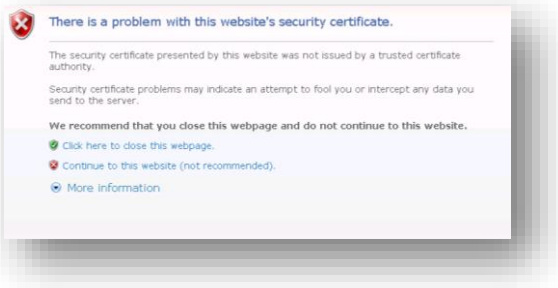
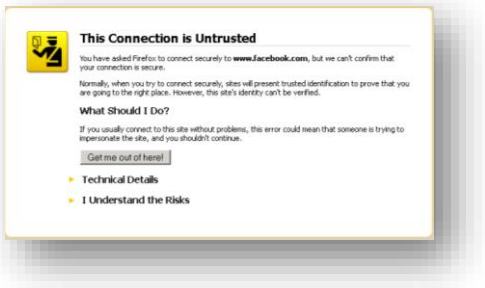
What happens if I don't install the certificate?

- If you don't install the certificate, browsers will warn you that there is a potential issue with a certificate for this web site.





- You have a choice. You can choose to "click-through" the warning, and accept the risk, continuing on to the web site. In most cases this will result in you being presented with either the web site you were expecting or a login page so that you can elevate your filtering privileges using User Based Filtering. The alternative is to not click-through, in which case you will not be able to access the web site.
- This will happen on all machines until the certificate is installed.

What happens if I can't install the certificate on my machine?

- You do not need "administrator" privileges to install the certificate, however, if your machine is being managed by your ICT team/administrator, it might be "locked down" preventing you from performing the installation yourself.
- We recommend you liaise with your ICT team and/or technician(s). Ask them to install the certificate for you following either of the two procedures in the appendices (whichever is most appropriate).

Appendix A Microsoft Active Directory Group Policy Installation Procedure

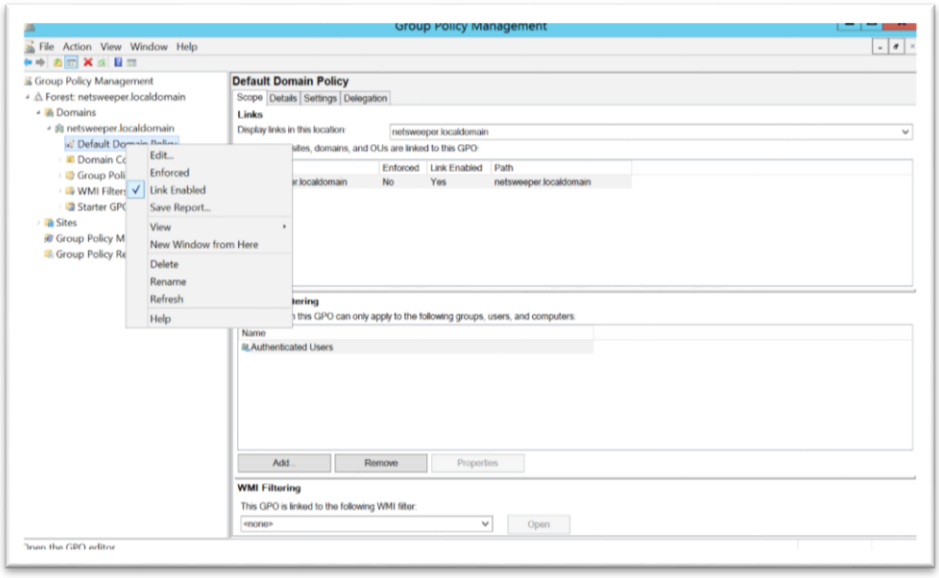
The certificate can be deployed to Windows computers using group policy.

Download the Certificate from http://ukcloud.netsweeper.com:8080/ca.cer

Save the certificate to a convenient location.

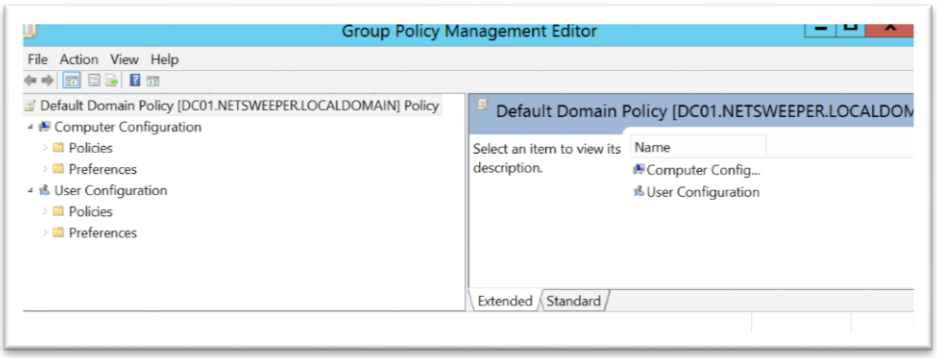
Once you have downloaded the root certificate, please follow the instructions below:

1. Open Group Policy Management Console.
2. Find an existing Group Policy Object (GPO) or create a new GPO to contain the certificate settings.
   i. Ensure that the GPO is associated with the domain, site, or organizational unit whose computers you want affected by the policy.
   ii. If you are utilising an existing policy object, please ensure the object is set to publish computer configuration or both computer and user configurations. (Publishing user configuration alone will not suffice).
3. For the purposes of this document we will use the a Windows Server 2012 R2, and we will edit the Default Domain Policy for the netsweeper.localdomain (your domain will differ)…

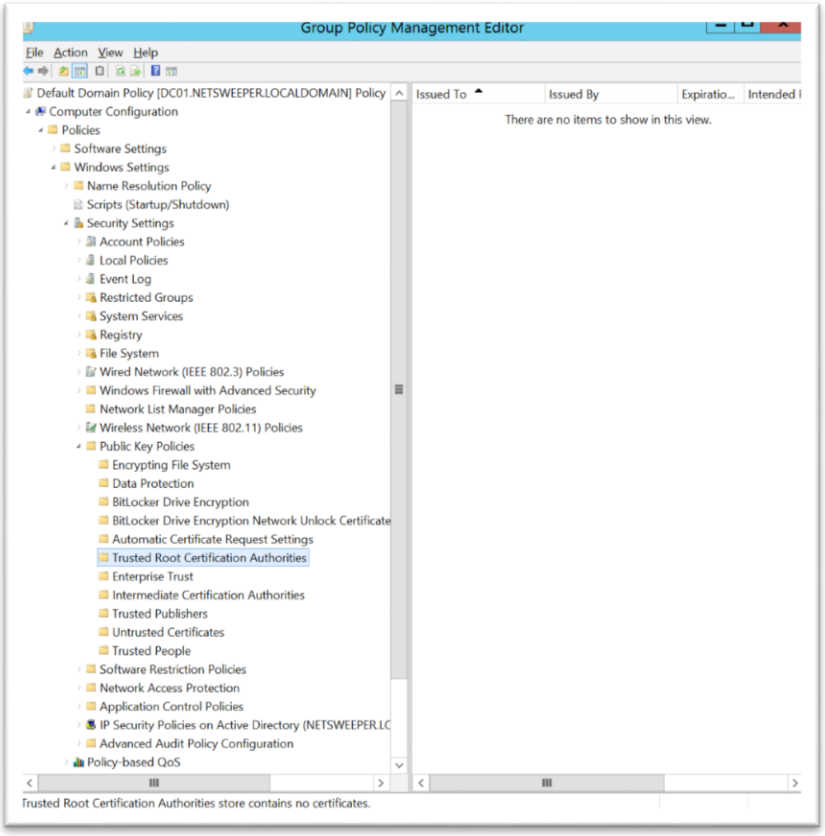


4. Right-click the GPO, and then select **Edit**.

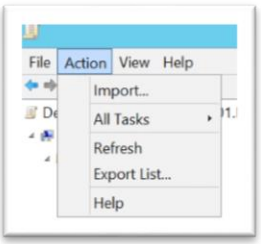
   Group Policy Management Editor opens, and displays the current contents of the policy object.



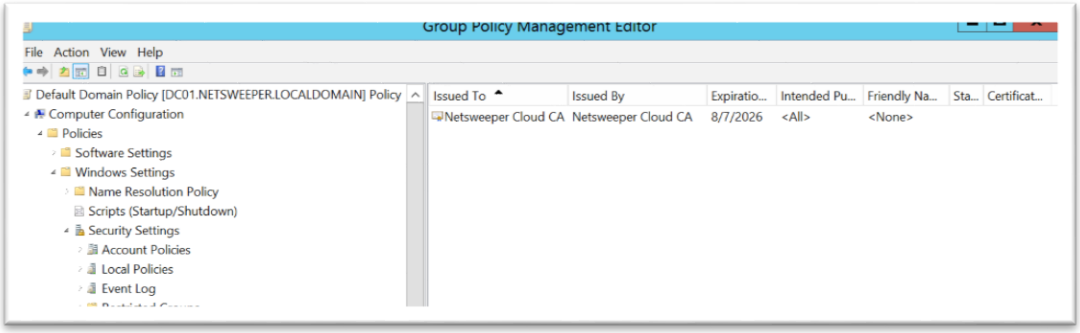
5. In the navigation pane,
    i. For Windows Server 2003, open **Computer Configuration \Windows Settings\Security Settings\Public Key Policies\Trusted Root Certification Authorities**.
    ii. For Windows Server 2008 and Windows Server 2012 R2, open **Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies\Trusted Root Certification Authorities**.



6. Click the **Action** menu, and then click **Import**.



7. Follow the instructions in the **Certificate Import Wizard** to find and import the certificate.

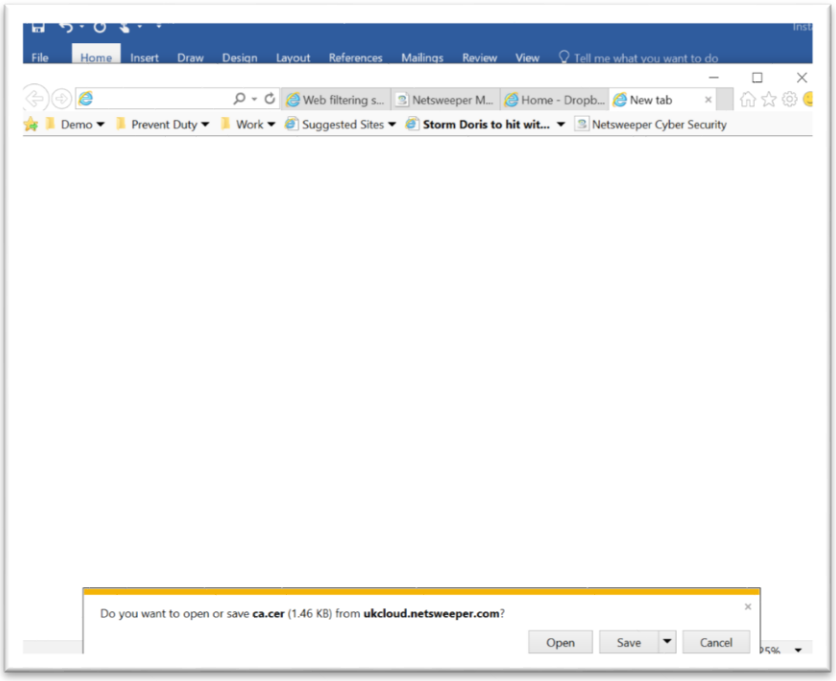


Appendix B Single Machine Installation Procedure

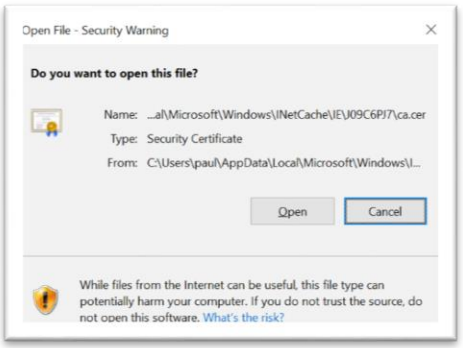
In order to access the full functionality of SSL filtering, an additional Web certificate needs to be installed on your computer.

1. You may be able to do this yourself, however you may find that your computer is set up to prevent you from making the necessary changes in which case you will need the assistance of your ICT administrator to make the changes for you.

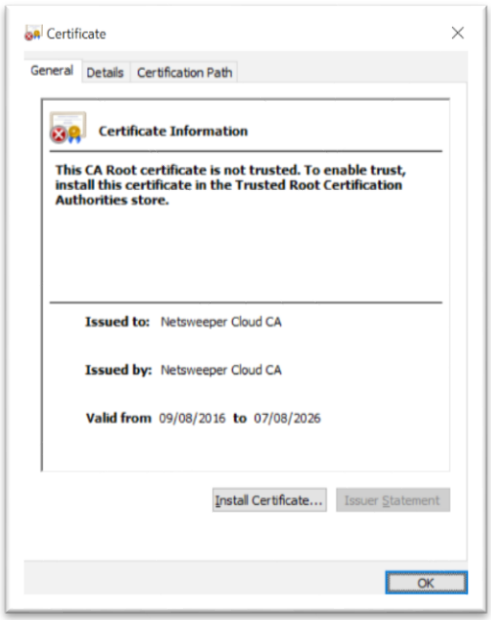
2. If you are using Microsoft Internet Explorer, when you click the following link:
   http://ukcloud.netsweeper.com:8080/ca.cer



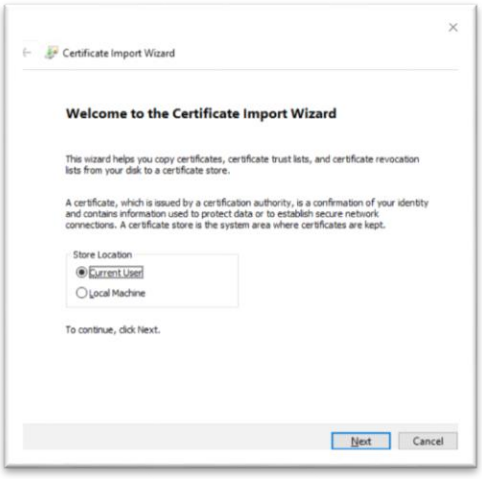
3. Your browser will ask you if you want to 'open or save' the file, click the [Open] button
4. You maybe prompted to open the file



5. A new window will pop up showing the certificate. Click the [Install Certificate...] button



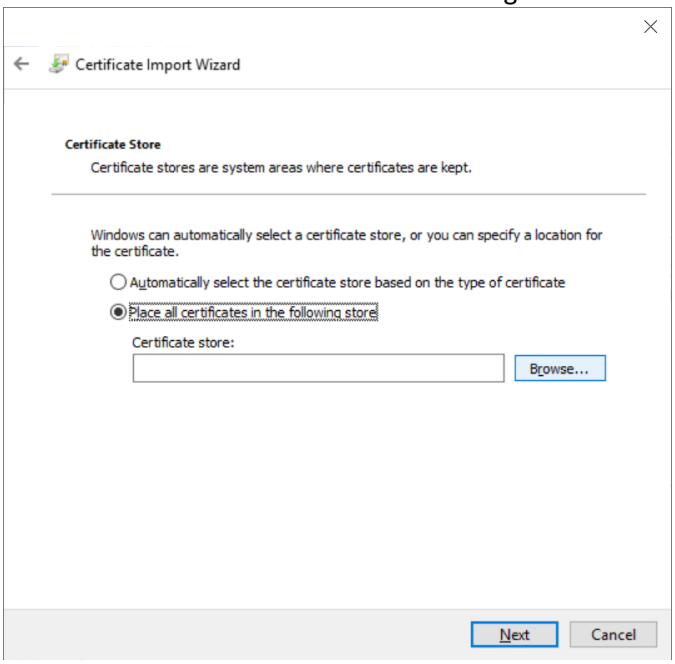
6. The Certificate Import Wizard starts, click [Next]



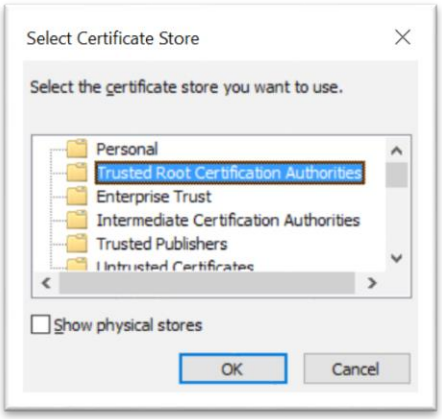
Choose Local Machine

7. You may be prompted to confirm the action by User Account Control

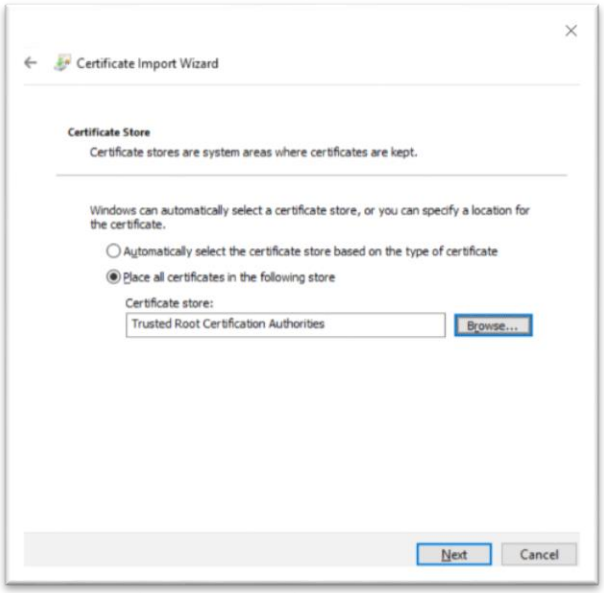
8. Select ‘Place all certificates in the following store’ and click [Browse]



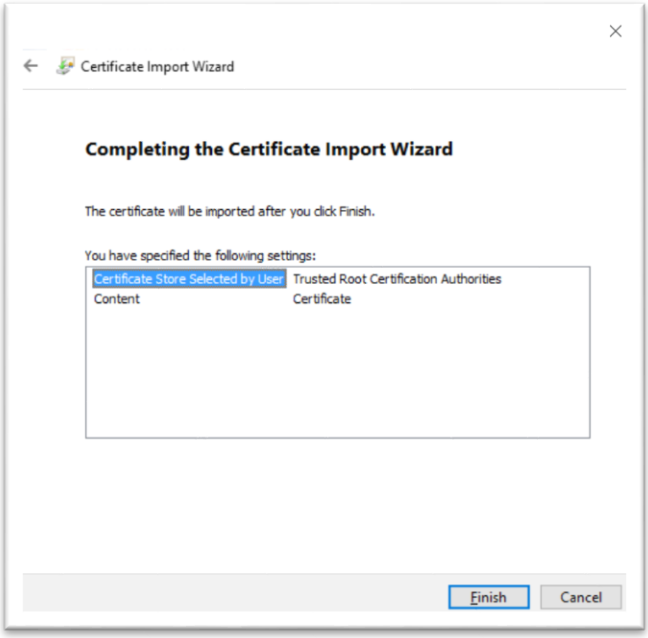
9. Select ‘Trusted Root Certification Authorities’ and click [OK]



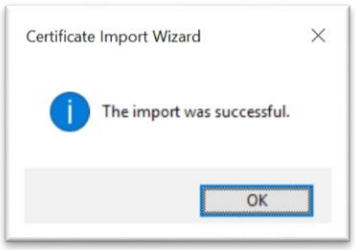
10. Click [OK]



11. Click [Next]



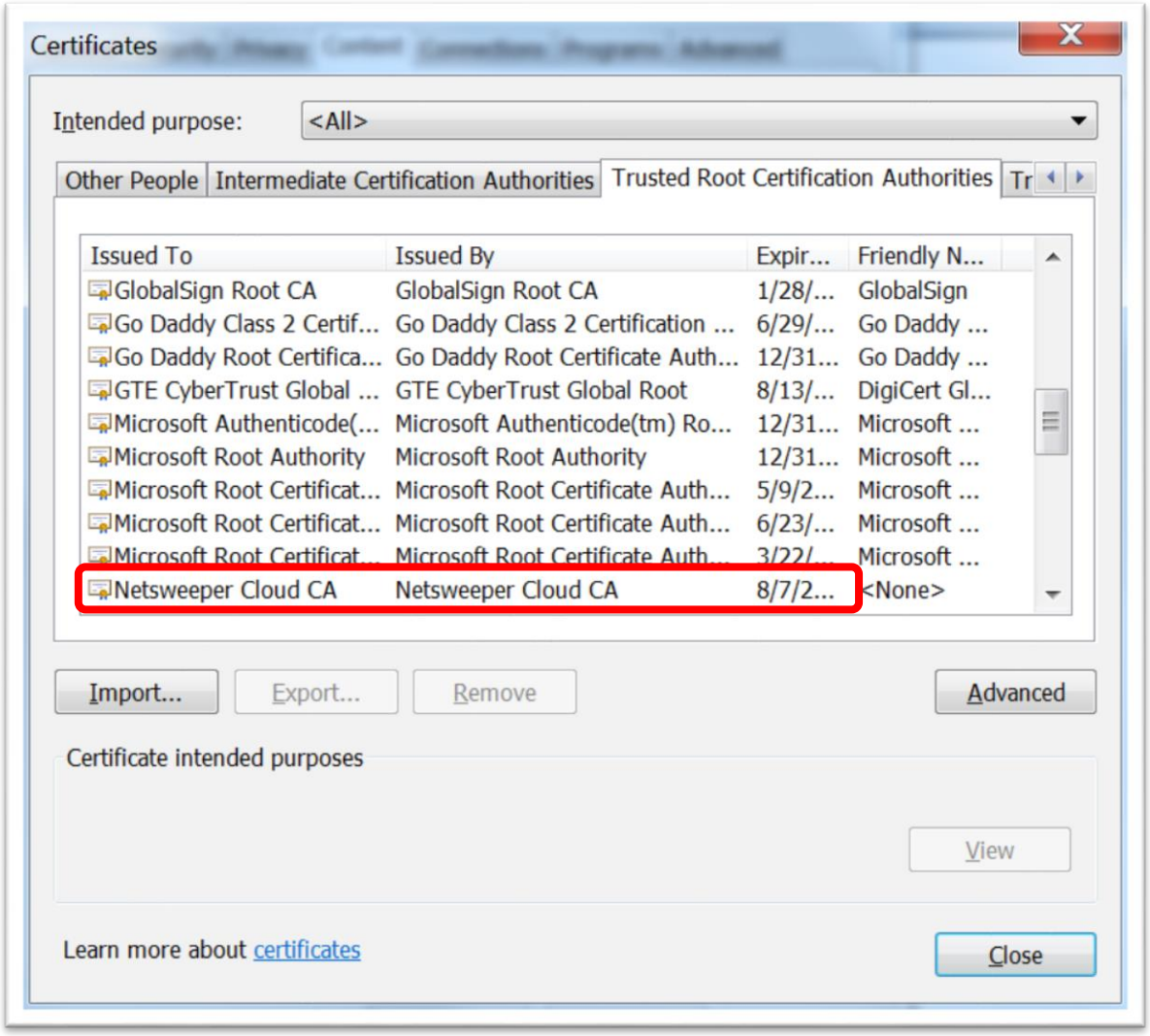
12. Then click [FINISH]



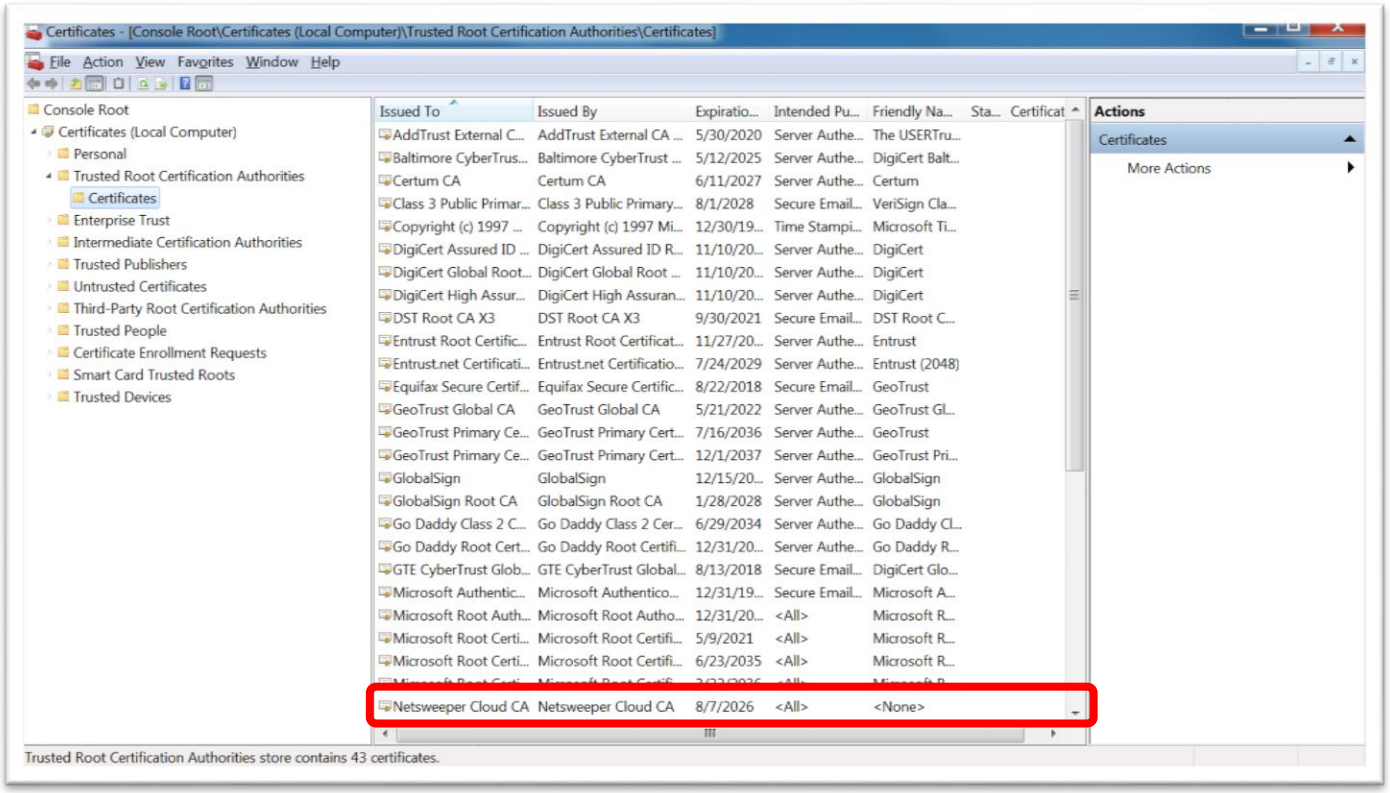
Appendix C Checking that the certificate has been installed on Windows

You can check that the certificate has been installed using two methods:

1. Using Internet Explorer, for example using IE10
   - Use the Tools > Internet options menu
   - Click the Content tab
   - Click the Certificates button
   - Click the Trusted Root Certificates tab
   - Ensure your Common Name (CN) appears in the Issued By column



2. Or use the MMC snap-in control
   - Start > Run > mmc
   - File > Add/remove snap-in
   - Click Certificates, click Add
   - Select Computer Account
   - Ensure Local Computer is selected
   - Click Finish
   - Click OK
   - Double-click Certificates (Local Computer)
   - Double-click Trusted Root Certification Authorities
   - Check for your certificate



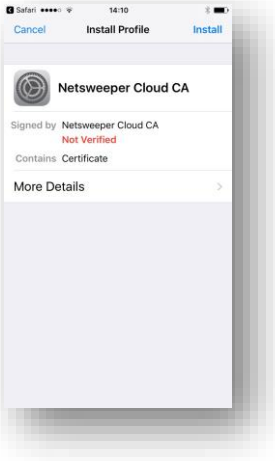
Appendix D – Apple devices

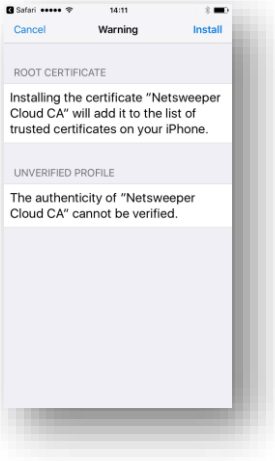
Appendix E1 – Single user installation

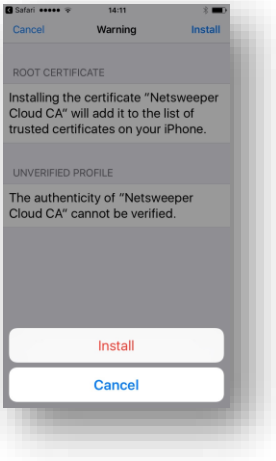
Most Apple devices have a simple method of “trusting” a certificate.

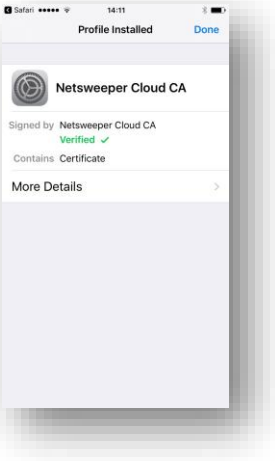
On IOS Devices

Using your web browser, navigate to http://ukcloud.netsweeper.com:8080/ca.cer then click on the Download link for the certificate.







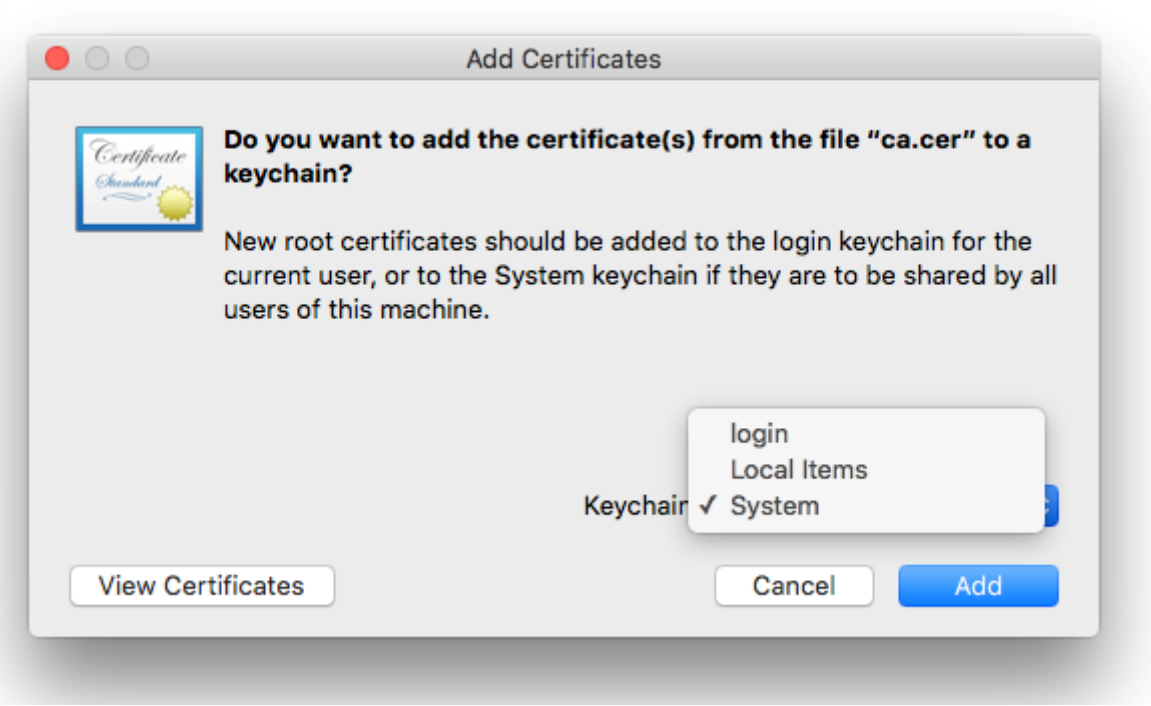


Click [Install], [Install], [Done]

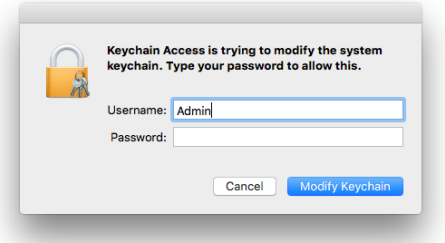
On MacOSX Desktops and Laptops

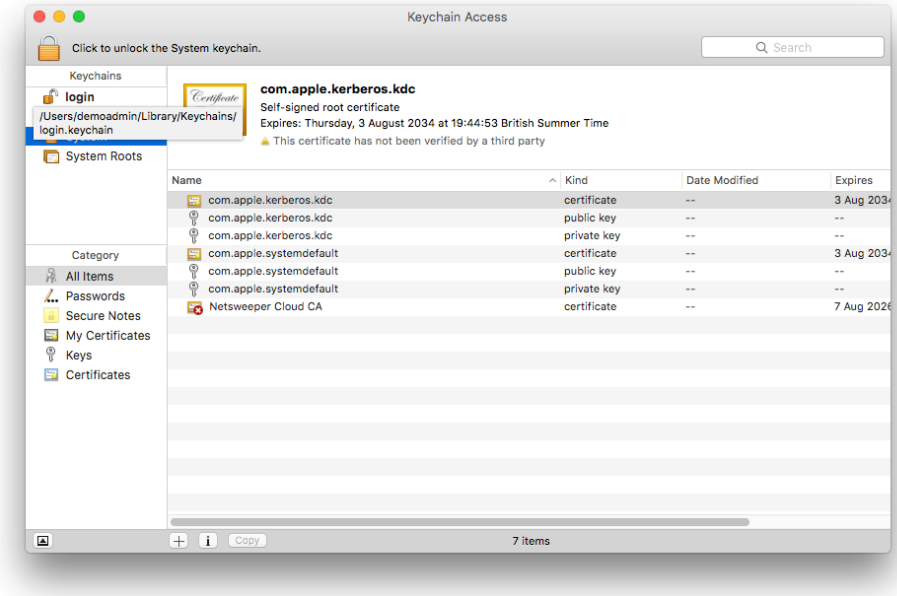
Using your web browser, navigate to http://ukcloud.netsweeper.com:8080/ca.cer

Double-click the downloaded file to install into the Keychain. Change the Keychain to System (for all users), click Add

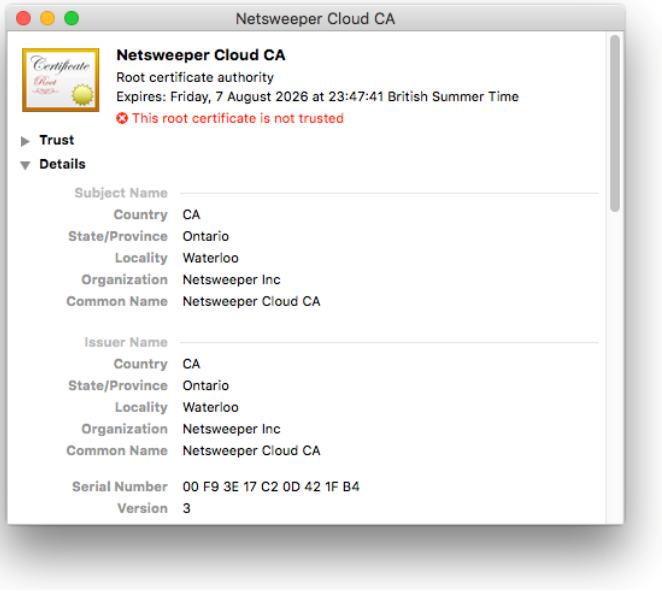


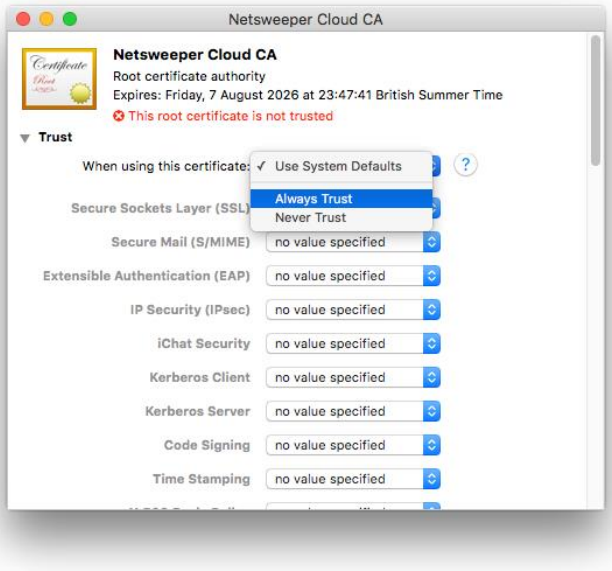
You may be asked to authenticate to unlock the key chain, use a login and password of a machine administrator.



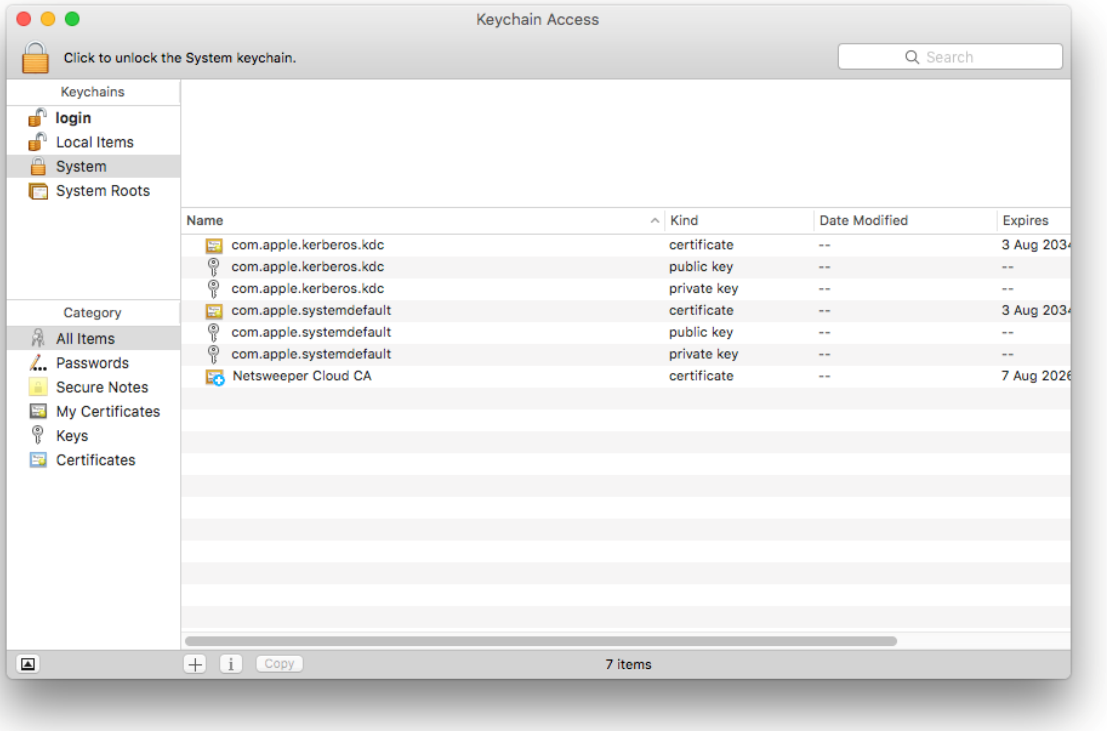


Select the System Keychain, double-click your certificate





Click [Always Trust]. You may be asked to authenticate to unlock the key chain, use a login and password of a machine administrator.



Notice the blue “plus” badge on the Netsweeper certificate.

Appendix E2 - To deploy a Macintosh desktop/laptop and IOS device profile

If you have Apple devices, you might want to consider a bulk deployment.

To perform a bulk deployment "the Apple way" you can download the "Apple Configurator 2" application from the Mac App Store https://itunes.apple.com/gb/app/apple-configurator-2/id1037126344?mt=12, or utilise a Macintosh running the Server extensions (the Profile Manager)

It is beyond the scope of this document to detail the exact deployment methods.

In general:

- Download the certificate
- Create a mobileconfig file (also known as Profiles)
- Use a Mobile Device Management tool (Apple's Server can act as an MDM) to push the configuration to your devices. (There are third party MDM tools available).
- OR
- Publish the mobileconfig file(s) on a web server, download the mobileconfig file from the web server and install on the local device.

Appendix E Android-based devices

Android-based devices are a bit trickier. There is no commonality for an installation method until devices running versions of Android 4 or higher.

NOTE: You must enable a PIN or a pattern lock for your device otherwise you may not be able to install the certificate.

If your device runs Android version 4 or higher

The process is very similar to the process for IOS devices...

1. Using your web browser, navigate to http://ukcloud.netsweeper.com:8080/ca.cer then click on the Download link for the certificate.
2. The built-in certificate installation wizard should start.
3. You will be asked to give the certificate a name
4. There should be no need for a passphrase, click through the remaining prompts.

If your device runs Android version 3 or lower

Some earlier versions of Android-based distributions include an application, sometimes called Certificate Manager, sometimes called Credential Manager. Using this method will require you to copy the certificate to the file system of your device (either the device memory or an SD card).

Access to the Certificate/Credential Manager is usually found at:

Settings > Personal > Security > Credential storage

You should consult the manual that came with your device to find out how to install a certificate, or contact the manufacturer.