SAP NetWeaver 2004s SPS 4

Security Guide

Security Guide for Guided Procedures

Document Version 1.00 – October 24, 2005

THE BEST-RUN BUSINESSES RUN SAP

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`

THE BEST-RUN BUSINESSES RUN SAP

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
SYN	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

Security Guide for Guided Procedures

⚠

This guide does not replace the daily operations handbook that we recommend customers to create for their specific productive operations.

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, whereby the security guides provide information that is relevant for all life cycle phases.

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 Guided Procedures (GP). To assist you in securing the GP, we provide this security guide.

About this Document

The security guide provides an overview of the security-relevant information that applies to GP.

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 GP.

- **User Administration and Authentication**

  This section provides an overview of the following user aspects of administration and authentication:

  - Recommended tools to use for user management.
  - Standard users that are delivered with GP.
  - Overview of how integration into Single Sign-On environments is possible.

- **Authorizations**

  This section provides an overview of the authorization concept that applies to GP.

- **Network and Communication Security**

  This section provides an overview of the communication paths used by GP and the security mechanisms that apply. It also includes our recommendations for the network topology to restrict access at the network level.

- **Data Storage Security**

  This section provides an overview of any critical data that is used by GP and the security mechanisms that apply.

- **Security for Third-Party or Additional Applications**

  This section provides security information that applies to third-party or additional applications that are used with GP.

- **Other Security-Relevant Information**

  This section contains information about security aspects when developing applications that are exposed in GP.

1 Before You Start

Guided Procedures builds upon the SAP Web Application Server and SAP Enterprise Portal. Therefore, the corresponding security guides also apply to GP. Pay particular attention to the most relevant sections or specific restrictions as indicated in the table below.

Fundamental Security Guides

Scenario, Application or Component Security Guide	Most Relevant Sections or Specific Restrictions
Security Guide for Usage Type AS [SAP Library]	SAP NetWeaver Application Server Java Security Guide [SAP Library] SAP NetWeaver Application Server ABAP Security Guide [SAP Library] Interactive Forms based on Adobe Software Security Guide [SAP Library]
Security Guide for Usage Type DI and Other Development Technologies [SAP Library]	
Portal Security Guide [SAP Library]	

For a complete list of the available SAP security guides, see the Quick Link securityguide on the SAP Service Marketplace.

Additional Information

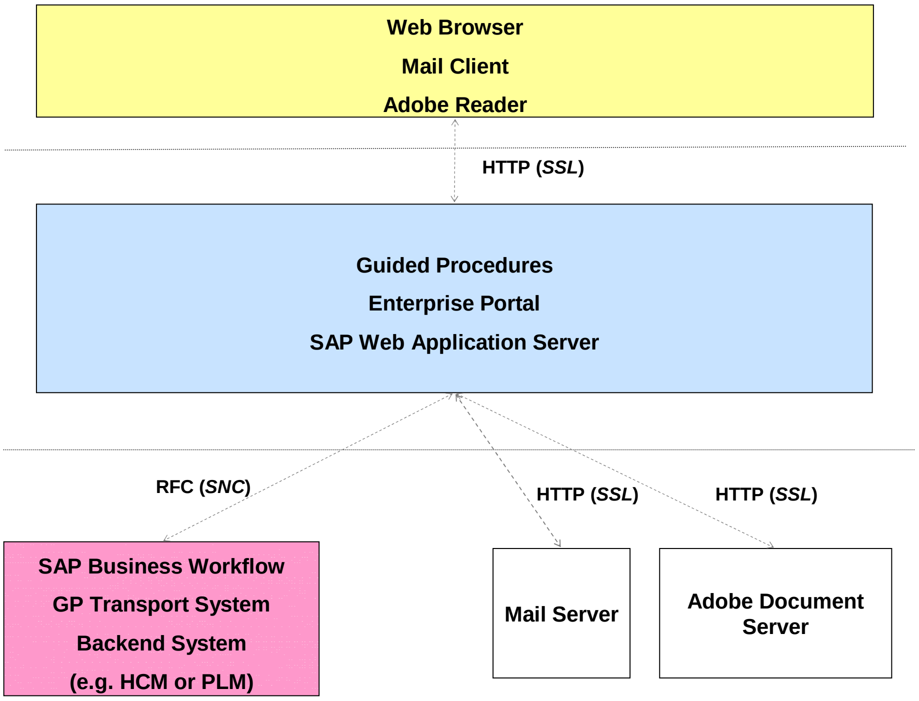
For more information about specific topics, see the Quick Links as shown in the table below.

Quick Links to Additional Information

Content	Quick Link on the SAP Service Marketplace
Security	service.sap.com/security
Security Guides	service.sap.com/securityguide
Related SAP Notes	service.sap.com/notes
Released platforms	service.sap.com/platforms
Network security	service.sap.com/network service.sap.com/securityguide
Technical infrastructure	service.sap.com/ti
SAP Solution Manager	service.sap.com/solutionmanager

2 Technical System Landscape

The figure below shows an overview of the technical system landscape for Guided Procedures.



GP System Landscape

Communication between the layers of the GP technical system landscape uses the following paths:

- Clients – Guided Procedures

  Communication with client applications is based on HTTP. Security is implemented using SSL.

- Guided Procedures – Backend Systems and SAP Business Workflow

  Communication is based on Remote Function Calls (RFC). Security is implemented using Secure Network Communication (SNC).

- Guided Procedures – Mail Server

  Communication is based on HTTP and SSL for security features.

- Guided Procedures – Adobe Document Server

  Communication is based on HTTP and SSL.

See also:

Communication Channel Security [Page 17]

3 User Administration and Authentication

Guided Procedures uses the user management and authentication mechanisms provided with the SAP NetWeaver platform, in particular the SAP Web Application Server Java. Therefore, the security recommendations and guidelines for user administration and authentication as described in the SAP Web AS Security Guide for Java Technology [SAP Library] also apply to GP.

In addition to these guidelines, we include information about user administration and authentication that specifically applies to GP in the following topics:

- User Management [Page 8]

  This topic lists the tools to use for user management, the types of users required, and the standard users that are delivered with GP.

- Integration into Single Sign-On Environments [Page 9]

  This topic describes how GP supports Single Sign-On mechanisms.

3.1 User Management

Use

User management for Guided Procedures uses the mechanisms provided by the SAP Web Application Server Java, for example, tools, user types, and password policies. For an overview of how these mechanisms apply for GP, see the sections below. In addition, we provide a list of the standard users required for operating GP.

User Administration Tools

The table below shows the tools to use for user management and user administration with GP.

User Management Tools

Tool	Detailed Description
User management administration console in SAP Enterprise Portal	For more information, see User Management Administration Console [SAP Library].
User management with SAP Web AS Java	For more information, see User Management Engine.

Standard Users

GP defines the following default user:

GP Default Users

User ID	Type	Description
caf_gp_scvuser	service user	The GP service user is created at service startup. It is used internally when the execution of a certain function requires administrator permissions, and the caller principal does not have this permission. The service user is used in the GP transport system – for example, for importing content. The GP framework also uses the service user to communicate with other J2EE Engine services.

This user is delivered with Guided Procedures.

3.2 Integration into Single Sign-On Environments

Use

Guided Procedures running in a portal environment supports the Single Sign-On (SSO) mechanisms provided by the SAP Web Application Server. Therefore, the security recommendations and guidelines for user administration and authentication as described in the SAP Web Application Server Security Guide also apply to GP.

The supported mechanisms are listed below.

Secure Network Communications (SNC)

SNC is available for user authentication and provides an SSO environment when using the SAP GUI for Windows or Remote Function Calls.

For more information, see Secure Network Communications (SNC) [SAP Library] in the SAP Web Application Server Security Guide.

SAP Logon Tickets

GP supports the use of logon tickets for SSO when using a Web browser as the frontend client. In this case, users can be issued a logon ticket after they have authenticated themselves with the initial SAP system. The ticket can then be submitted to other systems (SAP or external systems) as an authentication token. The user does not need to enter a user ID or password for authentication, but can access the system directly after the system has checked the logon ticket.

You can find more information under SAP Logon Tickets [SAP Library] in the SAP Web Application Server Security Guide.

Client Certificates

As an alternative to authentication with a user ID and password, users using a Web browser as a frontend client can also provide X.509 client certificates for authentication. In this case, user authentication is performed on the Web server with the Secure Sockets Layer Protocol (SSL Protocol) and no passwords have to be transferred. User authorizations are valid in accordance with the authorization concept in the SAP system.

You can find more information under Client Certificates [SAP Library] in the SAP Web Application Server Security Guide.

See also:

Integration Into Single Sign-On Environments [SAP Library] in the Portal Security Guide

4 Authorizations

Within Guided Procedures, authorizations are granted to the following role types:

- Portal roles

  GP provides a set of predefined portal roles that enable access to various functions of the framework – for example, administration, process design time, or process runtime.

  The following portal roles are created for GP:

  - Guided Procedures User
  - Guided Procedures Business Expert
  - Guided Procedures Administrator
  - Guided Procedures Superuser
  - Guided Procedures SAP System User

  For more information, see Portal Roles [Page 11].

- UME actions

  Permissions for GP tools and objects are available as UME actions that can be displayed in the user management administration console.

  For more information, see UME Actions for Guided Procedures [Page 12].

- Process roles

  GP defines a set of standard process roles that are automatically available for each process you create. You can define additional process roles and map existing users to them when the process is started.

  The default process roles are:

  - Owner
  - Administrator
  - Overseer

  These roles are relevant for the execution of the process steps.

  For more information, see Process Roles [Page 14]..

- Authorizations in the ABAP stack

  To enable the execution of certain functions in the ABAP stack, GP defines certain specific authorizations for ABAP. For more information, see Guided Procedures Authorizations in the ABAP Stack [Page 15].

4.1 Portal Roles

Use

Guided Procedures comes with a set of predefined SAP Enterprise Portal roles. They define the permissions for user access to a predefined GP workset.

Integration

The mapping between users and GP portal roles is an administrative task. It is done using the User Management console of SAP Enterprise Portal. For more information, see User Management Administration Console [SAP Library].

Features

Guided Procedures Portal Roles

Role	Technical Name	Description
GP User	com.sap.caf.eu.gp.roles. runtime	The GP runtime workset is added to the portal view of the users that are assigned to this role. They can initiate processes and execute the actions that are assigned to them. No special UME permissions are assigned for this role.
GP Business Expert	com.sap.caf.eu.gp.roles. designtime	This role enables access to the Guided Procedures design time toolset. Users assigned to this role are granted all permissions to manage folders and objects in the GP design time.

Role	Technical Name	Description
GP Administrator	com.sap.caf.eu.gp.roles.administration	This role enables access to the Guided Procedures administration and transport tools. Users assigned to this role can manage process instances, configure queues, transport GP content across systems, and so on.
GP Superuser	com.sap.caf.eu.gp.roles.superuser	All permissions defined for Guided Procedures are assigned for this role. 💡 Use this role in the following scenarios: • In local development installations for test purposes • In productive systems as an emergency user
GP SAP System User	com.sap.caf.eu.gp.roles.sap_system_user	This role enables the execution of callable objects in GP from the backend system side.

4.2 UME Actions for Guided Procedures

Definition

UME actions are sets of Java permissions. The actions are listed in the user management administration console, where you can group them together into roles.

Use

The following table describes the UME actions that are defined for Guided Procedures as well as the portal roles to which the action is assigned by default. You can assign additional actions to the portal roles in the user management administration console.

UME Actions and GP Portal Roles

UME Action	Permissions	Available in Role
`com.sap.caf.eu.gp.designtime.action`	Open action design time	GP Business Expert
`com.sap.caf.eu.gp.designtime.admin`	Open administration toolset	GP Administrator
`com.sap.caf.eu.gp.designtime.all`	All design time permissions	GP Superuser

UME Action	Permissions	Available in Role
`com.sap.caf.eu.gp.designtime.block`	Open block design time	GP Business Expert
`com.sap.caf.eu.gp.designtime.businessobject`	Open design time for object views	GP Business Expert
`com.sap.caf.eu.gp.designtime.callableobject`	Open design time for callable objects	GP Business Expert
`com.sap.caf.eu.gp.designtime.cpkgobject`	Open design time for content package objects	GP Business Expert
`com.sap.caf.eu.gp.designtime.process`	Open process design time	GP Business Expert
`com.sap.caf.eu.gp.designtime.transport`	Access GP transport tools	GP Administrator
`com.sap.caf.eu.gp.runtime.execute_callableobjects`	Execute callable object in the ABAP stack	GP SAP System User

You can set permissions for viewing and modifying each callable object, action, block, or process template that you create using Guided Procedures design time. For example, you can allow a user to see an object in the gallery, but not to enable him or her to change or delete the object.

These actions are not attached to particular portal roles. They can be assigned at design time for each individual object. For more information, see Granting Permissions [SAP Library].

UME Actions for Objects

UME Action	Permissions
`com.sap.caf.eu.gp.devobj.delete`	Delete objects in the GP gallery
`com.sap.caf.eu.gp.devobj.execute`	Initiate processes
`com.sap.caf.eu.gp.devobj.fullcontrol`	All available permissions on objects
`com.sap.caf.eu.gp.devobj.read`	See the object in the GP gallery and open its definition
`com.sap.caf.eu.gp.devobj.readwrite`	Both read and write permissions on the object
`com.sap.caf.eu.gp.devobj.write`	Change object definition

4.3 Process Roles

Use

A process role defines a set of tasks that a user assigned to the role can execute on a process. The assignments are made at process initiation in the Guided Procedures (GP) runtime. The concept is specific to GP and should not be confused with portal roles.

GP provides pre-defined process roles, but also allows the process designer to create additional roles.

The process designer also defines when the assignment of users to process roles is completed – either at process instantiation, or at process runtime, or the initiator is automatically assigned to the relevant process role. For more information, see Consolidating Roles [SAP Library].

Features

Standard Process Roles

The following roles are defined at process level.

Standard Process Roles

Role	Description
Administrator	The administrator of the process can: • Maintain assignments of users to process roles • Maintain process instances using the GP administration tools
Overseer	The overseer can: • See the process instance in the GP runtime • See all actions in a block
Owner	The owner role is similar to a superuser concept for processes. The owner of a process can: • Access all steps of the process • Maintain process instances

Customizable Roles

In addition to the standard process roles, there are also the following roles, which you can customize at design time.

Customizable Roles

Role	Description
Execute role	When you insert an action into a block, the system automatically creates a role for the action processor. At block level, you can consolidate the roles for various action processors into a block processor role. For more information, see Consolidating Roles [SAP Library].
Display role	At block level, you can define the visibility of each action in the block to the processors for the other actions. At process level, you can define such view permissions for the processors of the blocks. The authorized roles can only see the relevant action or block. For more information, see Granting View Permissions [SAP Library].

4.4 Guided Procedures Authorizations in the ABAP Stack

Use

The Guided Procedures (GP) framework integrates with the ABAP stack of SAP NetWeaver. For example, you can configure GP to use the SAP Business Workflow runtime. The GP transport system uses ABAP-based SAP systems, and you can also call RFC function modules and BSP applications within a process modeled with GP.

Features

The following security aspects are related to the GP functions on the ABAP side:

Portal Roles

Role	Description
Guided Procedures SAP System User	GP provides this portal role to enable users to trigger callable object execution from the ABAP stack.

Roles in the ABAP Stack

Role	Name
SAP_BC_BMT_WFM_GP_ SERVICE_USER	This role contains the authorizations required for the service user that is used to connect from the GP runtime to the SAP Business Workflow runtime in the ABAP stack. The role is not intended for dialog users. It contains RFC authorizations for the function groups `SWF_GP_CALLBACK`, `SWF_GP_DEF`, `SWF_GP_ROLES`, `SWF_GP_RUN` and `SWF_GP_UTL`.
SAP_BC_BMT_WFM_GP_ ADMIN	This role contains the authorizations and menu entries needed for accessing SAP Business Workflow transactions for GP. For example, you can use the administration transaction `SWF_GP` where the GP process instances that are deployed on the local Business Workflow Engine can be seen. This role must be assigned to the ABAP stack administrators for Guided Procedure environments, for example, to the existing Workflow administrators.
EUP_GP	This role contains the following authorization objects: • EUP_GP_TSP – contains an authorization field with value *Execute*, which defines a permission to import and export GP content. • EUP_GP_BSP – contains an authorization field with value *Execute*, which defines a permission to execute BSP applications in GP when an endpoint alias is used.

See also:

SAP Authorization Concept [SAP Library]

5 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 processes 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 Guided Procedures 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 GP. Details that specifically apply to GP are described in the following topics:

- Communication Channel Security

  This topic describes the communication paths and protocols used by GP.

- 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]

5.1 Communication Channel Security

Use

The table below shows the communication paths used by Guided Procedures and the protocols used for the connection.

Communication Paths

Communication Path	Protocol Used	Comments
Web browser ↔ Guided Procedures	HTTP(S)	For more information, see Configuring the Use of SSL on the SAP J2EE Engine [SAP Library].
Guided Procedures ↔ SAP Business Workflow	RFC (SNC)	For more information, see SNC User's Guide at http://service.sap.com/security.
Guided Procedures ↔ Backend systems	RFC (SNC)	
Guided Procedures ↔ Adobe Document Server	HTTP(S)	For more information, see: • Configuring the Use of SSL on the SAP J2EE Engine [SAP Library] • Web Services Security [SAP Library]
Guided Procedures ↔ Mail server	HTTP(S)	⚠ E-mail content is sent unencrypted, and Javamail does not support SSL over IMAP/SMTP/POP3. We recommend that you use HTTPS for communication with mail servers. For more information, see Configuring the Use of SSL on the SAP J2EE Engine [SAP Library].

RFC connections can be protected using Secure Network Communications (SNC). HTTP connections are protected using the Secure Sockets Layer (SSL) protocol.

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

See also:

Technical System Landscape [Page 7]

5.2 Communication Destinations

The table below shows an overview of the communication destinations used by Guided Procedures. The endpoint aliases for each destination as well as the configuration of the Web service destinations are created manually by the GP administrator.

Connection Destinations

Endpoint	Destination Name	Type	User, Authorizations	Description
SAP Business Workflow system	GPRuntime Service	RFC	To configure SAP Business Workflow with GP, you need Workflow System Administrator permissions. At runtime, you can use a reference system or portal user mapping if the Java and ABAP stacks use different user management.	Configure this communication destination and the relevant endpoint alias if you want to use SAP Business Workflow for the process management engine. For more information about the configuration of SAP Business Workflow, see the GP Administrator Guide.
GP transport system	-	RFC	To be able to process the transport request in the SAP system, you need the relevant transport permissions.	Configure an endpoint alias for the relevant SAP system that you want to use to create and process requests for the GP content transport. For more information about the transport system configuration, see the GP Administrator Guide.

Endpoint	Destination Name	Type	User, Authorizations	Description
Web service client for Adobe Document Server	-	Web service	The Web service client uses a basic authentication mechanism that requires the user and password to connect to the relevant Web service.	Configure these destinations if you use interactive forms with Guided Procedures. For more information, see the GP Administrator Guide.

6 Data Storage Security

At runtime, the Guided Procedures framework stores process context data without encryption. Therefore, process designers should ensure that if any security-sensitive information is passed in the process context, it should be encrypted in advance.

7 Security for Additional Applications

⚠

Guided Procedures enables the use of Adobe-based interactive forms that can be sent by e-mail or published to an URL.
To ensure security for the Adobe-based forms, we recommend that you use document signatures. For more information about signing documents, see Adobe documentation.

8 Other Security-Relevant Information

In Guided Procedures you can expose BSP and Web Dynpro applications as callable objects. For more information about the security aspects in their development, see:

- Security Aspects for BSP [SAP Library]
- Security Aspects of Web Dynpro for Java [SAP Library]