2017

Using PGP Encryption with Cornerstone MFT Server

Instructions for configuring and/or maintaining PGP in a Cornerstone MFT environment.

QuickStart Guide

PGP with Cornerstone MFT Server

PGP (Pretty Good Privacy) is a method of securing digital information developed by Phil Zimmerman in 1991, originally for the purpose of providing email privacy and authentication. PGP is usually used to encrypt data “at rest” as opposed to SSL or SSH, which encrypt data “in transit.” PGP now follows the standard called OpenPGP under RFC 4880.

PGP encryption uses a combination of hashing, data compression, symmetric-key cryptography, and public-key cryptography to provide security for data communication and storage. This protocol provides confidentiality, key management, authentication, and digital signature support.

When you use PGP encryption, you generate a pair of keys. One key is the public key; the other is the private key. You will send your public key to anyone who needs to encrypt data to send to you. You will then use the private key to decrypt the message sent to you encrypted using your public key. PGP also requires a password when you use your private key to decrypt the message.

Real-Time PGP

When you use Cornerstone PGP encryption, your encrypted data-in-motion immediately becomes encrypted data-at-rest. Your data never exists in an unencrypted state on your network. When the client uploads a file, Cornerstone generates a PGP encrypted packet and writes that to the disk in smaller blocks of data. Once the last block arrives, Cornerstone completes the file, generating the last PGP encrypted packet, writes and closes the file, and reports to the client that the file was uploaded successfully.

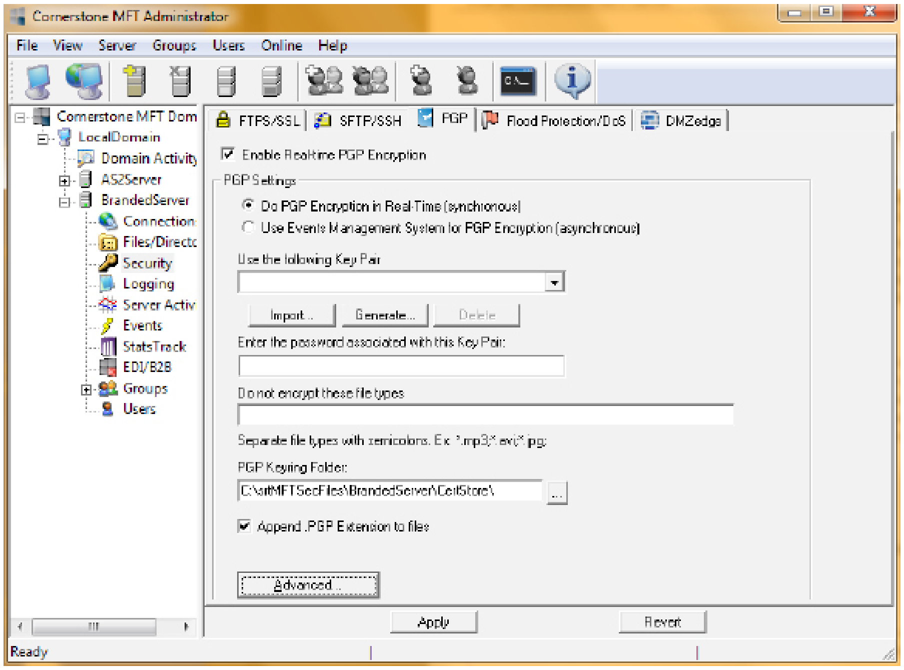
Activating PGP

PGP encryption settings are set at the Server level, on the PGP tab.

To access these settings at the Server level, expand the **Server** in the left-hand tree view, click **Security**, and then click the **PGP tab**.

Configuration Options

- **Enable Real-time PGP encryption** - Select this check box to encrypt your files in real-time (Recommended). PGP encryption is not enabled by default.



☑ Enable RealTime PGP Encryption

PGP Settings

● Do PGP Encryption in Real-Time (synchronous)

○ Use Events Management System for PGP Encryption (asynchronous)

Use the following Key Pair

Enter the password associated with this Key Pair:

Do not encrypt these file types

Separate file types with semicolons. Ex: *.mp3;*.avi;*.jpg;

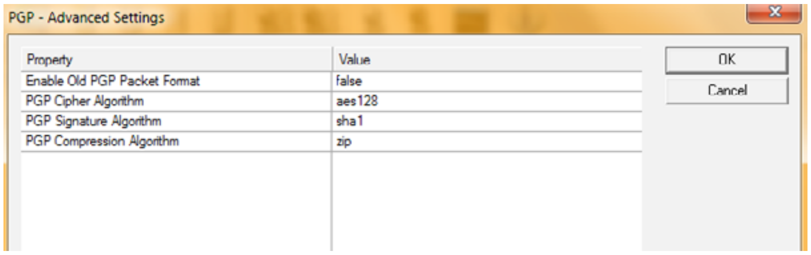
PGP Keyring Folder:

C:\srtMFTSecFiles\BrandedServer\CertStore\

☑ Append .PGP Extension to files

- **Do PGP Encryption in Real-Time** (synchronous) - Enabled automatically when real-time PGP is enabled. You also have the option to elect to use events management to leverage PGP.
- **Use Events Management System for PGP Encryption** (asynchronous) - Select this check box to use the events management system for PGP encryption. This will encrypt your data on a more selective basis, triggered by designated events, rather than on all data.
- **Use the following Key Pair** - Use the dropdown arrow to select your key pair. You can also import, generate, or delete a selected key pair, as explained later in this guide.
- **Enter the password associated with this Key Pair** - Type the password for this key pair.
- **Do not encrypt these file types** - Enter the file types you would like to exclude from encryption. Separate file types with semicolons (i.e., *.mp3;*.avi;*.jpg;).
- **PGP Keyring Folder** - Use the browse button "..." if you would like to change the default location of the PGP Keyring folder.

Clicking the **Advanced** button will open additional configuration options. If you need your server to remain compatible with pre-2000 implementations of PGP, set this option to True by either double-clicking the Property or selecting the shaded box on the right side of the Value.



Property	Value
Enable Old PGP Packet Format	false
PGP Cipher Algorithm	aes128
PGP Signature Algorithm	sha1
PGP Compression Algorithm	zip

Using an Event Handler to PGP Encrypt or Decrypt Files

You can configure an Event Handler to PGP encrypt or decrypt your files automatically in response to a specific action taken on the server. However, if you enabled **Do PGP Encryption in Real-Time (synchronous)** on the PGP tab, you do not need to configure an event handler for PGP encryption unless you excluded certain file types from real-time encryption and would like to use an event handler to encrypt or decrypt specific instances of these file types.

To Configure an Event Handler to PGP Encrypt or Decrypt Files:

1. In the left-hand tree view, expand the **Server > Events > Event Handlers tab**, and then click Add.
2. Expand File Events and File Upload/Write, then select Upload/Write successful. Click Next.
3. If you would like to set parameters on the File name, click File name. Otherwise, click Next.

4. Under Actions, select PGP Encrypt file or PGP Decrypt file. Click Next.
5. Specify a Name and Description for this Event Handler. This Event Handler is enabled by default. If you would like to disable this Event Handler, clear the Enable check box. Click Finish.

Your new Event Handler is now displayed on the Event Handlers tab. Event Handlers can be edited or deleted at any time. For more information about Cornerstone's Event Handling system, see the online Cornerstone MFT User Guide found here: **http://webdrive.com/product-support/cornerstone-mft/**.

Creating a PGP Key Pair

You can import, generate, or delete Key Pairs from the Cornerstone PGP tab. Access the Cornerstone PGP tab by expanding Server and Security in the left-hand tree view and clicking the PGP tab.

Use the dropdown arrow to select an existing Key Pair. If you would like to generate a new Key Pair, click Generate.

Generating a New Key Pair

1. When you click the Generate button, the PGP Key Generation Wizard will appear.
2. Use the dropdown arrow to select your PGP Key Type. Select your Key Size. Longer key-lengths are more secure but take slightly longer to process. Click Next.
3. Type a name for this PGP Key Pair. Type the Private Key password twice to confirm it.
4. Click Finish.

This key pair will now appear in the dropdown list. Select the key pair you would like to use for this server.

Troubleshooting

SRT Knowledgebase

Visit our Knowledgebase to read helpdesk articles and answers to frequently asked questions.

Reporting Problems

To search our knowledge base or report a problem, visit the SRT HelpDesk: **http://srthelpdesk.helpserve.com/**.

About South River Technologies

South River Technologies (SRT) is an innovator in secure file management software. SRT software allows users to securely access, manage, and collaborate on files over the Internet, streamlining business processes to improve productivity. SRT's products enhance customers' existing applications by instantly enabling secure access and collaboration within those applications. More than 90,000 customers in 140 countries use 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. South River Technologies, Cornerstone MFT, Titan FTP Server, WebDrive, and DMZedge Server are registered trademarks of South River Technologies, Inc. in the U.S. and other countries. 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.
1910 Towne Centre Blvd
Suite 250
Annapolis, Maryland 21401
USA

Toll Free: 1-866-861-9483
Main: 443-603-0290
Fax: 410-266-1191
Corporate Web site: www.southrivertech.com
Online Support: www.srthelpdesk.com

System Requirements

Supported Operating Systems

- Windows Server 2012, all editions, 32-bit and 64-bit
- Windows Server 2008-R2, all editions, 32-bit and 64-bit
- Windows Server 2008, all editions, 32-bit and 64-bit

Minimum Hardware Requirements

- 2 GHz Pentium® class processor
- 4GB of RAM is required; 8GB of RAM is recommended
- Minimum 100MB of free disk space for the application
- Minimum SVGA (800x600) resolution display is required to run the Administration console program.

Minimum Software Requirements

- Microsoft .NET Framework v4.0 is required
- Microsoft SQL Server 2005 or later is required
- Microsoft SQL Server Management Studio Express is recommended

Limitations

- Cornerstone MFT server is a multi-threaded, dynamic server solution for the Microsoft Windows operating system. While designed to handle an unlimited number of user connections and servers, like all software, Cornerstone is limited by the resources of the computer; most notably, those limitations imposed by the Windows Sockets (WINSOCK) Library.