Security Guide for End Users
SAP Product Stewardship Network
Copyright

© Copyright 2010 SAP AG. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

Microsoft, Windows, Excel, Outlook, and PowerPoint are registered trademarks of Microsoft Corporation.

IBM, DB2, DB2 Universal Database, System i, System i5, System p, System p5, System x, System z, System z10, System z9, z10, z9, iSeries, pSeries, xSeries, zSeries, eServer, z/VM, z/OS, i5/OS, S/390, OS/390, OS/400, AS/400, S/390 Parallel Enterprise Server, PowerVM, Power Architecture, POWER6+, POWER6, POWER5+, POWER5, POWER, OpenPower, PowerPC, BatchPipes, BladeCenter, System Storage, GPFS, HACMP, RETAIN, DB2 Connect, RACF, Redbooks, OS/2, Parallel Sysplex, MVS/ESA, AIX, Intelligent Miner, WebSphere, Netfinity, Tivoli and Informix are trademarks or registered trademarks of IBM Corporation.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Adobe, the Adobe logo, Acrobat, PostScript, and Reader are either trademarks or registered trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Oracle is a registered trademark of Oracle Corporation.

UNIX, X/Open, OSF/1, and Motif are registered trademarks of the Open Group.

Citrix, ICA, Program Neighborhood, MetaFrame, WinFrame, VideoFrame, and MultiWin are trademarks or registered trademarks of Citrix Systems, Inc.

HTML, XML, XHTML and W3C are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.

Java is a registered trademark of Sun Microsystems, Inc.

JavaScript is a registered trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.

SAP, R/3, SAP NetWeaver, Duet, PartnerEdge, ByDesign, Clear Enterprise, SAP BusinessObjects Explorer and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and other countries.

Business Objects and the Business Objects logo, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius, and other Business Objects products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP France in the United States and in other countries.

All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary.

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

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Caution</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td></td>
</tr>
<tr>
<td>Recommendation</td>
<td></td>
</tr>
<tr>
<td>Syntax</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Type Style</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Example text</em></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Example text</strong></td>
<td>Emphasized words or phrases in body text, graphic titles, and table titles.</td>
</tr>
<tr>
<td>EXAMPLE TEXT</td>
<td>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.</td>
</tr>
<tr>
<td>Example text</td>
<td>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.</td>
</tr>
<tr>
<td>Example text</td>
<td>Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.</td>
</tr>
<tr>
<td>&lt;Example text&gt;</td>
<td>Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.</td>
</tr>
<tr>
<td>EXAMPLE TEXT</td>
<td>Keys on the keyboard, for example, F2 or ENTER.</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>--------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>History of Changes</td>
<td>6</td>
</tr>
<tr>
<td>Introduction</td>
<td>7</td>
</tr>
<tr>
<td>Before You Start</td>
<td>9</td>
</tr>
<tr>
<td>Security Aspects of Data, Data Flow and Processes</td>
<td>10</td>
</tr>
<tr>
<td>User Administration and Authentication</td>
<td>12</td>
</tr>
<tr>
<td>User Management</td>
<td>13</td>
</tr>
<tr>
<td>Integration into Single Sign-On Environments</td>
<td>14</td>
</tr>
<tr>
<td>Data Storage Security</td>
<td>15</td>
</tr>
<tr>
<td>Other Security-Relevant Information</td>
<td>16</td>
</tr>
<tr>
<td>Services for Security Lifecycle Management</td>
<td>16</td>
</tr>
</tbody>
</table>
## History of Changes

<table>
<thead>
<tr>
<th>Date</th>
<th>Topic</th>
<th>Description of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 2011</td>
<td>See Highlighting</td>
<td>Adjustments to standard template for on-demand requirements</td>
</tr>
</tbody>
</table>
Introduction

SAP Product Stewardship Network is an on-demand networked application. Depending on which scenarios of the application you use, you can collaborate with your business partners through product compliance declarations, conflict minerals declarations, or surveys that address the sustainability of products you manufacture or purchase from suppliers. This guide addresses the security of your data on SAP Product Stewardship Network.

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

Target Audience

- End users

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.

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 of your system should not result in a loss of information or processing time.

Additionally, storing personal information leads to the necessity to comply with data protection rules and fulfill the corresponding legislation to prevent the leakage and misuse of personal data and information.

These demands for security apply to SAP Product Stewardship Network. We provide this Security Guide to assist you in using SAP Product Stewardship Network securely.

About this Document

The Security Guide provides an overview of the security-relevant information that applies to SAP Product Stewardship Network from an end user’s perspective.

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 information that builds the foundation for this Security Guide.

- **Security Aspects of Data, Data Flow and Processes**
  This section provides an overview of security aspects involved throughout the most widely-used processes within SAP Product Stewardship Network.

- **User Administration and Authentication**
  This section provides an overview of the following user administration and authentication aspects:
○ Features available for user management
○ User types that are required by SAP Product Stewardship Network
○ User roles that are delivered with SAP Product Stewardship Network
○ Information on the Single Sign-On environment

• Data Storage Security
  This section provides an overview of all critical data that is used by SAP Product Stewardship Network and the security mechanisms that apply.

• Other Security-Relevant Information
  This section contains information about the following:
  ○ Active code used in the front end
  ○ Session security protection
  ○ Security lifecycle management
Before You Start

Fundamental Security Information

SAP Product Stewardship Network is built on top of SAP HANA Cloud Platform (HCP) using SAP UI5 as user interface technology as well as SAP ID Service as Identity and Access Management solution.

Fundamental Security Information

<table>
<thead>
<tr>
<th>Security related material</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP HANA Cloud Solution Brief</td>
<td>SAP HANA Cloud Solution Overview</td>
</tr>
<tr>
<td>SAP HANA Cloud Announcement</td>
<td>Announcement of ISO 27001 Certification</td>
</tr>
<tr>
<td>SAP Data Center</td>
<td>Data center home page with focus on security and certification</td>
</tr>
<tr>
<td>SAP Security Certificates</td>
<td>General SAP IT Security Certifications</td>
</tr>
</tbody>
</table>

Additional Information

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

<table>
<thead>
<tr>
<th>Content</th>
<th>Quick Link on SAP Service Marketplace or SDN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Guides</td>
<td><a href="http://service.sap.com/securityguide">http://service.sap.com/securityguide</a></td>
</tr>
<tr>
<td>Related SAP Notes</td>
<td><a href="http://service.sap.com/notes">http://service.sap.com/notes</a></td>
</tr>
<tr>
<td>Related SAP Notes</td>
<td><a href="http://service.sap.com/notes">http://service.sap.com/notes</a></td>
</tr>
<tr>
<td>Related SAP Notes</td>
<td><a href="http://service.sap.com/securitynotes">http://service.sap.com/securitynotes</a></td>
</tr>
<tr>
<td>Released platforms</td>
<td><a href="http://service.sap.com/pam">http://service.sap.com/pam</a></td>
</tr>
</tbody>
</table>
Security Aspects of Data, Data Flow and Processes

The following general security measures are in place, and are applicable to all scenarios:

- Encrypted connection through HTTPS
- User and role mapping with functional restrictions
- Access control lists limiting access to data only to permitted roles, companies and users

The table below shows the security aspect to be considered for the process step and what mechanism applies.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Security Measure</th>
</tr>
</thead>
</table>
| User registration  | SAP Product Stewardship Network provides a self-registration service for new users. | • Standard methods of SAP ID Service are applied.  
• Self registered, non-invited companies are validated by the SAP Product Stewardship Network Business Operations Team. |
| User authentication| The user logs on to the system.                                               | • Authentication process based on SAML 2.0 Standard takes place.  
• Access credentials are not stored on site.  
• Invalid session IDs and cookies are intercepted.  
• Authentication of blocked users is prevented. |
| Document upload    | Users can upload documents, including Microsoft Excel files, images, and CSV files | • Virus scanning is in place for all uploaded documents. |
| Personal data      | SAP Product Stewardship Network stores the following company-related personal information:  
- Full name  
- Company address  
- E-mail address  
- Phone number | • Personal data is protected from modification or scanning.  
• Creation, modification, and transport of data are logged.  
• A complete wipe of personal data is supported.  
• Report of personal |
| User administrative tasks | Administrators can block and unblock user accounts, add and remove user accounts, and change the role assignments of user accounts. | - The user that registers the company is assigned the company administrator role.  
- Division of responsibilities ensures that only company administrators can carry out the listed user administrative tasks. |
|----------------------------|-------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| Web Services               | SAP Product Stewardship Network offers web service interfaces.                                  | - These interfaces are available only with the Enterprise edition.                 
- Web services use basic authentication through HTTPS. |
User Administration and Authentication

SAP Product Stewardship Network uses the authentication mechanisms provided by SAP ID Service. The user management itself is specific to SAP Product Stewardship Network and does not rely on any external tools.

Information about user administration and authentication that specifically applies to SAP Product Stewardship Network is provided in the following topics:

- **User Management [Page 13]**
  This topic lists the tools to use for user management, the types of users required, and the standard users that are delivered with SAP Product Stewardship Network.

- **Integration into Single Sign-On Environments [Page 14]**
  This topic describes how SAP Product Stewardship Network supports Single Sign-On mechanisms.
User Management

User management for SAP Product Stewardship Network uses its own self-service registration as well as making use of SAP ID Service facilities.

For an overview of how these mechanisms apply to SAP Product Stewardship Network, see the sections below. In addition, we provide a list of the standard users required for working with SAP Product Stewardship Network.

User Administration Features

The table below shows the features to use for user management and user administration with SAP Product Stewardship Network.

User Management Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Detailed Description</th>
<th>Prerequisites</th>
</tr>
</thead>
<tbody>
<tr>
<td>User profile management</td>
<td>Users can edit their user profile, including personal data, within SAP ID Service.</td>
<td>None</td>
</tr>
<tr>
<td>Contact data management</td>
<td>Users can edit their contact information, including personal data, within SAP Product Stewardship Network. Company administrators can determine which user acts as company contact.</td>
<td>None</td>
</tr>
<tr>
<td>Self registration</td>
<td>Users can register for an account themselves. Accounts are provisioned by SAP ID Service. Users finalize their accounts by completing their SAP Product Stewardship Network user and company profiles. All accounts undergo validation.</td>
<td>None</td>
</tr>
</tbody>
</table>

User Types

The user types that are required for SAP Product Stewardship Network include the following:

- Individual users
  - Standard users are used for working within a specific scenario, for example, Product Compliance Declaration or Conflict Minerals. Every standard user can read and write the data owned by his or her company except the company profile. Company administrator users are used for the administration of standard users and roles within a company's account. Only company administrators are able to edit the company's profile.

- Technical users:
○ Technical users are special standard users that are used to access the web service interfaces.

User Roles

The user roles that are required for SAP Product Stewardship Network include the following:

- Customer Contact
  Scenario-specific role that has access to the relevant work center to interact with the company’s customers.

- Supplier Contact
  Scenario-specific role that has access to the relevant work center to interact with the company’s suppliers.

- Administrator
  Application-specific role that allows a user to manage the company’s users and associated roles.

Integration into Single Sign-On Environments

SAP Product Stewardship Network supports the Single Sign-On (SSO) mechanisms provided by SAP HANA Cloud Platform in conjunction with SAP ID Service. Therefore, every end user that has an account on SAP Product Stewardship Network is able to use SSO for all SAP applications that use SAP ID Service as Identity and Access Management System, for example, sap.com, or SAP Developer Network, and SAP Community Network.
Data Storage Security

Use

Data Storage

SAP Product Stewardship Network saves data in a dedicated database provided by SAP HANA Cloud Platform. Access to the database comes preconfigured with the infrastructure environment.

The database contains personal data (user profiles and company profiles), operational business data, and preferences and configurations. Information is updated continuously upon change.

Documents, such as media files and PDFs, are stored in the SAP HANA Cloud document management system.

Data Protection

Neither users nor administrators can influence the modification of data protection in any way, as all protective measures are preconfigured.

By default, business-critical information (for example, business relations) is seen only by the respective owner of this information, and business partners have to be explicitly granted access to it.

Personal information is stored in the central database. Users who want to deregister their accounts can explicitly issue a request to the support team, who will then deregister the company and users.

SAP Product Stewardship Network uses browser cookies for session management and SSO as long as the session is valid. It is ensured that httpOnly and secure flags of the cookies are set.
Other Security-Relevant Information

Active Code Used in the Front End

SAP Product Stewardship Network is an SAP UI5-based application, and as such makes heavy use of HTML5 and Javascript. Active content (at least HTML5 and Javascript) has to be enabled. This is mandatory, as SAP Product Stewardship Network will not work without it.

Session security protection

SAP Product Stewardship Network is restricted to operating with Secure Socket Layer (SSL) and activated cookie handling in the browser only.

Security lifecycle management

SAP Product Stewardship Network is hosted and operated by SAP. The Cloud Operations, Business Operations, and Development Team continuously monitor security-relevant issues and keep the system and software up to date.