



ENOVIA SmarTeam

Network Configuration Requirements For SmarTeam Web Applications

© Dassault Systèmes, 2004, 2009. All rights reserved.

CATIA, ENOVIA, SMARTEAM and the 3DS logo are registered trademarks of Dassault Systèmes or its subsidiaries in the US and/or other countries.

PROPRIETARY RIGHTS NOTICE: This documentation is the property of Dassault Systèmes. This documentation shall be treated as confidential information and may only be used by employees or contractors of the Customer in accordance with the terms of the End-User License Agreement accepted by Customer.

Any use of the Licensed Program contained in this media or accompanying it, is subject to the terms of the End User License Agreement accepted by Customer. The Licensed Program is protected by international copyright laws and international treaties. Unauthorized use, reproduction and/or distribution of any of the Licensed Program, or any part thereof, may result in severe civil and/or criminal penalties, and will be prosecuted to the maximum extent possible under the law. Company names and product names mentioned herein are the property of their respective owners and certain portions of the Licensed Program contain elements subject to copyright owned by these entities. See the Documentation CD provided with the Licensed Program for details and/or additional terms and conditions relating to these entities.

Part No: WED-I5-190409

Contents

Chapter 1: Introduction	1
Purpose of this Document	1
Document Audience	1
SmarTeam - Web Application Server Components	1
Network Configuration Considerations	2
Chapter 2: Network Configuration Requirements	4
Requirements on Server Components	4
Chapter 3: Sample Configurations	6
Appendix A: Database Specific Details	8
Oracle	8
MS SQL Server	8
IBM DB2	8
Appendix B: System Specific Configuration Options	9
SmarTeam Vault Server Configuration	9
How to Enable Remote Copy Mode	9
SmarTeam Web Viewer Server Configuration	10
SmarTeam Session Management and System Configuration	10
SmarTeam Online Help Configuration	11

Chapter 1: Introduction

SmarTeam - Web applications such as SmarTeam - Web Editor or SmarTeam - Community Workspace are run on a Web Application server from client machines over the Internet. These applications require access to valuable data residing in SmarTeam database servers and vaults. As a result, there is a security requirement to prevent unauthorized access to SmarTeam data and files, both from the Internet and from local LANs.

However, restricting access to servers, if not implemented correctly, can affect the usability and the functionality of the SmarTeam - Web applications.

Thus there is a need to establish an optimum network configuration that can provide sufficient security and, at the same time, ensure the correct functionality of the applications.

Purpose of this Document

This document is applicable for SmarTeam versions V5R13 and above.

The purpose of this document is to define the minimum requirements that must be met in order to successfully deploy a SmarTeam Web Application, taking security and usability requirements into account.

These requirements must be communicated to and discussed with the customer's network administrators, in order to configure the various components correctly in a way that meets these requirements.

The document demonstrates a sample implementation of these requirements.

Document Audience

The document is targeted at implementers of SmarTeam Web Applications. Readers of this document should be familiar with SmarTeam Web Applications components and with common network topologies and terminology. Specifically, readers should be familiar with the concepts of a network Firewall.

SmarTeam - Web Application Server Components

The following table shows the SmarTeam - Web Applications server components and the applications or data that reside on them.

SmarTeam - Web Application Server Component	Description/Applications
Web Application Server	This server contains the SmarTeam Web applications: <ul style="list-style-type: none"> • SmarTeam - Web Editor • SmarTeam - Community Workspace
Viewer Server	This server contains the Viewer application.
Flow Server	This server contains the Flow Server application: SmarTeam - Workflow application
Database Server	This server contains SmarTeam data in a relational database.
Vault Server (incl. Markup Monitor Server)	This server contains SmarTeam data files.
License Server	This server manages SmarTeam licenses.
SmarTeam Web client machines: <ul style="list-style-type: none"> • SmarTeam - Web Editor client machine • SmarTeam - Community Workspace client machine 	
SmarTeam - Editor client machines	Applications: <ul style="list-style-type: none"> • SmarTeam - Editor
SmarTeam Session Management Service	Provides centralized authentication and user management services
SmarTeam System Configuration Service	Provides centralized repository for SmarTeam configuration data and user preferences

These components are often deployed on different machines, possibly residing in different network zones and communicating over several network components such as routers and firewalls.

Most corporate networks, which are connected to the Internet, use a firewall to protect access to machines on the corporate LAN. Often, the network is further divided into one or several DMZ (Demilitarized Zone) areas and an Internal LAN area, separated using an additional firewall.

Network Configuration Considerations

The correct operation of a SmarTeam Web Application requires that some of these components communicate and interact with other components. This usually requires the customer's system administrator to set up the network configuration in a way that allows such communication, while preserving the overall network security.

In designing a network configuration for a SmarTeam - Web application, the following considerations should be taken into account:

- The software components
- The hardware components

- The system architecture, including configuration of firewalls, uni-directional data lines, etc. by the customer system administrator.
- Installation and deployment of SmarTeam software components by the SmarTeam system administrator.

As the specific method and configuration parameters will vary from one network to another, and are highly dependent on the specific network topology, hardware, and software used, it is not possible to provide specific configuration instructions.

The components that have the highest security requirements are:

- Database Server
- Vault Server (including the Markup Monitor Server)
- SmarTeam Session Management Service
- SmarTeam System Configuration Service

Chapter 2: Network Configuration Requirements

This section describes the requirements that the network configuration must meet in order for these different components to work together correctly.

These requirements can be fulfilled using a combination of the following operations:

- Setting permissions on files and folders of specific machines
- Opening specific ports in network firewalls

Requirements on Server Components

The requirements below are of the types:

- Communication requirements between server components
- File access and read/write permission between server components
- Deployment of SmarTeam components on server components

The requirements on Server Components are:

- The **Web Application Server** process must be able to communicate with the Vault Server using TCP protocol using specific ports. One port is used to initiate the communication and is specified in the relevant SmarTeam Database (see [Appendix B](#) for details). Once communication is established, additional ports are selected from the free ports on the Vault Server machine in the range of 49152-65535. (their total number can be configured using the `MaxVaultListeners` parameter in the System Configuration Editor).
- The **Vault Server** process must have access to shared file system (SMB/CIFS) and have read/write permissions to the *working directory*¹ on the Web Application Server machine.
- The **Markup Monitor Service** must be deployed on the Vault Server machine.
- The **Markup Monitor Service** must have access to shared file system (SMB/CIFS) and have read/write permissions to the *markup directory*² on the Viewer Server machine.
- The **Web Application Server** process must have access to shared file system (SMB/CIFS) and have read/write permissions to the *markup directory*² on the Viewer Server machine.
- The **Viewer Server** machine must be accessible by a specific single IP address to ALL SmarTeam Web clients whether on internal LAN or external from the Internet.

¹ The *working directory* is the directory which checked out files are transferred for updating in the SmarTeam - Editor (for more details, see the SmarTeam - Editor Online Help).

² The *markup directory* is the directory in the SmarTeam - Web Viewer Server that has details on a document and its possible markup (for more details, see SmarTeam - Web Viewer Installation Guide)

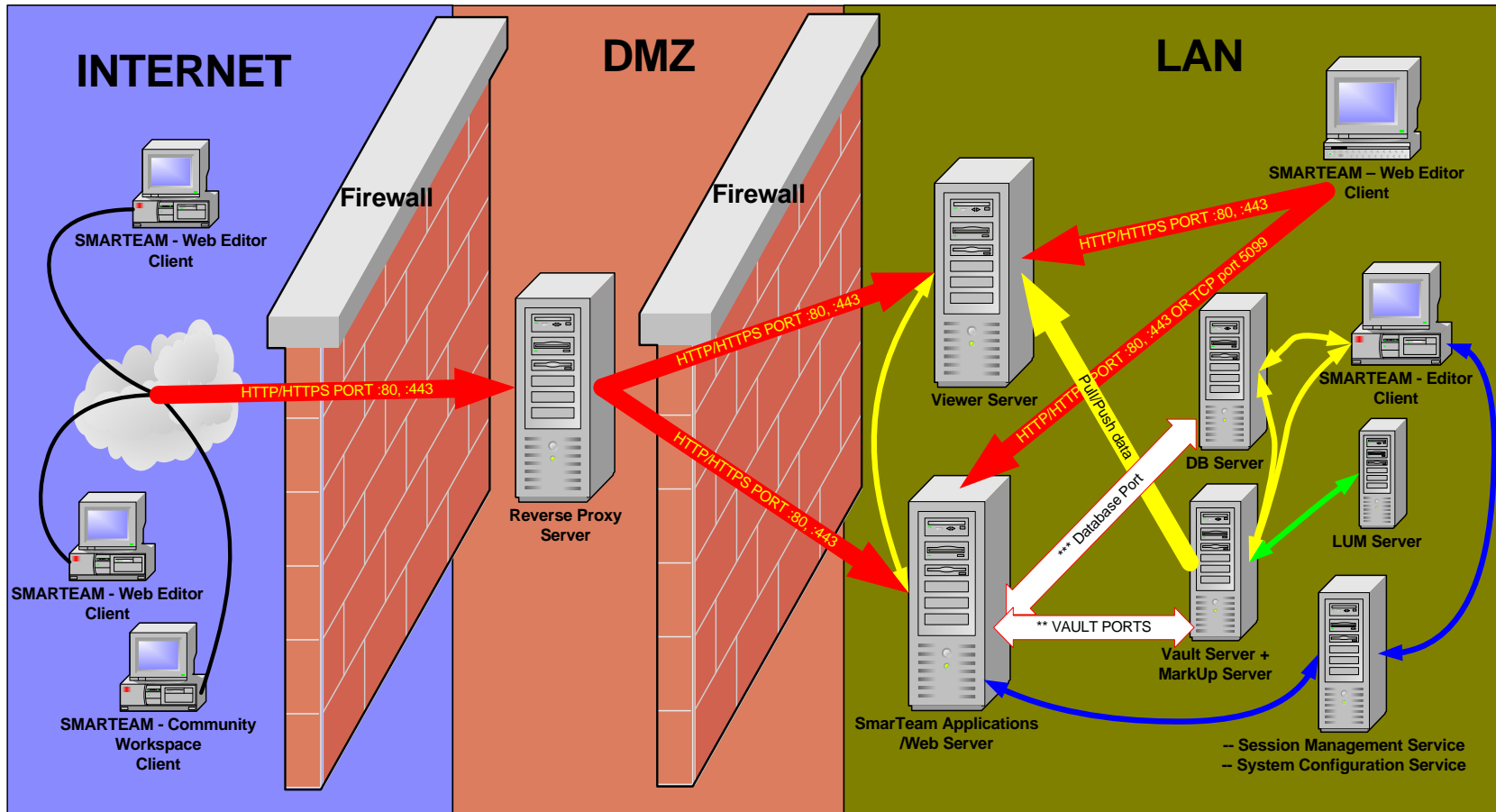
- All **SmarTeam - Web client** machines must be able to access the Viewer Server machine using TCP port 80 (if HTTP tunneling is used) and/or TCP port 443 (for HTTPS), or when not using HTTP tunneling, a TCP port which is defined by Viewer Server configuration (default port 5099). For more details on configuring the Viewer Server, see [Appendix B](#).
- All **SmarTeam - Web client** machines must be able to access the Web Application Server machine using TCP port 80 (for HTTP) and/or TCP port 443 (for HTTPS).
- The **Web Application Server** process must be able to communicate with the Database Server. The exact method and requirements for this communication depends on the type of database, see [Appendix A](#) for additional details.
- The **Flow Server** process must have access to the Database Server machine. The exact method and requirements for this access depends on the type of database, see [Appendix A](#) for additional details.
- The **Vault Server** process must have access to the Database Server machine. The exact method and requirements for this access depends on the type of database, see [Appendix A](#) for additional details.
- The **Vault Server** must have its temp directory `shared` (SMB/CIFS), be accessible and have read/write permissions to "everybody"
- **Licensing Servers**

LUM Server - A separate LUM server must be present for each subnet that has machines using its services. There should not be any restrictions on communication between the SmarTeam - Editor client or Web Application Server and the LUM server being used by them.
- The SmarTeam Session Management Service must be accessible to the SmarTeam Web application and the SmarTeam - Editor clients using the configured protocol (default TCP port 5606). For more details, see [Appendix B](#).
- The SmarTeam System Configuration Service must be accessible to the SmarTeam Web application and the SmarTeam - Editor clients using the configured protocol (default TCP port 5607). For more details, see [Appendix B](#).
- If the NLS Data Files are resident in a shared network location, these files must be accessible (SMB/CIFS) by SmarTeam Web application and by SmarTeam - Editor clients (It may be necessary to replicate the NLS Data files for use both within the internal network and on the Web). For detailed information about configuring the NLS Data files, please refer to SmarTeam - Editor Online Help.

Chapter 3: Sample Configurations

This section shows the possible configuration of SmarTeam components and the relationship between them.

The network configuration consists of an internal LAN and one DMZ network, which are separated by one firewall.



Appendix A: Database Specific Details

Oracle

The Oracle Database server requires ports to be open for clients to be able to establish communication with the servers. By default, the port is 1521 (configurable at the server, listener.ora file).

If a firewall is present between the client and Oracle server, these ports should be opened either manually from the firewall administration or by using the Oracle Connectivity Module, which is available for many of the major firewalls.

Consult the Oracle support site for the following articles: Note:45226.1 and Note:131524.1.

MS SQL Server

The MS SQL Server requires TCP and UDP ports to be open for incoming connections. By default (and also assigned by IANA), the port's SQL Server listens to its TCP port 1433 (configurable).

For more information, consult Microsoft KB article:

<http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q287932&>

IBM DB2

IBM DB2 requires listener TCP ports to be open, by default, these ports are 523 and 50000 and an additional port for each instance.

For more information, consult the following document from IBM:

<http://www.redbooks.ibm.com/pubs/pdfs/redbooks/sg245220.pdf>

Appendix B: System Specific Configuration Options

This section provides additional details on configuring specific components.

SmarTeam Vault Server Configuration

Note: This section is applicable if the Web application does not have direct access to the vault storage. For example, when the vault resides in a secure network and the application is in the DMZ network.

The Vault Setup utility allows you to set up SmarTeam vaults and define their locations on the network for each SmarTeam database. The VaultSetup.exe file is installed in the <SmarTeam>\bin directory by default.

The Vault Server Setup window displays the default SmarTeam vault structure, which is customizable, in the left window pane.

In this window, you can define the protocol and TCP port to use with the Vault Server.

Note:

- a** The Vault Server must be configured as "**High Security**".
- b** The property "**RemoteCopy to/from working directory**" must be set to True.

How to Enable Remote Copy Mode

To enable Remote Copy mode:

- 1** In SmarTeam - Editor, select **Tools** → **Administrative Options** → **Life Cycle Options**.
- 2** In the Life Cycle Options window, check "**Remote copy to/from working directory**".
- 3** If the lifecycle temporary directories are located on the same machine as the SmarTeam - Web Editor, the system configuration values that refer to them must be prefixed with the server IP address instead of the server name.

By default, the SmarTeam - Web Editor lifecycle temporary directory is located in <**SmarTeam Home Directory**>\WebEditor\Work\LCTemp. This directory must be accessible by the Vault Service user who runs the vault service, and the SmarTeam - Web Editor user who runs the SmarTeam - Web Editor application.

- 4** Create a network share in this directory and give full permissions for the Vault Service user and the SmarTeam - Web Editor user on this share.

- 5 The System Configuration key named "**temporaryDirectory**" refers to the SmarTeam - Web Editor lifecycle temporary directory. This key is stored in **SmarTeam.std.LifeCycle.config.xml**. In the System Configuration Editor, this key must be assigned with a value containing the network share name prefixed with the machine IP address.
- 6 In the System Configuration Editor, select **Miscellaneous Configuration --> Life Cycle Preferences**.
- 7 Find the entry **temporaryDirectory**. The default value for this key is <Home Directory>\WebEditor\Work\LCTemp>.
- 8 Replace this value with network share name (created in [Step 4](#)). For example, [\\172.16.150.1\LCTemp](#).

For more information, consult the SmarTeam documentation regarding the Vault Server configuration.

SmarTeam Web Viewer Server Configuration

SmarTeam Web Viewer is a Java-based viewing solution that provides SmarTeam Web applications, such as SmarTeam - Web Editor or SmarTeam - Community Workspace, with the ability to view and apply markups to documents and drawings.

SmarTeam Web Viewer is composed of three components:

- 1 A Java-based server component (AutoVue for Java) that:
 - Processes client viewing requests
 - Streams the results in a compact format to the Java applet on the client station.
- 2 A Java applet download client embedded inside HTML page of the SmarTeam Web application client (such as SmarTeam - Web Editor or SmarTeam - Community Workspace).
- 3 A Markup Service that manages all markups (redline files) created or requested by Web users. The service copies these files to and from the vault and prepares them for display by the SmarTeam - Web Viewer.

An additional component, the Servlet Engine, is deployed automatically by the SmarTeam - Web Viewer installation. This component enables access to the AutoVue for Java server when it is deployed behind a firewall, which prevents non-HTTP (port 80) communication.

For more details on Viewer Server configuration, please consult the "SmarTeam - Web Viewer installation guide.pdf" that is included with the SmarTeam Web Viewer installation. It can be found on the SmarTeam - Web Editor CD or the SmarTeam - Community Workspace CD.

SmarTeam Session Management and System Configuration

SmarTeam Session Management Service and SmarTeam System Configuration Service communicate with SmarTeam Web applications and SmarTeam - Editor clients using .NET Remoting infrastructure. For general information on .NET Framework Remoting, please refer to:

<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/cpguide/html/cpconnetremotingoverview.asp>

.NET Remoting can be configured to use various network protocols (for example, TCP, HTTP). For more detailed information, see:

<http://msdn.microsoft.com/library/en-us/cpgenref/html/gnconremotingsettingsschema.asp>

SmarTeam Online Help Configuration

To enable SmarTeam Online Help perform the following:

Using the System Configuration Editor, go to **Miscellaneous Configuration>Help Preferences>Virtual Root Path>** and add the following path:

`http://<computer_name>/SmarTeam/help`

If you are using the presented sample network configuration (using reverse proxy) the `<computer_name>` should be the web server published name.