

SAP NetWeaver Visual Composer Security Guide



SAP NetWeaver Visual Composer release 6.0



Document version 1.0

Copyright

© Copyright 2004 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, Outlook, and PowerPoint are registered trademarks of Microsoft Corporation.

IBM, DB2, DB2 Universal Database, OS/2, Parallel Sysplex, MVS/ESA, AIX, S/390, AS/400, OS/390, OS/400, iSeries, pSeries, xSeries, zSeries, z/OS, AFP, Intelligent Miner, WebSphere, Netfinity, Tivoli, and Informix are trademarks or registered trademarks of IBM Corporation 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.

MaxDB is a trademark of MySQL AB, Sweden.

SAP, R/3, mySAP, mySAP.com, xApps, xApp, SAP NetWeaver, 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 in several other countries all over the world. 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

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
<i>Sample text</i>	Words or characters quoted from the screen. These include field names, screen titles, pushbutton labels, menu names, menu paths, and menu options. Cross-references to other documentation.
sample text	Emphasized words or phrases in body text, graphic titles, and table titles.
SAMPLE 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.
Sample 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.
sample text	Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.
<sample text>	Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.
SAMPLE TEXT	Keys on the keyboard, for example, F2 or ENTER.

Contents

SAP NetWeaver Visual Composer Security Guide	5
Before You Start	6
Technical System Landscape	7
User Administration and Authentication.....	8
User Management.....	8
Integration into Single Sign-On Environments	8
Network and Communication Security.....	9
Data Storage Security	10
Other Security-Relevant Information	10
Trace and Log Files	11



SAP NetWeaver Visual Composer Security Guide

Introduction

SAP NetWeaver Visual Composer is a design tool that enables users to develop sophisticated content for SAP Enterprise Portal. The iViews created through Visual Composer are deployed to a connected portal so that at runtime, they can operate like all portal iViews, processing data from back-end systems. Visual Composer operates on top of SAP Enterprise Portal's general connector-framework interfaces so that connectivity is provided to other third-party applications in addition to SAP R/3 enterprise systems.

Why Is Security Necessary?

With the increasing use of distributed systems and the Internet for managing business data, the demands for tight security are also on the rise. When using a distributed system, you need to ensure 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 security demands also apply to SAP NetWeaver Visual Composer.

About this Document

This security guide provides an overview of the security-relevant information that applies to Visual Composer, operating in conjunction with SAP Enterprise Portal. It covers the following main topics:

- **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 used by the Visual Composer.

- **User Administration and Authentication**

This section explains how user administration and authentication are accomplished when connecting to Enterprise Portal.

- **Network and Communication Security**

This section provides an overview of the communication paths used by Visual Composer and the security mechanisms that apply.

- **Data Storage Security**

This section describes the security mechanisms that apply to the storage of Visual Composer data.

- **Other Security-Relevant Information**

- **Trace and Log Files**

This section details the trace and log files maintained for Visual Composer, on the Storyboard server and on the portal server.



Before You Start

Fundamental Security Guides

SAP NetWeaver Visual Composer version 6.0 can be used to create design-time models that include data services imported from the following systems:

- SAP R/3 Enterprise
- SAP BI and BW
- Siebel systems, versions 6.0 and above
- JDBC-compliant databases

The following table lists the security guides available for these systems. The SAP guides listed are all accessed through the *SAP NetWeaver Security Guide* on SAP Help portal, at: help.sap.com/nw04 → *SAP Library* → *SAP NetWeaver* → *Security* → *SAP NetWeaver Security Guide*

Product	See
SAP R/3 Enterprise	<i>SAP NetWeaver Security Guide</i> → <i>Security Guides for the SAP NetWeaver Components</i> → <i>SAP Web Application Server Security Guide</i>
SAP BI and BW	<i>SAP NetWeaver Security Guide</i> → <i>Security Guides for the SAP NetWeaver Components</i> → <i>SAP Business Information Warehouse Security Guide</i>
Siebel enterprise systems	Siebel eService <i>Administration Guide</i> and other relevant documentation available through: https://ebusiness.siebel.com/supportweb
JDBC-compliant databases	<i>SAP NetWeaver Security Guide</i> → <i>Security Guides for the SAP NetWeaver Components</i> → <i>SAP Business Information Warehouse Security Guide</i> → <i>Portal Security Guide</i> → <i>Communications with Backend Systems</i>

Portal Documentation

In order to create the design-time model, SAP NetWeaver Visual Composer imports data services through SAP Enterprise Portal. In run-time, the portal security mechanisms are applied. All of these measures are outlined in the *Portal Security Guide* and the *SAP NetWeaver Security Guide*.

For other security information relevant to SAP NetWeaver Visual Composer, see SAP Note 716752.

Technical System Landscape

Use

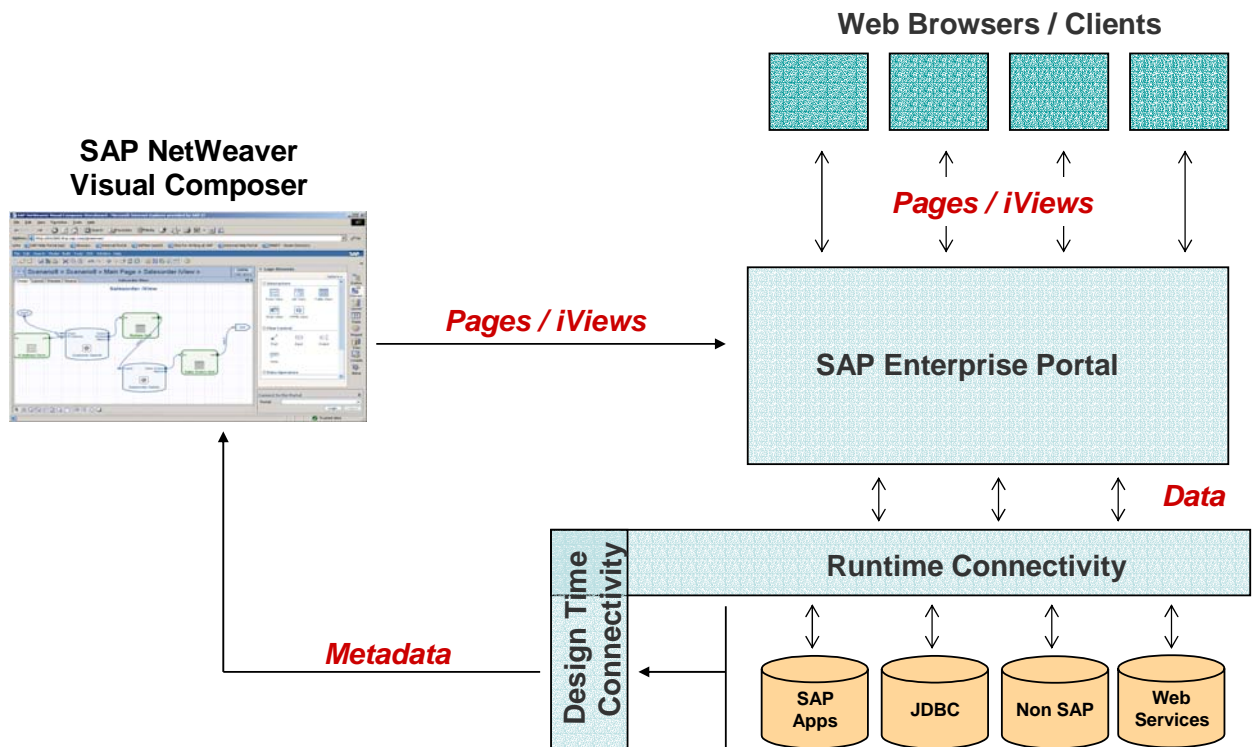
The Visual Composer compiler generates packages that can be deployed to any SAP Enterprise Portal using the standard deployment procedure. Once deployed, the pages and iViews created by Visual Composer can retrieve data from the SAP Enterprise Portal runtime connectivity framework and display this information just like any other hand-coded portal pages and iViews.

Visual Composer provides access, through the portal connectivity framework, to a range of function modules residing in SAP and third-party back-end systems. The Visual Composer installation is comprised of the following components:

- **Visual Composer Server**, made up of the following: Web Server (IIS), Storage Layer (MS SQL), Visual Composer Storyboard (the Visual Composer interface used for portal content development)
- Visual Composer **Addons to SAP Enterprise Portal** (connects Visual Composer to portal)

Being a fully Web-based application, Visual Composer users can access the Storyboard from any client machine.

The following figure depicts the technical system landscape for Visual Composer.





User Administration and Authentication

Being as Visual Composer is a design-time tool only, user administration and authentication is not implemented in the application. For runtime operation – through SAP Enterprise Portal – the standard user administration and authentication mechanisms of the portal apply.

See *SAP NetWeaver Security Guide* → *SAP NetWeaver* → *Security* → *User Authentication and Single Sign-On* → *Authentication on the Portal*.

For Siebel applications, see the Siebel eBusiness Applications *Authentication and Access Control Administration Guide*.

User Management

No user management is implemented in Visual Composer. For runtime operation, standard portal user management is implemented.

See *SAP NetWeaver Security Guide* → *SAP NetWeaver* → *Security* → *Security Guides for the SAP NetWeaver Components* → *Portal Security Guide* → *User Management and Security Files*

For Siebel applications, see the Siebel eService *Administration Guide*.

Integration into Single Sign-On Environments

In order to ensure smooth connectivity between Visual Composer and SAP back-end systems, the portal and the back-end system should be configured for single sign-on, using one of three methods:

- SAP logon tickets without user mapping
- SAP logon tickets with user mapping
- User ID and password with user mapping

For more information about these methods, see *SAP NetWeaver Security Guide* → *SAP NetWeaver* → *Security* → *User Authentication and Single Sign-On* → *Authentication on the Portal*.



Network and Communication Security

The runtime network topology for SAP NetWeaver Visual Composer is that of Enterprise Portal operating on the SAP NetWeaver platform. Therefore, the security guidelines and recommendations described in the *SAP NetWeaver Security Guide* also apply to the Visual Composer. The following sections outline communication details specific to Visual Composer.

Communication Channel Security

Protecting the information transferred between the client and the Visual Composer server, and between the Visual Composer server and SAP Enterprise Portal is important. The data transferred contains authentication credentials and possibly other sensitive data that must not be known to third parties. This kind of data must be encrypted using secure communication protocols such as Secure Sockets Layer (SSL).

The following communications channels are used with Visual Composer:

- Client to Visual Composer server
- Client to SAP Enterprise Portal
- Visual Composer to SAP Enterprise Portal
- SAP Enterprise Portal to back-end applications

HTTP, HTTPS and SSL technologies are used in the first three communication channels to transfer data and meta-data from back-end systems, and user authentication data from Visual Composer to the portal. For the last channel, see the *Portal Security Guide*.

The following table summarizes the communication paths used by Visual Composer, the protocol used for the connection, and the type of data transferred.

Communication Paths

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Client to Visual Composer server	HTTP, HTTPS, SSL	All application data	None
Client to portal	HTTP, HTTPS, SSL	User credentials, portal authentication	Passwords
Visual Composer server to portal	HTTP, HTTPS, SSL	All application data	None
Portal to back-end applications	HTTP, HTTPS, SSL, RFC, DIAG; see <i>Portal Security Guide</i>	Data and metadata	

DIAG and 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 the *Transport Layer Security* section in the *SAP NetWeaver Security Guide*.

Network Security

Visual Composer is a component designed for use in the SAP NetWeaver development environment. Generally, it is a client browser-based application, operating in most network environments, and connecting via HTTP ports to the various communication channels.



Data Storage Security

Use

All Visual Composer data is stored in a Microsoft SQL database created during Storyboard installation. Exported and imported models are stored in the file system. The default path for these exports on the Visual Composer server is:

```
. . . \inetpub\wwwroot\SAP NetWeaver Visual Composer\data.
```

Each time a user saves a model in Visual Composer Storyboard, the database is updated. To export/import a model between Storyboards, the user can export the model and then save the data in a different location.

In order to ensure a proper connection to the Microsoft SQL server, the database must be set up for authentication based on *SQL Server and Windows mode (mixed mode)*. If it is set up to run in *Windows only mode*, the connection will not work. This setup is explained in the *SAP NetWeaver Visual Composer Installation Guide*.

For more information about guaranteeing data protection in the Windows environment, see *SAP Library → SAP NetWeaver → Security → SAP NetWeaver Security Guide → Operating System and Database Platform Security Guides → SAP System Security under Windows*.

Visual Composer is a fully Web-based application. It uses cookies for storing desktop customization parameters entered by the user through the *Tools → Options* dialog boxes. This data is stored indefinitely in the cookies, requiring the user to take no security measures to maintain them.

Other data stored on the client is the information concerning the last model opened and modified on Storyboard. According to user preferences, this model can be automatically displayed when that Storyboard is next accessed. No user protection is required.

User details are not stored on the client because Visual Composer operates without a user management mechanism.



Other Security-Relevant Information

Use

In order to implement the two-dimensional graphics required for creating the models, Visual Composer uses the W3C SVG standard, implemented by Adobe as an ActiveX control in the Adobe SVG Viewer.

Adobe SVG Viewer 3.0 must be installed on the client machine; Visual Composer cannot operate without this software.



Trace and Log Files

Use

Events occurring in Visual Composer are logged both on the Visual Composer server and on the connected portal.

- **On the Visual Composer server**, events are logged, optionally, in the Output Console located at the bottom of the workspace. It can be viewed in Storyboard by dragging open the status bar at the bottom of the Storyboard desktop. Events are logged for the duration of the client session. The server administrator can control the display in the console, showing only errors, only warnings, or all information. The actual file that controls the display of information resides in the following path of the Visual Composer server:

```
...inetpub\wwwroot\SAP NetWeaver Visual  
Composer\server\~server.ini
```

Only administrators with access to the Visual Composer server machine can access this file; no direct access is available from the client machine. Any changes to the file affect all end users accessing Storyboard from that server.

- **On the portal**, all exceptions occurring in Visual Composer are registered and maintained in log files residing on the portal server.
 - On servers running Enterprise Portal 6.0 SP2, there are two log files:
visualComposer_NWHTMLBKit_logger.log and
guimachine_portalconnector.log.
They are located in the following path:
usr\sap\...\j2ee\j2ee_03\cluster\server\managers\log\portal
\logs
 - On servers with Enterprise Portal running on SAP NetWeaver 2004, a number of log files are located in the following path:
usr\sap\... \j2ee\cluster\server_0\log

A SAP NetWeaver log viewer contains all NetWeaver logs, including one for Visual Composer.

Only portal users with System Administrator authorization can access these files.