Magrathea Secure Services Access Guide

Encrypted connections to some Magrathea services are now available to all clients using existing login details. There is no need to request secure access as the following services can be used interchangeably with the current non-encrypted version of the same service.

This guide includes details of the various services which can now be accessed over fully encrypted, secure connections and we have included examples of common tools and utilities which may be used to access the services in a secure fashion.

We do not mandate that you use the access mechanisms listed but are unable to provide support for alternative methods of access due to the huge variation of client applications which may be used to make connections.

Table of Contents

Secure NTSAPI access

To make full use of the certificate verification that is possible with the secure connections, please see the *Magrathea Certificate Installation Guide* which provides information on how to install the Magrathea certificate on your systems. We would suggest that to minimise connection issues on Windows that as a minimum you follow the "Installing the Magrathea Root Certificate in Internet Explorer" section. Not all systems require this (you are free to make the connections without validating certificates or to ignore the fact that certificates are not validated) but we would suggest that it is installed to provide maximum security.

When this guide refers to configuration options relating to CA and/or a location of *"/home/certificate/mag-root-ca.crt"* then you should replace this with the appropriate location into which you have installed the certificate, or remove it should you not with to validate the certificates.

Should you have issues connecting using a mechanism not listed in this guide then please see your Systems Administrator for assistance in making the connection and installing the Magrathea Root CA for that application.

The NTSAPI can now be accessed through a TLS/SSL tunnel, offering encryption to the entire process including both the login phase and also all data passed in both directions.

To make a connection, please connect using port 777 to the secure.magrathea-telecom.co.uk server (instead of api.magrathea-telecom.co.uk).

Any SSL client can make this connection and you then login to the NTSAPI as normal, the only operational difference being that the connection is encrypted.

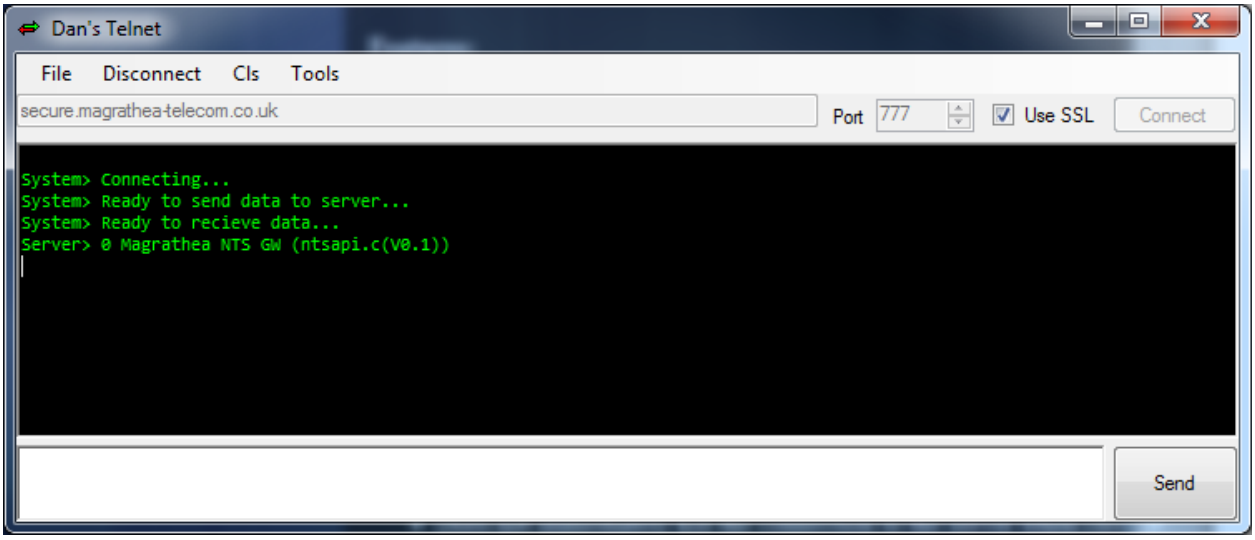
Unfortunately, PuTTY is not able to make connections using SSL so if you are currently using PuTTY then you will need to find an alternative client.

Interactive Access (Windows for those currently using PuTTY)

There are various Telnet over SSL clients available. One free example can be downloaded from http://www.apps.danbalthaser.com/telnet/index.htm

Some telnet clients will download the Magrathea certificate and request authorisation, others (this example is one) will require that you have already installed the Magrathea RootCA – please follow the instructions in the *Magrathea Certificate Installation Guide* on *Installing the Magrathea Root Certificate in Internet Explorer* before attempting a connection using the example Telnet client.

The basic setup is the same for any client: connect to secure.magrathea-telecom.co.uk on port 777 and enable SSL as the connection type:



Interactive Access (Linux or Windows with Cygwin)

As an example, from a Linux machine (or a Windows machine with Cygwin and OpenSSL installed), the OPENSSL client can be used to initiate the connection, instead of telnet:

```
openssl s_client -CAfile /home/certificate/mag-root-ca.crt
            -connect secure.magrathea-telecom.co.uk:777
```

In addition, any application which is capable of making use of an 'openssl' library should connect without any problems, so if you have automated connections into the NTSAPI (for example in PHP) then you should simply be able to change the connection type to use SSL.

System Based access (based on our example PHP)

If you are using our example PHP to connect then simply change the existing connection line as follows (you will need to ensure your PHP was built with the '—with-openssl' option for SSL to be available):

```
//$fp = fsockopen("api.magrathea-telecom.co.uk",777,&$errno,&$errdesc);
$fp = fsockopen("ssl://secure.magrathea-telecom.co.uk",777,&$errno,&$errdesc);
```

If you are using other connection methods, then please consult your developers to determine how you can change your existing connections so that they are encrypted. On most systems an SSL library (often OpenSSL) will need to be installed and configured.

Secure FTP CDR downloads

Daily CDRs can now be downloaded by FTP over a TLS/SSL connection.

Please note that this is an FTP connection which uses SSL to encrypt it and is different to SFTP.

To make a connection, please continue to connect to cdr.magrathea-telecom.co.uk on port 21 but set your FTP client to require a TLS/SSL connection and use your existing username and password.

Not all FTP clients are able to be configured to make these connections (neither the standard FTP on Windows or Linux are capable of encrypted SSL connections) so you may have to change the FTP client you are using.

Interactive FTP Client (Windows or Linux)

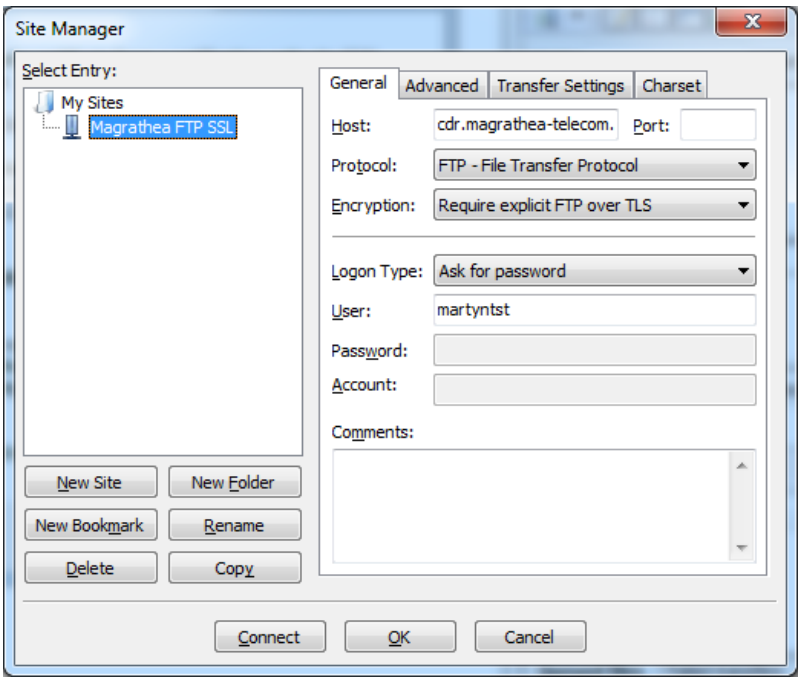
There are various FTP with TLS/SSL clients available and one free example is FileZilla which is supported on both Windows and Linux and can be downloaded from http://filezilla-project.org/ (though you can use any FTP client which supports FTP with TLS/SSL).

The following examples are taken from the Windows version.

To setup a connection to Magrathea for CDR download, open FileZilla then then select *"File->Site Manager"* from the main menu.

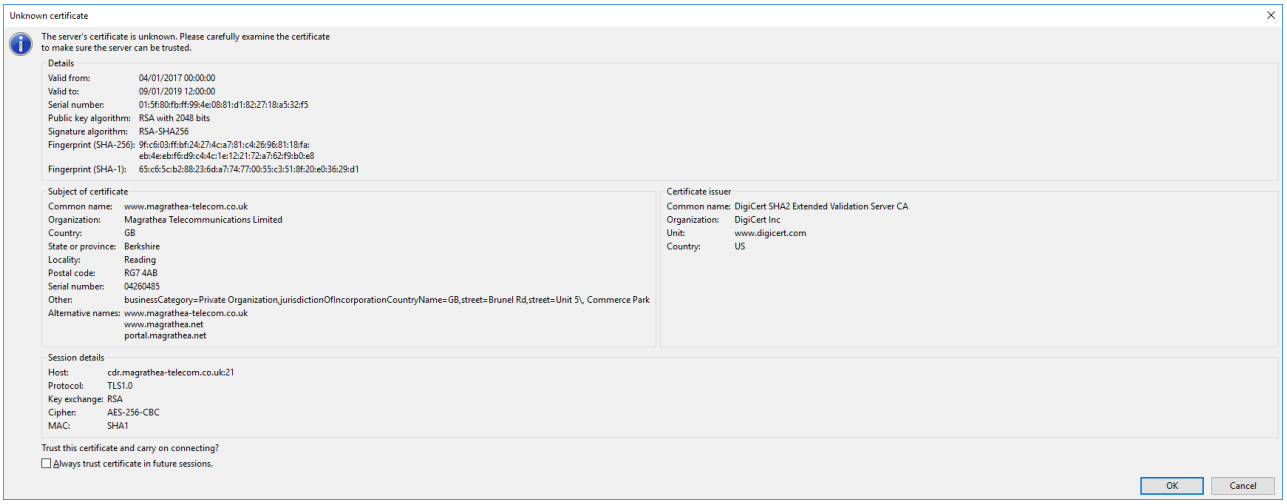
Click *"New Site"* and then *"Rename"* this to something meaningful (for example 'Magrathea FTP SSL')

Then set the Host to be *cdr.magrathea-telecom.co.uk*, change the Encryption setting to "*Require explicit FTP over TLS"* and set the Logon to be *"Ask for password"* and then enter your FTP username



Click 'Connect' and in the dialog that pops up, enter your password and click OK.

You will then be presented with the certificate dialog:



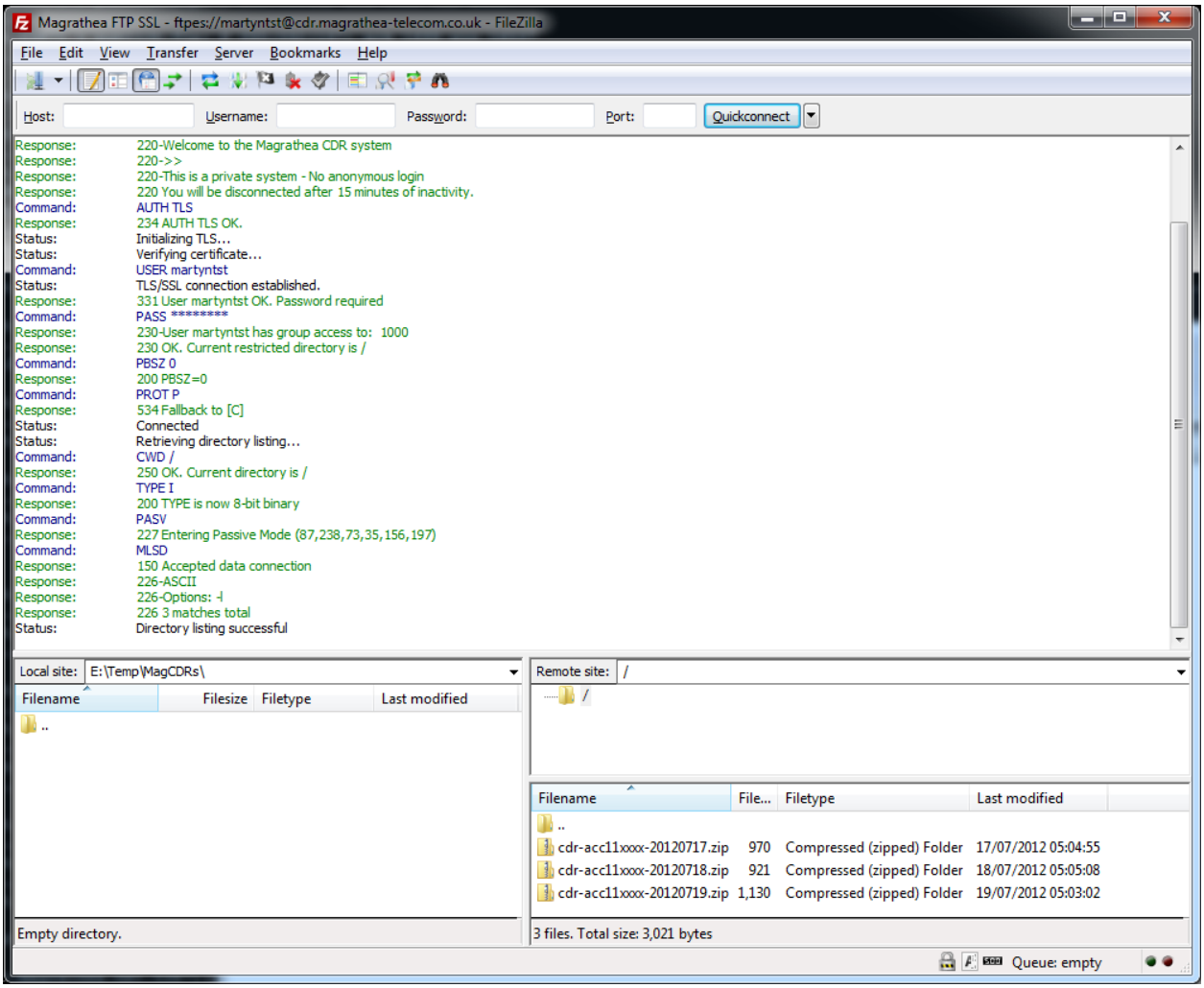
This is the server certificate for the CDR machine and so had a different fingerprint to the Root CA certificate referenced in the *Magrathea Certificate Installation Guide*.

The SHA1 Fingerprint for the Certificate used by cdr.magrathea-telecom.co.uk is

65:c6:5c:b2:88:23:6d:a7:74:77:00:55:c3:51:8f:20:e0:36:29:d1

Once you are satisfied that this is the genuine Magrathea certificate tick the ‘Always trust certificate in future sessions’ box and click OK to complete the connection.

Once connected, you simply drag and drop your CDR files from the Magrathea CDR site to your local PC



Automated or Command-Line access (Linux)

As an example, from a Linux machine, the LFTP client can be used to initiate the connection and force the TLS/SSL mode.

To do this, please either add the following to your lftp.conf file (usually found in /etc/lftp.conf) or enter the lines as commands once you have started lftp:

```
set ftp:ssl-force yes
set ftp:ssl-protect-data yes
set ftp:ssl-protect-list yes
set ssl:check-hostname yes
set ssl:verify-certificate yes
```

To make the connection:

```
lftp -u username,password cdr.magrathea-telecom.co.uk
```

Once connected, you can list the directory and enter commands as you would with any other FTP client.

Secure access to your Account Balance

Connections to retrieve the current balance of your account made via the RestAPI or Client Portal are made securely.

Secure Access to the Porting Portal

Connections to the Porting Portal can be made using a normal web browser to

https://portal.magrathea.net/portal/