Security Guide

Visual Composer for SAP NetWeaver Composition Environment

Document Version 1.00 – November 2007
SAP NetWeaver Composition Environment 7.1 SP 03

Typographic Conventions

Type Style	Represents
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 / Tip
	Recommendation
	Syntax

Contents

Document History

Document version	Description
V 1.0	SAP Library release of document, with SPS 03. The following section was updated since the SPS 01 release: ▪ *Data Storage Security:* Reference added to the SAP NetWeaver Application Server Java Security Guide

Visual Composer Security Guide

This security guide is an integral part of the *CE Security Guide* and outlines only those security issues that are specific to running Visual Composer for CE.

Topics

1 Technical System Landscape

The Visual Composer server is installed as part of the NetWeaver CE usage type, on the development server.

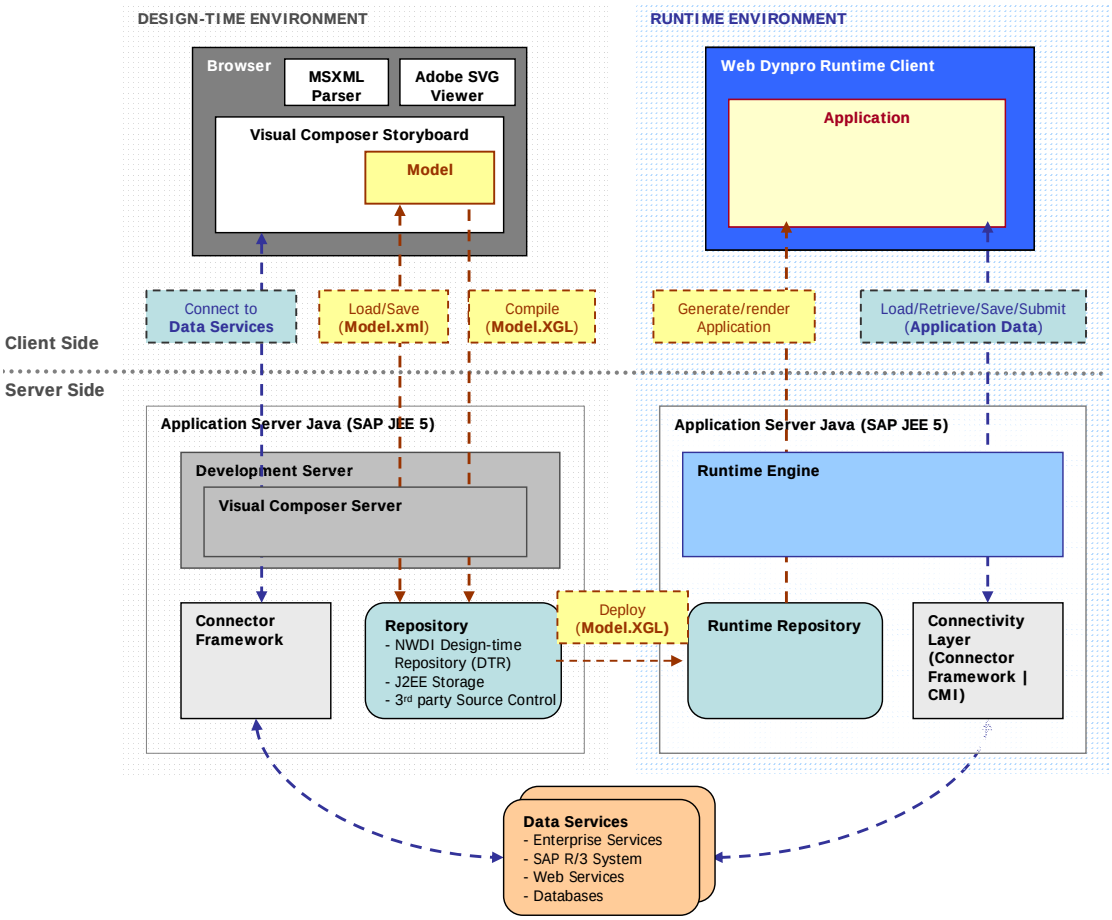
- At design time, the modeler accesses Visual Composer Storyboard from the client machine through Microsoft Internet Explorer, version 6.0 and higher.
- Models are compiled and deployed as Web Dynpro applications to the Web Dynpro runtime repository on the Application Server Java (AS Java).
- At runtime, a user accesses the deployed Web Dynpro application using the browser.

The technical system landscape for Visual Composer contains the following components:

- Server: on the AS Java
  - Visual Composer server: resides as a service on the development server
  - NetWeaver portal: optional component
- Model storage: for storing Visual Composer models in one of two possible locations:
  - JEE 5 database, in a repository dedicated to the development server. This storage has both user-specific private storage, and a shared storage that functions as a source control system.
  - Design-time repository (DTR), the NWDI source control system, into which models can be checked in.
- Visual Composer client
  - Design time:
    - Adobe SVG Viewer 3.0 or higher
    - Microsoft XML Parser 4.0
  - Runtime: Web Dynpro

In addition, a build plug-in is installed and added to the central build system (CBS) for performing automatic build operations on Visual Composer models.

The following figure shows an overview of the technical system landscape for SAP Visual Composer.



All server-side components are installed on a single host in both the development and production environments; they differ only in configuration.

Connectivity to the back-end systems is provided by the connector framework layer, as follows:

Connectivity

System	Design Time	Runtime (Web Dynpro)
ERP	Connector framework	Connector framework
Web services	Connector framework	Connector framework
Enterprise services/UDDI	Connector framework	Connector framework

Kit Extensions

Visual Composer Storyboard can be extended through use of dedicated kits, which extend both client-side and server-side functionality. This security guide relates to the Visual Composer core kits (which are part of the default installation) and the Web Dynpro for Visual Composer runtime. Other kits are BI and Voice (which connects to a third-party voice server). Each kit potentially presents a set of security vulnerabilities that are addressed in the Security Guide for that kit.

2 User Administration and Authentication

Visual Composer uses the user management and authentication mechanisms provided with the SAP NetWeaver platform, in particular the SAP NetWeaver Application Server Java (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 Visual Composer. For more information, see SAP NetWeaver Application Server Java Security Guide [External].

Visual Composer allows access to two AS Java roles: *Administrator* and *VisualComposerUser*. These roles have all the necessary permissions to allow a user to perform modeling tasks while working with Visual Composer Storyboard, such as create, develop, manage and deploy.

It is the administrator's responsibility to manage user accounts for the designers who create models with Visual Composer, and to assign them the *VisualComposerUser* role. All user administration and authentication is carried out through AS Java UME service. For more information, see the User Administration and Standard Users [External] section of the *SAP NetWeaver Application Server Java Security Guide*.

To provide access to back-end systems, each Visual Composer user should be assigned (at least) read permissions to the relevant system(s), to access the needed data services.

3 Network and Communication Security

Visual Composer is deployed to a single Application Server Java (AS Java) or to a cluster, rather than to a distributed environment. Therefore, there are no specific network security considerations other than those that apply to SAP NetWeaver Portal, AS Java or any other Java-based NetWeaver application server or application.

The network topology for Visual Composer is based on the topology used by the SAP NetWeaver platform. Therefore, the general security guidelines and recommendations described in the SAP NetWeaver Security Guide also apply to Visual Composer. Details that specifically apply to Visual Composer are described in the topics that follow.

The following table provides detailed information about the communication paths used by Visual Composer, the protocols used for the connection and the type of data transferred.

Communication Paths

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
Storyboard (client) to services in development server (Visual Composer server, Visual Composer builder and so on	XML over HTTP (or HTTPS)	Model data, requests from the Visual Composer server, requests for data services	
Check in model from development server to DTR	Standard SAP SDIC protocol	`.gml` files, `.xgl` files and other related files	
Deploy application to local AS Java runtime repository	Standard API of AS Java deployment mechanism	`.ear` file containing a set of modules (`.war` files or other types)	
Web Dynpro client to AS Java	As specified in the Security for Web Dynpro for Java [External] guide	As specified in the Security for Web Dynpro for Java [External] guide	As specified in the Security for Web Dynpro for Java [External] guide

4 Data Storage Security

For Visual Composer, the following points are relevant to data storage security:

- **Model persistence**

  Visual Composer models and related objects can be stored in the local Application Server Java (AS Java) database or deployed to a remote DTR.

  When a model is first created, it is saved as an empty component with all of its auxiliary files. With each subsequent save, all of the model data is saved once again, including its generated XGL.

- **Import and Export mechanisms**

  The *Model* → *Export to File* option in Storyboard enables users to export a `.zip` file containing the model `.gml` file and all related files. The `.zip` file can be saved on any computer or server in the network. Subsequently, using the *Model* → *Import from File* option, users can import the file back into a development component from which Visual Composer opens models. The Storyboard contains no function that can determine if the model file has been corrupted or otherwise altered since it was exported.

The security of all data in Visual Composer is covered by the security concept for the AS Java. For more information, see SAP NetWeaver Application Server Java Security Guide [External].

5 Dispensable Functions with Impacts on Security

SDK Tools and Debugging Capabilities

This feature is internal to SAP and is not supported for customers. Developers wishing to enhance Storyboard functionality through use of the SDK tools must receive formal authorization and special access rights.

The set of Software Developer Kit (SDK) tools is an advanced feature reserved only for Visual Composer kit developers for enhancing the capabilities of Visual Composer Storyboard. The SDK tools provide a view of all classes loaded to Visual Composer memory, and allow the developer to inspect in-memory JavaScript objects and modify them.

A significant risk is that computer hackers may gain access to these tools and sabotage the Visual Composer functionality. Therefore, precautions have been taken to prevent any unauthorized users from gaining access to the function that activates the SDK tools options.

Another tool included in the SDK tool set is the debugger, which enables a developer to see the JavaScript kit code, modify the code and run Visual Composer with the modified code. This tool is considered secure since a developer who wishes to modify code can only access the server through a well-defined channel API. The developer can make calls to back-end services only through specific methods, all of which are public APIs, and which perform valid application operations, such as model check-in and model save. This does, of course, assume that the developer has logged onto the tool and has proper authorization to work with it. The debugging session run by the kit developer affects only the local workspace of that developer.

6 Security for Additional Applications

Web Dynpro Runtime Engine for Visual Composer

At runtime, applications modeled in Visual Composer are run through the Web Dynpro for Visual Composer interpreter, which operates on XGL files. These files are created from the model `.gml` file during model compilation in the client, and are deployed to the AS Java database or to the DTR.

Generally, all security aspects of a standard Web Dynpro application apply to the Web Dynpro for Visual Composer interpreter.

7 Other Security-Relevant Information

To enable modelers to access Visual Composer Storyboard, the AS Java domain should be added to the trusted sites in the Internet Explorer settings. To do this, choose *Tools* → *Internet Options* → *Security* → *Trusted Sites* → *Sites* and add the domain name of your AS Java.

Visual Composer Storyboard uses the Microsoft XML (MSXML) parser for communication, and the Adobe SVG Viewer for vector graphics. Although these browser add-ons are not included as part of the Visual Composer installation, they must be installed on the client machine. Configure the custom security level for trusted sites to enable running of ActiveX controls and plug-ins. To do so, choose *Tools* → *Internet Options* → *Security* → *Trusted Sites* → *Custom Level* and choose *Running ActiveX controls and plugins* → *Enable.*