



ENOVIA SmarTeam

Microsoft® DFS Installation and Configuration Guide

© Dassault Systèmes, 2008. 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 Number: MUV-I1-180007

Contents

Chapter 1: Introduction	3
Overview	3
SmarTeam – Multi-site Vault Replication	3
Microsoft® DFS	3
Software Location	4
Related Documentation	4
SmarTeam Corporation Internet Site	4
Chapter 2: Installation Checklist	5
Chapter 3: System Requirements	6
Hardware and Software Requirements	6
DFS System Requirements	6
Order of Installation	6
Installation Environment	6

Chapter 4: Prerequisites	7
SmarTeam – Vault Server Installation	7
Vaults Backup	7
Folder Creation	7
Security Setup for Microsoft® Windows	8
Physical Location of Vaults	8
Vaults Security Mode	8
Security Users and Groups	8
SmVaultAdmins Group	9
SmVaultUsers Group	9
VaultAdmin User	9
SmDFSAdmin User	9
Security Implementation	10
Vault Root Security	10
SmVault and SmMirrorVault Security	11
Clients Root (SmTemp) Security	12
Chapter 5: Installation Process	14
DFS Installation	14
Chapter 6: Post Installation	15
DFS Group Configuration	15
Configuring Groups	15
Configuring Group Members	19
Configuration of Connections	20
Working Behind a Firewall	21
Microsoft® Installer	22
Chapter 7: Troubleshooting	23
Known Issues	23
Frequently Asked Questions	23

Chapter 1: Introduction

Overview

This guide describes Microsoft® DFS (Distributed File System) Replication and how the SmarTeam System Administrator can successfully configure and install DFS in a SmarTeam – Multi-site system.

SmarTeam – Multi-site Vault Replication

SmarTeam – Multi-site Vault Replication solution is an open solution that uses third party products for replicating and synchronizing vault files in different sites. While SmarTeam can replicate files from one vault to another on demand, it is preferable to replicate files in the background. Microsoft® DFS Replication can be used to replicate and synchronize different site vaults, in a Vault Replication environment. For additional information, see SmarTeam – Multi-site Administration Guide.

Microsoft® DFS

DFS Replication is a replication engine, which supports replication scheduling and bandwidth throttling. The DFS is a component of Microsoft® Windows Server 2003 R2 and runs on Vault storage units, which may be hosted on Vault servers or may be stand-alone units. Therefore, you must install DFS on every machine that contains a Vault storage unit.

DFS Replication uses a compression algorithm known as remote differential compression (RDC). RDC is a "diff-over-the wire" client-server protocol that is used to efficiently update files over a limited-bandwidth network. RDC detects insertions, removals, and re-arrangements of data in files, enabling DFS Replication to replicate only changed file blocks when files are updated.

DFS Replication uses many sophisticated processes to keep data synchronized on multiple servers.

Replication Characteristics:

- Any change that occurs on one server is replicated to all other servers in the replication group.
- DFS Replication detects changes in the volume by monitoring the update sequence number (USN) journal, and replicates changes only after the file is closed.
- DFS Replication uses a staging folder to stage a file before sending or receiving it.
- DFS Replication uses a version vector exchange protocol to determine which files need to be synchronized. The protocol sends less than 1 kilobyte (KB) per file across the network to synchronize the metadata associated with changed files on the sending and receiving members.
- When a file is changed, only the changed blocks are replicated, not the entire file. The RDC protocol determines the changed file blocks. Using default settings, RDC works for any type of file larger than 64 KB, transferring only a fraction of the file over the network.

- DFS Replication uses a conflict resolution process, which means the last writer wins for files that are updated at multiple servers simultaneously and are in conflict, and the earliest creator wins for name conflicts. Files and folders that lose the conflict resolution are moved to the Conflict and Deleted folder. Deleted files can also be configured to move to the Conflict and Deleted folder for retrieval if the file or folder is deleted.
- DFS Replication uses a Microsoft® Windows Management Instrumentation (WMI) provider, which enables the transfer of configuration and monitoring information from the DFS Replication service. This enables configuring DFS via script operations, or auto-install processes.

Software Location

The Microsoft® DFS component is an integrated part of Microsoft® Windows Server 2003 R2, but it is not installed by default.

Related Documentation

The following documents are referred to in this guide. All of these documents are available on the SmarTeam Documentation CD.

Document	Remarks
SmarTeam – Foundation Installation Guide	Provides information about Vault installation
SmarTeam – Multi-site Administration Guide	Provides administration procedures to successfully setup, customize and maintain a SmarTeam - Multi-site system in a corporate environment
Technical Advice Note SmarTeam Vault Server	Provides basic information about Vaults
SmarTeam Vault Redundancy, Core and Flow Setup Guide	Provides information about Vault setup

Internet Site

You are highly recommended to frequently visit our website for the latest updates and plug-in products, including the latest Service Packs, Program Directory (Release Notes), Hotfixes and technical support at <http://support.smarteam.com/>.

In addition, you will also be able to view any installation known issues.

Chapter 2: Installation Checklist

This checklist provides a detailed list of all the steps that need to be performed and the order in which they should be performed to successfully configure and install DFS.

Note: If SmarTeam – Foundation is already installed you may need to change the Vault Server service user after performing security setup. You do not need to uninstall SmarTeam – Foundation.

*Requirement: M = Mandatory, O = Optional

	Item	M/O*	Reference
Stage 1: Pre-Installation			
<input type="checkbox"/>	Verify that your hardware and software meet the requirements	M	SmarTeam Hardware and Software Requirements Guide
<input type="checkbox"/>	Install SmarTeam – Vault Server from SmarTeam – Foundation on the Vault Server machine Note: SmVaultAdmins and SmVaultUsers group must be defined as Global.	M	SmarTeam – Foundation Installation Guide and Security Users and Groups
<input type="checkbox"/>	Configure Vault and Vault Replication Note: Vaults must be located in separate NTFS partitions.	M	SmarTeam – Multi-site Administration Guide
<input type="checkbox"/>	Back up Vaults	O	
<input type="checkbox"/>	Set security mode for Vaults	M	Vaults Security Mode
<input type="checkbox"/>	Create SMDFSAdmin user	M	Security Implementation
<input type="checkbox"/>	Check for any additional prerequisites on the SmarTeam Web Site	O	Release Notes of Latest Service Pack in the Release or SmarTeam Support Site
Stage 2: Installation Process			
<input type="checkbox"/>	Add Microsoft® DFS component to your Windows application	M	DFS Installation
Stage3: Post-Installation			
	Configure groups	M	Configuring Groups
	Configure group members	M	Configuring Group Members
	Verify the connection between groups and group members	O	Configuration of Connections
	If a firewall exists, configure an alternate port	O	Working Behind a Firewall

Chapter 3: System Requirements

Hardware and Software Requirements

Refer to the SmarTeam – Multi-site Vault section in the Hardware and Software Requirements document. This document provides details of the hardware and software required for successful installation of Multi-site Vaults.

DFS System Requirements

The following is a description of the major requirements and limitations of Microsoft DFS with regard to the Vault Server system. The Vault server and the Vault storage can be on different machines.

Order of Installation

Refer to [Installation Checklist](#) for a detailed list of all the steps that need to be performed after verifying your hardware and software meet the requirements.

The installation procedure is split into three stages:

- Stage 1: Pre-Installation ([Prerequisites](#))
- Stage 2: Installation Process ([Installation Process](#))
- Stage 3: Post Installation ([Post Installation](#))

For a successful installation you must complete one stage before proceeding to the next stage.

Installation Environment

The SmarTeam – Multi-site Vault Replication environment for installing and configuring Vault Replication must be fully operational to successfully use DFS as a replication solution. The following requirements must be fulfilled:

- Vaults must be located on NTFS volumes.
- Vaults must be located in stand-alone partitions.

Chapter 4: Prerequisites

The pre-installation process consists of the following steps:

- [SmarTeam – Vault Server Installation](#)
- [Vaults Backup](#)
- [Folder Creation](#)
- [Security Setup for Microsoft® Windows](#)

For a successful installation, these prerequisites must be completed before proceeding to [DFS Installation](#).

SmarTeam – Vault Server Installation

SmarTeam – Vault Server is installed on the Vault Server machine via the SmarTeam – Foundation CD with Vaults. For more information, see the SmarTeam – Foundation Installation Guide.

Note: If SmarTeam – Foundation is already installed you may need to change the Vault Server service user after performing security setup. You do not need to uninstall SmarTeam – Foundation.

SmarTeam – Foundation installation is handled the same way in every SmarTeam Vault replication environment, with the following exceptions:

- Vaults must be located in separate partitions.
- SmVaultAdmins and SmVaultUsers group must be defined as Global.

Vaults Backup

It is highly recommended that you backup the Vaults before performing any presetup procedures or installing DFS.

Folder Creation

To set up a Vault Server, you must manually create a directory structure containing folders for each Vault. For more information, see the Technical Advice Note SmarTeam Vault Server.

Security Setup for Microsoft® Windows

Proper security planning is a major requirement to successfully configuring and installing Vault Replication using DFS. Proper security is required for the following reasons:

- To protect vault files from accidental deletion
- To limit access to vault files by authorized users only
- To ensure proper replication of files and folder security settings, which is part of DFS
- To ensure DFS administration, which includes specific security requirements.

Physical Location of Vaults

For proper security realization, Vaults should be located in the system in a separate partition with a distinct drive identification, such as V:\, which is dedicated only to Vaults. This partition should be located on Microsoft® Windows Server 2003 R2 Machine, and formatted to NTFS file system.

If vaults are already installed, do the following:

- 1 Move the primary Vault root under the Vaults partition.
- 2 Create the mirror roots and folders, and Clients root (SmTemp) directories (optional) in the Vaults partition, without any files. (The files will be replicated later by DFS.)
- 3 Share the folders, using former sharing names.
- 4 From Vault Server Setup, update the location of the Vault directories.

Vaults Security Mode

Every vault has its own security mode, which is set via the Vault Server Setup. The three security modes are: Low, Medium, and High.

Vault Replication with DFS must work in High security mode for all Vaults. Select **Vault Server Setup**, and verify all vaults are configured to work in High security mode.

The High security mode is required for:

- Proper security replication by DFS
- Protecting Vaults files from accidental deletion, because DFS replication is working in two directions. Deletion of a file from any of the mirrors results in deletion of the file from all the mirrors as well as the primary vault.

Note: Files should never be deleted from a mirror vault, as long as the Vault is configured as part of DFS replication group.

Security Users and Groups

Two groups and one user comprise a standard Vault Replication environment:

- [SmVaultAdmins Group](#)
- [SmVaultUsers Group](#)
- [VaultAdmin User](#), (member of SmVaultAdmins)

Group names can be changed by SmarTeam system configuration.

An additional [SmDFSAdmin User](#), should also be created.

The SmDFSAdmin has the highest resource access in the system. It is recommended to first create and then log in as the SmDFSAdmin user to continue security setup. The SmDFSAdmin user, has the required privileges to set necessary operations.

SmVaultAdmins Group

The SmVaultAdmins group sets global security access for Vault services, which run under the VaultAdmin user, and must be defined in an active directory. If it is currently local, create a new SmVaultAdmins group in an active Users and Groups directory, and delete it from the local computer.

If more than one Domain Controller exists in the network topology, only one SmVaultAdmins group should be created. Since all the Domain Controllers are in the same forest, the SmVaultAdmins group is recognized in all domains.

SmVaultUsers Group

The SmVaultUsers group sets global security access for SmarTeam users and must be defined in an active directory. If it is currently local, create a new SmVaultUsers group in the active Users and Groups directory, and delete it from the local computer.

If more than one Domain Controller exists in the network topology, SmVaultUsers group should be created in every Domain Controller used to define SmarTeam users in the network. This is because users in one Domain Controller cannot be members of a group in other Domain Controller.

Every user in SmarTeam should be part of a SmVaultUsers group and defined in a specific Domain Controller.

VaultAdmin User

The VaultAdmin user logs in to run the Vault server service. The VaultAdmin user should be a uniquely defined, global user in the network topology who is also defined in the Domain Controller, which contains the SmVaultAdmins group. The VaultAdmin user is a member of SmVaultAdmins group.

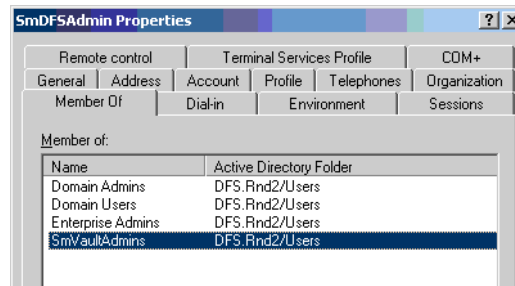
After setting up the VaultAdmin user, verify the following:

- All Vault Server services in all machines are running under VaultAdmin user rules.
- From Administrative > Tools, select **Local Security Policy**. Select Local Policies > User rights assignments, and verify that SmVaultAdmins is configured with the following settings:
 - Act as part of the operating system.
 - Log in as a service.

SmDFSAdmin User

The SmDFSAdmin user configures DFS, and Vaults security and should be created and saved in the location where SmVaultAdmins is defined. The SmDFSAdmin user should be a member of:

- Domains Admins
- Enterprise Admins
- SmVaultAdmins



In addition, the SmDFSAdmin user must be a member of every local Administrators group, in every computer that stores Replicated Vaults. This is configured by editing every Administrators group on any storage machine, and adding the SmDFSAdmin user to this group.

Security Implementation

Some of the following steps require administrator privilege. To be sure you have the proper authorization for configuring the system, it is recommended to choose one of the following options:

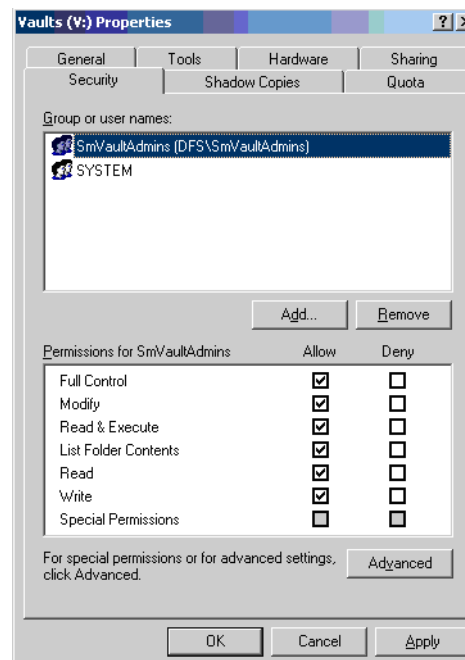
- 1 Log in to any computer that requires change, as SmDFSAdmin user.
- OR**
- 2 Select Run As... to run every program required to change settings, as SmDFSAdmin user.

Vault Root Security

To ensure Vault root security:

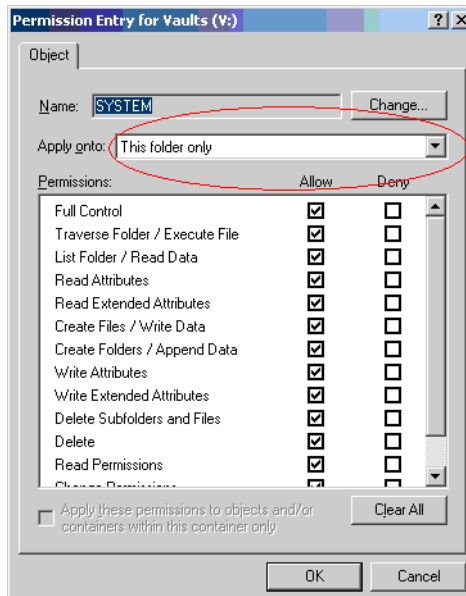
This procedure applies to every Vault drive in the system.

- 1 From the Vaults (V:) Properties window, select the Security tab.



- 2 Add **SmVaultAdmins** and select **Full Control**.

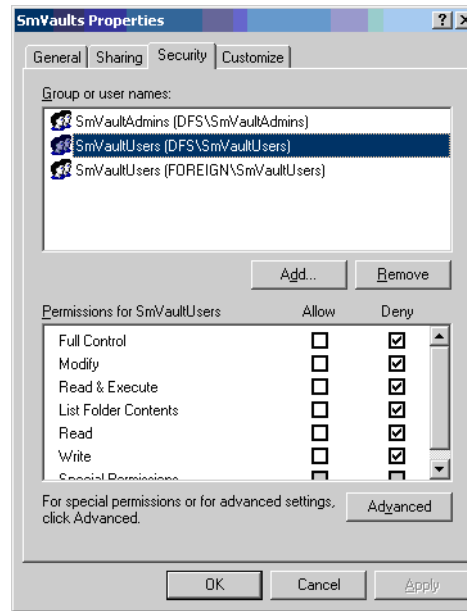
- 3 Delete all Groups or user names except **SYSTEM**.
- 4 Select **Advanced** to enable the Advanced System.
- 5 From the Permission Entry for Vaults window, for **SYSTEM**, change **Apply Onto** field, to **This folder only**, and then click **OK**.



SmVault and SmMirrorVault Security

To ensure SmVault and SmMirrorVault security:

- 1 From the SmVaults Properties window, select the Security tab.
Only SmVaultAdmins should appear.
- 2 Add **SmVaultUsers** group and select **Deny** for all permissions for every Domain Controller connected with SmVaultUsers.

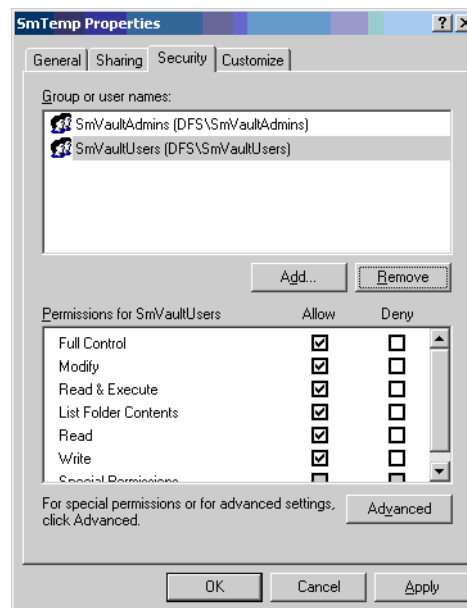


- 3 Repeat [Step 2](#) for the SmMirrorVault folder.

Clients Root (SmTemp) Security

To ensure Clients Root (SmTemp) security:

- 1 From the SmTemp Properties window, select Clients Root > Security tab.
- 2 Add **SmVaultUsers** group, and select **Allow** for all permissions for the local Domain Controller.



If Client Root is located near the Vaults in the same partition, it receives SmVaultAdmins security from its parent partition.

If Clients Root is not located near the Vaults, the security list to which it is assigned is different.

In this case, add **SmVaultUsers** in [Step 2](#) and add SmVaultAdmins with **Full Control** permissions.

Chapter 5: Installation Process

To successfully and securely implement DFS Vaults Replication, it is important to understand some of DFS key features, and how they influence SmarTeam behavior. Incorrect implementation can lead to loss of data.

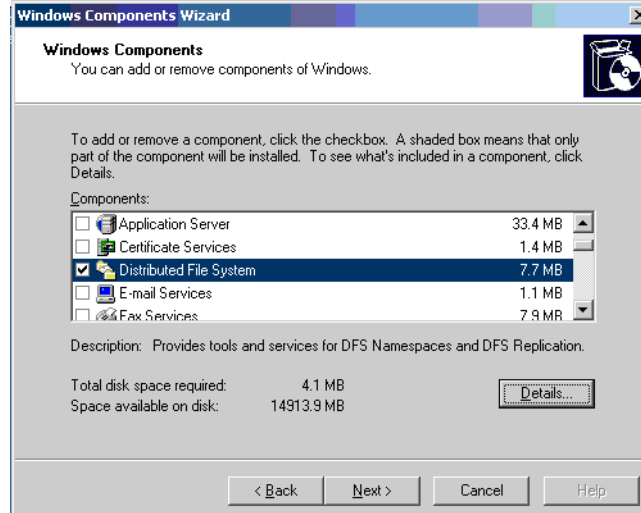
DFS Installation

DFS is an integrated part of Microsoft® Windows Server 2003 R2.

Installation is required on every Vault storage machine that participates in replication.

To install DFS:

- 1 From the Add/Remove Windows Components Wizard, select **Distributed File System** and click **Next**.



- 2 Complete the Wizard steps by clicking **Next** as indicated and then click **Finish**.
DFS is installed.

Chapter 6: Post Installation

DFS Group Configuration

Replicating directories in DFS is done by configuring Groups. Each group defines a set of directories in different machines. Each replicated directory is called a Member. The DFS services that run on member machines handle synchronization between directories. Each Group has its own settings.

Note: A separate DFS Group should be created for every primary Vault.

The number of groups required to replicate all the Vault directories with the Vault Mirror directories is equal to the number of primary Vaults. Each Group represents the replication from one Vault to all other appropriate Mirror Vaults.

For example, to configure two sites with mirrors with a default of three Vaults per site, six DFS Groups are required.

To begin declaring a Group, from Administrative Tools, select **DFS Management Console**. This must be installed first using the Add-Remove Windows Components Wizard on the machine used for configuring the replication system.

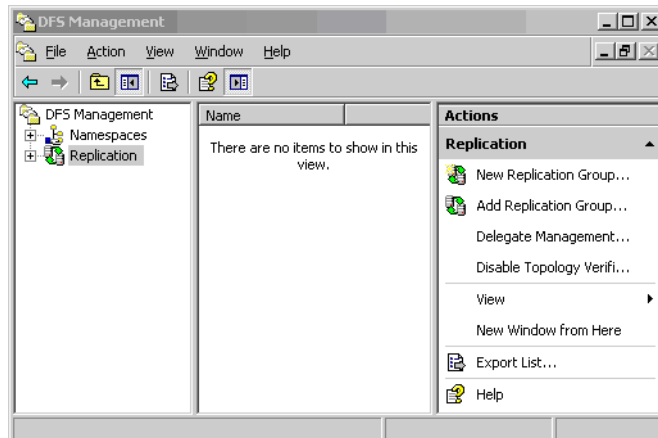
Note: Either you must be logged on as SmDFSAdmin when running the **DFS Management Console**, or you must run the **DFS Management Console** with SmDFSAdmin permissions by selecting **Run As...**

Configuring Groups

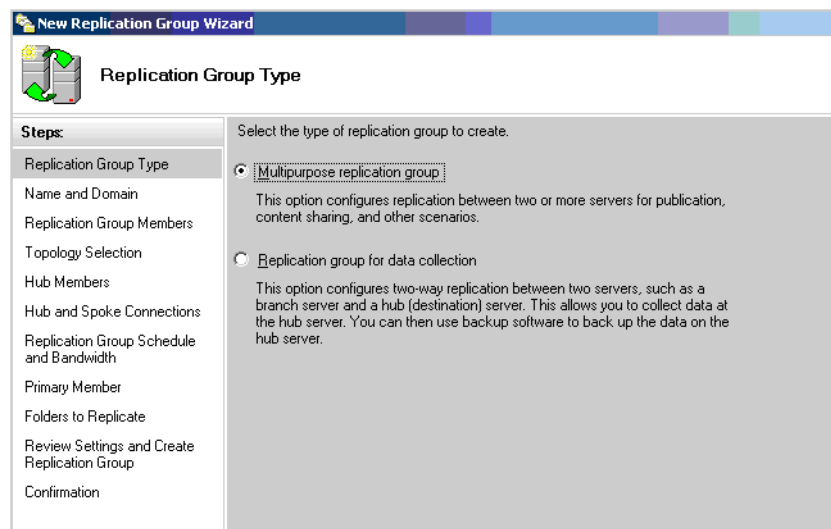
To configure DFS groups:

- 1 From Administrative Tools, select **DFS Management Console**.

The DFS Management window appears.



- 2 Click **New Replication Group** to create a new group.
- 3 Select **Multipurpose replication group** and click **Next**.

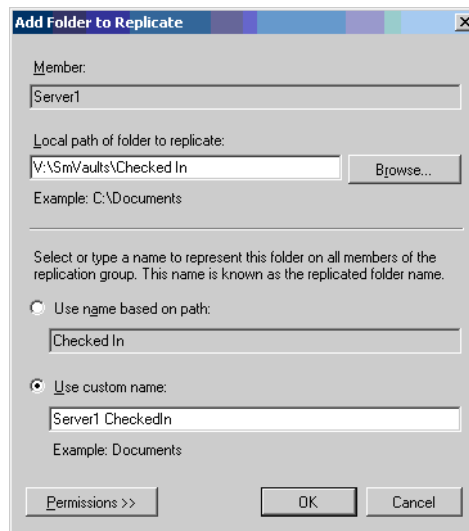


- 4 Complete the Wizard requirements as indicated and click **Next**.

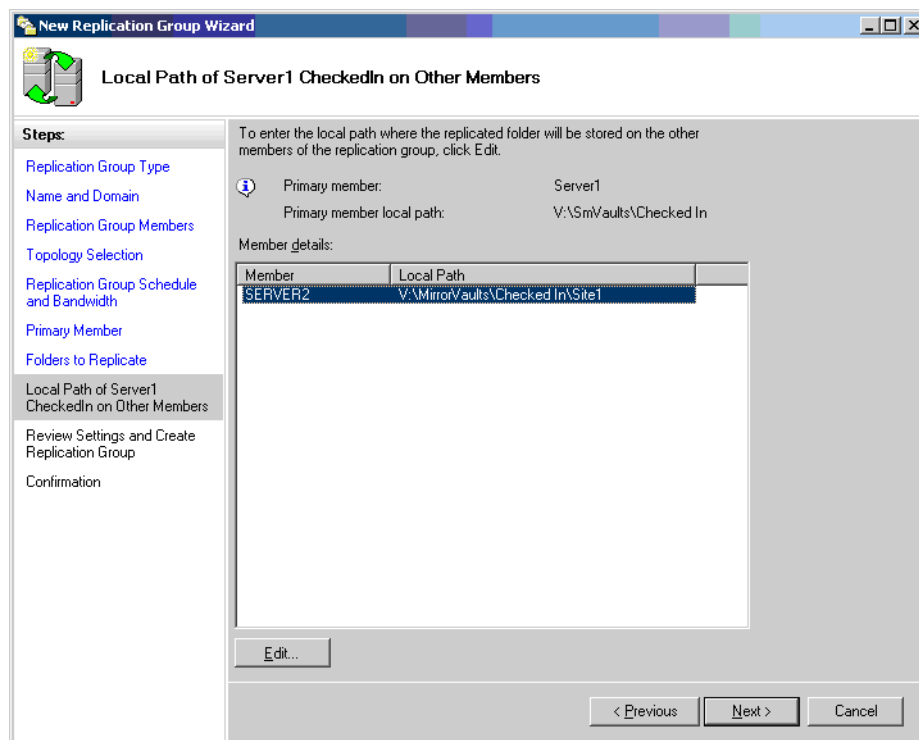
The following values should be used:

- a **Name and Domain:** Includes the name of the group, such as 'Site1 CheckIn Mirroring', and the domain that stores group details.
- b **Replication Group Members:** Add all computers that contain Vault directories. The computer names include the computer that contain the primary Vault, and additional computers that contain mirrors for this primary Vault.
- c **Topology Selection:** Full Mesh
- d **Replication Group Schedule and Bandwidth:** Set as required or use default values.
- e **Primary Member:** Select the computer that contains the primary Vault to be replicated.
- f **Folders to Replicate:** Click **Add** to add the primary Vault directory, and complete the Use Custom Name field.

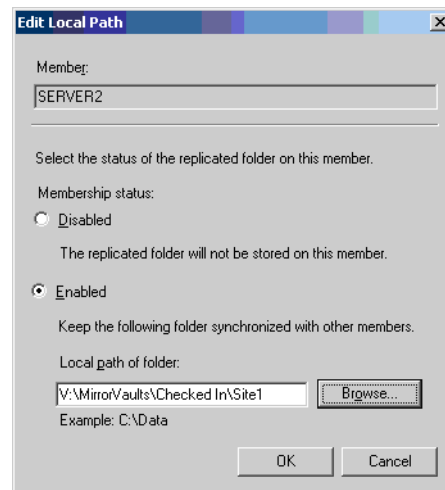
- 5 From the Add Folder to Replicate dialog box, complete the relevant fields and click **OK**.



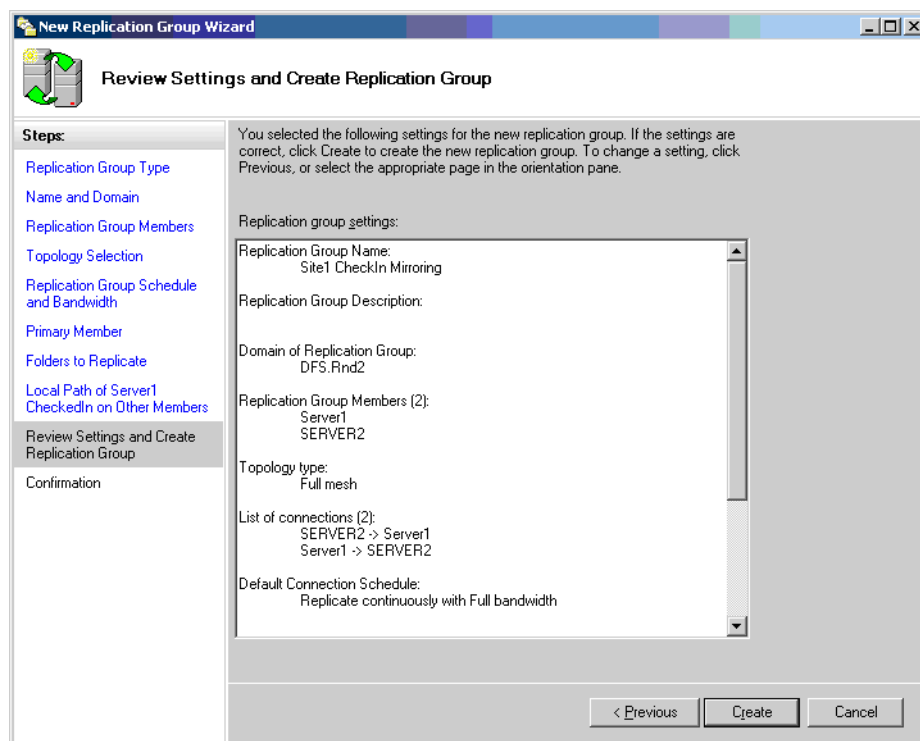
- 6 From the Wizard window that appears, click **Next**.
- 7 From the Local path of primary Vaults on Other Members window, click **Edit** to configure the first local mirror Vault location.
(Only one mirror appears in this example.)



- 8 From the Edit Local Path dialog box, select **Membership Status > Enabled** and browse to the local path of the appropriate mirror Vault on the server. Click **OK**.



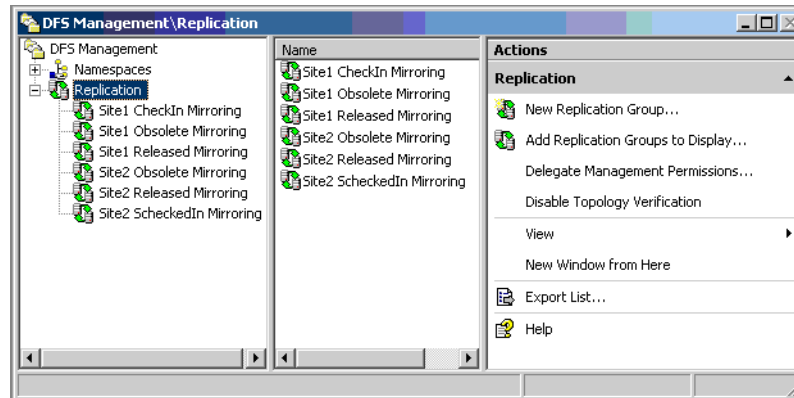
- 9 Repeat [Step 7](#) for every mirror in the list and then click **Next**.
- 10 From the Review Setting and Create Replication Group window, click **Create** to finish creating the group.



- 11 Repeat [Step 2](#) for every primary Vault.

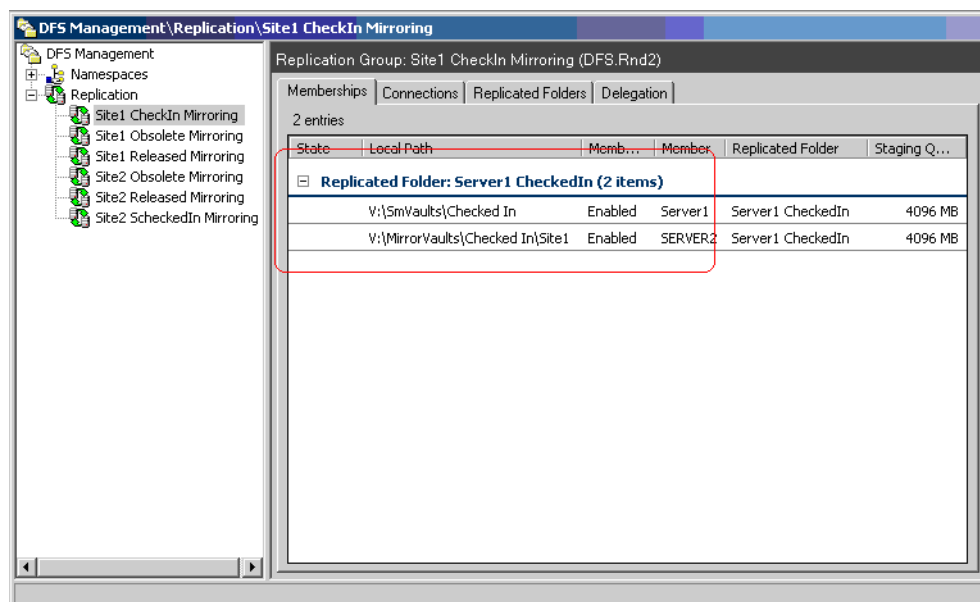
The result is N groups, where N is the number of replicated primary Vaults.

For example, the following graphic shows a typical Six-Group definition for replicating two sites. Each Group, which has its own directory and is composed of all members (Servers), participates in the replication.



- 12 Select one of the groups in the left area of the window to view its details.

The following graphic shows the SmVaults\CheckIn directory group member as a primary Vault, and its compatible VaultMirrors\CheckedIn\Site1 directory as the mirrored Vault.

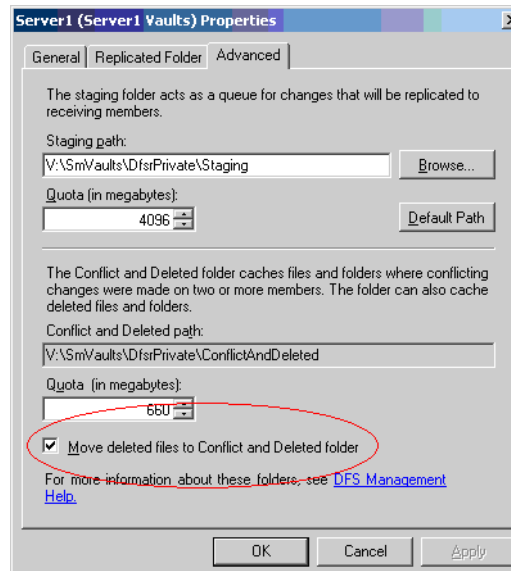


Configuring Group Members

DFS can be configured to save all deleted files in a special folder. In DFS Management Console, Select the Primary Member, and open its Properties. Click on the Advanced tab as follows:

To configure DFS group members:

- 1 From Administrative Tools, select **DFS Management Console**.
- 2 Select the **Primary Member** and open its Properties.
- 3 From the Server1 (Server1 Vaults) Properties window click the Advanced tab.



- 4 Verify that **Move deleted files to Conflict and Deleted folder** is selected to copy all deleted files from SmVault to DfsrPrivate\ConflictAndDeleted directory.
- 5 Select the **First Mirrored Member** and open its Properties.
- 6 From the Properties window click the Advanced tab.
- 7 Deselect **Move deleted files to Conflict and Deleted folder**.
- 8 Repeat [Step 5](#) for every mirrored member.

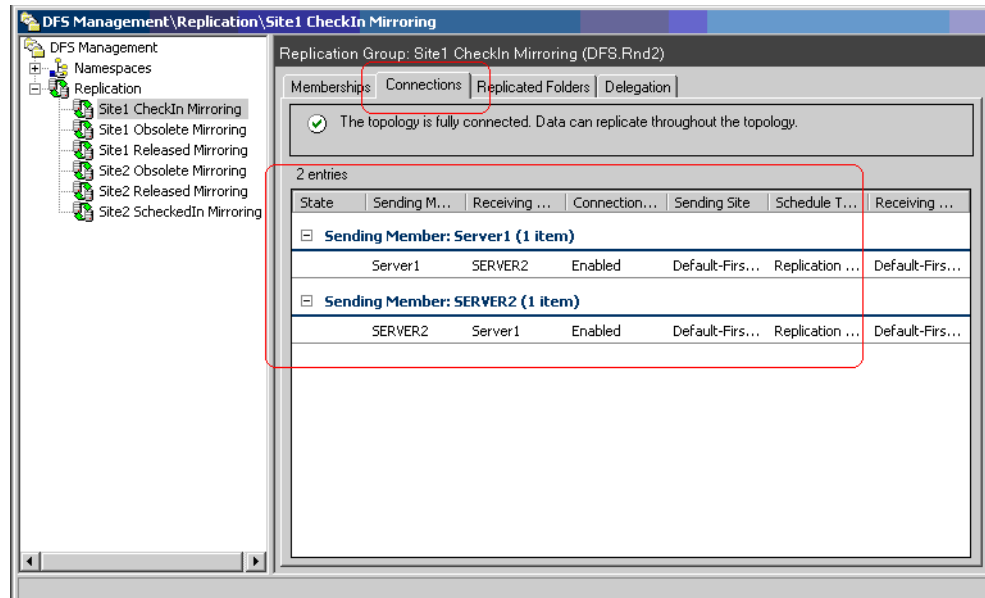
Note: Empty the The DfsrPrivate\ConflictAndDeleted folder on the Primary Server on a regular basis to ensure the contents remain below the stated quota.
 Since all members contain at least one primary Vault, they should also perform the process of deleting old files.

For more information, see Microsoft® DFS documentation.

Configuration of Connections

For each DFS group, one member is defined the Primary member. The files are distributed from the primary member to the replicated folders, which are called Vault mirrors. The replication typically occurs in two directions. A connection must be configured for each direction by using the Connection tab. Each connection has a Sending Member and a Receiving Member.

The following graphic shows the DFS Management window for Site1 with typical bi-directional replication connections.



Although Vaults in SmarTeam only require replication in one direction, from the SmVaults to the compatible VaultMirror, the two connections are required to replicate redline files.

For each connection there are additional optional settings. While the default settings are suitable for simple SmarTeam installation, see DFS documentation for more information.

Working Behind a Firewall

DFS Replication uses the RPC Endpoint Mapper (port 135) and a randomly assigned ephemeral port above 1024. Since this is a randomly assigned port, it cannot be used by default when there is a firewall. The DFS Replication service can be configured to use a static port instead of the ephemeral port.

The Distributed File Replication Service includes the Dfsrdiag.exe command-line tool, which is located in the System32 directory. Dfsrdiag.exe is used to set the server RPC port, which is used for administration and replication.

To set the server RPC port:

- Run `DFSRDIAG.EXE StaticRPC /port:1234 [/Member:Server1]`

Where:

- **1234** represents a single, static RPC port that DFSR uses for replication.
- **Server1** represents the DNS or NetBIOS name of the target member computer. If a member is not specified, Dfsrdiag.exe uses the local computer.
- Every member should be configured separately.

To check the port used for a server:

- Run `DFSRDIAG.EXE DumpMachineCfg [/Member:name]`

To request more information:

- Type the following at the command line:

■ `DFSRDIAG.EXE StaticRPC /?`

OR

■ `DFSRDIAG.EXE DumpMachineCfg /?`

Microsoft® Installer

After installing any SmarTeam product, do not remove or rename any file or directory.

The Microsoft Installer may appear when you launch a SmarTeam application if a directory or file has been deleted, changed or renamed. To prevent this, do the following:

1 Open the computer's Event Viewer.

2 Search for information or an error event related to the Installer.

For example, a possible cause could be the deletion of the UpdatedScripts folder under the script directory.

3 After finding the cause, take the required action: for example, restore a modified file name to its original name, or restore a file that had been deleted.

Chapter 7: Troubleshooting

Known Issues

For installation known issues, refer to the [SmarTeam Support Web](#) Site.

Frequently Asked Questions

For Frequently asked Questions (FAQ) refer to the [SmarTeam Support Web](#) Site.