SAP Sourcing 9.0

# Security Guide

May 2015

# Table of Contents

# 1 Introduction

**Caution**

This guide does not replace the administration or operation guides that are available for productive operations.

## 1.1 Target Audience

- Technology consultants
- System administrators

This document is not included as part of the Installation Guides, Configuration Guides, Technical Operation Manuals, or Upgrade Guides. Such guides are only relevant for a certain phase of the software life cycle, whereas the Security Guides provide information that is relevant for all life cycle phases.

### 1.1.1 Why Is Security Necessary?

With the increasing use of distributed systems and the Internet for managing business data, the demands on security are also on the rise. When using a distributed system, you need to be sure that your data and processes support your business needs without allowing unauthorized access to critical information. User errors, negligence, or attempted manipulation on your system should not result in loss of information or processing time. These demands on security apply likewise to the SAP Sourcing application. To assist you in securing the SAP Sourcing application, we provide this Security Guide.

### 1.1.2 About this Document

The Security Guide provides an overview of the security-relevant information that applies to the SAP Sourcing application.

#### 1.1.2.1 Overview of the Main Sections

The Security Guide comprises the following main sections:

- **Before You Start**
  This section contains information about why security is necessary, how to use this document and references to other Security Guides that build the foundation for this Security Guide.
- **Technical System Landscape**
  This section provides an overview of the technical components and communication paths that are used by SAP Sourcing.
- **User Administration and Authentication**
  This section provides an overview of the following user administration and authentication aspects:
  - User types that are used in the SAP Sourcing application.
  - Standard users that are delivered with SAP Sourcing.
  - Overview of the user synchronization strategy.
  - Overview of how integration into Single Sign-On environments is possible.
- **Authorizations**
  This section provides an overview of the authorization concept that applies to SAP Sourcing.
- **Network and Communication Security**
  This section provides an overview of the communication paths used by SAP Sourcing and the security mechanisms that apply. It also includes our recommendations for the network topology to restrict access at the network level.
- **Security Logging and Tracing**
  This section provides an overview of the trace and log files that contain security-relevant information.
- **Appendix**
  This section provides references to further information.

# 1.2 Before You Start

## 1.2.1 Fundamental Security Guides

SAP Sourcing is deployed on the SAP NetWeaver Java Application Server. Therefore, the corresponding Security Guides also apply to SAP Sourcing. Pay particular attention to the most relevant sections or specific restrictions as indicated in the table below.

| Scenario, Application or Component Security Guide | Most Relevant Sections or Specific Restrictions |
|---|---|
| *SAP NetWeaver 7.3 Security Guide* (help.sap.com SAP NetWeaver → **SAP NetWeaver 7.3** → Security Information) | Network and Communication Security, Data Storage |

**Note**

For a complete list of the available SAP Security Guides, see the SAP Service Marketplace at service.sap.com/security and click the *Security Guides* link.

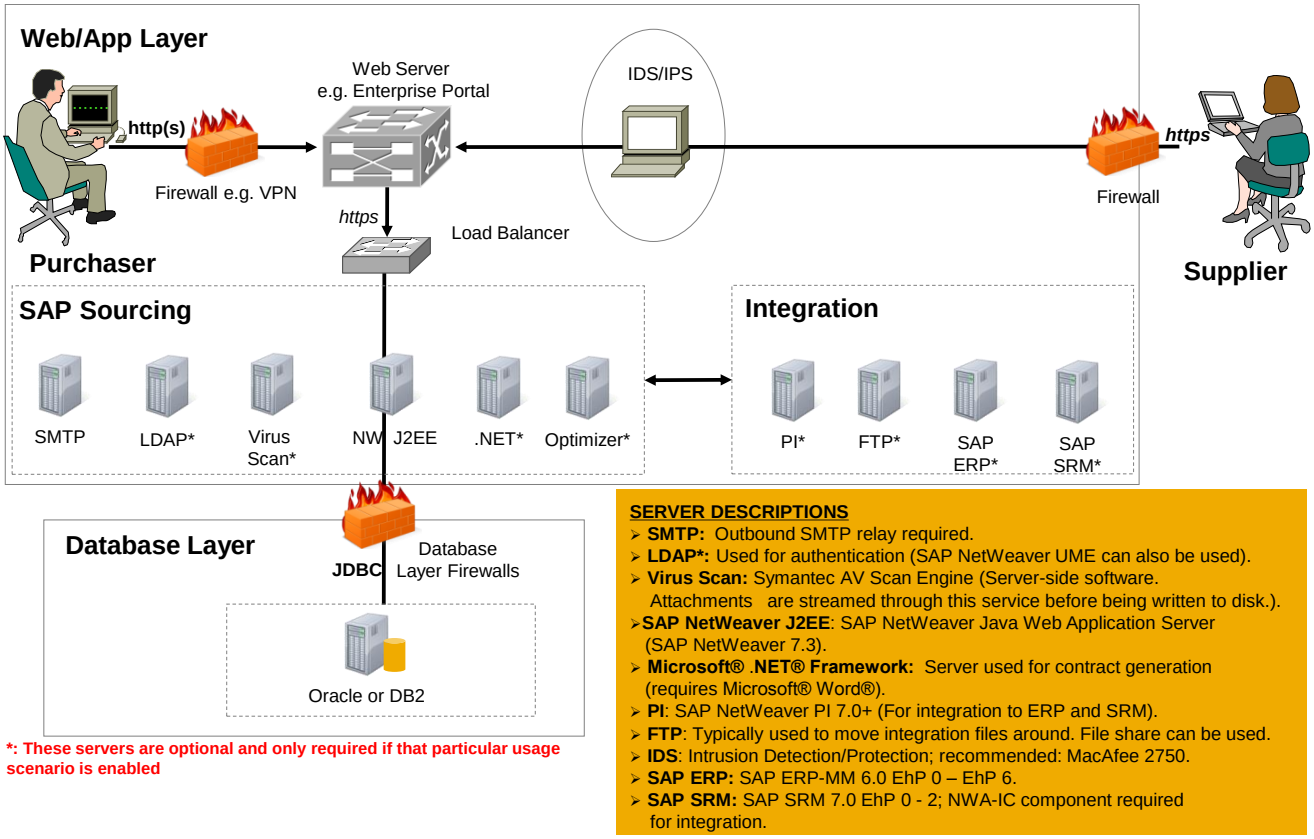
## 1.2.2 Additional Information

For more information about specific topics, see the addresses on the SAP Service Marketplace as shown in the table below.

| Content | SAP Service Marketplace Address |
|---|---|
| Security | service.sap.com/security |
| Related SAP Notes | service.sap.com/notes |
| Released platforms | service.sap.com/platforms |
| Network security | service.sap.com/security |
| SAP Solution Manager | service.sap.com/solutionmanager |

# 1.3 Technical System Landscape

The figure below shows an overview of the technical system landscape for SAP Sourcing.




For more information about the technical system landscape, see the resources listed in the table below.

| Topic | Guide / Tool | Quick Link to the SAP Service Marketplace |
|---|---|---|
| Technical description for SAP Sourcing and the underlying components such as SAP NetWeaver | Master Guide | service.sap.com/instguides |
| Security | Information about security at SAP | service.sap.com/security |

# 1.4 User Administration and Authentication

SAP Sourcing provides multiple mechanisms for user administration and authentication to allow for customizable solutions.

SAP Sourcing users can be integrated with the user management and authentication mechanisms provided with the SAP NetWeaver platform, in particular SAP NetWeaver Application Server Java, 7.3, and the User Management Engine (UME) functionality it provides. SAP Sourcing uses the programmatic authentication method as supported by SAP NetWeaver UME. Therefore, ***most*** of the security recommendations and guidelines for user administration and authentication as described in the *SAP NetWeaver Application Server Java Security Guide* also apply to SAP Sourcing. For more information about user administration and authentication in SAP NetWeaver 7.3, see the SAP Library at help.sap.com, or more specifically http://help.sap.com/saphelp_nw73ehp1/helpdata/en/37/ef19f99d514fc486209421f4253dfb/frameset.htm.

**Note**

Please note that authorization for SAP Sourcing is **not** managed by the SAP NetWeaver UME module. This type of loosely coupled integration provides an opportunity to allow you to manage user administration from within SAP Sourcing.

In addition to the guidelines in the *NetWeaver Application Server Java Security Guide*, information and options about user administration and authentication related to SAP Sourcing is provided in the sections listed below:

- User Management
  This topic lists the tools to use for user management, the types of users required, and the standard users that are delivered with SAP Sourcing.
- User Data Synchronization
  SAP Sourcing can be configured to share user data with other sources such as SAP NetWeaver. This topic describes how the user data is synchronized with these other sources.
- Single Sign-On User Authentication
  This topic describes how SAP Sourcing supports Single Sign-On mechanisms.
- User Impersonation
  Allows one user to log on as another user.

**Note**

In addition, see the SAP Sourcing configuration guides in the SAP Library at help.sap.com. Use the navigation path: *SAP Business Suite* → *SAP Sourcing* → “List of All Configuration Guides”.

## 1.4.1 SAP Sourcing Authentication Using SAP NetWeaver User Management Engine (UME)

### 1.4.1.1 Recommended Landscape

The recommended setup for SAP Sourcing in the standard scenario using the tools and setup described in the technical landscape to ensure extensibility with user authentication and single sign-on is to use the landscape below.

The setup, shown below, using SAP NetWeaver UME for authentication, provides support for a wide variety of active directories. SAP NetWeaver UME provides a standard stackable authentication architecture.

The recommended SAP Sourcing setup landscape appears in the figure below:

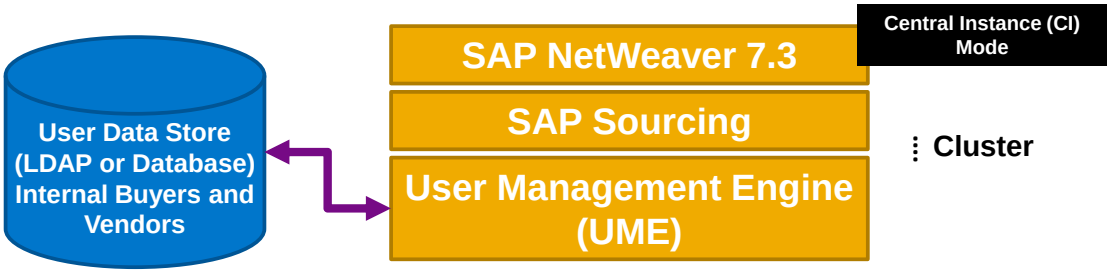



**Figure 1: Recommended SAP Sourcing Landscape**

#### 1.4.1.2 Authentication Using SAP NetWeaver UME

The following describes SAP Sourcing authentication using SAP NetWeaver UME:

- SAP NetWeaver UME is used for user authentication for both buyers and vendors
- You can maintain a user data store in SAP Sourcing or the SAP NetWeaver UME datastore, which supports LDAP and various databases, and so on.
- A SAP Sourcing-specific active directory or other user repository is not required with this configuration, unless there is a very serious need to keep the internal and external users separate.

  **Recommendation**

  If you need to keep the buyer and vendor user repositories separate and isolated, then we recommend that you use SAP NetWeaver UME for internal users, and use a supported SAP Sourcing active directory for the vendor user data store.

- User synchronization occurs using the defined protocol in the directory configuration functionality in SAP Sourcing. For more about directory configuration, see the SAP Sourcing online help.
- SAP NetWeaver needs to be in central instance (CI) mode.
- User authorization profiles are still maintained in SAP Sourcing.
- SAP NetWeaver instances can be clustered.
- A specific external role needs to be entered in the directory configuration which matches a role to which users are assigned in SAP NetWeaver UME. For more information about external roles, see the section "Working with External Roles".

## 1.5 User Management

User management for SAP Sourcing is performed inside the SAP Sourcing application.

### 1.5.1 User Administration Tools

The user administration tools that you can use depend on the authentication method that you are using.

The table below shows the tools to use for user management and user administration with the SAP Sourcing application.

| Tool | Detailed Description |
|---|---|
| SAP Sourcing | The administration of SAP Sourcing users must be done in the SAP Sourcing application. Depending on the details of the configuration, it may be necessary to also administer users in the SAP NetWeaver Administrator. Consult the SAP NetWeaver Security Guide for documentation. |
| SAP NetWeaver Administrator | This is applicable only when SAP NetWeaver UME is being used as the driver. Administration of SAP NetWeaver UME is done in the SAP NetWeaver Administrator. Consult the SAP NetWeaver Security Guide for documentation. |

| Tool | Detailed Description |
|---|---|
| Identity Provider's user management tool | If SAML 2.0 is used as the authentication mechanism, users should be managed on the Identity Provider's (IdP) side as well as on the SAP Sourcing side. Since SAP Sourcing can be used with different IdPs, a tool that should be used for user management on the IdP side depends on the specific Identity Provider. For example, for the SAP NetWeaver IdP the SAP Identity Management or the SAP NetWeaver Administrator can be used to perform user management tasks. |

## 1.5.2 User Types

SAP NetWeaver allows special types of users to be created, such as technical users. If SAP Sourcing is configured to be able to create SAP NetWeaver users, they will always be created as the default user type. All other types of users must be provisioned in SAP NetWeaver separately.

## 1.5.3 System-Defined Users

SAP Sourcing has special system-defined users. Each instance of SAP Sourcing has one user with the user name `system`. Each tenant has a user with the user name `enterprise`.
It is recommended to only use the system-defined accounts when absolutely necessary. Each user should have his or her own regular user account and should not share his or her password. These user accounts should always be used, whenever possible.
The system user and the enterprise user each have a separate login URL that can be independently blocked from being accessed over the internet. These users are needed to configure some parts of the application. Once the application is configured and master data is set up, it is recommended to lock down access as these users. The passwords for these accounts should be changed and the passwords locked away in case they are needed for an emergency.

**Note**

The system user can reset the password of an enterprise user, if necessary.

These user account types are created by default, and the user credentials and attributes are held in a special user store within SAP Sourcing.
The access to each system and enterprise user account can only be through special contexts which have been provided. For more information, see the SAP Sourcing Installation Guide in the SAP Library at help.sap.com. Use the navigation path: *SAP Business Suite → SAP Sourcing*.

**Note**

For security reasons, the first time these accounts are accessed, the user is asked to change the default passwords.

**Caution**

These users have unlimited administrative permissions in the SAP Sourcing application. Therefore, we recommend that you set sufficiently strong password and auditing policies for all users.

### 1.5.3.1 Resetting the System Password

The following instructions reset the system password to "manager".

1. Set a temporary password by adding the following line to the ***<sourcing home directory>/config/fcilocal.properties*** file:

   system.tmp.system.password=<temp password>
2. Run the Dbimporter script ***fciinstall.jar → scripts/product/reset_system_password.xml*** and enter the temporary password.
3. Close the DBimporter and remove the extra line in the ***fcilocal.properties*** file.

## 1.6 User Data Synchronization

User data synchronization is configured in the SAP Sourcing directory configuration by mapping SAP Sourcing user data fields with SAP NetWeaver UME attributes. Along with each mapping, the synchronization mode is configured to either push or pull. When set to **`push`**, the user field can be edited in SAP Sourcing and any changes to that field will be written to the SAP NetWeaver UME attribute. When set to **`pull`**, any changes made to the SAP NetWeaver UME attribute will be replicated to the SAP Sourcing user field, when the user data is synchronized.

The following table shows the mapping attributes between SAP Sourcing and SAP NetWeaver UME:

| SAP Sourcing Attribute | SAP NetWeaver UME Attribute | Description |
|---|---|---|
| NAME | uniquename | User ID |
| EMAIL | email | Email address |
| FIRST_NAME | firstname | First name |
| LAST_NAME | lastname | Last name |

# 2 Single Sign-On User Authentication

SAP Sourcing supports the Single Sign-On (SSO) user authentication mechanisms provided by SAP NetWeaver. Therefore, the security recommendations and guidelines for user administration and authentication as described in the *SAP NetWeaver Security Guide* also apply to SAP Sourcing.

The recommended configuration of using SAP NetWeaver UME for user management and authentication, allows any type of authentication, including Single Sign-On (SSO), supported by SAP NetWeaver to work with SAP Sourcing.

There are additional steps that need to be configured for setting up SAML 2.0 for SSO user authentication.

**Recommendation**

The recommended and supported Identity Provider (IdP) for SAP Sourcing when using SAML 2.0 is SAP NetWeaver IDM 7.2 or higher.

## 2.1 Configuring the IdP

1. Activate SAML 2.0 authentication service in your SAP NetWeaver IDM environment.
2. Create a trusted Service Provider (SP) in SAP NetWeaver IDM by importing the metadata file as extracted from the Sourcing / SAP NetWeaver instance.
3. Export IdP metadata from SAP NetWeaver IDM.

## 2.2 Configuring the Service Provider (Sourcing)

1. Activate the SAML 2.0 authentication service on the service provider.
2. Export the service provider metadata and make it available for the IdP to import.
3. Create a trusted entry for IdP, by importing the IdP metadata file.
4. Update the authentication stack on the SP.
5. Update the directory configuration in the SAP Sourcing application.

## 2.3 Setting Up Single Sign-On for SAP Sourcing Integration with SAP Spend Performance Management (SPM)

This setting enables Single Sign-On between SAP Sourcing and SAP Spend Performance Management (SPM).

1. Export a PSE file of the SPM portal server. To use the `keystore` administration tool, administrators must be assigned to the system administration role. They must also be assigned to the J2EE Engine security role administrators. By default this role is assigned to the group administrators so it should suffice to assign the user to the administrators group.
    a. In the portal, choose *System Administration*→*System Configuration* → *Keystore Administration* → *Content*.
    b. Choose *Download verify.pse File*.
    c. Download the PSE file to a location available to the application server.
2. Log on as enterprise administrator of the corresponding cluster for the SPM-SAP Sourcing integration.

3. Create the following system properties:
   - `system.sap.ticket.pse.file` The value of this property should be the full path of the PSE file (Personal Security Environment) of the SPM portal server.
   - `system.sap.ticket.pse.password` The value of this property should be the password of the PSE file of SPM's portal server, if the PSE requires a password.
4. Set the port in Cluster Configuration if needed. If the port used in the SAP Sourcing URL is not the default port of HTTP (or HTTPS), set the port in the Cluster information.
   a. Log on as Administrator of System Context in SAP Sourcing.
   b. Choose *Cluster Configuration* on the *Setup* page.
   c. Choose the cluster for SPM-SAP Sourcing integration.
   d. Edit the Cluster Information and set the value of the *Port* field as the port used by SAP Sourcing.
5. To configure the directory for SSO in SAP Sourcing, do the following:
   a. Log on to system context, choose *Directory Configuration* on the *Setup* page, and edit the active internal directory configuration on the cluster used for SPM-SAP Sourcing integration.
   b. On the *Directory Configuration* tab, deselect *Case Sensitive Username*.
   c. Set the value of the *Driver* field to *Basic*.
   d. Under *Driver Configuration*, set the value of the *Authentication* field to *com.sap.odp.security.auth.LogonTicketAuthenticator*.
   e. On the *Properties* tab, create the following properties:
      - `Ext_login_page` The format of the value of this property is `http://<SPM Server Base URL>/eslogin/eslogin?url=<SAP Sourcing Login URL>`

        For example if the base URL for the SPM server is `http://vmw3011.wdf.sap.corp:50000`, and the base URL for SAP Sourcing is `http://nvpad428.pal.sap.corp:8080`, then the value of this property should be `http://vmw3011.wdf.sap.corp:50000>/eslogin/eslogin?url=http%3a%2f%2fnvpal428.pal.sap.corp%3a8080%2ffsbuyer%2fportal%2flogin`.
      - `bypass_error_check` Set this value to **`TRUE`**.
6. Install dynamic libraries for ticket authentication. Single Sign-On uses SAP Assertion ticket for user authentication of webservice calls between SPM and SAP Sourcing systems. Two dynamic libraries should be installed on the SAP Sourcing environment to authenticate the tickets.

   **Note**

   The SAP Assertion Ticket option should be specified for the two webservice clients on the SPM system. The instruction is available in the SPM Installation and Configuration Guide at http://service.sap.com/instguidesssa.

   The two dynamic libraries are platform dependent. They have either the `.dll` extension (Windows version) or .the `.so` extension. Their filenames are `SAPSSOEXT`, and `SAPCUSEC`.

   a. To download `SAPSSOEXT`, choose *SMP → Downloads → SAP Support Packages → Entry By Application Group → Additional Components →* `SAPSSOEXT`.

      **Note**

      See SAP Note 1040335 for information about this library.

   b. To download `SAPCUSEC`, choose *SMP → Downloads → SAP Support Packages → Entry By Application Group → Additional Components →* `SAPCUSEC`.

**Note**

See SAP Note 870138 for information about this library.

c. If the downloaded file has a .sar extension, download the SAR extraction tool. Choose SMP Downloads SAP Support Packages Entry By Application Group Additional Components SAPCAR

d. Extract the files from the SAR file with the following command:
**`sapcar-xvf< path to SAPSSOEXT*.SAR>`**

e. Copy library files to a directory in `%PATH%` (for windows), `$LD_LIBRARY_PATH` or `$LIBPATH`.

# 3 User Impersonation

User impersonation is a feature which allows one user to log on as another user. For example, if a user is on vacation, an administrator can use the user impersonation feature to log on as that user and complete his or her tasks.

In the case of a supplier, a designated user could act on behalf of another, or in the case of support, a support person can impersonate a particular user to gain firsthand knowledge of an issue that a user is experiencing without needing to obtain the user‘s password.

In addition, anyone using the impersonation feature is identified in the SAP Sourcing logs and document history. This provides for historical accuracy of events when impersonation is used.

## 3.1 Setting Up Impersonation

The following subsections describe how to set up impersonation for enterprise users and how to modify the system property for impersonation.

### 3.1.1 Activate or Inactivate Impersonation for Purchasers

To allow impersonation as a purchaser, do the following:

1. Choose the navigation path: Setup → System Administration → Security Profiles.
2. Open any profile with Class Level usage.

   **Caution**

   Only change these settings for administrative or other special users. Otherwise, all the users of the type you select will be granted impersonation access.
3. Select the *Access Rights* tab.
4. In the dropdown list, select *Users and Security*.
5. Navigate to the second page.
6. Choose the *Edit* button.
7. Do one of the following:
   - To log in as a purchaser, set *User Impersonation for Internal User* to **`Allow`**.
   - To log in as a supplier, set *User Impersonation for External User* to **`Allow`**.

### 3.1.2 Activate or Inactivate Impersonation for Suppliers

1. Click the *Setup* link.
2. On the *Master Data* tab, in the *Organization and Accounting Information* area, click *Suppliers*.
3. On the *Supplier* page, select a supplier for whom you want to enable impersonation.
4. Choose the *Edit* button.
5. Select the *Impersonation Enabled* checkbox.
6. Choose the *Save* button.

## 3.2 Impersonating a User

After you have correctly configured user impersonation, to impersonate a particular user, do the following:

1. Open the user’s account page.
2. Choose *Actions* → *Log In As This User*.

# 4 Working with External Roles

You can use SAP NetWeaver UME to store purchasers and suppliers, and they can potentially also exist in different user data repositories. To support such a landscape, while keeping the users adequately segregated, the *External Role* field in the directory configuration module in Sourcing / CLM is mandatory when using either the SAP NetWeaver UME or SAML 2.0 driver.

The purpose of this field is to separate users that are stored in one SAP NetWeaver UME instance. This means that suppliers are not be allowed to view or access any user data for purchasers through SAP Sourcing.

All directory configuration examples apply to the SAP NetWeaver UME driver, but you can use similar procedures to set up the external role with the SAML 2.0 driver.

Below are the various scenarios and detailed steps for specifying external roles within SAP Sourcing / CLM, and ensuring they correspond to the role specified in SAP NetWeaver UME.

**Recommendation**

We recommend that you set up the driver as follows. The driver configuration in SAP Sourcing / CLM needs to have a driver set up to use either SAP NetWeaver UME or SAML 2.0 for authentication.

## 4.1 Configuring the SAP NetWeaver UME Driver Only for Purchasers or Suppliers

**Caution**

Please note that the steps below are to be configured only when SAP Sourcing is set up to use SAP NetWeaver UME driver for the purchaser **OR** supplier directory **ONLY**. The *External Role* field value should **not** be set to **`Everyone`** in either the purchaser or the supplier directories.

For setting up **both** purchaser and supplier directories to use the SAP NetWeaver UME driver, follow the steps in section 4.2 “Configuring the SAP NetWeaver UME Driver for Both Purchasers and Suppliers”.

The following configuration applies when you are planning to use the SAP NetWeaver UME driver only for purchasers or suppliers. This means that it is not necessary to apply any kind of separation between users in SAP NetWeaver UME. In this case SAP Sourcing can assume that all UME users will belong to one directory (purchasing or supplier).

### 4.1.1 Configuring the Directory

1. Log on as a user with rights for modifying directories.
2. Navigate to the SAP Sourcing *Directory Configuration* screen:
   *Setup* → *System Setup* tab → *Configuration* area → *Directory Configuration*
3. Open the purchasing or supplier directory that you want to modify.

4. Choose the *Edit* button. Fill in all mandatory fields according to the table below and save your work.

| Field | Recommended Value |
|---|---|
| External ID | Any unique value |
| Display Name | Any |
| Usage | Active Internal or Active External |
| Authentication Support | Checked |
| External Role | Everyone – Make sure that you enter `Everyone` in the *External Role* field. This means that all UME users will be available for this directory. The *Everyone* role is assigned to all UME users automatically during the user creation process. |
| Driver | SAP NetWeaver UME |

5. On the *Attribute Mapping* tab, you must configure at least the *NAME* attribute.
6. In the *Directory ID* column, set the *NAME* attribute as **uniquename**. To modify the *NAME* attribute, click the Pencil icon.
7. In the *Edit Mode* column, in the dropdown list, select **Pull**.
   Additionally, you can configure other attributes.
8. Choose the *Save* button to apply your changes.

# 4.2 Configuring the SAP NetWeaver UME Driver for Both Purchasers and Suppliers



**Note**

The following scenario applies when you are planning to use the SAP NetWeaver UME driver for both purchasers and suppliers.

The configuration below ensures that purchasers cannot view or access suppliers' private data through SAP Sourcing and the reverse: suppliers cannot view or access purchasers' private data.

## 4.2.1 Creating a Purchaser / Supplier Role in SAP NetWeaver UME

1. Open the *SAP NetWeaver User Management* page and log on as an administrator:
   http://<host>:<port>/useradmin
2. In the *Search Criteria* dropdown list, select *Role*.
3. Choose the *Create Role* button.
4. In the *Unique Name* field, specify a name for the role. For example, you can use the following for purchasers: `Sourcing_purchaser_role`.
5. Choose the *Save* button.
6. Follow steps 1-5 and create a *Role*, with a unique name. For example, you can use the following for suppliers: `Sourcing_supplier_role`.

## 4.2.2 Configuring the Purchaser / Supplier Directory

1. Log on as a user with rights for modifying directories.
2. Navigate to the SAP Sourcing *Directory Configuration* screen:
   *Setup* → *System Setup* tab → *Configuration* area → *Directory Configuration*
3. Open the purchasing directory that you want to modify.

4. Choose the *Edit* button. Fill in all mandatory fields according to the table below and save your work.

| Field | Recommended Value |
|---|---|
| External ID | Any unique value |
| Display Name | Any |
| Usage | Active Internal |
| Authentication Support | Checked |
| External Role | Your purchaser role name. For example, you can use `Sourcing_purchaser_role` as the purchaser name. |
| Driver | SAP NetWeaver UME |

5. On the *Attribute Mapping* tab, you must configure at least the *NAME* attribute.
6. In the *Directory ID* column, set the *NAME* attribute as **uniquename**. To modify the *NAME* attribute, click the Pencil icon.
7. In the *Edit Mode* column, in the dropdown list, select **Pull**.
   Additionally, you can configure other attributes on the *Attribute Mapping* tab.
8. Choose the *Save* button to apply your changes.

   
   **Note**

   Make sure that you create the SAP NetWeaver UME role beforehand. If the role does not exist in SAP NetWeaver UME, you cannot proceed. In this case refer to step 1 to create the role.
9. Repeat steps 1-8 and create another external role, with a unique name. For example, you can use `Sourcing_supplier_role` for suppliers.

# 4.3 Assigning Purchasers / Suppliers to a Role

Since purchasers and suppliers need to be associated with an external role in SAP Sourcing and with a corresponding role in SAP NetWeaver UME, it is important to ensure that the roles in both systems are aligned for users.

There are several methods of assigning roles to users:

- Assigning an SAP NetWeaver UME role to a user – Can be used if it is needed to assign a role to one or few users.
- Assigning a user to an SAP NetWeaver UME role – Can be used if it is needed to assign a role to one or few users.
- Assigning an SAP NetWeaver UME role during user import to SAP NetWeaver UME – Can be used to assign a role to users during initial user import to SAP NetWeaver or during an upgrade scenario.
- Assigning an SAP NetWeaver UME role during user creation in SAP Sourcing – Can be used during initial user import to SAP Sourcing.

These methods are described in the following sections.

## 4.3.1 Assigning an SAP NetWeaver UME Role to a User

1. On the *SAP NetWeaver User Management* page, log on as an administrator.
   http://<host>:<port>/useradmin
2. Select a user to whom you want to assign a role.
3. Choose the *Modify* button and navigate to the *Assigned Roles* tab.
4. Enter the search criteria and select the role which you want to assign.
5. Choose the *Add* button, then choose the *Save* button to apply the changes.

### 4.3.2 Assigning a User to an SAP NetWeaver UME Role

1. On the *SAP NetWeaver User Management* page, log on as an administrator.
   http://<host>:<port>/useradmin
2. Select a user to whom you want to assign a role.
3. Choose the *Modify* button and navigate to the *Assigned Roles* tab.
4. Enter the required search criteria and select the users to whom you want to assign the role. If you want to select several users at once, press the `CTRL` key.
5. Choose the *Add* button, and then the *Save* button to apply the changes.

### 4.3.3 Assigning an SAP NetWeaver UME role during User Import to SAP NetWeaver UME

This particular option can be used for the following scenarios:

- Users exist in SAP Sourcing, but not in SAP NetWeaver UME;
- Users exist in SAP Sourcing and SAP NetWeaver UME, but these users do not have synchronized roles.

#### 4.3.3.1 Creating an Extension Definition for a User Account

1. Log on to SAP Sourcing as an enterprise user or as an advanced user.
2. Do one of the following:
   a. If you want to assign a role to purchasers, choose the following navigation path:
      *Setup* → *System Setup* tab → *Configuration* area → *Extension Definition* → *User Account*
   b. If you want to assign a role to suppliers, choose the following navigation path:
      *Setup* → *System Setup* tab → *Configuration* area → *Extension Definition* → *Contact*
3. Choose the *Edit* button, then in the *Attributes* area, choose the *Add* button.
4. Fill in required fields as shown in the screen shot below.

   **Note**

   You can specify any unique value in the *Internal Name* field and any resource value in the *Display Name* field.
5. To hide the extension on the user account page, select the *Inactive* checkbox.
6. Save the extension definition.

#### 4.3.3.2 Enabling the User Export Feature

1. Choose the following navigation path:
   *Setup* → *System Setup* tab → *Configuration* area → *System Properties*
2. In the *System Property* list, find and click the link of the property:
   `upp.account.enable_accounts_export`
   By default the property is set to **`false`**.
3. In the *Display* screen choose the *Edit* button. In the *Value* field enter **`TRUE`** and save the property.

#### 4.3.3.3 Adding an Additional Export Attribute



**Note**

To specify mapped attributes and export users the directory should be active. The export feature is inactive for inactive directories.

1. Log on to SAP Sourcing as an enterprise or advanced user.
2. Choose the navigation path:
   *Setup* → *System Setup* tab → *Configuration* area → *Directory Configuration*
3. Open a directory from which you want to export users.
4. Select the *Attributes Mapping* tab and choose the *Edit* button.
5. In the *Mapped Attributes for Export* area, add additional attributes if required. Mandatory attributes are shown in the screen shot below.
6. In the *Editing: New Directory Attribute Mapping* screen, for the `EXTERNAL_ROLE` attribute, in the *Mapping ID* field, enter **`role`**.
7. In the *Define Custom Attribute Value* field, enter the name of the SAP NetWeaver UME role that you want to assign to users.
8. Save the directory.

#### 4.3.3.4 Exporting Users from SAP Sourcing



**Note**

To specify mapped attributes and export users the directory should be active. The export feature is inactive for inactive directories.

1. Log on to SAP Sourcing as an enterprise or advanced user.
2. Choose the navigation path:
   *Setup* → *System Setup* tab → *Configuration* area → *Directory Configuration*
3. Open a directory from which you want to export users.
4. On the directory screen, in the *Actions* dropdown list, select *NW Format Export*.
5. SAP Sourcing generates a file that contains user data in the SAP NetWeaver UME format. Save this file.

#### 4.3.3.5 Importing Users into SAP NetWeaver UME

1. On the *SAP NetWeaver User Management* page, log on as an administrator.
   http://<host>:<port>/useradmin
2. Choose the *Import* button.
3. Under *Text File Upload* area choose the *Browse* button and navigate to the file containing the users created by SAP Sourcing.
4. Choose the *Open* button.
5. Select the *Overwrite Existing Data* checkbox and choose the *Upload* button to start import process. During the import, the role is assigned to all imported users.

## 4.3.4 Assigning an SAP NetWeaver UME Role during User Creation in SAP Sourcing

In SAP Sourcing, you can assign an SAP NetWeaver UME role automatically to a user during its creation. Below are two scenarios about how you can create a user with an SAP NetWeaver UME role assignment.

### 4.3.4.1 Prerequisite

- You have enabled the *New Accounts* feature. For more information, see the procedure in the next section.

### 4.3.4.2 Enabling a New Accounts Feature

1. Log on to SAP Sourcing as a system or advanced user.
2. Choose the navigation path:
   *Setup* → *System Setup* tab → *Configuration* area → *Directory Configuration*
3. Open a directory where you want to create a user and select the *New Accounts* checkbox.
4. Modify the directory according to your requirements and save changes.

### 4.3.4.3 Creating a User Manually



**Note**

The scenario described in this section applies only when the SAP NetWeaver UME driver is enabled. If the SAML 2.0 driver is enabled, it is not allowed to create users manually in SAP Sourcing.

1. Log on to SAP Sourcing as an enterprise user or as a user with rights to create new accounts.
2. Choose the navigation path:
   *Setup* → *System Administration* tab → *Accounts and Security* area → *Internal User Accounts*
3. Choose the *New* button.
4. Fill in all required fields.
5. On the *Account Management* tab, select the *Create Directory Account* checkbox.
6. Choose the *Save* button.
   During the save process a new user is created in SAP Sourcing and in SAP NetWeaver UME. The role that is specified on the directory configuration page is automatically assigned to the user.

### 4.3.4.4 Creating a User with the Data Import Feature

You can import user accounts to SAP Sourcing using the data import feature. This process is not described in detail in this guide.

To be able to automatically assign the role to users make sure that following columns contain the `TRUE` value:

- `CREATE_DIR_ACCOUNT`
- `GENERATE_NEW_PWD`

# 5 Authorizations

## 5.1 Default Security Profiles

**Recommendation**

Security profiles are completely customizable. It is, however, recommended that you include the default ones.



**Note**

The *Application User* profile is a required profile and it is automatically assigned to all users. Keep this in mind when assigning rights to this profile as these rights are given to all users.

The table below shows the default security profiles, with an impact on security, that are used by SAP Sourcing.

**Caution**

External IDs of default profiles should not be modified.

The following security profiles are delivered:

| Security Profile | Description |
|---|---|
| System Administrator | System administrators can create and manage all type of setup and configuration data. |
| Application User | Application users can login, manage their workbench, and navigate the SAP Sourcing system. This profile is required for all users. |
| Document Owner | This profile gives one individual all rights to a business document. This person typically is responsible for the business document. |
| Document Collaborator | This profile allows editing of a document. |
| Document Approver | This profile allows edit and workflow approval rights on a document. |
| Master Data Manager | This profile allows edit rights on all master data. |
| Report User | This profile allows view and execution rights to a report and can be assigned to multiple groups or individuals. |
| Report Developer | This profile allows all rights to a report and can be assigned to multiple groups or individuals. |
| SAP Support User | SAP Support Users can view all objects but modify none. |

## 5.2 Standard Authorization Objects

The table below shows the security-relevant authorization objects that are used by SAP Sourcing.

| Authorization Object | Description |
|---|---|
| Security Profile | Equivalent to a security Role. Defines the set of rights that are granted to users or groups who are assigned the profile. |
| Group | Groups of users. A user may be assigned to zero or more groups. Each group is assigned one or more security profiles. |
| Internal User Accounts | Represents users who are allowed to log into the application. Each user may be assigned one or more security profiles. |
| Supplier Contacts (aka External User Accounts) | Represents supplier users, some of which are allowed to log into the application. Each user is assigned one or more security profiles. |
| Document Security Template | Defines the set of collaborators that are added to newly created business documents. |
| Collaborator Role Definition | Defines the rights that each collaborator has on a business document. |
| Context | Defines data isolation rules. Data is only assessable to users within the same context (or subcontext). |
| Directory | Defines the configuration settings for the user store and authentication driver. This is where LDAP or SSO is configured. |
| Tenant Configuration | Configures all initial security settings for new tenants in a multi-tenant deployment. |

## 5.3 Network and Communication Security

Your network infrastructure is extremely important in protecting your system. Your network needs to support the communication necessary for your business needs without allowing unauthorized access. A well-defined network topology can eliminate many security threats based on software flaws (at both the operating system and application level) or network attacks such as eavesdropping. If users cannot log on to your application or database servers at the operating system or database layer, then there is no way for intruders to compromise the machines and gain access to the backend system's database or files. Additionally, if users are not able to connect to the server LAN (local area network), they cannot exploit well-known bugs and security holes in network services on the server machines.

The network topology for SAP Sourcing is based on the topology used by the SAP NetWeaver platform. Therefore, the security guidelines and recommendations described in the SAP NetWeaver Security Guide also apply to SAP Sourcing. Details that specifically apply to SAP Sourcing are described in the following topics:

- Communication Channel Security
  This topic describes the communication paths and protocols used by SAP Sourcing.
- Network Security
  This topic describes the recommended network topology for SAP Sourcing. It shows the appropriate network segments for the various client and server components and where to use firewalls for access protection. It also includes a list of the ports needed to operate SAP Sourcing.

- Communication Destinations
  This topic describes the information needed for the various communication paths, for example, which users are used for which communications.

For more information, see the following sections in the SAP NetWeaver Security Guide:

- Network and Communication Security [SAP Library]
- Security Aspects for Connectivity and Interoperability [SAP Library]

# 5.4 Communication Channel Security

The table below shows the communication channels used by SAP Sourcing, the protocol used for the connection and the type of data transferred.

| Communication Channel | Protocol Used | Type of Data Transferred |
|---|---|---|
| Front-end client using a Web browser to application server | HTTP | All application data |
| File-based data transfer | FTP | Master data, Business Objects |
| E-mail notifications | SMTP | Messages outbound from SAP Sourcing to internal users, external users, groups of users, or simple email addresses. |

HTTPS connections are HTTP connections protected by the Secure Sockets Layer (SSL) protocol. SAP Sourcing should be configured to only allow HTTPS connections. This is the recommended production configuration.

FTP connections are NOT secure, only standard FTP is supported. If FTP over unsecured networks is desired, a separate FTPS (or similar) infrastructure is recommended. This infrastructure will be outside of the SAP Sourcing application. The SAP Sourcing application must be on the same network as this external infrastructure, having access to its files directly or via unsecured FTP.

SMTP connections can be configured with or without username/password authentication. It's also possible to configure the SMTP port, if the server is not on the standard port (25).

For more information, see Transport Layer Security [SAP Library in the SAP NetWeaver Security Guide.

# 5.5 Data Storage Security

For information on the topic of Data Storage when SAP Sourcing is executed on the SAP NetWeaver CE Application Server Platform, refer to the SAP NetWeaver CE Security Guide: help.sap.com → *Security Guides for CE Core Components → SAP NetWeaver Application Server Java → Data Storage Security*.

SAP Sourcing contains two types of data requiring security. These two types are technical configuration data and business data. This data may be stored in one of several locations depending upon its current usage.

## 5.5.1 Technical Configuration Data

At the time of SAP Sourcing installation or upgrade the user running the installation or upgrade process is required to designate a directory on the application server in which to install the SAP Sourcing software. This directory is known as the 'FCI.HOMEDIR' directory. The user executing the installation and upgrade must have full permissions (READ, WRITE, EXECUTE) on this directory and all of its child directories during the installation or upgrade.

During and after the SAP Sourcing installation or upgrade, technical configuration data gathered during the installation process by the setup utility is stored in the FCI.HOMEDIR\config directory in a file named **fcisystem.properties** and in another file in the FCI.HOMEDIR\deploy directory named **sap.application.global.properties**. This data consists of the configuration data which specifies low level application configuration such as the information needed to connect to the database and certain configuration parameters related to logging. The database password associated with the database service account used for database access is stored in these files in an encrypted form.

When executing on SAP NetWeaver, the applicability of this copy of the configuration data stored in the **fcisystem.properties** file is limited to use by the DbImport tool used in executing the installation and upgrade processes. The same technical configuration data as well as additional SAP NetWeaver-specific technical configuration data is also stored in the SAP NetWeaver Configuration manager using a SAP NetWeaver-specific deployment descriptor, **sap.application.global.properties**.

This deployment descriptor is included by the SAP Sourcing installation process in the SAP NetWeaver deployable SCA produced by the installation or upgrade process. Once installed in the SAP NetWeaver Configuration manager during the SAP Sourcing deployment, this copy of the technical configuration data is secured by NetWeaver along with the other technical configuration properties maintained by SAP NetWeaver. This SAP Sourcing technical configuration data deployed in SAP NetWeaver is accessible using the SAP NetWeaver `configtool` utility included with SAP NetWeaver. Use of this tool requires a suitably permissioned NetWeaver administrative account.

### 5.5.2 Business Data

Other directories under the FCI.HOMEDIR directory which are notable from a security standpoint are the import, logs and `tmp` subdirectories. The logs subdirectory will contain log files resulting from use of the `DbImport` tool. These logs all begin with the prefix **`install`**. The import and `tmp` subdirectories are used for temporary file storage. These temporary files may contain application data under some circumstances such as the use of the `DbImport` utility to import data in Microsoft Excel® spreadsheet format.

### 5.5.3 Recommended Security for FCI.HOMEDIR

**Recommendation**

We recommended that the FCI.HOMEDIR directory tree be fully accessible to system administrators of the application server and anyone else authorized to run the DbImport tool but need not be accessible to other users.

### 5.5.4 SAP Sourcing – SAP NetWeaver Temporary Directories

During runtime while executing on the SAP NetWeaver application server the SAP Sourcing application requires a readable and writable temporary directory tree. For this purpose the SAP Sourcing application creates a directory tree within the SAP NetWeaver directory tree. SAP Sourcing requires a separate temporary directory tree for each SAP NetWeaver Application Server node on which it executes. This directory is created in the following location of the SAP NetWeaver directory tree:

**${INSTANCE_DIR}/esourcing-${NODE_INDEX}**

Where ${INSTANCE_DIR} is the SAP NetWeaver installation directory and ${NODE_INDEX} is the SAP NetWeaver node index number. For example:

**D:\usr\sap\FRF\J00\esourcing-00**

These directory trees will contain temporary files of various types in the various child directories. The operating system user account under which the SAP NetWeaver application server is executing must have full access to these directories. This user must also have sufficient permissions to enable creation of these directories which will be created as required by the SAP Sourcing application.

These directories contain temporary data files which will frequently contain application data in various formats, for example, data exports or imports in `csv` format, or reports in PDF format, and so access to these directories should be secured to a similar degree as that used to secure the database storing the SAP Sourcing application data.

### 5.5.5 Recommended Security for SAP Sourcing NetWeaver Temporary Directories

Generally is required that the operating system user under which the SAP NetWeaver Application server is run have full (READ, WRITE, EXECUTE) access to these directories while other users should have a level of access necessary to perform their roles. It should be noted that because the application server accesses these directories on behalf of SAP Sourcing application users, SAP Sourcing application users typically need no access to these directories.

### 5.5.6 Primary Store for SAP Sourcing Application Data is the Database

All of the SAP Sourcing business application data is stored in the database management system configured for SAP Sourcing usage. This data is secured using the facilities of the database management system in use. The SAP Sourcing application uses a single database user account for access to the database. The database security profile required by this account is described in detail in the SAP Sourcing Installation Guide for your database management system.

### 5.5.7 SAP Sourcing Temporary Application Data Stored On Client

SAP Sourcing business application data may also be stored in temporary files in various formats on client machines used to access the SAP Sourcing application server via a supported web browser. When users of SAP Sourcing request attachment download or export data in XLS or CSV format or execute certain PDF reports, the client web browser frequently stores this data as temporary files on the client machine. Consult your client operating system and browser documentation for the exact locations where these files may be stored. It should be noted that if local security policies prohibit users from downloading documents either because of applied operating system file system security settings or policies or because of client browser setting then those features of the SAP Sourcing application which require downloading of attachments, exports or reports will be non-functional. Because these features are key components of the SAP Sourcing application, SAP Sourcing assumes that clients support the ability to download these types of files, users of clients which do not support this ability will likely receive client side errors if operations requiring file downloads are requested. Assuming that clients support the SAP Sourcing file download functionality then regardless of where this temporary data is stored it should be recognized that these downloaded files contain formatted business data which should be secured. Consult your operating system and browser documentation for available methods for securing this data. It is also recommended that this temporary data be deleted frequently since once downloaded these downloaded files which typically contain dynamic application date are never reused by the SAP Sourcing application.

### 5.5.8 Avoid Caching of SAP Application Data File Downloads

All data in the SAP Sourcing application is secured and any data downloaded to a client on user request is intended specifically for the user making the request that has permission to access the downloaded data, you should not configure your local network infrastructure to cache this downloaded data. Firstly, caching of this data serves no purpose since this specific data set will never be downloaded more than once. Secondly, delivery of cached data based on a client request can under rare circumstances result in delivery of data to a user without authorization to view the cached data.

## 5.6 Security for Additional Applications

For information on the topic of database security when executing SAP Sourcing on the SAP NetWeaver CE Application Server platform, refer to the *SAP NetWeaver CE Security Guide*: help.sap.com → *Security Guides* for the Operating System and Database Platforms.

### 5.6.1 Database Security

Refer to the documentation provided by your database vendor for vendor specific security consideration relevant to your database.

All SAP Sourcing business application and configuration data is stored in the associated database selected during SAP Sourcing installation. The SAP Sourcing application accesses this data using a single database service account which is specified during SAP Sourcing installation or upgrade. Refer to the SAP Sourcing installation guide specific for your database for specific information regarding the required configuration of the database service account.

Although it is most convenient to configure your database service account password to not expire, you may find that local security policies require the expiration and changing of this password at regular intervals. If this is the case then you will need to coordinate the change in password for this account in the database with the SAP Sourcing deployment. Changing the database service account password requires running the setup utility in your FCI.HOMEDIR/bin directory in order to reset the database parameters including the new database service account password. It also requires rebuilding the SAP Sourcing SCA file followed by redeployment of SAP Sourcing in the SAP NetWeaver Application Server. Refer to your SAP Sourcing Installation Guide for specific instructions on how to perform this operation.

**Caution**

In an emergency, you can change the SAP Sourcing database service account password using the SAP NetWeaver `configtool` provided with your SAP NetWeaver Application server. You should store the new database service account password in plaintext in SAP NetWeaver since the password can only be encrypted using the SAP Sourcing setup utility. If you change this password using this method you will need to restart all instances of the SAP Sourcing application in order for the change to take effect. If you resort to using this method to change the password in an emergency then you will still need to update the password using the setup program in your `FCI.HOMEDIR/bin` directory in order make the changed password available to the `DbImport` utility program which uses the encrypted password stored in the `FCI.HOMEDIR/config/fcisystem.properties` file. The only way to update this encrypted copy of the password is through use of the `FCI.HOMEDIR/bin/configure` utility.



**Note**

Although you may change the database service account using the previously described methodology, you should never change the database user associated with the database service account since your SAP Sourcing data is typically associated with this user in the database and changing the user of the database service account will render your SAP Sourcing data inaccessible in most cases.

Because SAP Sourcing upgrades require running the `FCI.HOMEDIR/bin/setup` utility to build a new deployment unit in order to deploy the upgraded software, it is recommended to coordinate any required database service account password changes with SAP Sourcing upgrades.

## 5.7 Dispensable Functions with Impacts on Security

For information on the topic of SAP Sourcing executed on the SAP NetWeaver CE Application Server platform, refer to the SAP NetWeaver CE Security Guide: help.sap.com → *Security Guides for CE Core Components* → *SAP NetWeaver Application Server Java* → *Dispensable Functions with Impacts on Security*.

Other than the general information provided by the reference cited, this topic is not relevant to the SAP Sourcing application.

## 5.8 Security Logging and Tracing

For information on Security Logging and Tracing, refer to the *SAP NetWeaver CE Security Guide* at help.sap.com → *Security Guides for CE Core Components* → *SAP NetWeaver Application Server Java* → *Tracing and Logging*.

SAP Sourcing security specific logging and tracing information can be found in the SAP NetWeaver logs available in *NetWeaver Administrator* → *Availability and Performance Management* → *Resource Monitoring* → *Log Viewer*.

You can fine tune the log and trace information using the SAP NetWeaver Administrator Guide at: help.sap.com *NetWeaver Administrator* → *Configuration Management* → *Infrastructure* → *Log Configuration*.

SAP Sourcing log information can be configured using the SAP NetWeaver Administrator Log Configuration tool under *Logging Categories → Applications → E-Sourcing → eso category*.

SAP Sourcing trace information can be configured using the SAP NetWeaver Administrator Log Configuration tool under *Tracing Locations → ROOT → E-Sourcing → eso → java → com → sap → odp*.

The security related logging and tracing information is primarily related to system login and logout. All system login and logout requests are logged as are any failed user authentications. Authorization failures are also logged. Review of the SAP Sourcing logs can be used to determine any security related issues associated with system login attempts or failed authorizations.

# Copyrights, Trademarks, and Disclaimers