Security Guide
Composite Application for Taxpayer Online Services

HELP.SECGUIDETEMPLATE

Version 2.0

Copyright

Icons in Body Text

Icon	Meaning
	Caution
	Example
	Note
	Recommendation
	Syntax

Additional icons are used in SAP Library documentation to help you identify different types of information at a glance. For more information, see *Help on Help → General Information Classes and Information Classes for Business Information Warehouse* on the first page of any version of *SAP Library*.

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`.

Introduction

This guide does not replace the administration or operation guides that are available for 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 lifecycle, whereas the Security Guides provide information that is relevant for all lifecycle 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 the composite application for taxpayer online services (eTax). To assist you in securing the composite application for TPOS, we provide this Security Guide.

About this Document

The Security Guide provides an overview of the security-relevant information that applies to the composite application for TPOS.

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 the composite application for TPOS.

- **User Administration and Authentication**

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

  - Recommended tools to use for user management.
  - User types that are required by the composite application for TPOS.
  - Standard users that are delivered with the composite application for TPOS.

- **Authorizations**

  This section provides an overview of the authorization concept that applies to the composite application for TPOS.

- **Network and Communication Security**

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

Before You Start

Fundamental Security Guides

The composite application for online tax return creation and filling is developed following the guidelines for SAP industry composite applications. Therefore, the corresponding Security Guides also apply to the composite application for backorder processing.

Fundamental Security Guides

Scenario, Application or Component Security Guide	Location
SAP NetWeaver Application Server Java Security Guide	**`help.sap.com`** → *SAP NetWeaver* → *SAP NetWeaver CE* → *SAP NetWeaver Composition Environment Library* → *Administrator's Guide* → *SAP NetWeaver CE Security Guide* →*Security Guides for CE Core Components* → *SAP NetWeaver Application Server Java Security Guide*
Portal Security Guide	**`help.sap.com`** → *SAP NetWeaver* → *SAP NetWeaver CE* → *SAP NetWeaver Composition Environment Library* → *Administrator's Guide* → *SAP NetWeaver CE Security Guide* → *Security Guides for CE Additional Components* → *Portal Security Guide*
Security Aspects of Web Dynpro for Java	**`help.sap.com`** → *SAP NetWeaver* → *SAP NetWeaver CE* → *SAP NetWeaver Composition Environment Library* → *Administrator's Guide* → *SAP NetWeaver CE Security Guide* → *Security Guides for CE Core Components* → *Security Aspects for Development Technologies* → *Security Aspects of Web Dynpro for Java*
Composite Application Framework Security Guide	**`help.sap.com`** → *SAP NetWeaver* → *SAP NetWeaver CE* → *SAP NetWeaver Composition Environment Library* → *Administrator's Guide* → *SAP NetWeaver CE Security Guide* → *Security Guides for CE Additional Components* → *Composite Application Framework Core Security Guide*
Security Aspects for Web Services	**`help.sap.com`** → *SAP NetWeaver* → *SAP NetWeaver CE* → *SAP NetWeaver Composition Environment Library* → *Administrator's Guide* → *SAP NetWeaver CE Security Guide* → *Security Guides for CE Core Components* → *Security Aspects for Web Services*

Scenario, Application or Component Security Guide	Location
Security Guide for Connectivity with the AS Java	**help.sap.com** → *SAP NetWeaver* → *SAP NetWeaver CE* → *SAP NetWeaver Composition Environment Library* → *Administrator's Guide* → *SAP NetWeaver CE Security Guide* → *Security Guides for CE Core Components* → *Security Guide for Connectivity with the AS Java*

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

Additional Information

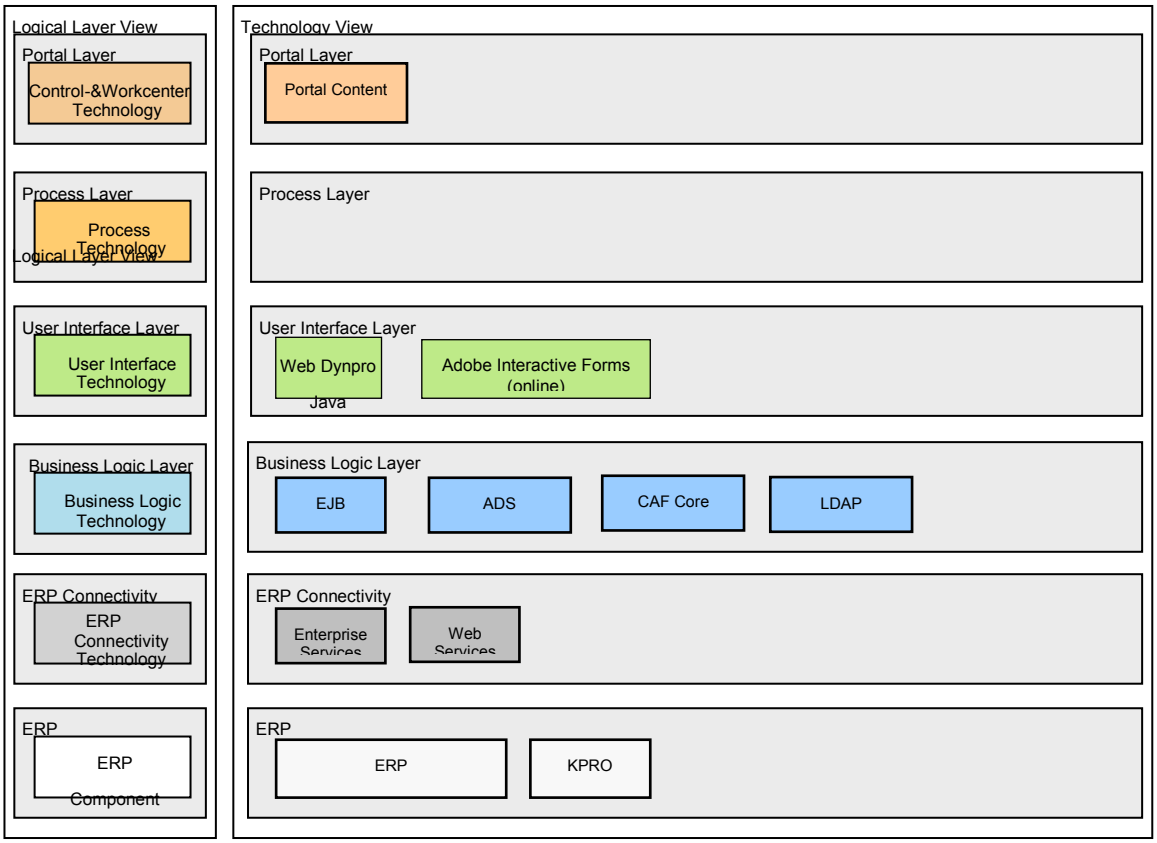
For more information about specific topics, see the addresses on the SAP Service Marketplace as shown in the table below.

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

Technical System Landscape

Use

The figure below shows the overview of the technical system landscape for the composite application for TPOS.



TPOS is an SAP industry composite application. Composite applications comprise several individual components that are loosely coupled to interact in a predetermined manner through network connections for calling application-specific functionality. This unique feature of composite applications might impose special considerations, notably the increased need for securing communication links between application components.

Logical Layer View

User Administration and Authentication

The composite application for TPOS uses the user management and authentication mechanisms provided with the SAP NetWeaver platform, in particular the SAP NetWeaver Application Server (AS) Java. Therefore, the security recommendations and guidelines for user administration and authentication as described in the SAP NetWeaver Application Server Java Security Guide also apply to TPOS.

User Management

Use

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

User management for the composite application for TPOS uses mechanisms provided with the SAP NetWeaver AS Java, for example, tools, user types, and password policies. For an overview of how these mechanisms apply to TPOS, see the sections below.

User Administration Tools

The composite application for TPOS uses the User Management Engine (UME) of SAP NetWeaver AS Java for user administration. For more information, see the relevant chapter in the SAP NetWeaver Application Server Java Security Guide.

LDAP Integration

The UME engine uses LDAP as a data source. A custom attribute is added to the LDAP users, the BusinessPartnerID field assigns the LDAP user to a backend business partner number. See the TPOS Installation & Configuration Guide for further reference.

Technical Users

The following table lists the technical users that are necessary for operating TPOS.

Technical Users

System	User ID	Type	Description
ERP	etax_itp1	Service user	Technical user used by individual taxpayer for interaction with the backend.
ERP	etax_tad1	Service user	Technical user used by tax adviser for interaction with the backend.
ERP	etax_tac1	Service user	Technical user used by tax accountant for interaction with the backend.
ERP	etax_guest	Service user	Technical user used on unauthorized area for backend interaction.

Authorizations

Use

The composite application for TPOS uses the authorization concept provided by SAP NetWeaver. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide Java also apply to TPOS.

The SAP NetWeaver authorization concept is based on assigning authorizations to users linked to roles. For role maintenance, use the user administration console in the User Management Engine (UME) on the AS Java.

For more information about how to create roles, see *Authorizations* in the SAP NetWeaver Application Server Java Security Guide.

Standard Roles

The following table lists the standard roles that are used by the composite application for TPOS.

Standard Roles

Role	Description
ArchivedDataBrowser	The user is allowed to browse the content of the archived data of TPOS.
BAdIAdministrator	The user is allowed to set and manage the BAdI configuration of TPOS.
BALAdministrator	The user is allowed to set and manage the Business Abstraction Layer configuration of TPOS.
ConfigUploader	The user is allowed to upload the standard configuration and standard content of TPOS.
ContentAdministrator	The user is allowed to set and manage the content of TPOS such as help texts, and so on.
NavAdministrator	The user is allowed to set and manage the UI navigation of TPOS.
BusinessAdministrator	The user is allowed to set and manage the business content of TPOS such as help texts, and so on.
TabAdministrator	The user is allowed to manage the Horizontal Contextual Navigation Panel (HCMP).
TechnicalAdministrator	The user is allowed to set and manage the technical configuration of TPOS.
QuestionAdministrator	The user is allowed to manage the questionnaire framework.
RoadmapAdministrator	The user is allowed to manage the RoadMaps
End-User	The end is allowed to use the TPOS functionalities (Filing, payment, and so on).

Standard Groups

You must create standard groups in LDAP. For more information, see the Installation and Configuration Guide for TPOS.

Standard Groups

Group	Description
etax_tad	Required to access the TPOS as a tax adviser.
etax_tac	Required to access the TPOS as a tax accountant.
etax_itp	Required to access the TPOS as an individual taxpayer.
etax_guest	Required to access the TPOS as a guest user on unauthorized area.

Standard Authorization Objects

The following table lists the technical roles delivered with the composite application for TPOS.

Technical Roles

Role	Description
com.sap.cmp.ETAX.eTAXArchivedDataBrowser	Required to access the archived data of the TPOS.
com.sap.cmp.ETAX.eTAXBAdIAdministrator	Required to access the TPOS as a BAdI Administrator.
com.sap.cmp.ETAX.eTAXBALAdministrator	Required to access the TPOS as a Business Abstraction Layer Administrator.
com.sap.cmp.ETAX. eTAXConfigUploader	Required to access the standard configuration upload.
com.sap.cmp.ETAX.eTAXContentAdministrator	Required to access the TPOS as a Content Administrator.
com.sap.cmp.ETAX.eTAXNavAdministrator	Required to access the TPOS as a Navigation Administrator.
com.sap.cmp.ETAX.TOSBusinessAdministrator	Required to access the TPOS as a Business Administrator.
com.sap.cmp.ETAX.eTAXTabAdministrator	Required to access the HCMP management of TPOS.
com.sap.cmp.ETAX.TOSTechnicalAdministrator	Required to access the TPOS as a Technical Administrator.
com.sap.cmp.ETAX.TPOSQuestionAdministrator	Required to access the Questionnaire Framework management for TPOS
com.sap.cmp.ETAX.TPOSRoadmapAdministrator	Required to access the RoadMap configuration of TPOS.
com.sap.cmp.ETAX.UserRole	Required to access the TPOS as and End-User in the Enterprise Portal.

Access Controls

Object	Role	Access type
StandardProperty	com.sap.cmp.ETAX.eTAXBAdIAdministrator	read
	com.sap.cmp.ETAX.eTAXBALAdministrator	read
	com.sap.cmp.ETAX.eTAXContentAdministrator	read
	com.sap.cmp.ETAX.eTAXNavAdministrator	read
	com.sap.cmp.ETAX.TOSBusinessAdministrator	read/write/delete
	com.sap.cmp.ETAX.TOSTechnicalAdministrator	read/write/delete

Object	Role	Access type
StandardProperty	com.sap.cmp.ETAX.eTAXBAdIAdministrator	read
	com.sap.cmp.ETAX.eTAXBALAdministrator	read
	com.sap.cmp.ETAX.eTAXContentAdministrator	read
	com.sap.cmp.ETAX.eTAXNavAdministrator	read
	com.sap.cmp.ETAX.TOSBusinessAdministrator	read/write/delete
	com.sap.cmp.ETAX.TOSTechnicalAdministrator	read/write/delete
	com.sap.cmp.ETAX.UserRole	read
CustomProperty	com.sap.cmp.ETAX.eTAXBAdIAdministrator	read/write/delete
	com.sap.cmp.ETAX.eTAXBALAdministrator	read/write/delete
	com.sap.cmp.ETAX.eTAXContentAdministrator	read/write/delete
	com.sap.cmp.ETAX.eTAXNavAdministrator	read/write/delete
	com.sap.cmp.ETAX.TOSBusinessAdministrator	read
	com.sap.cmp.ETAX.TOSTechnicalAdministrator	read
	com.sap.cmp.ETAX.UserRole	read
	com.sap.cmp.ETAX.eTAXConfigUploader	read/write/delete
	com.sap.cmp.ETAX.eTAXTabAdministrator	read/write/delete
	com.sap.cmp.ETAX.TPOSQuestionAdministrator	read/write/delete
	com.sap.cmp.ETAX.TPOSRoadmapAdministrator	read/write/delete
JavaScriptContent, PlainTextContent, URLContent, XHTMLContent	com.sap.cmp.ETAX.eTAXBAdIAdministrator	no access
	com.sap.cmp.ETAX.eTAXBALAdministrator	no access
	com.sap.cmp.ETAX.eTAXContentAdministrator	read/write/delete
	com.sap.cmp.ETAX.eTAXNavAdministrator	no access

Object	Role	Access type
StandardProperty	com.sap.cmp.ETAX.eTAXBAdIAdministrator	read
	com.sap.cmp.ETAX.eTAXBALAdministrator	read
	com.sap.cmp.ETAX.eTAXContentAdministrator	read
	com.sap.cmp.ETAX.eTAXNavAdministrator	read
	com.sap.cmp.ETAX.TOSBusinessAdministrator	read/write/delete
	com.sap.cmp.ETAX.TOSTechnicalAdministrator	read/write/delete
	com.sap.cmp.ETAX.TOSBusinessAdministrator	read/write/delete
	com.sap.cmp.ETAX.TOSTechnicalAdministrator	read/write/delete
	com.sap.cmp.ETAX.UserRole	read
	com.sap.cmp.ETAX.eTAXConfigUploader	read/write/delete
AdobeDocument (cache)	com.sap.cmp.ETAX.eTAXBAdIAdministrator	no access
	com.sap.cmp.ETAX.eTAXBALAdministrator	no access
	com.sap.cmp.ETAX.eTAXContentAdministrator	no access
	com.sap.cmp.ETAX.eTAXNavAdministrator	no access
	com.sap.cmp.ETAX.TOSBusinessAdministrator	no access
	com.sap.cmp.ETAX.TOSTechnicalAdministrator	no access
	com.sap.cmp.ETAX.UserRole	read/write/delete

Communication Channel Security

Use

The following table shows the communication channels used by composite application for TPOS, the protocol used for the connection, and the type of data transferred:

Communication Channels Used in the Composite Application for TPOS

Communication Channel	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Composite application for tax &revenue management (TRM) connecting to ERP backend via **eSOA services**	HTTP	Tax returns, fillings, and business partner data.	None
Composite application for tax &revenue management (TRM) connecting to ERP backend via **Web services**	HTTP	Value helps.	None
Composite application to the client browser	HTTP	Content of the web pages.	None

HTTP connections are protected using the Secure Sockets Layer (SSL) protocol.

For more information, see *Transport Layer Security* in the SAP NetWeaver Application Server Java Security Guide.

Communication Destinations

Use

The following table gives an overview of the communication destinations used by the composite application for TPOS:

Connection Destinations

Destination	Delivered	Type	User, Authorizations	Description
ERP	Yes	HTTP	etax_itp1, etax_tad1, etax_tac1, etax_guest	Communication destination for the TRM.
LDAP	Yes	HTTP	etaxadminos	Communication destination for the user directory.

Data Storage Security

Use

The composite application for TPOS uses data storage functionalities provided by SAP NetWeaver AS Java and the Composite Application Framework (CAF). Data is also stored in the individual systems used by TPOS as a backend system. Different backend systems have different methods for ensuring data storage security. Depending upon which backend system type you are using, we recommend you refer to the guides below:

Scenario, Application or Component Security Guide	Location
SAP NetWeaver Application Server Java Security Guide	**help.sap.com** → *SAP NetWeaver* → *SAP NetWeaver CE* → *SAP NetWeaver Composition Environment Library* → *Administrator's Guide* → *SAP NetWeaver CE Security Guide* →*Security Guides for CE Core Components* → *SAP NetWeaver Application Server Java Security Guide*
Composite Application Framework Security Guide	**help.sap.com** → *SAP NetWeaver* → *SAP NetWeaver CE* → *SAP NetWeaver Composition Environment Library* → *Administrator's Guide* → *SAP NetWeaver CE Security Guide* → *Security Guides for CE Additional Components* → *Composite Application Framework Security Guide*
User Management Engine Security Guide	
Security Guide for ERP Backend System(s)	**help.sap.com** → *SAP Solutions* → *SAP ERP* → *ERP Central Component 6.0 SR1 (English)* → *mySAP ERP Security Guides*

For more information about securing CAF business objects, see SAP Library documentation on the following topics:

Topic	Location
Managing the Business Object Rules List	**help.sap.com** → *SAP NetWeaver* → *SAP NetWeaver CE* → *SAP NetWeaver Composition Environment Library* → *Developer's Guide* → *Composing Services with CAF* → *Tasks* → *Securing Your Composite Application* → *Protecting Access to Business Object Operations* → *Managing the Business Object Rules List*
Managing the Access Control List	**help.sap.com** → *SAP NetWeaver* → *SAP NetWeaver CE* → *SAP NetWeaver Composition Environment Library* → *Developer's Guide* → *Composing Services with CAF* → *Tasks* → *Securing Your Composite Application* → *Protecting Access to Business Object Operations* → *Managing the Access Control List*

Topic	Location
Managing the Conditions List	**help.sap.com** → *SAP NetWeaver* → *SAP NetWeaver CE* → *SAP NetWeaver Composition Environment Library* → *Developer's Guide* → *Composing Services with CAF* → *Tasks* → *Securing Your Composite Application* → *Protecting Access to Business Object Operations* → *Managing the Conditions List*

For more information about securing storage in SAP systems, see *Data Storage Security* in the SAP NetWeaver Application Server Java Security Guide.

Data Protection and Privacy

Use

SAP industry composite applications use technologies provided by the CAF for storing data. That way, data can be stored either within the composite by means of CAF entity services or on a service-enabled remote SAP system by using CAF external services indirectly via entity services.

For more information about securing data, see the relevant documentation as listed in the following table:

Type of Data Storage	Location
Securing CAF entity services	**help.sap.com** → *SAP Solutions* → *SAP NetWeaver* → *SAP NetWeaver CE* → *SAP NetWeaver Composition Environment 7.1* → *SAP NetWeaver Composition Enviornment Library* → *Developer's Guide* → *Developing and Composing Applications* → *Composing Services with CAF* → *Tasks* → *Composite Application Service Security* → *Protecting Access to Business Object Operations*
Securing CAF external services	**help.sap.com** → *SAP NetWeaver* → *SAP NetWeaver CE* → *SAP NetWeaver Composition Environment Library* → *Administrator's Guide* → *SAP NetWeaver CE Security Guide* →*Security Guides for CE Core Components* → *SAP NetWeaver Application Server Java Security Guide*
Securing storage in SAP systems	**help.sap.com** → *SAP Solutions* → *SAP NetWeaver* → *SAP NetWeaver CE* → *SAP NetWeaver Composition Environment 7.1* → *SAP NetWeaver Composition Enviornment Library* → *Administrator's Guide* → *Administration of SAP NetWeaver CE* → *General System Administration* → *Administration Tools* → *Config Tool* → *Managing Secure Store Data*

Other Security-Relevant Information

Use

TPOS administrators can create xHTML content that is used by the application. Since xHTML creation may pose security risks, the application checks the HTML tags before sending them the client browser.

The application applies a whitelist against the unwanted xHTML tags. This security check is performed in two points of the application.

1. The check is executed when the administrator uploads the xHTML content
2. The check is executed when the UI layer of the application request for the xHTML content.

The whitelist allows the following xHTML tags as is:

`bbr,acronym,address,blockquote,br,cite,code,dfn,div,em,h1,h2,h3,h4,kbd,p,pre,q,samp,span,strong,var,DI,dt,dd,ol,ul,li,a,img`

The administrators must use the opening and the closing pair of a tag, for example,
</BR>.

No other tags, and no further attributes are allowed in the xHTML content.

Modifying the Whitelist

The list of the tags can be modified through a JAVA resource file called XHTMLWHITELIST. The modification can be performed in the ConfigTool.

Security Logging and Tracing

Use

The composite application for TPOS uses the logging features of the SAP NetWeaver AS Java.

For more information about logging and tracing in the SAP NetWeaver AS Java, see *Logging and Tracing* in the SAP NetWeaver Application Server Java Security Guide.

The following table lists the logging category and tracing location used by SIR:

Logging Category	*/Applications/etax*
Tracing Location	*com.sap.is.cmp.etax.<package name>*