Communicator

Secure FTP Configuration **–** *Setup Guide | June 2017*

Version 2.1

This guide explains how to set up a secure FTP connection to Communicator.

∞MMUNICATOR

Contents

Overview

When sharing customer data, it is always recommended that data is transferred using the File Transfer Protocol (FTP). This provides a secure way of transferring data and allows for compliance with our data security policy. This guide provides the background to FTP and supplies the settings required to connect to the FTP site which Communicator has provided you.

Secure FTP (FTP over SSL/TLS)

Secure FTP (FTP over SSL/TLS) comes under many guises. Communicator only supports the use of FTPES (explicit mode) and FTPS (implicit mode). These 2 connection types should not be confused with other types of connections called SSH FTP or SFTP. These connection methods pass data via the Secure Shell (SSH) protocol which is not compatible with enhanced secure technologies like SSL certificates.

Secure FTP works in a similar way to the security on websites. Both methods use SSL certificates which are assigned by a trusted authority, encrypt data over the connection and ensure that the company who owns the domain is who they say they are.

The ability to resume FTP uploading/downloading to/from Communicator's servers is supported; this resume capability is dependent upon the FTP client feature set. If the FTP client supports this feature, resumes will automatically be enabled.

Connectivity

Communicator does not support the use of the "Active" transport Mode in line with recommendations across the Internet community; all file transfer connections are configured for passive mode only. The vast majority of new FTP clients are preconfigured to use the "AutoDetect" mode; this will automatically re-configure the FTP client to use the supported transport mode of "Passive".

Due to the nature that the passive transport mode works, you may need to open up a range of ports on your firewall to enable connectivity to Communicator's FTP servers. If you are unsure of how to perform this action, please contact your IT Department for further information.

The below tables show the information required to allow access to the FTP service. Please be aware that most FTP connectivity issues are caused by incorrect firewall rule configuration.

Settings

Due to the wide range of potentially supported configurations Communicator only supports the following configuration:

FTPES (Explicit Mode) – Preferred Method	
Host/ Destination	data.communicatorcorp.com (current IP address 185.131.229.130*)
TCP Port	21 (FTP Control Channel)
TCP Ports	53000 – 54999 (FTP Data Channel)

FTPS (Implicit Mode)	
Host/ Destination	data.communicatorcorp.com (current IP address 185.131.229.130*)
TCP Port	990 (FTP Control Channel)
TCP Ports	53000 – 54999 (FTP Data Channel)

*Important Note

To enhance security between the user and Communicator, the user can configure their firewall rules to have an inbound/outbound rule that only uses the information defined above and only allowing traffic between the user's external IP address and Communicator's external IP address, thereby restricting potential abuse by external sources.

Please note that Communicator may in time change the external IP address associated with data.communicatorcorp.com. For this reason, where possible, please reference the host name rather than the IP address.

Communicator recommends that users connect to Communicator's secure FTP servers using explicit mode (sometimes referred to as FTPES in older FTP clients). This mode uses the same control port as normal FTP – TCP Port 21, and TCP Data Ports: 53000 – 54999 (inclusive).

Compatibility Note

To help protect Communicator against any potential security threats, the "SYST" command has been blocked, and all directory listings are displayed in the standard UNIX format. Communicator will not divulge whether they are running UNIX or Windows Operating Systems.

FTP File Clean-up Information

Any files that are stored in the user FTP area are automatically deleted after 14 days.

Troubleshooting

The following sections discuss solutions to queries that Communicator regularly receives about its secure FTP service.

Connectivity / Logon Problems

- Basic DOS and UNIX / Linux FTP programs do not support secure FTP communication. To connect to the FTP servers, use a valid FTP client which supports FTPS (explicit or implicit mode). See the end of this document, for tested clients on a number of platforms.

- UNIX / Linux platform by default support SFTP or FTP over SSH; however, Communicator only supports FTP over SSL / TLS. For UNIX / Linux platforms please use either a client which supports this functionality (see supported clients later in document) or integrate OpenSSL in to your environment.

- Verify FTP connectivity by going to a DOS prompt and type:

"ftp data.communicatorcorp.com"

If this is successful, a message is shown which is similar to the screenshot in Figure 1: Note UNIX / Linux commands can also be used but may look different to below.

If a prompt for the username is not displayed, check with your IT department to ensure the correct rules are applied to the firewall.

Figure 1 – Screenshot of Success Message on Windows Command Prompt
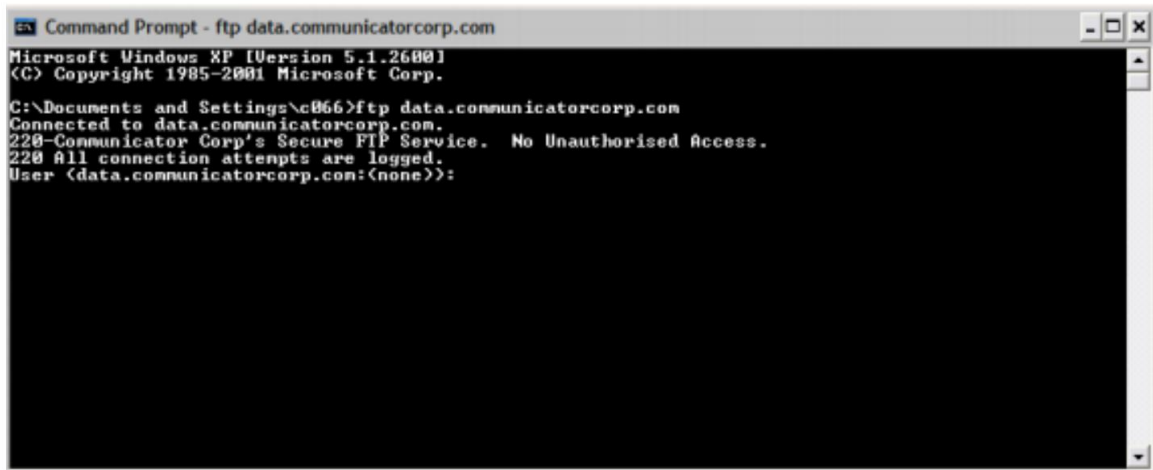
FTP User Account Related

- FTP account passwords are case sensitive. If connectivity fails at the username/password stage, ensure the password is entered correctly and in the same case as defined by the Communicator Support Team. If the password is correct, ensure that the username has been entered correctly. Please ensure that spaces do not appear before or after the username or password.

If this still doesn't work, please contact the Communicator Support Team to request that they reset your FTP password and attempt the connection again.

- Sometimes if a user has attempted to connect to Communicator's FTP servers unsuccessfully a number of times, the server's cache will become confused and keep denying access even if the logon credentials are correct. Please wait 5-10 minutes and try to connect again.

- Communicator's FTP servers support resume capability. If for any reason the connection is dropped during the uploading or downloading of a file, the upload/download will resume from the last position that was received by the server.

SSL Certificate Warnings

- On the first connection to Communicator's FTP servers using FTP client FileZilla the user may receive a warning about an "Unknown Certificate", saying:

  "The server's certificate is unknown. Please carefully examine the certificate to make sure the server can be trusted".

- This is an issue with FileZilla not automatically supporting the use of domain wildcard certificates. The user can check the checkbox saying they trust this connection and remember for future use. If this is not acceptable, please use an alternative FTP client

Firewall Related

- If you are able to connect to Communicator's FTP servers yet attempts to perform directory listings or upload/downloads fail, this is normally due to the firewall not allowing all the TCP data ports. The firewall has to be configured to allow TCP port 21, and TCP ports: 53000 – 54999 (all inclusive).

- There is a known issue with all versions of Microsoft ISA Server. If the client has the "FTP access filter" enabled, they will need to disable this to allow secure FTP sessions. This is located under the configuration > add-ins section of the ISA Server management console, as shown below.

Figure 2 – Microsoft ISA Server Configuration Add-ins
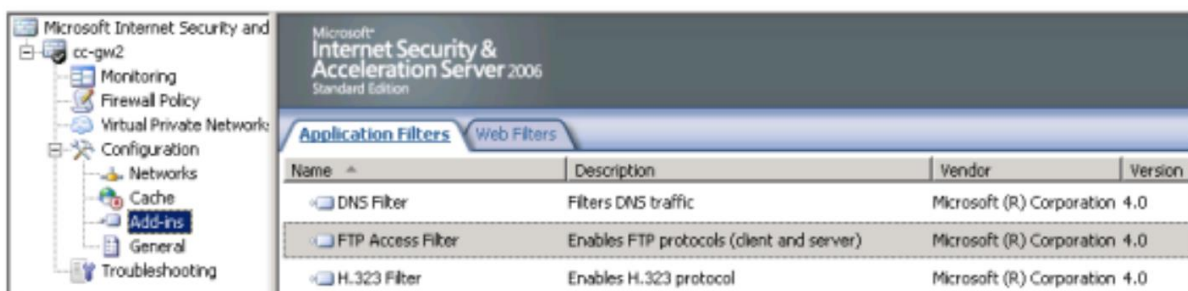
- If you do not want to disable the application filter, you can create a custom Port definition which is configured to an access rule, but is not assigned to the FTP access filter. This will allow both normal FTP traffic and secure FTP traffic. Please note that this change is not supported by Communicator or by Microsoft.

- If the user can't successfully establish a connection to the FTP servers, the user's corporate firewall may be denying the FTP connection; some companies don't allow outbound FTP access by default. If this is the case, see the above section about Connectivity.

- If you are running a Cisco security appliance (such as a PIX firewall) you will be unable to connect to the secure FTP servers as Cisco do not currently

support this.

Cisco recommends one possible workaround in this situation. This is to use an FTP client that supports the use of a "clear command channel" while still using TLS/SSL to encrypt the data channel. With this option enabled, the PIX should be able to determine what port needs to be opened.

Tested FTP Clients for MS Windows & Unix / Linux Platforms

The basic DOS / Linux FTP utilities do not support establishing connections over "FTP over SSL/TLS". You will need to use a 3rd party client or write your own FTP application. Below is a list of some of the FTP clients that have been tested in Windows and Linux platforms and support FTP over SSL.

FileZilla - https://filezilla-project.org/download.php	
Operating System	Microsoft Windows
Host	data.communicatorcorp.com
Protocol/Encryption	FTP – Require explicit FTP over TLS
Transfer Mode	Passive Mode
Port	21

Classic FTP - http://www.nchsoftware.com/classic/	
Operating System	Microsoft Windows
FTP Server	data.communicatorcorp.com
Use Secure FTP (Explicit SSL)	Checked

Alex FTPS - http://ftps.codeplex.com/

Operating System	Microsoft Windows (Command Line), Linux
Command	ftps –h data.communicatorcorp.com –ssl all –l

CuteFTP - https://www.globalscape.com/cuteftp

Operating System	Microsoft Windows
Host Address	data.communicatorcorp.com
Protocol Type	FTP with SSL (AUTH SSL - Explicit)
Port	21

Core FTP LE - http://www.coreftp.com/download.html

Operating System	Microsoft Windows
Host / IP / URL	data.communicatorcorp.com
PASV	Checked
Connection	AUTH TLS

SSLFTP - https://netwinsite.com/surgeftp/	
Operating System	Microsoft Windows / MS-DOS
Host / IP / URL	data.communicatorcorp.com
PASV	PASV: Checked
Connection	Connection: AUTH TLS
SSL Options	SSL Listings - Checked, SSL Transfer - Checked

| SSLFTP - https://netwinsite.com/surgeftp/	
Operating System	UNIX / Linux
Host / IP / URL	data.communicatorcorp.com
PASV	PASV: Checked
Protocol	FTP over TLS/SSL (explicit)
Port	21

Troubleshooting

As FileZilla is commonly used by Communicator clients, we have provided step by step instructions of how to connect to your FTP account using this program.

As above, firstly download FileZilla from http://filezilla-project.org/download.php. Once downloaded, click on File and Site Manager.

In the General tab:

- Enter data.communicatorcorp.com as the Host.
- Leave the Port field empty
- Select the FTP Protocol
- Select Require explicit FTP over TLS Encryption
- Select Normal as the Logon Type
- Enter your username in the User field
- Enter your password in the Password field
- Leave the Comments field blank

Please note, a username and password will have been specifically provided for FTP. This is not the same as your Communicator login details.
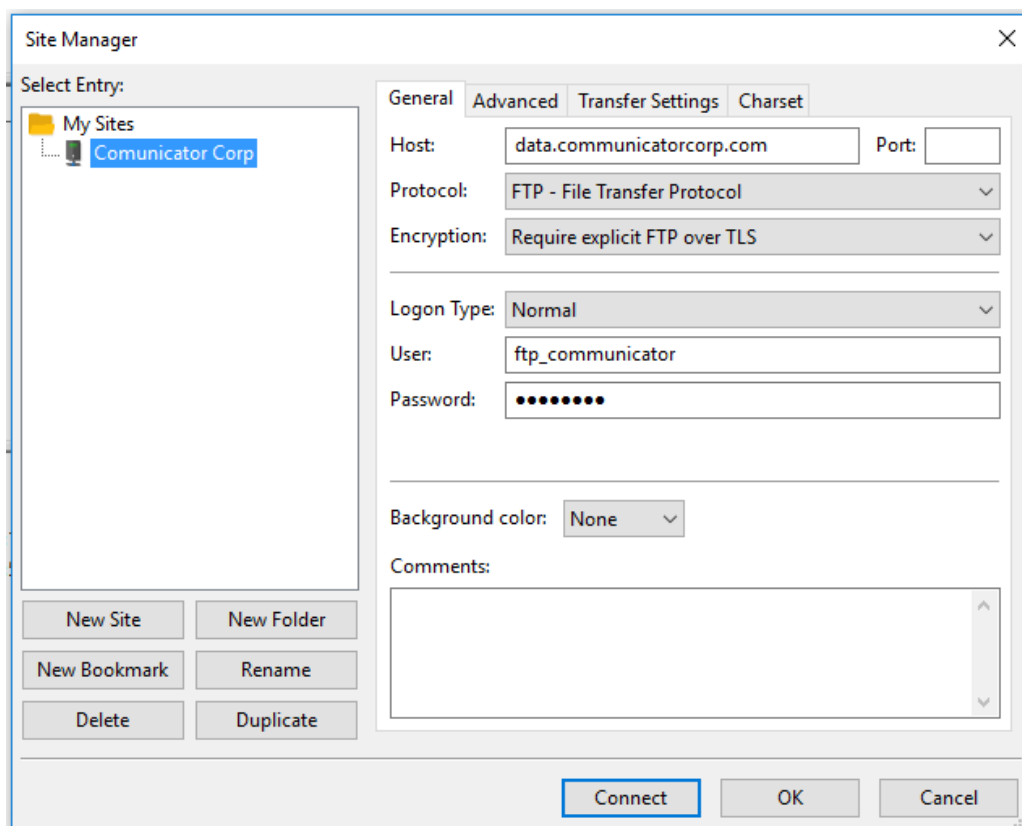
For any queries, please contact Communicator Support on +44 (O)844 87O 8974.