

# Technical summary for customers

ftp.morningstar.com

## Introduction

Hosted in North America, ftp.morningstar.com is one of our mechanisms for delivering and receiving data from clients and providers.

This document provides a brief technical overview designed to answer the most asked questions and provide best practices for using the service.

## Site design

ftp.morningstar.com runs from two geographically diverse locations in North America to ensure redundancy and reliability of the service.

The IP addresses for the two locations are:

- 216.228.224.25
- 216.228.237.25

Only one of the above sites will be live at any time, with the other acting as DR for the service. Traffic can be directed to either site as required by Morningstar to provide a reliable service. **Client firewalls and proxy servers need to be opened to both addresses to ensure reliable access to the service.**

Each location consists of a pool of gateway servers deployed in Morningstar's DMZ. These gateway servers accept client connections and provide a secure tunnel to a pool of backend FTP servers.

## Protocols and ports

The FTP environment supports all the below transmission protocols over the detailed ports.

We would recommend clients use **SFTP** where possible:

- SFTP (SSH FTP) TCP 22
- HTTPS TCP 443
- Active FTP TCP 20, 21
- Passive FTP TCP 21, 24200-24249
- HTTP TCP 80
- FTPS (SSL FTP) TCP 21, 990

Morningstar reserves the right to designate a secure transmission protocol on a per client basis at our discretion.

## Accounts and files

All newly created accounts will require the end user change their password before first use. Details on how to do this can be found in the FAQ.

The site supports SFTP login authentication using password, key exchange, or password and key exchange. If you wish to use key exchange for authentication please let your relationship manager know.

Morningstar maintains a strict retention policy for data on this system. Files are removed from the server after a specific number of days—please consult your product documentation for the retention policy time frame.

Please limit filenames to the ASCII character set avoiding common illegal characters and symbols. This will help to ensure that any systems processing the file run without error.

## Recommended best practices

- Morningstar strongly recommend that you reset your FTP account password annually. Password should be 8 characters long, includes letters (both upper and lower case), digits and symbols. Details on how to change your password can be found in the FAQ
- Use the file naming conventions (and date stamps included in the name) to verify that the day's files have been posted. Please refrain from using commands like "mdtm" or "list" as these commands check each file and can cause slow response times for all clients
- Implement a smart checking mechanism in your processes to avoid unnecessary duplicated downloads. This means that once a file is found and downloaded, your processes shouldn't look for the file again until the next scheduled delivery time frame
- Please keep in mind that processes downloading the same files many times a day are unnecessarily tying up FTP and processing resource. Consider how you can make your process as efficient as possible to save on resources. Morningstar's FTP systems may automatically block clients that generate intense activity

- For secure file transfers, FTP over SSH (SFTP) is recommended over FTP over SSL (FTPS). SFTP is a newer protocol, more efficient and Firewall configuration is much simpler for SFTP than it is for FTPS. Support is available for any client wishing to transition to any of the supported secure transfer protocols
- Implicit FTPS is now considered a deprecated standard therefore if FTPS is a requirement then explicit FTPS should be the preferred choice
- Idle-time out settings should be set to 300 seconds
- Passive mode FTP is recommended over active mode
- Consider implementing retry mechanisms for reliable downloads. Your process should retry downloading a file only when the previous process fails. The retry interval should be at least 15 minutes after the previous attempt fails

### Frequently Asked Questions

#### **I cannot connect to ftp.morningstar.com. Does Morningstar have any firewall restrictions?**

Morningstar does not restrict access to ftp.morningstar.com to individual client IP addresses. Please check with your network team to ensure the required rules are in place to permit outgoing FTP connections to ftp.morningstar.com.

#### **What are the required firewall rules that should be put in place to allow access to ftp.morningstar.com?**

To ensure reliable access to the service please ensure you whitelist both 216.228.224.25 and 216.228.237.25 for the port numbers specific to your chosen protocol.

- |                  |                     |
|------------------|---------------------|
| • SFTP (SSH FTP) | TCP 22              |
| • HTTPS          | TCP 443             |
| • Active FTP     | TCP 20, 21          |
| • Passive FTP    | TCP 21, 24200-24249 |
| • HTTP           | TCP 80              |
| • FTPS (SSL FTP) | TCP 21, 990         |

#### **Can I access the service by IP address instead of by URL?**

**We strongly recommend against this.**

Morningstar directs traffic between our two sites by updating the IP address that ftp.morningstar.com resolves as. We reserve the

right to make this change at any time to ensure reliability of this service to all customers.

Any connections being made to an individual IP address may result in you targeting the non-live site. In some circumstances this may result in stale data or failed connections

#### **What FTP client software does Morningstar support:**

ftp.morningstar.com supports all ftp clients that implement standard FTP protocols. For example, WinSCP, FileZilla, FTP voyage from RhinoSoft and WS\_FTP from Ipswich.

#### **How many concurrent connections can we have to the FTP?**

Each client (login) is limited to open up to 10 concurrent connections, at any time, additional connections could be rejected, refused or forced to be terminated unexpectedly.

#### **I can login but the connection is not stable. What should I do?**

Please ensure the FTP client idle time is set to 300 seconds to match the FTP server's setup. If you continue to experience instability after this change, please contact your client manager.

#### **How often do you test the failover of the FTP service?**

We will perform at minimum one scheduled failover per annum, monitoring, documenting and remediating any errors in the process to ensure the process will be reliable if needed.

#### **When connecting via a secure FTP method, what are the protocols and options that Morningstar recommends?**

Partners that use secure FTP connections need to ensure their software supports and enables the following Cryptographic protocols, Ciphers, Message Authentication Code (MAC) and Key Exchange Algorithms.

Secure FTP connections are only supported with the TLS 1.2 protocol using a combination of cipher/MAC/key exchange options listed below:

#### **HTTPS/FTPS ciphers**

- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA256
- AES256-GCM-SHA384
- AES256-SHA256

### SFTP/SSH ciphers

- AES-256-CBC
- AES-256-CTR

### SSH MACs

- SHA2 256
- SHA2 256-96
- SHA2 512
- SHA2 512-96

### SSH Key Exchange Algorithms

- ECDH-SHA2-NISTP256
- ECDH-SHA2-NISTP384
- ECDH-SHA2-NISTP512

As stronger cryptography protocols and cipher options become available, support for weak and deprecated protocols/ciphers will be dropped. Notification of such a change will be communicated to clients in advance to avoid issues.

### Where can I obtain a copy of the root and intermediary certificates for this service?

#### Root Certificate Authority:

DigiCert Global Root G2

Valid until: 15/Jan/2038

Serial #: 03:3A:F1:E6:A7:11:A9:A0:BB:28:64:B1:1D:09:FA:E5

Download location:

<https://dl.cacerts.digicert.com/DigiCertGlobalRootG2.crt>

#### Intermediate Certificate Authority:

Thawte TLS RSA CA G1

Valid from: 11/02/2017 to 11/02/2027

Serial #: 09:0E:E8:C5:DE:5B:FA:62:D2:AE:2F:F7:09:7C:48:57

Download location:

<https://cacerts.digicert.com/ThawteTLRSACAG1.crt.pem>.

### When reporting issues related to the FTP, what information should I provide to Morningstar?

- Your company name
- Your Morningstar FTP account name (username)

- The full path e.g.

<ftp://ftp.morningstar.com/Monthly/DataWarehouse>

- File name(s)

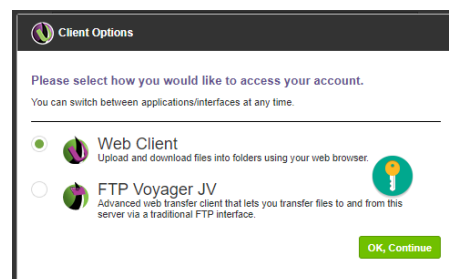
- Public Internet IP address that is used to access the FTP.
- If you don't know it you can either ask your company's IT staff/provider, or try [www.whatismyipaddress.com](http://www.whatismyipaddress.com) from the machine on which the FTP client is running
- A description of the problem
- Name of the relationship manager that works with your company (please include the RM in any email messages)

Data issues will need to be addressed by the data team and relationship manager during normal business hours.

### How do I change my FTP account password?

From a machine with internet access open [HTTPS://ftp.morningstar.com](https://ftp.morningstar.com) from a preferred browser.

1. At the login screen enter your FTP login ID and existing password. Click **Login**.
2. When prompted to select your client option, choose **Web Client**. Click **OK, Continue**



3. In the top right corner, you will see your FTP account name and a down arrow. Click this and then select **Change Password**.
4. Enter your Old Password, then enter your new password in the New and Verify password boxes.
  - a. Your password should be at least 8 characters long, include letters (both upper and lower case), digits and symbols. Click **OK**
5. Your password has now been changed.
6. Click the down arrow next to your account name again and select Log out.
7. Please log back in to verify your password has changed correctly, then proceed to update and test your processes.