

## Magrathea Root Certificate Authority (Root CA) installation

In order to successfully validate that the connections you are making are to Magrathea systems you need to obtain and use or install the Magrathea Root Certificate, from which all our other certificates are signed.

Included in this document are instructions of how to obtain and install this certificate on the most common systems.

If you are using other systems, or you get errors messages during the installations which suggest that the ability to install new certificates is against the policies enforced by your organisation, please check with your own Systems Administrator/IT Department as Magrathea are unable to help with specific installation or configuration issues related to certificate installations.

### Table of Contents

Magrathea Root Certificate Authority (Root CA) installation .....	1
Validating the Certificate .....	2
Installing the Magrathea Certificate in Firefox .....	3
Installing the Magrathea Root Certificate in Internet Explorer .....	4
Obtaining the Magrathea Certificate on Linux machines .....	7

## Validating the Certificate

To ensure that the certificate you download and install is the genuine Magrathea Root CA, please validate the Fingerprint of the certificate using one of the following methods (or whatever method is preferred by your Systems Administrator).

On Linux, you can calculate the Fingerprint using the command:

```
cat mag-root-ca.crt | openssl x509 -sha1 -fingerprint
```

The Magrathea Root CA has a fingerprint of:

```
AB:63:97:0C:C1:B1:9E:CC:AD:41:64:9B:EA:41:B8:30:38:18:80:43
```

During installation using the Windows Certificate Import Wizard, you will be presented with a Dialog box asking you to confirm the installation. Windows refers to the Thumbprint, which is identical to the fingerprint listed above for Linux, however will be presented slightly differently:

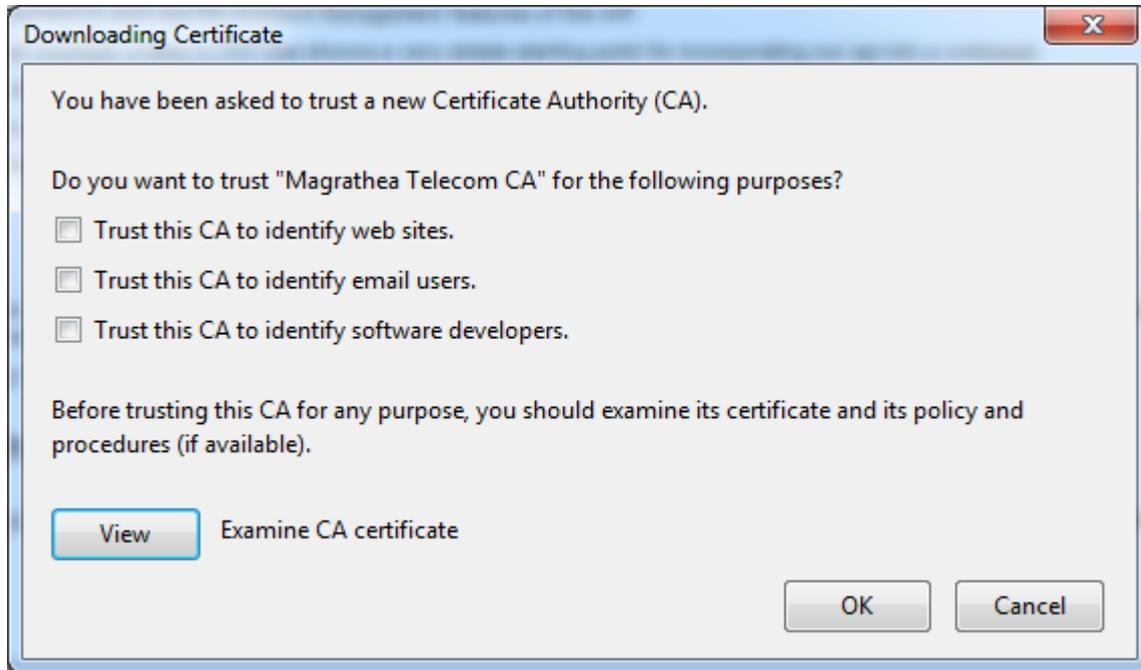
```
AB63970C C1B19ECC AD41649B EA41B830 38188043
```

On other systems, the fingerprint/thumbprint may be represented in a different way, but as you can see from these examples it should ALWAYS contain the same actual values, once presentation differences are accounted for.

## Installing the Magrathea Certificate in Firefox

Go to the Magrathea Client Download page and find the Magrathea Certificate Authority (<http://www.magrathea-telecom.co.uk/assets/Client-Downloads/mag-root-ca.crt>)

Click on the certificate and you will be presented with the following dialog (or similar):

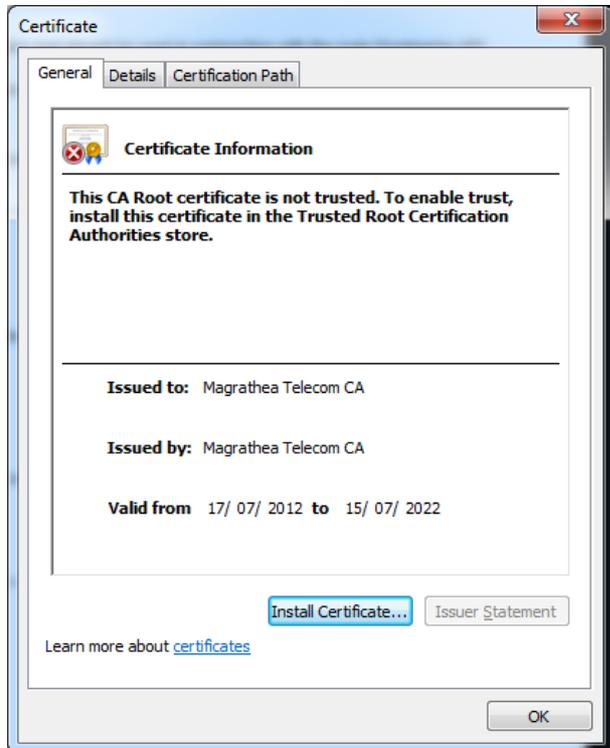


Tick the 'Trust the CA to identify web sites' and click OK to install the certificate

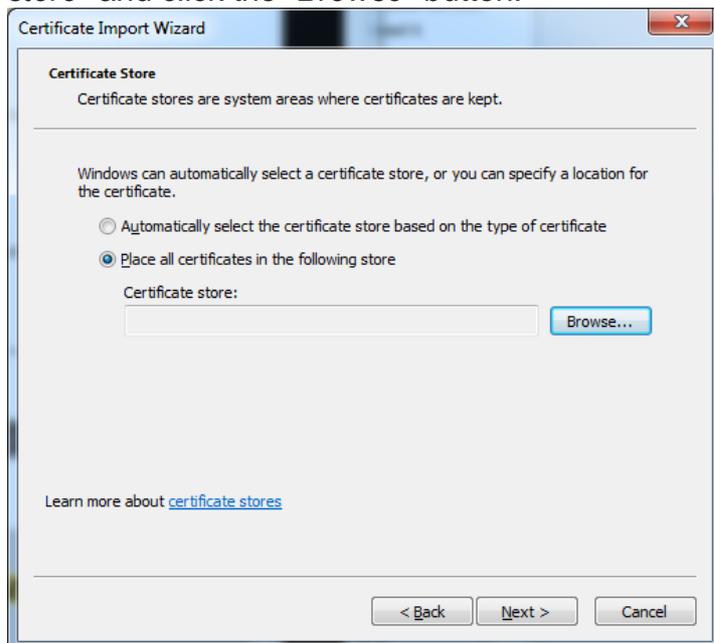
## Installing the Magrathea Root Certificate in Internet Explorer

Go to the Magrathea Client Download page and find the Magrathea Certificate Authority and click on it (<http://www.magrathea-telecom.co.uk/assets/Client-Downloads/mag-root-ca.crt>)

Then select *“Open”* to bring up the Certificate and click *“Install Certificate”* to open the Certificate Import Wizard:



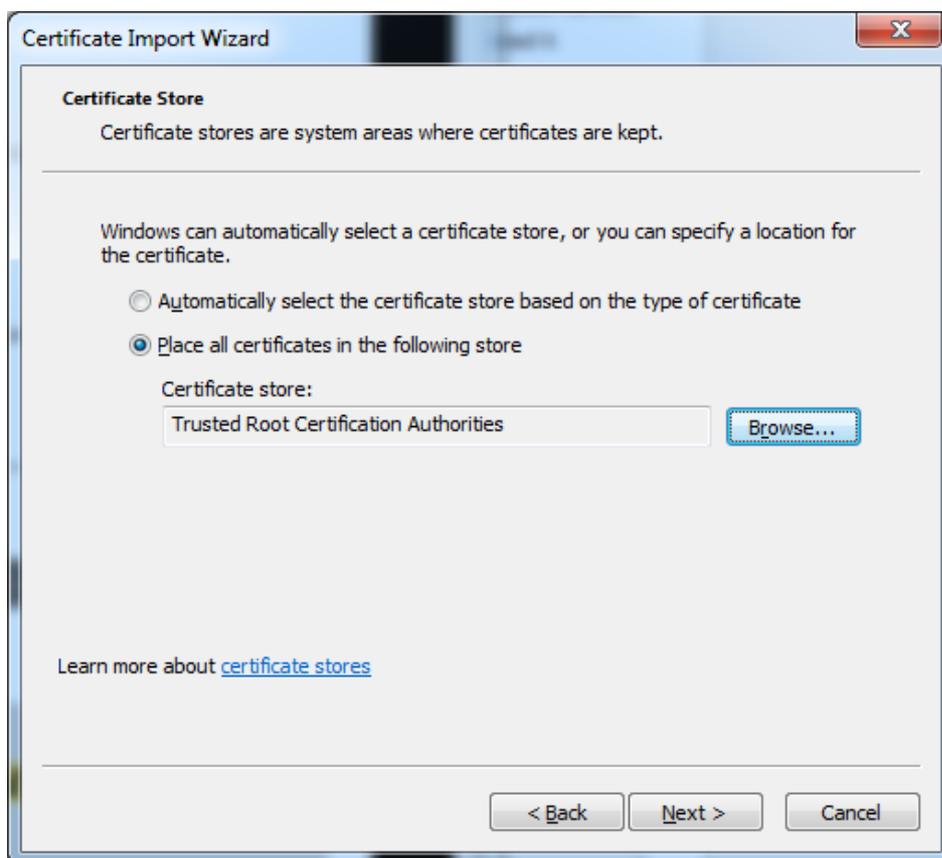
Select *“Next”* on the Welcome page, then select *“Place all certificates in the following store”* and click the *“Browse”* button:



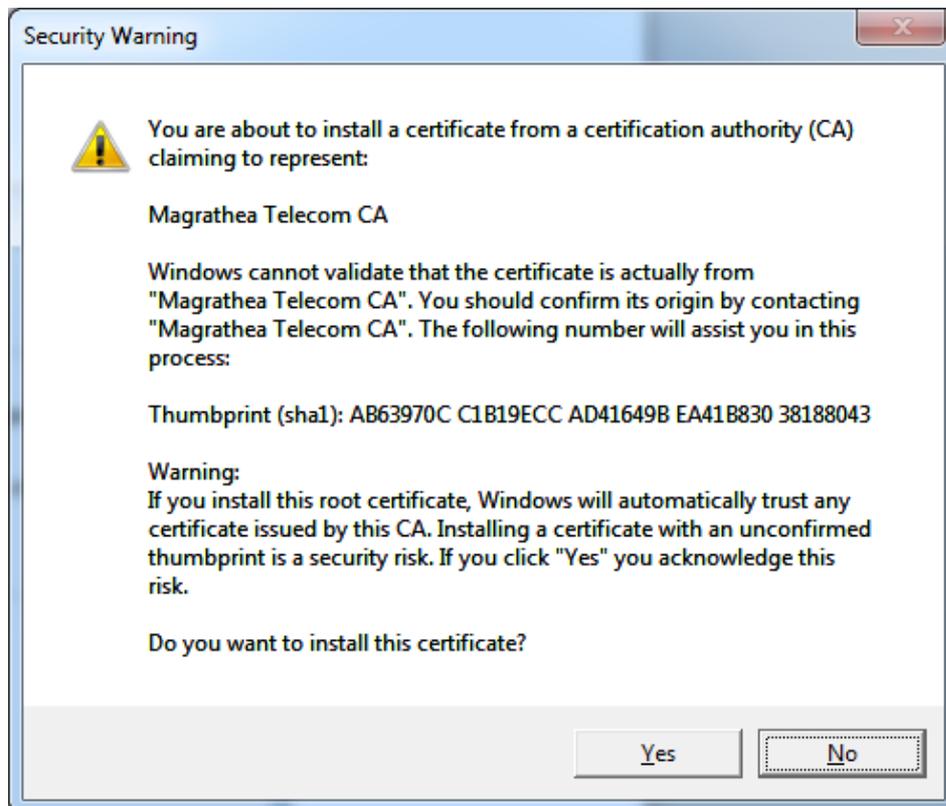
Now Select the *“Trusted Root Certification Authorities”* and click OK:



Now click "Next":



Click "Finish", then click "Yes" when asked if you want to trust the Magrathea Telecom CA:



## Obtaining the Magrathea Certificate on Linux machines

Most Linux utilities are able to be told what CA Root certificates they should be using so it is not usually necessary to install the Magrathea certificate to a specific location on your Linux machine, you can usually download the certificate to a convenient location and then reference it in the configuration files or command-line of any Linux command you use to make a connection to a Magrathea system.

Download the file to a directory you can reference, for example /home/certificate

```
cd /home/certificate
wget http://www.magrathea-telecom.co.uk/assets/Client-Downloads/mag-root-ca.crt
```

Then simply use this when connecting as your CA Root. For example, when using the openssl command you can add this on the command-line:

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

In any LINUX configuration file or command relating to the CA you should replace the above example location with your own location.