2018

Cornerstone MFT Server Security Best Practices

A guide to utilizing Server, Group, and User level settings for efficient server setup.

QuickStart Guide

Securing Your Server Environment

Security is all about a balance between education—for every user from the ground up, including ongoing administration training—and administrator-enforced measures. These can be as simple as forcing complex passwords or as advanced as implementing a front-door-guarding DMZ server. This guide focuses on the steps you can take to harden your server environment.

Turn off Anonymous Access (and FTP, if possible!)

First things first: **Disable FTP on your server**. Ftp is one of the oldest protocols, created to send data in plain text, without built-in encryption or authentication. Attackers can steal packets in transit or even alter the data. Even with added encryption, FTP is inherently less secure. Encryption methods can vary in strength, depending on hashing algorithms and key length used.

If at all possible, use FTPS or SFTP. SFTP is often preferred, because it only needs to use one port through the firewall, while FTPS requires multiple connections. SFTP can also utilize a SSH key for dual-factor authentication. Use of certificates adds a vital layer of security.

If using FTPS, bear in mind that SSL 1.0-3.0 and TLS 1.0 are defunct versions which have been broken with a variety of attacks and should never be used. Use TLS 1.1 or later versions.

If you absolutely must use FTP, disable anonymous access and use it to send only data that is not security-intensive. PCI-DSS and HIPAA require that credit card and health data be sent and stored securely, so do not use FTP with this data.

FTP vs. FTPS

It is worth noting that Explicit FTPS uses the same ports as FTP. So, if you turn off/disable FTP on the Cornerstone server, Explicit FTPS will not work. The configuration setup to address that is:

1. FTP will need to be enabled.
2. On the FTPS/SSL tab, enable “Require all FTP connections from clients to be secure”

This setup will effectively disable plain/insecure FTP while allowing explicit FTPS to work properly.

Keep your software up-to-date

Large enterprises often delay updates to check for stability—an unstable update could slow or halt an organization, and if the software is working, why update? Because in the months or even years many organizations wait to install updates, important security patches may have been added to the software. If software is left out of date for too long, large changes may be required to bring a new version of the software online. Compliance standards might change, leaving you with unsecure software without your knowledge. Some organizations allow the maintenance to lapse until it fails a security audit, or worse, they experience a breach.

For instance, when significant problems with the SHA-1 hashing algorithm were discovered, all compliance standards demanded that systems drop the old standard and move to SHA-2. Legacy systems, or very out of date software, frequently still run SHA-1 and are unsecure. Cornerstone MFT Server not only has SHA-1 disabled by default, it includes SHA-3 capability, in case SHA-2 fails.

If your servers are critical to your enterprise, and 24/7 uptime is essential, create a clustered environment. With two or more servers working from the same database for settings and information, one can be taken offline for maintenance and patching without interrupting the flow of access.

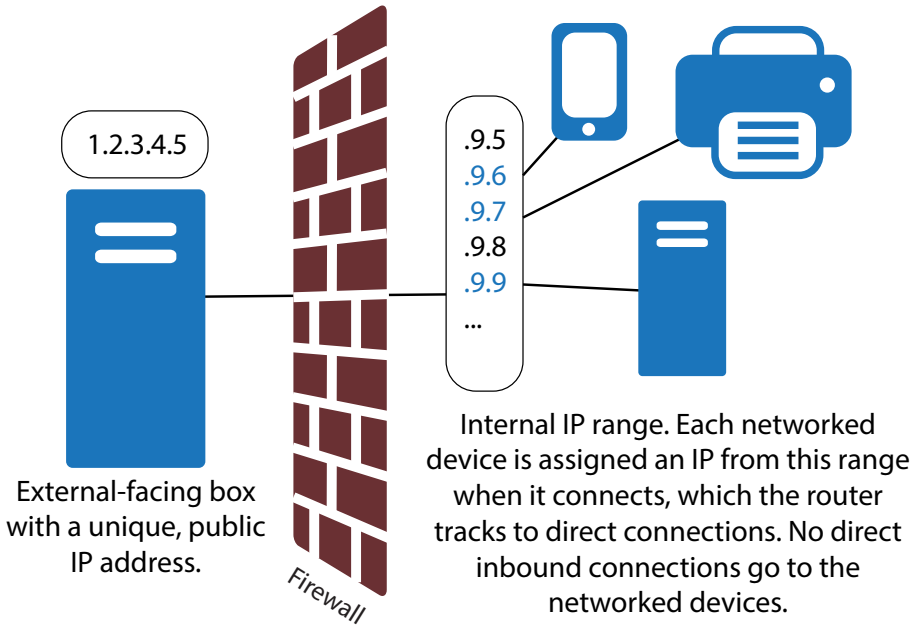
Limit access

Grant only the amount of access that the user needs. If a user only needs to view files in a folder, don't give them edit or write permissions, etc.

Most companies take a liberal stance with need-to-know in order to facilitate fast access to files, assuming that those with the most access won't abuse that power. Unfortunately, even if high-access users have the best intentions, granting too much access to too many users is a security nightmare. The more administrators you have, the more chance there will be for small security breeches, and the more chance they will go unnoticed for long periods of time. For instance, an admin might make a one-time change to grant special access to files to a lower-access user. Years pass, and that user still has access to files that may have become more sensitive. If the original admin is no longer with the company, it may go unnoticed indefinitely. Administrator changes are often not catalogued or included in audits, so they may go unnoticed.

Enforce rigorous adherence to procedure. This is best handled with inherited settings, which go from broad (at the admin level) to more specifice (down through to single users or vendors who only need read or write access to a single directory). A more detailed breakdown of this is shown in the Appendix of this document.

Do not use default accounts like root or admin for administration, as the defaults are vulnerable to hacking attempts. Many free FTP server alternatives require new user accounts to be created on the OS itself, which is unsecure, so use caution when choosing your software.



Port Forwarding and Mapping

To start a connection between a client and a server, you need the IP address of the server you want to connect to and a port to latch onto. Most routers have a public-facing IP address that connections can target, with a range of internal-use-only IPs behind it, one for each different device on that network. Each device can use a different IP number from that range anytime it reconnects to the network; the router keeps track of which device is using which IP so incoming traffic is directed to the correct device. The router in this case is working as a firewall by presenting a public face, screening traffic, and passing it along without allowing the incoming traffic to interact directly with the networked devices. Keeping an outward-facing IP that is very different from the range of internal IPs provides an extra layer of defense to the network.

Firewalls can be configured to forward information that comes into the default port to the same port on the internal network. To ensure users have access to a server on the internal LAN without endangering the computers linked through the LAN, companies regularly use

port forwarding through the firewall to direct the TCP/IP traffic to the proper computer. Port forwarding is used by most routers/firewalls. Port forwarding literally forwards data incoming on a specific port to the same port on a different computer.

During port forwarding, the firewall will redirect traffic to the server based on IP address. Therefore, the networked computers must use a static IP address that the firewall can always refer to. If the server's IP address is DHCP (Dynamic Host Configuration Protocol) based, the firewall could forward the data to the wrong computer.

Both your router/firewall and server will need to be configured to use port forwarding, however.

To set up a static IP on a Cornerstone installed on an internal LAN-based computer:

1. Retrieve the external public IP address of the firewall, the internal IP address of the router, and the internal LAN IP address of the Cornerstone server.

2. Have the Network/LAN Administrator reconfigure the firewall to forward server traffic to the Cornerstone Server according to the following table:

Protocol	Ports to Route
FTP	21, 20, 50000-50050
FTP/S	21, 990
SFTP	21
HTTP/WebDAV	80
HTTPS/WebDAVS	443
AS/2	443

3. The passive port range should be 2 times the number of user accounts created. A server with 100 users should have a passive port range of 200 (which could be ports 50000-50200). These ports will be used for transferring data and directory listings to the client. Do not use a single port, as this may result in data transfer failures for clients.

Encryption and Hashing

Use the strongest hashing (MAC) and encryption ciphers available, and disable older options which have been proven to be unsecure (Blowfish, DES, MD5, SHA-1). Also use the largest key length your system can support. The higher the key length, the greater your security; however, very long key lengths may slow your system if computing resources are limited or traffic volumes rise.

Set your server to reject incoming connections which use less secure encryption and hashing as well.

Perimeter security and Streaming PGP

The DMZ (demilitarized zone), or the space outside your internal network where external users attempt to connect, is one of the most vulnerable areas of your system. Information should never be stored on a server outside your firewall, even encrypted. To facilitate movement of secure files into the internal database, set up a DMZ gateway. This is server software installed on a server in the DMZ with only one control channel going **from** the private network server **to the DMZ** server, with no traffic allowed inbound at all. When users attempt to login to your network, they will access the DMZ server, which will transfer that data through the established control channel, without requring any open ports in the firewall.

Real-Time PGP

PGP (Pretty Good Privacy) is a method of securing digital information usually used to encrypt data "at rest," as opposed to SSL or SSH, which encrypt data "in transit." 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.

In most implementations of PGP, the data is sent to the server, likely using a SSL or SSH to encrypt in-transit. Once on the server, the data is encrypted using PGP to store it at rest. However, there is an instant—microseconds—where the file sits on the server in an unprotected state before being encrypted. For an algorithm written specifically to target files like this, that is more than enough time to copy the data to an infiltrator's repository.

Cornerstone uses real-time or streaming PGP encryption. 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 by generating the last PGP encrypted packet, writes and closes the file, and reports to the client that the file was uploaded successfully. The data is sent and PGP encrypted as one action, so data never exists in an unencrypted state on the network.

Hacking Prevention

Use white or blacklisting to limit the IPs users can log in from. You can blacklist notorious IPs (for instance, IPs known to come from Russia or China), or create a whitelist of

individuals who are trusted, while all other connections will be rejected. Whitelisting is most secure, but is less efficient, and might be impossible for companies with many trading partners or vendors with changing IP addresses.

Using events, which are explored further in this article, automatically ban IPs which log in too many times in a short space of time or use incorrect root or admin credentials, preventing DoS and other routine hacking attacks. Users should be locked out after 3-5 invalid attempts.

Events, Automation, and Logging for Auditing

Automated notifications are the fastest, easiest way to keep tabs on your server's security and collect data to increase visibility into your system.

You should have automated notifications set up for these events at minimum:

- When a vendor or trading partner account login fails/a user is added to the banned IP list
- DoS or other brute force attacks
- When uploads/downloads fail
- Potential virus

These alerts should also be added to an internal syslog for auditing purposes. Make sure your event gathers the following information:

- The reason for the alert
- User account involved
- IP address
- Date and time

Your logs should contain comprehensive data on all activity on the server, including both user and admin actions while logged in, and when accounts were created and deleted.

Two-(or more)Factor Authentication

The most convenient and common method of authentication is software-based, single-factor authentication. The computer handles the entire encryption and data transfer process, including generating the public and private keys. Your key pair is stored securely on the computer or server on which it was generated, and the private key is stored in hidden locations or encrypted (or both).

The absolute necessity of keeping the private key secure can be a hindrance, however. If the private key absolutely must be shared—for instance, an employee needs to use the same key to access the server, but gets a new computer—it should be transferred on a physical piece of hardware, such as a CD or flash drive. It should never be transferred digitally.

If the private key is never shared, this form of authentication has only one other, very slight vulnerability. While a data transfer is in progress, the private key may briefly appear in the computer's memory as it decrypts incoming data. An extremely sophisticated attacker could capitalize on this moment of vulnerability to snag the private key.

Two-factor authentication answers this problem by adding a second, physical form of proof to complement the usual password protection. Even if the correct credentials are present, the physical second factor must also be there, making it significantly more difficult for someone to access data illegitimately. This method is preferred for enterprises where sophisticated attacks are highly likely, and the vulnerabilities of single-factor authentication are too risky.

Some two-factor authentication systems use biometrics for their secondary proof, such as fingerprint or retinal scanning technologies. The most versatile (and foolproof) second factor, however, comes in the form of a token.

The token is a separate piece of hardware which contains all of the algorithms necessary to create a secure public and private key pair on its own and perform encryption and decryption of data. This ensures that the private key absolutely never leaves its home hardware. It will also never appear in the memory of a computer, even for an instant. This provides mobility, since you carry your private key with you rather than having it tied to a single computer. This works well for employees that need to move around the company or to off-site locations.

Force Complex Passwords and Periodic Changes

Password enforcement is where hardcoded requirements work particularly well to eliminate human error. Enforce complex passwords for **all accounts (including the admin account)**. The Cornerstone complex password requirement is an 8 character minimum and supports special characters in addition to letters and numbers through native authentication. Have accounts expire after a few months and require each user to select a new password. Also, set user accounts to expire after a certain length of inactivity, to keep old, forgotten accounts with inappropriate access levels from being used. Set sessions to time out in 15 minutes or fewer to prevent session hijacking. This is in accordance with PCI DSS compliance.

Make certain user accounts are individual and unique. Each user, vendor, and trade partner needs their own account to meet compliance standards for visibility and auditing.

Appendix: Server Permissions Organization

Cornerstone MFT Server is designed to provide a streamlined user setup process without sacrificing customizability. The administrator can configure Shared Attributes at the Server, Group, or User level.

Create templates by setting attributes at the Server or Group level bypasses the step of manually editing each user's configuration to save time and reduce the risk of user error.

The following example illustrates the effectiveness of the Server/Group/User organization.

In this case, company XYZ wishes to provide certain files via FTP to all of its employees and customers, with these parameters:

- Customers should only be able to view a few marketing-related documents, which XYZ's Marketing Team maintains.
- XYZ's Management Team needs access to all files on the server.
- XYZ's Artwork Team will use the FTP server to upload, download, and share bitmap images.

Using Cornerstone server software, XYZ can create groups for each category of user and adjust their permissions.

Implementation

To implement this setup, the administrator must create a new server leading to a designated database, create subdirectories in that database, and create groups linked to each database and adjust their permissions.

Create a New Server

First, create a new server. As a precaution, stop any other running FTP servers to avoid a port conflict. Create a new server with default settings, making sure that the data directory is something like "C:\srtMFTData\XYZ\".

Add Directories

Using either the command prompt or Windows Explorer, set up two subdirectories: "\XYZ\Marketing\" and "\XYZ\Artwork\". Since access permissions are primarily granted through directory structure, these subdirectories allow us to partition the different user classes. The Marketing Team will have no access to the Artwork Team's files (in fact, they won't even know the files exist), and vice versa. Add a few files into each directory for testing purposes.

Create Groups

Now, launch the New Group Wizard and create four different groups for the server: Marketing, Artwork, Management, and Customers. All user home directories should default to group directory. Otherwise, use the following configurations:

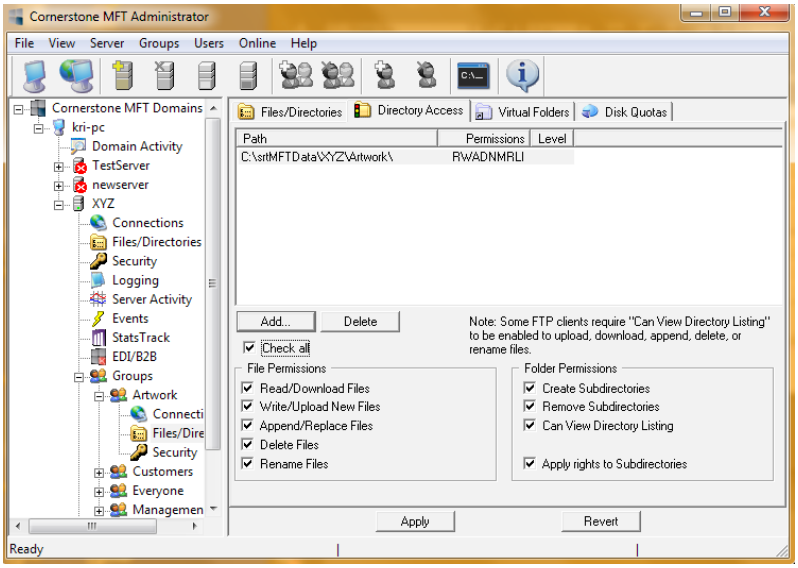
Marketing: Group Directory: C:\srtMFTData\XYZ\Marketing\

Artwork: Group Directory: C:\srtMFTData\XYZ\Artwork\

Management: Group Directory: C:\srtMFTData\XYZ\

Customers: Group Directory: C:\srtFtpData\XYZ\Marketing\

Adjust Access Permissions



After creating each user, adjust the access permissions for each group's directory. Expand each group in the tree pane and select Files/Directories. Click the Directory Access tab and add a new access item for each of the directories as follows:

- Marketing—Add C:\srtMFTData\XYZ\Marketing\ and "Check all" to give full access permissions.
- Artwork—Add C:\srtMFTData\XYZ\Artwork\ and "Check all" to give full access permissions.
- Management—Add C:\srtMFTData\XYZ\ and "Check all" to give full access permissions.
- Customers—Add C:\srtMFTData\XYZ\Marketing\ and check "Read/Download Files", "Can View Directory Listing", and "Apply rights to Subdirectories".

Make sure to click Apply after setting each path.

Create Users

Using the New User Wizard, let's create four different users (one for each group) for testing purposes. Use the following configuration:

Marketing-testuser

- Group Membership: Add "Marketing"

- Select a Primary Group for this User: Select "Marketing"
- Select "Inherit home directory from group"

Artwork-testuser

- Group Membership: Add "Artwork"
- Select a Primary Group for this User: Select "Artwork"
- Home Directory: Select "Inherit from Group"

Management-testuser

- Group Membership: Add "Management"
- Select a Primary Group for this User: Select "Management"
- Home Directory: Select "Inherit from Group"

Customers-testuser

- Group Membership: Add "Customers"
- Select a Primary Group for this User: Select "Customers"
- Home Directory: Select "Inherit from Group"

Conclusions

The server is now configured to provide access to four different classes of users:

4. Marketing Team (Group: Marketing) which has full access to the "C:\srtMFTData\XYZ\Marketing\" directory and all subdirectories but no access to any other directory.
5. Artwork Team (Group: Artwork), which has full access to the "C:\srtMFTData\XYZ\Artwork\" directory and all subdirectories but no access to any other directory.
6. Management Team (Group: Management), which has full access to the "C:\srtMFTData\XYZ\" directory and all subdirectories, including the \Artwork\ and \Marketing\ directories.
7. Customers (Group: Customers), which has limited, read-only access to the "C:\srtMFTData\XYZ\Marketing\" directory and all subdirectories, but no access to any other directories.

By organizing the server configuration with groups that correspond to each user class, the amount of work required to add a new user is trivial. Configurations should be modified at the highest level possible (Server or Group) in order to prevent the Server Administrator from having to manually edit configurations for each individual user. Since users can be members of multiple groups, Cornerstone will combine the settings from each group to determine an individual user's configuration.

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
- Windows Server 2016, 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.

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