SAP xIEP 1.0 Security Guide

ADDON.XAP_IEP_SECURITY

Release 644_1

Copyright

These materials are subject to change without notice. These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

Icons in Body Text

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*.

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`.

SAP xIEP 1.0 Security Guide

Introduction

About this Guide

This xApp security guide provides security-relevant information about the SAP xApp Integrated Exploration and Production (SAP xIEP).

This xApp is based on the following components:

- SAP NetWeaver ‘04 Enterprise Portal 6.0
- Composite Application Framework (CAF) 1.0
- Guided Procedures (GP) 1.0
- SAP R/3 4.72

The SAP NetWeaver Security Guide is an important document that should be referred to with respect to this security guide.

Many details that support the SAP xIEP Security Guide are explained in the SAP NetWeaver Security Guide; it is available on the SAP Help Portal **`help.sap.com`** under *Documentation → SAP NetWeaver → English → SAP NetWeaver → Security → SAP NetWeaver Security Guide*.

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 also apply to the SAP NetWeaver platform. To assist you in securing your products, we provide this SAP xIEP Security Guide.

Target Groups

- Technical 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 time frames.

Important SAP Notes

Check regularly which SAP Notes are available about the security of the application.

Important SAP Notes

SAP Note Number	Title	Comment

198498	Single Sign-On Solutions	Information about Single Sign-On Solutions for SAP systems.

Technical System Landscape

The following table specifies where you can find more information about the technical system landscape.

Topic	**Guide**	**Quick link to the SAP Service Marketplace (service.sap.com)**
Application and industry-specific components such as SAP Financials and SAP Retail, Technology components such as SAP Web Application Server	Master Guide	`instguides`
Technical configuration, High availability	Technical Infrastructure Guide	`ti`
Security		`security`

User Administration and Authentication

This section contains information about user administration and authentication in an SAP system landscape.

This involves:

- Management of users
- Synchronization of user data

User Management

User management for the xApp Integrated Exploration and Production (xIEP) uses the mechanisms provided by the SAP Web Application Sever, for example, tools, user types, and password policies. For an overview of how these mechanisms apply to SAP xIEP, see the sections below. In addition, we provide a list of the standard users required for operating SAP xIEP.

User Administration Tools

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

User Management Tools

SAP NetWeaver provides the following user management tools for Java application platforms.

Tool	**Detailed Description**
User Management Engine (UME) administration console	Use the Web-based UME administration console to maintain users, roles, and authorizations in Java-based systems that use the UME for the user store, for example, the SAP J2EE Engine, and the Enterprise Portal. The UME also supports various persistency options, such as the ABAP Engine or a directory server.
SAP J2EE	Use the Visual Administrator to maintain users and roles on the SAP J2EE Engine. The SAP J2EE Engine also supports a pluggable user store concept. The UME is the default user store.

For a detailed description of the user management tools available in SAP NetWeaver, see the SAP Service Marketplace: **`service.sap.com/securityguide`** → *SAP NetWeaver Security Guide* → *User Administration and Authentication* → *User Management* → *User Management Tools*.

In addition, for sizing information, see **`service.sap.com/sizing`**.

User Types

It is often necessary to specify different security policies for different types of users. For example, your policy may specify that individual users who perform tasks interactively have to change their passwords on a regular basis, but not those users under which background processing jobs run. Therefore, we classify different user types in the different products.

The primary classification consists of either individual users or technical users, however, the exact classification depends on the tool used. On the J2EE Engine, the user types are classified according to the group assignment and security policies.

For more information, see the topics *Users and Passwords* and *Standard Users and Groups* in the SAP Help Portal **`help.sap.com`** under *Documentation* → *SAP NetWeaver* → *English* → *SAP NetWeaver* → *Security* → *SAP NetWeaver Security Guide* → *Security Guides for the SAP NetWeaver Components* → *SAP Web Application Server Security Guide* → *SAP Web AS Security Guide for Java Technology*.

Identity Management

SAP xIEP does not impose a limit on the number of users or user types.

For more information, go to the following:

- **`service.sap.com/instguides`** → *SAP xApps* → *SAP xApp Integrated Exploration and Production* → *SAP xIEP 1.0* → *SAP xIEP 1.0 Installation and Configuration* → *SAP xIEP Roles*
- SAP Help Portal **`help.sap.com`** → *Documentation* → *SAP NetWeaver* → *English* → *Security* → *SAP NetWeaver Security Guide* → *Identity Management*

User Data Synchronization

SAP xIEP uses Enterprise Portal 6.0 (which is a must), and it uses the User Management Engine of the Enterprise Portal (EP). EP 6.0 uses the UME 4.0 to enable the integration of the portal with a customer's existing Lightweight Directory Access Protocol (LDAP) or other user management solution.

The Lightweight Directory Access Protocol (LDAP) option is capable of hosting a user repository of both SAP and non-SAP users, in which certain users that are created in LDAP can later be replicated to SAP systems. To allow the use of directory services for SAP systems, SAP delivers the SAP Web Application Server with the LDAP Connector. The LDAP connector controls the information flow between the SAP Web Application Server (SAP Web AS) and a directory server. Currently, this synchronization occurs as a batch process and is not real-time. Only SAP systems of version 6.10 and higher support this capability.

Users are created from the portal and saved to the LDAP directory. The portal accesses the LDAP directory for all users, but the Web Dynpro applications authorize users from SAP. This involves the following scenarios for user creation, deletion, and SAP synchronization:

- **New User with SAP Access**

  The system creates the user created in the portal and saves the user to the LDAP directory. The LDAP selects the user for SAP synchronization. Synchronization occurs during a scheduled batch process.

- **New User without SAP Access**

  The system creates the user in the portal and saves the user to the LDAP directory. No additional steps are required for SAP, but configuration may be required for third-party software.

- **User in SAP Only**

  A scheduled batch process synchronizes the user in SAP to the LDAP.

- **LDAP User Deleted**

  During synchronization, the system removes the user from SAP.

- **SAP User Deleted**

If the user is also in the LDAP and selected for synchronization, the system removes the user from the LDAP during the next scheduled synchronization.

For information about user data synchronization, see the SAP Service Marketplace at **`service.sap.com/securityguide`** under *SAP NetWeaver Security Guide* → *User Administration and Authentication* → *Integration of User Management in Your System Landscape*.

Integration into Single Sign-On Environments

The xApp Integrated Exploration and Production (xIEP) 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 SAP xIEP.

The supported mechanisms are listed below.

Secure Network Communications (SNC)

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

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

SAP Logon Tickets

The SAP xApp Integrated Exploration and Production 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.

SAP xIEP accesses SAP logon tickets, which enable Single Sign-On. The logon ticket represents user credentials and allows instant log on to applications within the portal. Once the system authenticates a user, the portal issues a logon ticket to the user. The system stores the logon ticket as a cookie on the client and sends it with each request of that client. External applications such as SAP systems can then use it to authenticate the portal user without additional log ons.

Since SAP xIEP accesses only SAP R/3 Enterprise systems, we recommend SAP logon tickets. Other Single Sign-On methods will be evaluated on an as-needed basis for future third-party software.

If the portal and Web AS are on separate servers, then both the SAP Web AS and the SAP system need to be configured to accept SAP logon tickets. Only SAP systems with release 4.0B or higher support SAP logon tickets.

Users must exist in both the Portal and the SAP backend.

For more information, see *Configuring Single Sign-On* (**`service.sap.com/instguides`** → *SAP xApps* → *SAP xApp Integrated Exploration and Production* → *SAP xIEP 1.0* → *SAP xIEP 1.0 Installation and Configuration Guide*) and *SAP Logon Tickets* in the *SAP Web Application Server Security Guide*.

Client Certificates

As an alternative to user authentication using a user ID and passwords, users using a Web browser as a frontend client can also provide X.509 client certificates to use for authentication. In this case, user authentication is performed on the Web server using 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* in the *SAP Web Application Server Security Guide*.

Network and Communication Security

The network topology for SAP xIEP 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 xIEP infrastructure. Details that specifically apply to SAP xIEP infrastructure are described in the following topics.

- Communication Channel Security

  This topic describes the communication paths and protocols used by the SAP xIEP.

- Network Security

  This topic describes the recommended network topology for SAP xIEP. 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 xIEP.

- 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*
- *Security Aspects for Connectivity and Interoperability*

Communication Channel Security

We recommend that all communication channels be encrypted for security.

As communication channels transfer all kinds of business data, they should be protected against unauthorized access. SAP offers general recommendations and technologies to protect your system landscape based on SAP NetWeaver.

⚠

You should activate the Secure Network Communication (SNC) for RFC and Secure Sockets Layer Protocol (SSL) for http within all communication channels in SAP xIEP infrastructure to achieve a secure system landscape.

In addition, we strongly advise that you only use mobile devices which can communicate via Secure Sockets Layer Protocol (SSL).

💡

For information about the communication security of SAP NetWeaver, see the SAP Service Marketplace at **`service.sap.com/securityguide`** → *SAP NetWeaver Security Guide* → *Network and Communication Security*.

For information about security aspects for connectivity and interoperability of SAP NetWeaver, see the SAP Service Marketplace at **`service.sap.com/securityguide`** → *SAP NetWeaver Security Guide* → *Security Aspects for Connectivity and Interoperability*.

For more information, go to the SAP Help Portal **`help.sap.com`** and choose *Documentation* → *SAP NetWeaver* → *English* → *SAP NetWeaver* → *Security* → *SAP NetWeaver Security Guide* → *Security Aspects for Connectivity and Interoperability*.

Network Security

Your network infrastructure is extremely important in protecting your system. SAP offers general recommendations to protect your system landscape based on SAP NetWeaver.

For information about network security of SAP NetWeaver, see the SAP Service Marketplace at **`service.sap.com/securityguide`** → *SAP NetWeaver Security Guide* → *Network and Communication Security*.

A minimum security demand for your network infrastructure is the use of a firewall for all your services provided via the Internet.

A more secure variant is to protect your systems (or groups of systems) by locating the different "groups" in different network segments, each protected with a firewall against unauthorized access. (Note that external security attacks can also come from "inside" if the intruder has already taken over control of one of your systems.)

For information about access control using firewalls, see the SAP Service Marketplace at **`service.sap.com/securityguide`** → *SAP NetWeaver Security Guide* → *Network and Communication Security - Using Firewall Systems for Access Control*.

For more information, go to the SAP Help Portal **`help.sap.com`** and choose *Documentation* → *SAP NetWeaver* → *English* → *SAP NetWeaver* → *Security* → *SAP NetWeaver Security Guide* → *Network and Communication Security* → *Additional Information on Network Security*.

Communication Destinations

SAP xIEP communicates to SAP R/3 using the SAP Java Connector (JCo). There is no independent initiation of communication from SAP R/3 to SAP xIEP; rather, it is always triggered from SAP xIEP. Using JCo, it calls the BAPIs listed below.

For this communication, two logical names are required for metadata and model data exchange. (Metadata is the structure of the data that is passed, while model data is the actual data that is passed.)

Destination	**Deliv-ered?**	**Type**	**User Authorizations**	**Description**
Metadata – WD_RFC_METDATA_DEST _XIEP	Yes	JCO.MODELDATA	SAP R/3 Enterprise User Authorizations	Metadata
Model data – WD_MODELDATA_DEST _XIEP	Yes	JCO.MODELDATA	SAP R/3 Enterprise User Authorizations	Metadata

For local data, SAP xIEP executes a Composite Application Framework validation.

In addition, ports are not fixed, but can vary depending on the set up at the customer base. We cannot hard code any port.

BAPI/RFC Destinations

- Purchase Requisition Create - BAPI_REQUISITION_CREATE
- Purchase Requisition Display - BAPI_REQUISITION_GETDETAIL
- Purchase Requisition Release - BAPI_REQUISITION_RELEASE_GEN
- Purchase Requisition Change - BAPI_REQUISITION_CHANGE
- Goods Receipt Create - BAPI_GOODSMVT_CREATE
- Purchase Order Create - BAPI_PO_CREATE
- Purchase Order Change - BAPI_PO_CHANGE
- Notification Create - BAPI_ALM_NOTIF_CREATE
- Notification Display - BAPI_ALM_NOTIF_GET_DETAIL
- Notification Change - BAPI_ALM_NOTIF_DATA_MODIFY
- Purchase Order Display - BAPI_PO_GETDETAIL
- Purchase Order Release - BAPI_PO_RELEASE
- Work Order Create - BAPI - BAPI_ALM_ORDER_MAINTAIN
- Work Order Change - BAPI - BAPI_ALM_ORDER_MAINTAIN
- Work Order Display - BAPI_ALM_ORDER_GET_DETAIL
- Notification Work Order Report - BAPI_ ALM_NOTIF_LIST_FUNCLOC,BAPI – BAPI_ ALM_NOTIF_LIST_FUNCLOC, BAPI_ALM_NOTIF_GET_DETAIL,BAPI - BAPI_ ALM_ORDERHEAD_GET_LIST, BAPI_ALM_ORDER_GET_DETAIL

- MM Tracking Report - BAPI_GOODSMVT_GETITEMS / BAPI_GOODSMVT_GETDETAIL

Data Storage Security

Use

The data storage security of SAP NetWeaver and components installed on this base is described in detail in the SAP NetWeaver Security Guide.

For information about the data storage security of SAP NetWeaver, see the SAP Service Marketplace at **service.sap.com/securityguide** → *SAP NetWeaver Security Guide* → *Operation System and Database Platform Security Guides*.

JavaScript

The JavaScript-scripting capabilities of the Internet Explorer must be activated.

If the JavaScript-scripting capabilities of the Internet Explorer are switched off, portal eventing will not work.

Trace and Log Files

The trace files, which can be viewed from the SAP Web Application Server, trace the program flow and provide details intended for development and support organizations, while the log files provide basic information intended for the administrator or user.

Traces are written to locations, and logs are written to categories. The categories for SAP xIEP are:

- /System
- /Applications
- /Performance

The following predefined sub-categories are available below the /System category:

- /System/Database
- /System/Network
- /System/Server
- /System/UserInterface
- /System/Audit

To view the logs, you use the Log Viewer of the SAP Web Application Server.

For more information about the Log Viewer, go to **help.sap.com** → *Documentation* → *SAP NetWeaver* → *English* → *SAP NetWeaver* → *Java Technology in SAP Web Application Server*.

Related Security Guides

You can find more information about the security of SAP applications on the SAP Service Marketplace, Quick Link **security**. Security guides are available using the Quick Link **securityguide**.

Quick Links to Related Information

Content	**Quick Link on the SAP Service Marketplace**
Master Guides, Installation Guides, Upgrade Guides, Solution Operations Guides	**instguides** **ibc**
Related SAP Notes	**notes**
Released platforms	**platforms**
Network security	**network** **security guide**
Technical infrastructure	**ti**