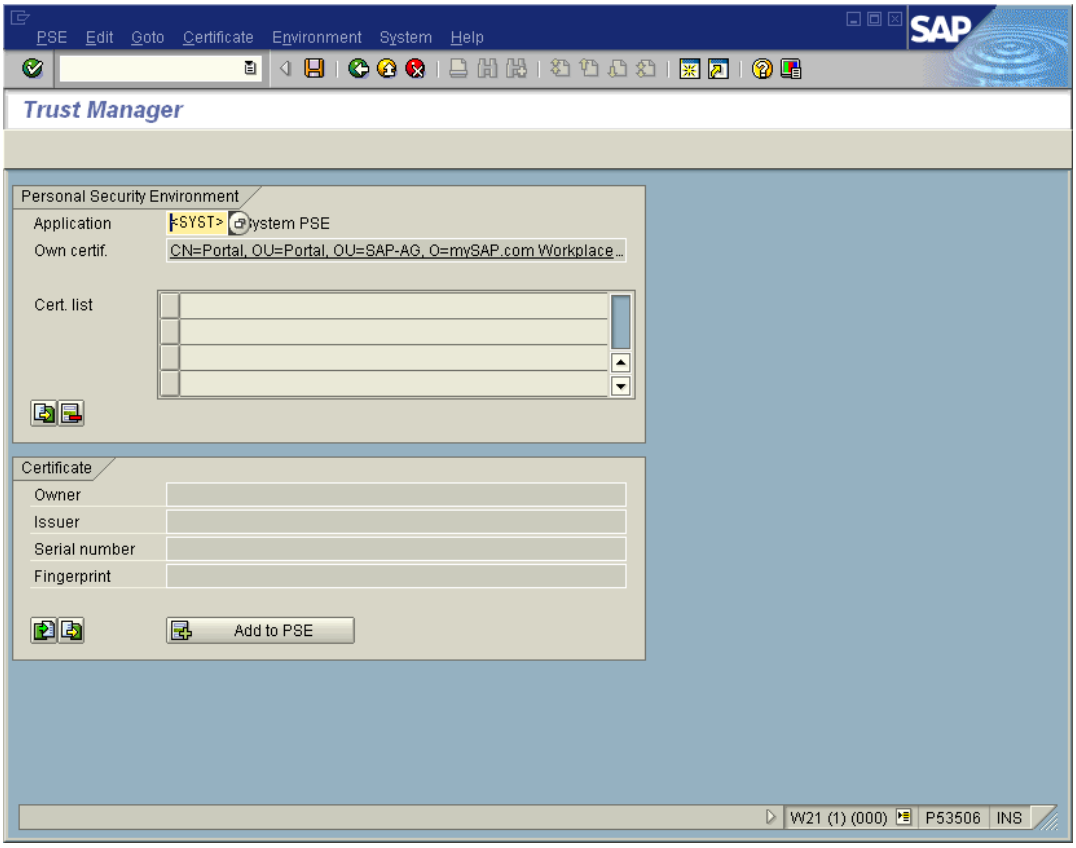
- If not, copy the verify.pse [Page 59] file from the portal into the *DIR_PROFILE* directory of the component system and rename it to `SAPSSO2.pse`. You can download verify.pse using the Keystore Administration [Page 41] tool.
- If yes, check whether it is still needed, for example if there is a current SAP Workplace installation that will still be used after SAP Enterprise Portal is set up. If it is not needed, replace it with the renamed verify.pse [Page 59]. If it is still needed, perform the steps outlined below.

If you need to keep the existing PSE file in your component system

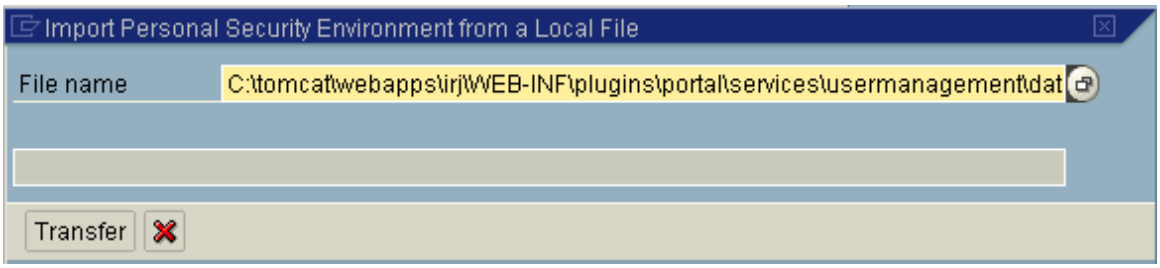
You can use the Trust Manager to import the portal certificate into the existing PSE file. To do this, you need any SAP System with Release 4.6C or higher.

1. In a SAP System with Release 4.6C or higher, start transaction *STRUST*.

   The following screen appears.



2. In the *Application* field, choose <*FILE*>, and enter the path to the SAPSS02.pse file of your component system. Choose *Transfer*.



3. Choose *Import certificate*. Enter `verify.der` from Portal Server.
4. Choose *Add to PSE*.
5. Save the updated SAPSS02.pse.
6. Copy the updated SAPSS02.pse to the *DIR_PROFILE* directory of your component system.

3.2.3 Using More Than One Portal

Use

In some cases you may want to allow two portals to access the same SAP system via Single Sign-On with SAP logon tickets.

Each portal installation is uniquely identified by system ID, client, and the distinguished name in the portal server certificate. If you want to connect two portals to the same SAP system, the combination of these three items must be unique for each portal, so that the SAP System can tell them apart.

The following table provides an overview of distinguished name, system ID, and client. If these values are the same for both portal installations, you will need to change one of the values on one of the portal installations.

	Default value	**How can I change it?**
Distinguished name	Distinguished name entered during installation of the portal.	Create a new portal server certificate (and cryptographic key pair) using the Keystore Administration [Page 41] tool.  If you create a new certificate for a portal installation, you will have to reconfigure Single Sign-On for all backend systems that accept SAP logon tickets.
System ID	Common name (CN) of Distinguished name entered during installation.	Change the value of the `login.ticket_issuer` property in user management properties.
Client	000	Change the value of the `login.ticket_client` property in user management properties.

3.3 Single Sign-On with User ID and Password

Purpose

The Single Sign-On (SSO) mechanism with user name and password provides an alternative for applications that cannot accept and verify SAP logon tickets. With this SSO mechanism the Portal Server uses user mapping information provided by users or administrators to give the portal user access to external systems. The portal components connect to the external system with the user's credentials.

As the user's user ID and password are sent across the network, you should use a secure protocol such as Secure Sockets Layer (SSL) for sending data.

Process Flow

There are different procedures depending on the requirements.

Single Sign-On to SAP Systems

You can access SAP Systems that do not support SAP logon tickets via Single Sign-On with user ID and password. These are SAP Systems with release 3.1I. For more information, see Configuring SSO with User ID and Password to SAP Systems [Page 40].

Single Sign-On to non-SAP systems via a Java iView developed specifically for the customer

The system must be defined in the system landscape. For details, see *Enterprise Portal Administration Guide → Portal → System Administration → System Landscape → System Landscape Editor → Creating a System Object*.

The administrator or user must map user data to user data in the system. For more information, see *Enterprise Portal Administration Guide → Portal → User Administration → User Mapping*.

The iView through which the user tries to access the system must be programmed to get the mapped user data from the data repository and write the user credentials (user ID and password) in a header field of the request. The system can then log on the user with these credentials. This can be done using the Java APIs provided with SAP Enterprise Portal.

3.3.1 Configuring SSO with User ID and Password to SAP Systems

Use

This procedure describes how to configure SAP Enterprise Portal and a SAP System for Single Sign-On with user mapping. In general we recommend using Single Sign-On with SAP logon tickets or client certificates. Single Sign-On with user ID and password should only be used if no other Single Sign-On method is possible. It has the following advantages:

- It can be used for Single Sign-On to SAP Systems that do not support SAP logon tickets (that have a release lower than 4.0B).
- You do not have to have Central User Administration (CUA) in place. Users can have a different user ID and password in the SAP System in question than in the reference SAP System used for the logon ticket.

When Single Sign-On with user ID and password is used, the user ID and password are transmitted in plain text using HTTP POST. We strongly recommend that you protect the connections to the SAP System using HTTPS or SNC to prevent the user ID and password being eavesdropped by an external party.

Procedure

1. In the system object defining the SAP System in the portal, set the property *Logon Method* to *UIDPW*. For more information on defining system objects, see *Enterprise Portal Administration Guide → Portal Platform → System Administration → System Landscape*.
2. Either the administrator or the users must map users' user ID and password to their user ID and password in the SAP System. For more information on user mapping, see *Enterprise Portal Administration Guide → Portal Platform → User Administration → User Mapping.*

Result

When the user tries to access the SAP System through the portal, the user mapping information is used to access the component system

3.4 Keystore Administration

Use

The keystore administration tool allows administrators to download the `verify.der` and `verify.pse` files which contain the Portal Server's certificate.

The keystore administration tool only contains *TicketKeystore* which contains the private and public key of the Portal Server and its certificate. You manage all other keystores using the Key Storage service in the Visual Administator. Certificates of Certification Authorities (CA) that the portal trusts are stored in the *TrustedCAs* keystore.

Integration

The keystore administration tool is based on the portal component *com.sap.portal.usermanagement.admin.KeystoreComponent*. This component is included in the *System Administration* role.

Features

With the keystore administration tool you can:

- View contents of `TicketKeystore`
- Import certificates into `TicketKeystore`
- Download portal server certificate (`verify.der`) as a ZIP file
- Download all certificates trusted by the portal in PSE form (`verify.pse`) as a ZIP file

Activities

Accessing Keystore Administration

In the portal, choose *System Administration* → *System Configuration* → *Keystore Administration.*

Using Keystore Administration

Activity	Action
View contents of `TicketKeystore`	Choose *Content*.
Import certificates of trusted entities into `TicketKeystore`	1. Choose *Import Trusted Certificate*. 2. Browse to the certificate file. The file must be in DER format. PSE format is not supported. 3. Enter an alias for the certificate. The alias must have less than 150 characters and may not contain double quotation marks ("), dollar signs ($), braces ({, }), spaces, and asterisks (*). 4. Choose *Upload*.
Download `verify.der` or `verify.pse`.	1. Choose *Content*. 2. Scroll to the bottom of the screen. 3. Choose *Download verify.der File* or *Download verify.pse File* as required.

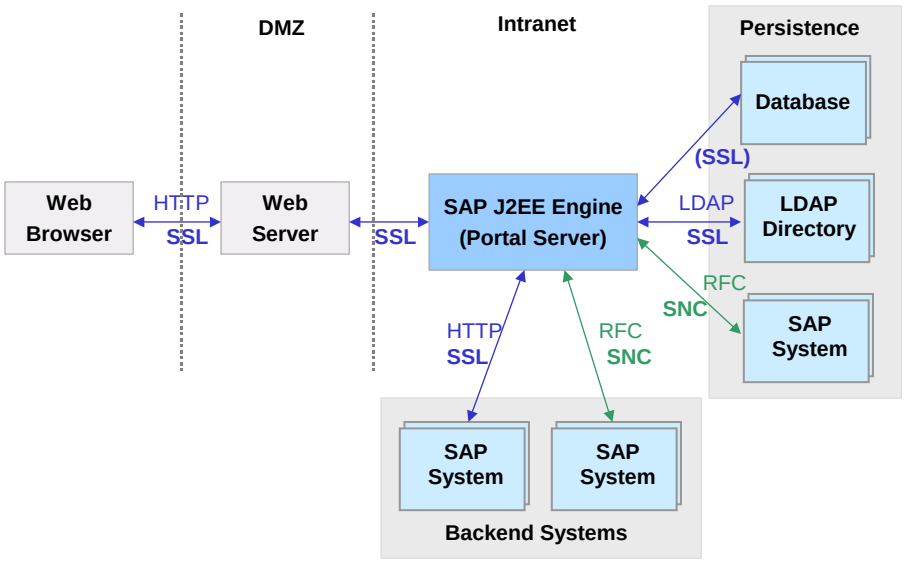
4 Secure Communications

Protecting the information transferred between the client and the Portal Server and between the internal components of the SAP Enterprise Portal is important. The data transferred contains authentication credentials and possibly other sensitive data that must not be known to third parties. This kind of data must be encrypted using secure communication protocols such as Secure Sockets Layer (SSL) or Secure Network Communications (SNC).

We recommend that you protect all communication channels used during normal operation of the SAP Enterprise Portal.

4.1 Communication Between Internal Components

The following diagram provides an overview of the communication channels between the components of the Enterprise Portal.



This diagram displays a secure network architecture where a Web server is placed in a demilitarized zone (DMZ) in front of the Portal Server. It is also possible to have a network architecture in which the client communicates directly with the Portal Server.

The Portal Server uses a database to store portal-related data such as content objects. It can use any combination of database, LDAP server and SAP System to store user management data. As user-related data is sensitive data, you should protect all communication channels to user data stores.

There are also communication channels between the Portal Server and any backend systems used for providing content to display in the portal. Depending on the nature of the data passed from the backend systems to the Portal Server, these communication channels should also be protected. For example, the Portal Server can connect to SAP Systems using the remote function call (RFC) protocol. These connections can be secured using Secure Network Communications (SNC).

The following table gives you a quick overview of where to find detailed documentation on securing the communication channels shown in the diagram.

Connection	Secure Protocol	Documentation
Web browser ↔ SAP J2EE Engine	Secure Sockets Layer (SSL)	See the document Configuring the Use of SSL on the SAP J2EE Engine [Page 59] or, if you are using an intermediary server such as an IIS, see Using SSL With an Intermediary Server [Page 59].
Portal Server ↔ Database	SSL	No documentation currently available.
Portal Server ↔ LDAP Directory	SSL	No documentation currently available.
Portal Server ↔ SAP System	Secure Network Communications (SNC)	Configuring SNC Between User Management Engine and SAP System [Page 46]

Unification Server

If you are using unification in your portal installation, we recommend that you configure SSL to the Unification Server. For details, see the section on *Secure Sockets Layer Support* in the *SAP Unification Server Administration Guide.*

4.2 Communication with Backend Systems

We also recommend that you configure secure communications to application servers accessed in the back end by SAP Enterprise Portal components. For example, if an iView accesses a backend ERP System via HTTP, you need to configure Secure Sockets Layer (SSL) on this connection.

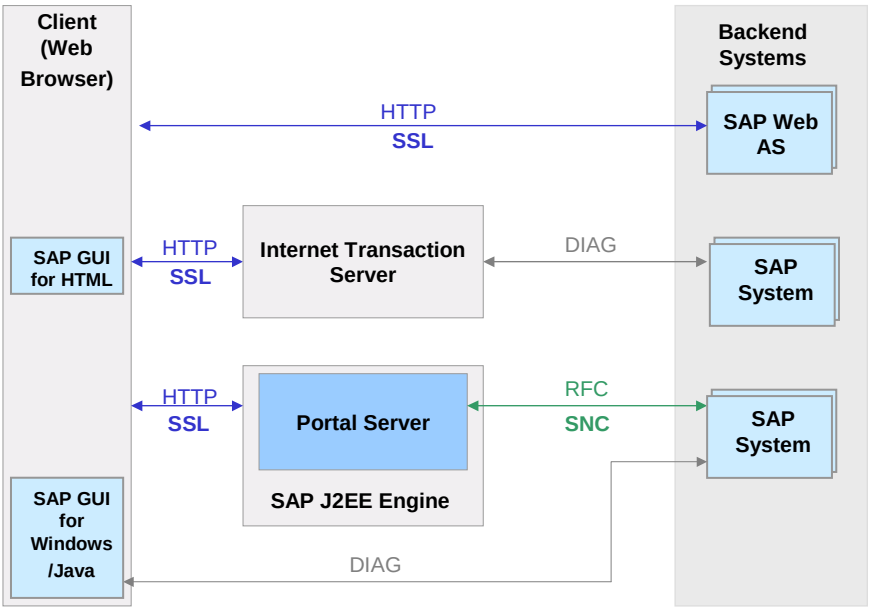
Communication with SAP Systems in the Back End

The portal's iView technology allows you to integrate a broad range of SAP applications, such as:

- R/3 transactions
- Business Server Pages (BSPs)
- Business Warehouse (BW) reports
- Internet Application Components (IACs)
- MiniApps

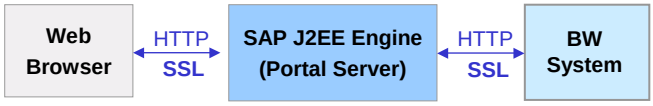
In each of these cases, the portal needs to connect to the SAP system in the back end to retrieve the required data and (in some cases) user interface.

The following diagram illustrates how SAP Enterprise Portal connects to SAP systems.



For most iViews that integrate SAP applications, the corresponding SAP systems are accessed via HTTP or HTTPS connections. This is the case for BSPs, IACs, MiniApps, BW reports, and Web R/3 transactions that use SAP GUI for HTML. For example, if the browser sends a request to the portal server with a URL for an iView that integrates an IAC, the portal server converts the URL into a URL to the Internet Transaction Server (ITS) containing all the parameters that the ITS requires, such as the ID of the SAP system, the ID of the IAC, user information, and so on. It sends this URL to the browser, which redirects the URL to the ITS. The ITS then gets the data that it requires from the SAP system through a DIAG connection and finally sends a HTTP(S) response to the browser. There is no direct connection between the portal server and the SAP system in the backend.

If the portal is set up to run BW reports in caching mode, then the process is slightly different. When the portal server receives a request for a BW report, it sends a request via HTTP to the BW system. When the BW system sends its response, the portal server caches it, before sending it to the browser. In this case, there is a direct HTTP connection between the portal server and the BW system. This is illustrated in the following diagram.



In the case of iViews that integrate R/3 transactions using SAP GUI for Windows or SAP GUI for Java, the browser accesses the SAP system using a DIAG connection.

If SAP systems are accessed through iViews that use the SAP Java Connector (JCo) to access the SAP System, the system is accessed via remote function calls (RFC).

If sensitive data, such as passwords, financial information, or data that underlies particular legal protection, is being sent over these connections, we recommend that you secure the connection. The following table provides an overview of the communication channels and where to find the relevant documentation.

Connection	Protocol	Documentation
Web browser ↔ Web Application Server	HTTP or HTTPS	Configuring the Use of SSL on the SAP J2EE Engine [Page 59]
Web browser ↔ Internet Transaction Server	HTTP or HTTPS	SNC User's Guide [Page 59]
Portal Server ↔ SAP System	RFC or Secure Network Communication (SNC)	SNC User's Guide [Page 59]
SAP GUI for Windows/Java ↔ SAP System	DIAG – can be protected using SNC	SNC User's Guide [Page 59]

If you have set up a network architecture with one or more firewalls and your portal integrates iViews for BSPs, IACs, MiniApps, BW reports, and so on, you need to set up a direct access in the firewall between the client machine and the ITS or WAS.

Communication with Databases in the Back End

The portal provides an iView wizard framework for creating iViews over database applications via a JDBC provider. The wizard enables you to build a data query based on a function predefined in the database, or based on a customized query.

If the database in the back end is a Microsoft SQL server, it must be set up for authentication based on SQL *Server and Windows NT* mode (mixed mode). If it is set up for *Windows only* mode, the connection does not work.

4.3 Configuring SNC Between User Management Engine and SAP System

Use

This section describes how to configure Secure Network Communications (SNC) on connections between SAP User Management Engine (UME) and SAP Systems. You can use this procedure to activate SNC both on connections between UME and an SAP System that it uses as a persistence store and between UME and SAP Systems to which UME replicates user data.

We strongly recommend that you protect these types of connections with SNC as sensitive user data is passed over these connections.

The following procedure applies both for UME integrated with SAP Enterprise Portal and used as a standalone component with other solutions. It describes a scenario where the SAP Cryptographic Library is used as the security product.

You have a choice between the following two scenarios for configuring the use of SNC between UME and an SAP System:

- You can create a single Personal Security Environment (PSE) that is shared by UME and the SAP Systems by copying it to each of the server hosts. This option is better if you have only one UME and one SAP System, for example, in a test environment. It is the simpler option.
- You can create individual PSEs for each of the system components. This option is more complicated to configure, but is recommended if you intend to configure UME for SNC with several SAP Systems.

The configuration steps for both of these scenarios are described below. This documentation focuses on configuration required in UME. For detailed documentation on how to configure the SAP System, see:

- SNC *User's Guide*: This guide provides a full description of how to use SNC with SAP Systems. You can find this guide on the SAP Service Marketplace at: *http://service.sap.com/security* → Security in Detail → *Secure System Management.*
- SAP Web Application Server documentation at *SAP Web Application Server → Security (BC-SEC) → Secure Network Communications (BC-SEC-SNC).*

Prerequisites

- You must be able to receive the SAP Cryptographic Library as stated by the German export regulations. The library is available on the SAP Service Marketplace at http://service.sap.com/swcenter.
- You must know your SNC naming convention and the SNC names for the application server and UME.

The server may use additional PSEs for other purposes, for example, UME also has a PSE that it uses to digitally sign SAP logon tickets. To avoid naming conflicts, use a unique Distinguished Name for UME's SNC PSE.

Procedure

Depending on the scenario you use, see either:

- Configuring SNC When Using a Single PSE [Page 48]
- Configuring SNC When Using Individual PSEs [Page 48]

4.3.1 Configuring SNC When Using a Single PSE

Purpose

In this case, you create a single PSE that is used by both SAP User Management Engine (UME) and the SAP System application server. If the SAP System already has an SNC PSE you can copy this PSE to UME. Otherwise you create a new PSE on UME and copy it to the SAP System.

Prerequisites

The SAP R/3 System is already SNC-enabled. For details, see the *SNC User's Guide*, which you can find on the SAP Service Marketplace at http://service.sap.com/security → *Security in Detail* → *Secure System Management.*

Process Flow

1. Make sure that the SAP Cryptographic Library is available on the host on which UME is installed. If it is not available, install it [Page 49].
2. Set the `SECUDIR` environment variable to the location in which you wish to store the SNC PSE file. Then restart the UME host.
3. If the SAP System already has an SNC PSE file, copy the file to the UME machine [Page 50]. Otherwise, create a PSE file for UME [Page 50] and copy it to the SAP System application server to the directory defined in the `SECUDIR` environment variable.
4. Create credentials for UME [Page 52].
5. Set SNC properties for SAP System in User Management Engine [Page 55].
6. Configure the SAP R/3 System [Page 57] to allow an SNC protected connection with UME.

4.3.2 Configuring SNC When Using Individual PSEs

Purpose

In this case, you generate a separate PSE for the application server and SAP User Management Engine (UME) and exchange their public keys so that the two components can communicate with each other using SNC.

Prerequisites

The SAP R/3 System is already SNC-enabled. For details, see the *SNC User's Guide*, which you can find on the SAP Service Marketplace at http://service.sap.com/security → *Security in Detail* → *Secure System Management.*

Process Flow

1. Make sure that the SAP Cryptographic Library is available on the host on which UME is installed. If it is not available, install it [Page 49].
2. Set the `SECUDIR` environment variable to the location in which you wish to store the SNC PSE file. Then restart the UME host.
3. Create a PSE file for UME [Page 50].
4. Create credentials for UME [Page 52].
5. Exchange the servers' public-key certificates [Page 53].
6. Set SNC properties for SAP System in User Management Engine [Page 55].
7. Configure the SAP R/3 System [Page 57] to allow an SNC protected connection with UME

4.3.3 Step-By-Step Procedures

In the following section, you can find step-by-step instructions for the different steps required to configure SNC between SAP User Management Engine and a SAP System.

Installing SAP Cryptographic Library

Prerequisites

You have access to the SAP Cryptographic Library.

Procedure

Copy the SAP Cryptographic Library (`sapcrypto.dll`) for your platform, the configuration tool (`sapgenpse.exe`), and the corresponding license ticket (`ticket`) to local directories on the machine on which User Management Engine is installed.

You can download the Cryptographic Library from the SAP Service Marketplace at *http://service.sap.com/swcenter* → *SAP Cryptographic Software* → *SAP Cryptographic Library <your platform>* using your customer user ID. See also SAP Note 397175.

Copying SAP System's PSE to UME (Single PSE)

Prerequisites

- The SAP System already has an SNC PSE.
- On the SAP User Management Engine (UME) host, the environment variable `SECUDIR` is set to the location where the PSE is stored.

Procedure

1. Export the SAP System's SNC PSE using transaction *STRUST*.
2. Copy the exported PSE to the `SECUDIR` directory on the UME machine.

Creating PSE for UME

Use

Use the command `get_pse` to generate a PSE for SAP User Management Engine (UME). This PSE includes the public and private key pair and a public-key certificate. If you are using a trusted CA, then you can also use the `get_pse` command to generate a certificate request. The following procedure describes how to create a PSE with a self-signed certificate.

Prerequisites

- The SAP Cryptographic Library is installed on the UME host.

Procedure

1. On the UME host, set the `SECUDIR` environment variable to the location where you want to store the PSE file by entering the following at the command line prompt:

   ```
   set SECUDIR=<path_to_PSE_file>
   ```

   We suggest that you store the PSE in the same directory in which you installed the SAP Cryptographic library:

   ```
   <DRIVE>:\snc\SAPCryptoLib
   ```

Example:

```
set SECUDIR=C:\snc\SAPCryptoLib
```

As an alternative, you can change to the desired directory and set `SECUDIR` as indicated below:

```
cd C:\snc\SAPCryptoLib
set SECUDIR=.
```

By using this technique, you can avoid problems such as case-sensitivity or shortened directory names in Windows that use the tilde character (~).

2. Use the command line tool `sapgenpse` to create a PSE by entering the following at the command line prompt:

   ```
   sapgenpse get_pse -p <pse_file> -noreq -x <PIN>
   <Distinguished_Name>
   ```

   where

Parameter	Description	Allowed Values
`<pse_file>`	Path and file name for UME's PSE.	Path description (in quotation marks, if spaces exist)
`<Distinguished_Name>`	Distinguished Name (DN) for the server. The Distinguished Name is used to build UME's SNC name.	Character string (in quotation marks, if spaces exist). The DN must be in the following format: `CN=<common_name>, OU=<organizational_unit>, O=<organization>, C=<country>.` The DN used for the SNC PSE must be different to the DN used for the certificate for signing logon tickets.
`<PIN>`	PIN that protects the PSE	Character string

```
sapgenpse get_pse -p c:\snc\SAPCryptoLib\UME.pse –noreq –x
abcpin "CN=UME, OU=MYCOMPANY, O=SAP-AG, C=DE"
```

This generates a PSE file located at `c:\snc\SAPCryptoLib\UME.pse` which includes a public key, private key and self-signed certificate. For details on the `sapgenpse.exe` tool, see the SAP Web Application Server documentation at *SAP Web Application Server → Security (BC-SEC) → Secure Network Communications (BC-SEC-SNC) → Configuring the Use of the SAP Cryptographic Library for SNC → Configuring SNC for Using the SAPCRPYTOLIB Using SAPGENPSE*

Result

UME's PSE is created in the directory you specified.

Check the contents of the directory at the operating system level to make sure the PSE was created in the correct location before proceeding with the next step.

Creating Credentials for UME

Use

To be able to access its PSE at run-time, SAP User Management Engine (UME) requires active credentials, which you create by using the configuration tool to "open" UME's PSE.

The credentials are located in the file `cred_v2` in the directory specified in the environment variable `SECUDIR`. Make sure that **only the user under which the J2EE Engine runs** has access to this file (including read access).

It is also very important to create the credentials for the **user who runs the J2EE Engine's processes**.

Prerequisites

- The server possesses a PSE and you know where it is located.
- You know the user that runs the J2EE Engine's processes.

  If you are unsure which user this is, see Checking the Java Servlet Engine's User [Page 53]. Make sure that **only this user** has access to the credentials file!
- The environment variable `SECUDIR` is set to the location where the PSE is stored for the user under which the servlet engine is running.

Procedure

1. Open a shell and go to the `SECUDIR` directory (make sure the `SECUDIR` environment variable is active).
2. Enter the following at the command line prompt to open the server's PSE and create credentials:

   ```
   sapgenpse seclogin –p <PSE_name> -x <PIN> -O <J2EE_Engine_user>
   ```

   where

Parameter	Description	Allowed Values
`<PSE_name>`	Path and file name for the server's PSE	Path description (in quotation marks, if spaces exist)
`<PIN>`	PIN that protects the PSE	Character string
`<J2EE_Engine_user>`	User for which the credentials are created. (The user that the servlet engine is running under). If you are unsure which user this is, see Checking the Java Servlet Engine's User [Page 53].	

```
sapgenpse seclogin -p UME.pse –x abcpin -O SYSTEM
```

In this example, the command opens the UME's PSE that is located in the `SECUDIR` directory in the file `UME.pse`, and creates credentials (`cred_v2`) for the user `SYSTEM` in the `SECUDIR` directory. The PIN that protects the PSE is `abcpin`.

3. Adjust the file permissions for the PSE (`<file_name>.pse`) and credentials file (`cred_v2`) so that the server's user can access them at run-time.

Result

The credentials file (`cred_v2`) for the user specified with the `-O` option is created in the `SECUDIR` directory. This user can then access the credentials at run-time.

Checking the Java Servlet Engine's User

Use

Use this procedure to determine which user the Java servlet engine of the Portal Server uses to run its processes so that you can create credentials for the correct user.

Procedure

On the Portal Server machine:

1. Choose *Start* → *Control Panel* → *Administrative Tools* → *Services*.

   The *Services* screen appears.

2. Select the service for the Java servlet engine. For SAP J2EE Engine, the service is called *SAP J2EE Engine.*

3. Right-click on the service and choose *Properties* → *Log On*.

   The *Properties* screen for the service appears.

   - If *Local System Account* is selected, then the user used by the Java servlet engine to run its processes is SYSTEM.
   - Otherwise, the user used by the Java servlet engine to run its processes is the user displayed in the *This Account:* field.

Exchanging the Servers' Public-Key Certificates

Use

Use the following procedure if each server possesses an individual PSE. In this case, you must exchange the servers' public-key certificates so that they can identify each other using SNC. You must import the partner's certificates on each host for each set of communication partners.

For details on the `export_own_cert` and `maintain_pk` options of the configuration tool, see SAP Web Application Server documentation at *SAP Web Application Server* → *Security (BC-SEC)* → *Secure Network Communications (BC-SEC-SNC).*

Prerequisites

- Both SAP User Management Engine (UME) and the SAP System application server possess their own PSE and you know where they are located.
- SECUDIR has been set to the location where the credentials are to be stored.

Procedure

On the UME host:

1. Export UME's public-key certificate by executing the following configuration tool command line:

```
sapgenpse export_own_cert -o <output_file> -p <PSE_name>
[-x <PIN>]
```

The following command line exports UME's certificate and stores it in the file UME.crt in the directory in which you called the command:

```
sapgenpse export_own_cert -o UME.crt -p UME.pse -x abcpin
```

2. Make the certificate available to the SAP System application server. For example, copy it to a shared directory in the file system.

On one of the SAP System application server hosts:

3. Export the application server's public-key certificate by executing the following configuration tool command line:

```
sapgenpse export_own_cert -o <output_file> -p <PSE_name>
[-x <PIN>]
```

The following command line exports the application server's certificate and stores it in the file D:\usr\sap\ABC\DVEBMGS28\sec\ABC.crt:

```
sapgenpse export_own_cert -o D:\usr\sap\ABC\DVEBMGS28\sec\
ABC.crt -p D:\usr\sap\ABC\DVEBMGS28\sec\ABC.pse -x abcpin
```

4. Make the certificate available to UME. For example, copy it to a shared directory in the file system.

On each of the SAP System application server hosts:

5. Import UME's certificate into the application server's certificate list using the following configuration tool command line:

```
sapgenpse maintain_pk [<additional options>] [-a <cert_file>]
[-d <number>] -p <PSE_name> [-x <PIN>]
```

The following command line imports the previously exported UME's certificate (now located at D:\usr\sap\ABC\DVEBMGS28\sec\UME.crt) into the application server's certificate list:

```
sapgenpse maintain_pk -a
D:\usr\sap\ABC\DVEBMGS28\sec\UME.crt -p
D:\usr\sap\ABC\DVEBMGS28\sec\ABC.pse -x abcpin
```

On the UME host:

6. Import the application server's certificate into UME's certificate list using the following configuration tool command:

```
sapgenpse maintain_pk [<additional options>] [-a <cert_file>]
[-d <number>] -p <PSE_name> [-x <PIN>]
```

The following command line imports the previously exported application server's certificate (now located at `c:\SAP_J2EEEngine6.20\SAPCryptoLib\ABC.crt`) into UME's certificate list:

```
sapgenpse maintain_pk -a
"c:\SAP_J2EEEngine6.20\SAPCryptoLib\ABC.crt" -p
"c:\SAP_J2EEEngine6.20\SAPCryptoLib\UME.pse" -x abcpin
```

Result

The two servers have exchanged their public-key certificates so that they can identify each other when using SNC connections.

Setting UME Properties for SNC

Use

To activate the SNC connection between SAP User Management Engine (UME) and an SAP System, you must set properties relating to the SAP System in the UME properties file, `sapum.properties`.

For details on how to change user management properties, see *SAP Enterprise Portal Administration Guide → Portal → System Administration → User Management Configuration → User Management Properties.*

Procedure

1. In the UME properties file, add the following properties to the properties already maintained for the SAP System:

Property Name	Description
`ume.r3.connection.<adapterID>.user`	Service user in SAP System. For more details, see Requirements for Service User Used to Connect to SAP Systems [Page 56].
`ume.r3.connection.<adapterID>.snc_lib`	Location of cryptographic library.
`ume.r3.connection.<adapterID>.snc_myname`	SNC name of SAP User Management Engine. This is the distinguished name in the UME PSE in the following format: `p:<distinguished_name_of_UME_PSE>`

Property Name	Description
ume.r3.connection.<adapterID>.snc_partnername	SNC name of SAP System. This is the distinguished name in the SAP system's SNC PSE in the following format: p:<distinguished_name_of_R/3_PSE>
ume.r3.connection.<adapterID>.snc_mode	To activate SNC, this must be set to 1.

The default value for <adapterID> is master, however you can change it by assigning a different value to the property ume.logon.r3master.adapterid. For example,
ume.logon.r3master.adapterid=ABC

The following is an example of an excerpt of sapum.properties:

```
ume.r3.connection.master.client=123
ume.r3.connection.master.r3name=ABC

ume.r3.connection.master.user=sapjsf2
ume.r3.connection.master.snc_lib=c:\snc\SAPCryptoLib\sapcrypto.dll
ume.r3.connection.master.snc_myname=p:CN=UME, OU=MYOU, O=MYCOMPANY,
C=DE
ume.r3.connection.master.snc_partnername=p:CN=ABC, OU=MYOU,
O=MYCOMPANY, C=DE
ume.r3.connection.master.snc_mode=1
```

Requirements for Service User Used to Connect to SAP Systems

To connect from SAP User Management Engine (UME) to an SAP System using RFC (with or without Secure Network Communications), you need to specify a service user with which to establish the connection. You must create this service user in the SAP System and it must fulfill the requirements listed below.

- **User ID:** We recommend that you use the user ID SAPJSF_<SAPSID_of_SAP_Web_AS_Java> for the service user. You can use any password.
- **User Type:** The user must be of type *communication user* (or *CPIC* in older releases).

- **Authorization:** The user requires authorizations for read access to user data, for authenticating remote users, and RFC authorizations.

  As of Release 6.20, SAP Web Application Server is shipped with two roles that provide the required authorizations:

  - *SAP_BC_JSF_COMMUNICATION_RO* provides all authorizations for read access to user data, for authenticating remote users, and several low-level RFC authorizations.
  - *SAP_BC_JSF_COMMUNICATION* is the same as the above role, but additionally provides authorization to modify and delete all user-related data.

  We recommend using *SAP_BC_JSF_COMMUNICATION_RO*.

- **SNC name:** If the connection is secured with SNC, the user must be assigned to the SNC name used by the SAP System. To do this, in transaction SU01, on the SNC tab, enter the SNC name of the SAP System. You can find the SNC name of the SAP System in table USRACL.

See Also:

For SAP Systems with release higher than or equal to 6.20, see *Integration of the Security Functions of the ABAP Stack and J2EE Stack*. You can find this document on SAP Service Marketplace at http://service.sap.com/security → *Security in Detail -> Hot Topic: J2EE*.

Configuring SAP R/3 System for SNC

Use

Use this procedure to configure the SAP R/3 System to allow an SNC protected connection with SAP User Management Engine (UME).

Prerequisites

The SAP R/3 System is already SNC-enabled. For details, see the *SNC User's Guide*, which you can find on the SAP Service Marketplace at http://service.sap.com/security → *Security in Detail* → *Secure System Management.*

Procedure

There are two types of access control lists (ACLs) that you need to maintain in the SAP R/3 System: a system ACL and a user ACL.

Add UME SNC Name to System Access Control List

After you add the UME SNC name to the system ACL, the SAP R/3 System allows UME to establish an SNC protected connection to the SAP System application server.

1. In the SAP R/3 System, start table maintenance for table VSNCSYSACL (for example, use transaction SM30, enter the table name, and choose *Maintain*).
2. For *Type of ACL entry* enter *E*.
3. Choose *New entries*.

4. Enter data in the fields as follows:

Field Name	Entry	Comments
System ID	Leave this field blank	
SNC Name	p:<distinguished_name_of_ UME_PSE>	The distinguished name is the one you specified when you created the PSE for UME [Page 50]. This entry should have the same value as `ume.r3.connection.master.snc_myname` in the UME properties file [Page 55].

5. Activate the *Entry for RFC activated* indicator.
6. Save your entries.

Add UME SNC Name to User Access Control List

This allows portal users to connect to the SAP System using UME's SNC connection. The users themselves are explicitly authenticated at connection time.

1. In the SAP R/3 System, start table maintenance for table USRACLEXT (for example, use transaction SM30, enter the table name, and choose *Maintain*).
2. Choose New entries.
3. Enter data in the fields as follows:

Field name	Entry	Comments
User	asterisk symbol (*)	The wildcard entry allows all users to be able to connect to the SAP system using the SNC protected connection from UME.
Seq. number		Not required
SNC name	p:<distinguished_name_of_ UME_PSE>	The distinguished name is the one you specified when you created the PSE for UME [Page 50]. This entry should have the same value as `ume.r3.connection.master.snc_myname` in the UME properties file [Page 55].

4. Save your entries.

4.3.4 Troubleshooting

If you experience problems with the SNC connection, do the following:

- Check whether the `SECUDIR` environment variable is set correctly.
- If you have SECUDE PSE management on the computer, log off (otherwise the two credentials may interfere with each other).
- Check that you created credentials for the correct user.
- Set the `TRACE` option for the JCo connection by entering the following in the UME properties file, `sapum.properties`:

  ```
  ume.r3.connection.<adapterID>.trace=1
  ```

  The RFC layer will then create log files called `dev_rfc.trc` and `rfc_XXXXX_XXXXX.trc` (where `X` denotes a digit).

5 User Management and Security Files

Files used by user management and security components

File description	Where to find it
Propertysheet com.sap.security.core.ume.service Contains configuration parameters for user management and security	These files are stored in the configuration store of SAP Web Application Server Java. You can view and modify them using the Config Tool. For more information, see *SAP Library* → *SAP NetWeaver* → *Security* → *Identity Management* → *User Management Engine* → *UME Configuration* → Editing UME Properties and Files [SAP Library].
authschemes.xml Contains definition of authentication schemes available in the portal.	
verify.der Certificate of the Portal Server in DER format.	You can download these files using the Keystore Administration [Page 41] tool in the portal.
verify.pse Certificate of the Portal Server in Secude PSE format. Includes any certificates that were imported into ticketKeyStore.	

6 Documentation References

The following table lists external documentation referenced in the Security Guide and indicates where to find the documentation.

Document Name	Location
Configuring the Use of SSL on the SAP J2EE Engine	*SAP Library* → *SAP NetWeaver* → *Application Platform (SAP Web Application Server)* → *J2EE Technology in SAP Web Application Server* → *Administration Manual* → *Server Administration* → *SAP J2EE Engine Security* → *Transport Layer Security on the SAP J2EE Engine* → Configuring the Use of SSL on the SAP J2EE Engine
Configuring the Use of Client Certificates for Authentication	*SAP Library* → *SAP NetWeaver* → *Application Platform (SAP Web Application Server)* → *J2EE Technology in SAP Web Application Server* → *Administration Manual* → *Server Administration* → *SAP J2EE Engine Security* → *Authentication on J2EE Engine* → *Using Client Certificates for User Authentication* → Configuring the Use of Client Certificates for Authentication
Using SSL With an Intermediary Server	*SAP Library* → *SAP NetWeaver* → *Application Platform (SAP Web Application Server)* → *J2EE Technology in SAP Web Application Server* → *Administration Manual* → *Server Administration* → *SAP J2EE Engine Security* → *Transport Layer Security on the SAP J2EE Engine* → Using SSL With an Intermediary Server
SNC User's Guide	**`service.sap.com/security`** → Security in Detail → Secure System Management → SNC User's Guide.