



DMZ *edge*

**Administrator User's Guide**

Version 3

March 2010

## Notices

Copyright 2010 South River Technologies, Inc. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement, OEM, or reseller agreement. The software may be used or copied only in accordance with the terms of those agreements. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of South River Technologies, Inc.

South River Technologies®, GroupDrive Collaboration Server®, Cornerstone MFT™, Titan FTP Server®, DMZedge Server™, and WebDrive® are trademarks of South River Technologies, Inc. in the U.S. and other countries. Microsoft, Windows, Windows NT, Windows XP, and Windows Vista are trademarks of Microsoft Corporation, Inc. The names of other actual companies and products mentioned herein may be the trademarks of their respective owners. Any information in this document about compatible products or services should not be construed in any way to suggest SRT endorsement of that product or service.

### Contact Information

South River Technologies, Inc.  
2635 Riva Road  
Suite 100  
Annapolis, Maryland 21401  
USA

Telephone: 410-266-0667  
Fax: 410-266-1191

Sales Office e-mail: [sales@southrivertech.com](mailto:sales@southrivertech.com)  
Online Support: <http://www.srhelpdesk.com>  
Support e-mail: [support@southrivertech.com](mailto:support@southrivertech.com)  
Corporate Web site: [www.southrivertech.com](http://www.southrivertech.com)

Office Hours: 8:30 A.M. to 5:30 P.M. Eastern Time, GMT-5:00

## Table of Contents

Notices .....	ii
Contact Information .....	ii
Table of Contents .....	iii
Introduction to DMZedge® .....	4
How DMZedge Works.....	4
Key Features .....	4
System Requirements.....	5
Supported Platforms.....	5
Requirements & Limitations .....	5
Installation and Removal.....	6
Installing DMZedge Server .....	6
Uninstalling/Removing DMZedge Server .....	7
Starting the DMZedge Service.....	8
Configuring the DMZedge Server .....	9
Status Tab .....	10
Settings Tab.....	11
About Tab.....	13
Obtaining Support .....	14
Terminology .....	15

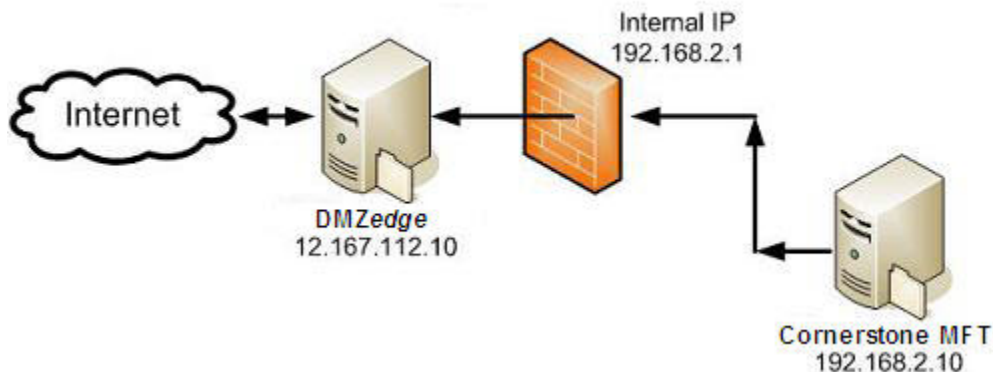
## Introduction to DMZedge<sup>®</sup>

Thank you for purchasing DMZedge<sup>®</sup>.

The DMZedge Server enables you to close inbound ports on your firewall, reducing the risk of network intrusion and enabling the highest level of security for both data storage and transfers. When combined with the [Cornerstone MFT<sup>®</sup>](#) (Managed File Transfer) Server or the [GroupDrive<sup>®</sup>](#) Server, the DMZedge Server uses a two-way connection originating from the Secure Cornerstone MFT (Managed File Transfer) or GroupDrive<sup>®</sup> Server that is inside of the firewall on your corporate LAN (Local Area Network). The DMZedge works as a communication proxy, shielding your internal network from unsecure inbound connections.

### How DMZedge Works

The DMZedge Server works as a proxy between users on the Internet and your secure corporate LAN. The DMZedge Server resides in the Demilitarized Zone (DMZ), outside of your corporate firewall and functions as a subnetwork buffer between your corporate LAN and potential threats from inbound traffic. The GroupDrive<sup>®</sup> or Cornerstone MFT<sup>®</sup> Server that resides on your network initiates a session with the DMZedge through a secure outbound connection. All incoming client requests and data are forwarded to the back end server through a connection that has already been established between the MFT Server and the DMZedge Server. The Cornerstone MFT or GroupDrive Servers reside securely behind your corporate firewall, although ease of access for your end users is as simple as if the servers were in your DMZ. Data storage and authentication takes place on the back end server, and no inbound ports are opened through your firewall.



## Key Features

- No requirement for opening inbound ports through your corporate firewall; instead the internal [Cornerstone MFT](#) or [GroupDrive](#) Server initiates an outbound connection to the *DMZedge* Server.
- Enables Managed File Transfers and secure collaboration by working in conjunction with either the [Cornerstone MFT](#) Server or [GroupDrive](#) Server products.
- Virtual authentication – *DMZedge* Server acts as a [proxy](#) for authentication to the back end server, including authentication to existing [Active Directory](#) or [LDAP](#) server implementations.
- Secure protocol support including full [FTPS](#), [SFTP](#), [HTTPS](#), and [WebDAV](#) over [SSL](#).
- Complete pass-through capability - no storage or replication of user database information is required on the *DMZedge* Server.
- Simple, wizard-driven installation that reduces implementation time.

## System Requirements

### Supported Platforms

The following Windows platforms are supported:

- Windows Server 2008, 32-bit or 64-bit
- Windows Server 2003, 32-bit or 64-bit

### Requirements & Limitations

DMZedge Server is a multi-threaded, dynamic server for the Windows operating system. While it is designed to handle an unlimited number of user connections and servers, it is limited by the resources of the machine; most notably, those limitations imposed by the Windows Sockets (WINSOCK) Library.

**The minimum hardware requirements for DMZedge Server are:**

- 2GHz Pentium® class processor
- 2GB of RAM is required, 4GB is recommended
- Minimum 100MB of disk space for the program and log files
- Minimum SVGA (800x600) resolution is required to run the Administration program
- All Windows Service Packs and Hot Fixes must be applied to the computer prior to installing DMZedge Server

## Installation and Removal

### Installing DMZedge Server

1. Make sure that you have the most recent version of DMZedge Server. The latest version can be downloaded from our Web site at <http://www.dmzedge.com/>
2. Double-click the installation file to start the installation process.
3. Once the installation process has completed, you will need to restart Windows.
4. After Windows has restarted, the DMZedge Service will be running. The DMZedge Service runs as a system service and starts when the operating system loads. You can monitor the status of the DMZedge Service using the Windows Services applet in the *Administrative Tools* folder of the Windows Control Panel.
5. Once DMZedge Server has been installed, you can begin to configure your server. Use the *DMZedge Administrator* program located in the DMZedge Server Program Group to configure your server.

## Uninstalling/Removing DMZedge Server

Use the following procedure to completely uninstall DMZedge Server from your computer:

1. From the **Windows** Start menu, select **Settings** > **Control Panel** to open the *Windows Control Panel*.
2. Double-click on the **Add/Remove Programs** icon in the **Control Panel**.
3. Select **DMZedge Server** as the application to uninstall.
4. Follow the instructions on the dialog screens to remove DMZedge from your machine.
5. Close the **Add/Remove Programs** applet.

 You will need to **restart Windows** to have DMZedge completely removed from your machine.

## Starting the DMZedge Service

DMZedge Server is designed to run as a system service or background process. You can configure DMZedge Server so that it either starts when Windows boots, or you can have it set to be started manually.

**To check and/or modify the startup setting for the DMZedge Service:**

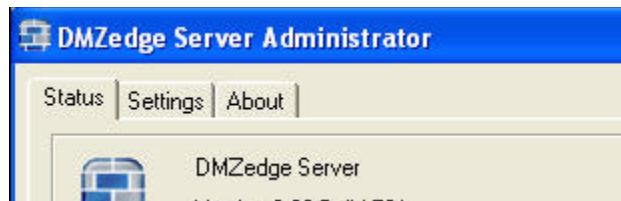
1. Open the **Windows Control Panel**.
2. Double-click **Administrative Tools**, and then double-click the **Services** applet.
3. Right-click on the entry labeled **DMZedge Server Daemon**, and select **Properties** from the pop-up menu.

The DMZedge Service runs under the context of the standard **LocalSystem** or **LocalService** NT User Account.

## Configuring the DMZedge Server

The DMZedge Server can be configured using the DMZedge Server **Administration** utility found in the DMZedge Server Program Group. To start the **Administration** utility, double-click on the icon in the Program group.

The **Administration** utility has three tabs, **Status**, **Settings**, and **About**.



- The **Status** tab displays the current status of the DMZedge Server.
- The **Settings** tab is used to configure the DMZedge server properties.
- The **About** tab displays information about the DMZedge Server, including licensing, version, and activation status.

## Status Tab

The **Status** tab displays the current status of the *DMZedge* Server Service.

**Version Information** - The current product version and build number is displayed. We recommend that you use the **Check For Program Update** utility in the **DMZedge Server Program group** frequently to check for new releases of the product. Use the **Check For Program Update** utility to review the latest release notes and download any updates to the product.

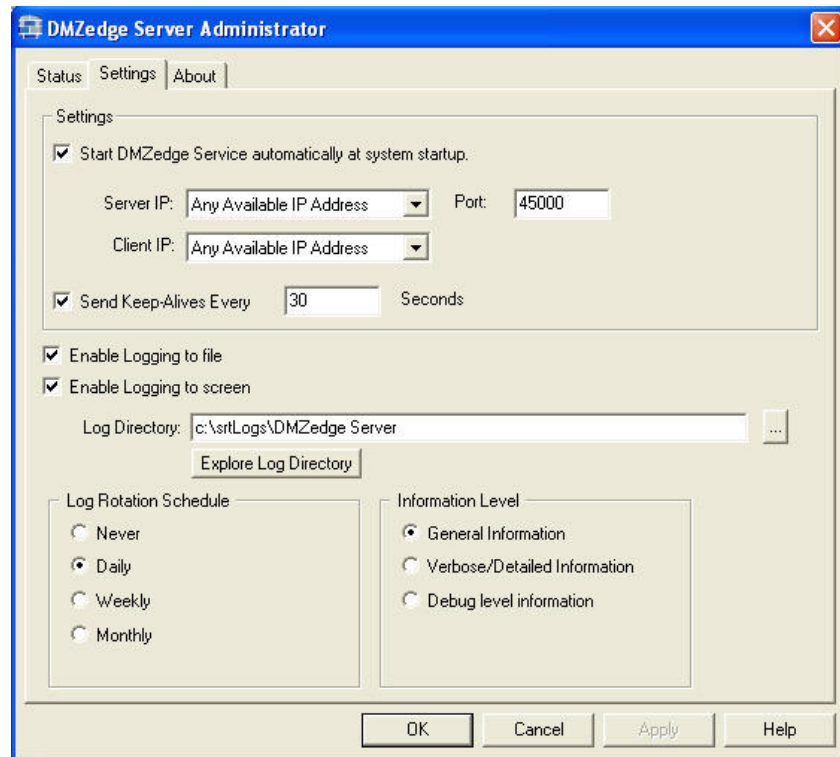
**Service** - This section displays the current running status of the Service. You can also use the **Start** and **Stop** buttons to toggle the running state of the *DMZedge* Service.

**Status** - If the service is running, this section displays the connection information

- **Active DMZedge Client Connections** – This value reflects the current number of connections to the *DMZedge* Server from clients on the Internet (forward facing).
- **Active DMZedge Server Connections** – This value reflects the current number of connections to the *DMZedge* Server from internal Cornerstone MFT or GroupDrive Servers (inward facing). These are connections that have originated from inside your firewall out to the *DMZedge* Server.
- **Listening On Ports** – This value contains a comma separated list of ports on which the *DMZedge* Server is listening for client connections.
- **Client Bytes Received** – This value indicates the number of bytes that have been received from forward facing client connections.
- **Client Bytes Sent** – This value indicates the number of bytes that have been sent by the *DMZedge* Server to clients.

## Settings Tab

The **Settings** tab is used to display and access configuration options for the DMZedge Server Service.



**Start DMZedge Service automatically at system startup** - Enable this feature to have the Service start each time Windows boots. This is the default and preferred setting.

**Server IP** - This is the Inward Facing IP address that the DMZedge Server will listen on for outbound connections from Cornerstone MFT and GroupDrive Servers located in your secure LAN environment. When you configure the DMZedge settings in Cornerstone MFT and GroupDrive, you will supply this **Server IP** address as the DMZedge server address.

**Port** - This is the Inward Facing port that the DMZedge Server will listen on for outbound connections from Cornerstone MFT and GroupDrive Servers located in your secure LAN environment.

**Client IP** - This is the Forward/Outward Facing IP address that the *DMZedge* Server will listen on for client connections. The **Ports** that will be used are configured on the *DMZedge* settings tab in the Cornerstone MFT and GroupDrive Server Administration utilities.

**Send Keep-Alives every X Seconds** - Enable this option to send a "Keep Alive" signal to the server. This will keep the connection open. The default is 30 seconds.

**Enable Logging To File** - Enable this feature to have *DMZedge* log information to a file. This is recommended.

**Enable Logging To Screen** - Enable this feature to have *DMZedge* log information the screen.

**Log Directory** - Specifies the location for log files. Use the '...' browse button to choose a directory.

**Explore Log Directory** - Click this button to launch Windows Explorer and browse the contents of the log files directory.

**Log Rotation Schedule** - Specifies how frequently the log files will be rotated..

**Information Level** - This value specifies the level of detail written to the log file. **General Information** is sufficient for normal program execution. **Verbose/Detailed Information** will display more detailed information. **Debug Level Information** will record the most information and should only be enabled if instructed to do so by a support technician. Debug Level Information could degrade performance under heavy loads.

## About Tab

The **About** tab displays information about the DMZedge Server Program.

**Version Information** - The current product version and build number will be displayed. It is recommended that you use the Check For Program Update utility in the DMZedge Server Program group frequently to check for new releases of the product. Using this utility, you will be able to review the latest release notes and download any updates to the product.

**Product Registration Information** - The current license information will be displayed in this area. If you are evaluating the software, you will not see a valid Product Registration Code. Once you purchase the product, you will be prompted to enter the registration code on the Trial Splash screen. Once you have activated your product, the product registration code will appear on this screen. The product registration code will be needed for obtaining technical support on our website.

## Obtaining Support

Support for DMZedge Server is available online at our Web site at <http://www.dmzedge.com/support/dmzedge/>

## Terminology

**Active Directory (AD)** – An implementation of Microsoft’s LDAP directory services. AD provides central authentication and authorization services for Windows-based computers.

**Firewall** – A technology that inspects network traffic and permits or denies access based on a set of rules. It prevents unauthorized access to or from private networks. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks that are connected to the Internet, especially Intranets. All messages entering or leaving the Intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

**FTP** – Abbreviation for File Transfer Protocol, the protocol used on the Internet for exchanging files. FTP uses the Internet's TCP/IP protocol suite to enable data transfer. FTP is most commonly used to download a file from a server using the Internet or to upload a file to a server (for example, uploading a Web page file to a server). The FTP file transfer is not random access (for example, seeks are not allowed in the file). This is why the entire file is downloaded into the cache when you open it. Most companies use FTP to enable their customers to download software updates or patches. Most access to FTP servers is done by way of an anonymous logon. This type of logon usually allows the user to have read-only access to the FTP server. Some companies also allow users to upload files to the FTP server into specific directories.

**FTPS (FTP/SSL)** – An FTP encryption protocol used in conjunction with public key certificates.

**GroupDrive<sup>®</sup>** – Refers to the WebDAV server with custom extensions developed by South River Technologies. [GroupDrive<sup>®</sup> Collaboration Server](#) is a multi-threaded, dynamic WebDAV Server for the Windows operating system.

**HTTP** – Abbreviation for Hypertext Transfer Protocol, the underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.

**HTTPS (Hypertext Transfer Protocol over Secure Sockets Layer)** – Combines HTTP with an encrypted secure sockets layer (SSL).

**LAN** – Acronym for Local Area Network, a computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings.

**Lightweight Directory Access Protocol (LDAP)** – An application protocol for querying and modifying directory services running over TCP/IP.

**Proxy Server**– A server that acts as a gateway between a client and another server (the "real" server). A proxy server sits between a client application, such as a Web browser, and forwards requests to another server. A proxy server intercepts all requests to the "real" server to see if the requests should be permitted. If the request is permitted, the proxy server will forward the request.

**SFTP** – Refers to an SSH (Secure Shell) based encryption protocol that is more efficient and secure than FTP.

**SSL** – Abbreviation for Secure Sockets Layer, a secure protocol developed by Netscape for transmitting private documents over the Internet. SSL works by using a private key to encrypt data that is transferred over the SSL connection.

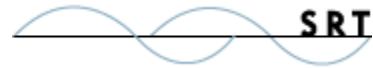
**Select** – Refers to an instruction given in the help system, meaning to click with your mouse on a specific icon or file.

**TCP/IP** – Abbreviation for Transmission Control Protocol/Internet Protocol, the suite of communication protocols used to connect hosts on the Internet. TCP/IP combines several protocols, the two main protocols being TCP and IP. TCP/IP is built into the UNIX operating system and is used by the Internet, making it the de facto standard for transmitting data over networks. Even network operating systems that have their own protocols, such as Netware, also support TCP/IP.

**Cornerstone MFT Server** – A multi-threaded, dynamic SFTP/FTPS/FTP Server for the Windows operating system.

**TLS** – Abbreviation for Transport Layer Security, a protocol that ensures privacy between communicating applications and their users on the Internet. TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to SSL.

**WebDAV** – Refers to the Web-Based Distributed Authoring and Versioning Protocol. An extension to the HTTP protocol that many servers now support on the Internet.



## **About South River Technologies**

South River Technologies (SRT) is an innovator in managed file transfer and document collaboration software. SRT's software seamlessly integrates access to remote files into the desktop applications that users rely on, creating an instantly familiar interface for collaborating, sharing, and accessing files. SRT's enterprise class server products are built using industry standard encryption, highly granular security configuration controls, and technologies to reduce the risk of network intrusions. Over 60,000 customers, including more than 70 colleges and universities, government agencies such as NASA and FAA and other blue chip companies in more than 110 countries rely on SRT's software to make remote file access and collaboration more efficient for their customers, partners, and distributed workforce. For more information, please visit [www.southrivertech.com](http://www.southrivertech.com).