SAP NetWeaver 2004s SPS 4

Security Guide

Security Guide Communication Interfaces

Document Version 1.00 – October 24, 2005

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`

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
	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 Communication Interfaces

Purpose

This section provides information on the security aspects of the Integrated Communication Interface [SAP Library] (ICI), specifically the relevant security settings required for the Business Communication Broker (BCB) which is part of the ICI.

Further Information

The detailed information on BCB/ICI security settings you can find here:

1 BCB/ICI Security

Purpose

This guide describes the security aspects for the Business Communication Broker (BCB) and the underlying Integrated Communication Interface [SAP Library] (ICI). Since both components are running on the SAP J2EE Engine - the BCB as library, the BCB administration as web application and the ICI as enterprise application resp. web service - most of its security features are explained in the *SAP Web AS Security Guide for Java Technology*.

Why Is Security Necessary?

As the SAP part of the ICI is implemented as web service communicating with the external contact center software via HTTP, there could be attacks from the Internet to this web service. To be safe against such attacks the SAP Web AS with the deployed ICI as well as the external contact center software should be placed behind a firewall at customer side.

With the current ICI version on SAP NetWeaver 04 only HTTP will be supported. Using a HTTPS connection between the SAP J2EE Engine and the external contact center software for exchanging the ICI-related SOAP messages is not possible.

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, whereby the Security Guides provide information that is relevant for all time frames.

Further Information

See also the Security Guide for the SAP J2EE Engine:

- SAP Web AS Security Guide for Java Technology [SAP Library]

2 User Administration and Authentication

There are no special users needed for working with the BCB/ICI. So no BCB/ICI-specific user administration and authentication is implemented.

3 Authorizations

- This section provides an overview of the different BCB authorization areas and measures that are required their protection.

Changing the BCB settings

Calling the BCB administration page that is part of the Web application "bcbadm" and changing the BCB settings, e.g. changing the contact center URL, is allowed to J2EE Engine users with administrator privileges only (see note 752579).

Working with the Contact Center Simulator UI

Working with the CCS User Interface that is part of the web application “ccsui” is allowed to J2EE Engine users with administrator privileges only.

Requesting contact center functions

Within every SOAP message header there is a parameter for the user who requested a specific function, e.g. drop a phone call or send an email. Thus, the receiving system has the possibilty to check the authorization of this user for invoking the function.

Getting SAP J2EE Engine installation data at runtime

The ICI queries SAP J2EE Engine installation data such as host name and http port at runtime using the SAP J2EE Engine adminadapter service. This information is needed to let the contact center software know where to send back its SOAP messages signaling status changes of phone calls, messages, chat sessions and contact center agents.

Since using the adminadapter service at runtime is allowed for users with administrator rights only, a new security role *BcbAdmin* mapped to the server role *administrators* is defined in the deployment descriptor *ejb-j2ee-engine.xml* of the ICI application *tc~bcb~ici*.

This role *BcbAdmin* is then used in the *run-as*-element in the deployment descriptor *ejb-jar.xml* of the ICI application *tc~bcb~ici* to ensure that the ICI is running with administrator rights when querying host and port of the actual SAP J2EE Engine installation.

4 Communication Channel Security

Communication between BCB library and ICI enterprise application

The standard J2EE technologies JNDI, EJB and JMS are used for the communication between the BCB library and the ICI enterprise application.

Communication between ICI enterprise application and external contact center software:

The technology used for the communication between ICI and the external contact center is SOAP over HTTP as provided by the SAP J2EE Engine Web Service Framework. Please note, that the ICI currently does not support HTTPS.

The data transferred within the SOAP messages is described in detail in the ICI specification, e.g. a phone number to dial, call attached data, an internet message in MIME format. There are no specific security mechanisms to protect these data.

To protect both partners of this communication channel against attacks from the Internet a firewall must be installed at customer-site.

5 Communication Destinations

The destination to the SAP Contact Center Simulator is computed out off the SAP J2EE Engine's host name and http port during the first call of the BCB administration page. It is stored in the text file `usr/sap/<SID>/SYS/global/bcb/bcb_customizing.properties`.

The destination to the real contact center must be set by a system administrator via the BCB administration page. It is also stored in the `bcb_customizing.properties` file.

Connection Destinations

Destination	Delivered?	Type	User, Authorizations	Description
… to the SAP Contact Center Simulator that is part of the ICI application	Yes	HTTP	-	Please see the ICI online documentation for more information.
… to the real external contact center software	No	HTTP	-	Please see the ICI online documentation for more information.

6 Data Storage Security

- No secure data that has to be protected is stored in BCB / ICI.

7 Security for Additional Applications

- Security features of the external contact center software connected to SAP via ICI are not in the scope of this document. Please contact the vendor of this 3rd-party software for this information.

8 Other Security-Relevant Information

Disabling Java Script

The BCB administration home pages uses JavaScript to check the values entered when customizing the BCB, i.e. when entering the contact center URL. If JavaScript is disabled and the system administrator enters a wrong contact center URL, e.g. URL without port, the system administrator won't get a warning pop-up saying that the settings can not be saved.

Starting and stopping the BCB Web application:

If you do not use the BCB application live, but nevertheless fear a security gap, you can simply stop the BCB. To do this, call the Deploy Service in the Visual Administrator of the SAP J2EE Engine and stop the application "bcbici" (Release 6.20) resp. tc/bcb/ici" (Release >= 6.30). This causes the two "bcbadm" (BCB Administration) and "ccsui" (SAP Contact Center Simulator) Web applications to deactivate.