

Installing the RM SafetyNet Certificate – Managed Windows

Contents

Introduction.....	1
About the RM SafetyNet SSL Certificate.....	2
System requirements.....	2
Identifying your filtering mode.....	3
Transparent proxy scenario.....	3
Non-transparent proxy scenario.....	3
Before you start.....	6
Server downtime.....	6
Deploying the certificate.....	7
Create a Windows Group Policy Object.....	7
Deploying the certificate to servers.....	7
Deploying the certificate to computers by GPO.....	8
Installing the certificate manually.....	9
Deploying proxy server settings.....	9
CC4 networks.....	9
Ranger networks.....	10
Other Windows Server networks.....	10
Group Policy Preferences (Registry Settings) and Scripts.....	11
Group Policy Preferences (Internet Settings import).....	12
Internet Explorer Maintenance (IEM).....	12
Manual proxy settings on computers.....	13
Checking that SSL interception is active.....	14
Appendix I: Creating the GPO manually.....	16
Appendix II: SHA256 Hotfix for Windows Server 2003 networks.....	19

Introduction

This guide describes how to deploy the RM SafetyNet certificate to managed Windows clients in a CC4 or other Windows network, and how to reconfigure the proxy server settings (if required).

If your RM SafetyNet devices include unmanaged Windows computers and other operating systems, make sure you download the files and documentation you need from <http://www.rm.com/googlessl>

About the RM SafetyNet SSL Certificate

Google searches now utilise encryption technologies for added security. In order to perform filtering on all Google searches the RM SafetyNet filtering service needs to decrypt, analyse, and then re-encrypt all traffic using the RM SafetyNet security certificate. We have recently updated our security certificate to use a stronger SHA-384 hash algorithm.

To prevent browsers showing a warning that the connection is insecure, this certificate must be deployed as a Trusted Root Certificate to all computers and devices that browse via a RM SafetyNet internet connection.

System requirements

- Your network servers need to be running one of the following operating systems:
 - Windows Server 2003 Service Pack 2
 - Windows Server 2008 R2
 - Windows Server 2012 R2
 - Windows Server 2016
- Your client Windows devices need to be running one of the following operating systems:
 - Windows XP Service Pack 3
 - Windows 7
 - Windows 8/8.1
 - Windows 10
- You need a Domain Administrator account for the local network.
- You need to be using one of the following browsers:
 - Internet Explorer
 - Google Chrome
 - Microsoft Edge (Windows 10)
- If you are running Windows Server 2003, then you need to install Microsoft hotfix 938397 (Applications that use the Cryptography API cannot validate an X.509 certificate in Windows Server 2003). For instructions see **Appendix II: SHA256 Hotfix for Windows Server 2003 networks**.

Identifying your filtering mode

The RM SafetyNet certificate is used in both transparent and non-transparent filtering scenarios.

Mixed scenarios – where some devices use a transparent proxy, and some use a non-transparent proxy – are fully supported, and you can continue to configure your devices in this way if required.

Please read the following sections to determine the mode of use for your devices. If you are not sure what modes you are using in your environment, please contact RM Support.

Transparent proxy scenario

If computers on your network do not need to have a proxy server specified in Internet Explorer or other browsers in order to access the internet, then you are using the RM SafetyNet filtering system in transparent mode.

On networks where transparent mode is in use, RM's Internet Hosting Group (IHG) needs to switch the entire network over to the Google SSL filtering proxy servers.

The RM SafetyNet certificate needs to be deployed to all client devices **before** RM IHG makes this change – otherwise your end users will receive certificate errors when using Google search sites.

You do not need to add or change any proxy settings if your network is currently operating in transparent proxy mode.

Non-transparent proxy scenario

If computers on your network need to have a proxy server specified in Internet Explorer or other browsers to access the internet, then you are using the RM SafetyNet filtering system in non-transparent mode.

On networks where non-transparent mode is in use, the proxy server setting must be changed to reflect the new RM SafetyNet Google SSL filtering proxy servers.

The RM SafetyNet certificate needs to be deployed to all client devices **before** the proxy server settings are changed.

Use the following table to determine the new RM SafetyNet proxy address and port number for your network. You will need this information to complete the process.

Installing the RM SafetyNet Certificate – Managed Windows

Current proxy address	New proxy address	Port number
cache.rmplc.co.uk	sslfilter.proxy.rmplc.co.uk	8080
proxy.rmplc.co.uk	sslfilter.proxy.rmplc.co.uk	8080
userproxy.rmplc.co.uk	sslfilter.userproxy.rmplc.co.uk	
proxy.swgfl.org.uk	sslfilter.proxy.swgfl.org.uk	8080
cache.swgfl.org.uk	sslfilter.proxy.swgfl.org.uk	8080
userproxy.swgfl.org.uk	sslfilter.userproxy.swgfl.org.uk	
proxy.swgfl.ifl.net	sslfilter.proxy.swgfl.org.uk	8080
cache.swgfl.ifl.net	sslfilter.proxy.swgfl.org.uk	8080
proxy.segfl.ifl.net	sslfilter.proxy.segfl.ifl.net	8080
cache.segfl.ifl.net	sslfilter.proxy.segfl.ifl.net	8080
proxy.sln3.net	sslfilter.proxy.sln3.net	8080
proxy.sgfl.org.uk	sslfilter.proxy.sgfl.org.uk	8080
proxy.webfiltering.ja.net	sslfilter.proxy.webfiltering.ja.net	8080
proxy.wigan.ifl.net	sslfilter.proxy.wiganschoolsonline.net	8080
proxy.wiganschoolsonline.net	sslfilter.proxy.wiganschoolsonline.net	8080
proxy.empsn.ifl.net	sslfilter.proxy.empsn.ifl.net	8080
cache.<school domain name>	One of the above depending on schools geographical location	8080
Proxy.<school domain name>	One of the above depending on schools geographical location	8080
Staff proxies		
staff.proxy.empsn.ifl.net	sslfilter.staff.proxy.empsn.ifl.net	8080
staff.proxy.rmplc.co.uk	sslfilter.staffproxy.rmplc.co.uk	8080
staffproxy.internal.slc.ifl.net	sslfilter.staffproxy.internal.slc.ifl.net	8080
staffproxy.rmplc.co.uk	sslfilter.staffproxy.rmplc.co.uk	8080
staffproxy.salford.bsf.ifl.net	sslfilter.staffproxy.salford.bsf.ifl.net	8080
staffproxy.segfl.ifl.net	sslfilter.staffproxy.segfl.ifl.net	8080
staffproxy.slc.ifl.net	sslfilter.staffproxy.slc.ifl.net	8080

Installing the RM SafetyNet Certificate – Managed Windows

Current proxy address	New proxy address	Port number
staffproxy.sln3.net	sslfilter.staffproxy.sln3.net	8080
staffproxy.stoke.bsf.ifl.net	sslfilter.staffproxy.stoke.bsf.ifl.net	8080
staffproxy.surrey.segfl.ifl.net	sslfilter.staffproxy.surrey.segfl.ifl.net	8080
staffproxy.swgfl.org.uk	sslfilter.staffproxy.swgfl.org.uk	8080
User Based Filtering proxies		
userproxy.empsn.ifl.net	sslfilter.userproxy.empsn.ifl.net	8080
userproxy.webfiltering.ja.net	sslfilter.userproxy.webfiltering.ja.net	8080
userproxy.luton.ifl.net	sslfilter.userproxy.luton.ifl.net	8080
userproxy.rmplc.co.uk	sslfilter.userproxy.rmplc.co.uk	8080
userproxy.salford.ifl.net	sslfilter.userproxy.salford.ifl.net	8080
userproxy.segfl.ifl.net	sslfilter.userproxy.segfl.ifl.net	8080
userproxy.sgfl.ifl.net	sslfilter.userproxy.sgfl.ifl.net	8080
userproxy.slc.ifl.net	sslfilter.userproxy.slc.ifl.net	8080
userproxy.sln3.net	sslfilter.userproxy.sln3.net	8080
userproxy.swgfl.org.uk	sslfilter.userproxy.swgfl.org.uk	8080

Use the examples below to help with finding your new proxy values:

- Example 1:

You are currently using *proxy.swgfl.org.uk* for students and *staffproxy.swgfl.org.uk* for staff.

Your new values will be *sslfilter.proxy.swgfl.org.uk* for students and *sslfilter.staffproxy.swgfl.org.uk* for staff.

The port for both new addresses will be 8080.

- Example 2:

You are currently using *proxy.wigan.ifl.net* and there is no staff version of the proxy.

Your new value for all proxy changes will be *sslfilter.proxy.wiganschoolsonline.net*.

The port number will be 8080.

- Example 3:

For user-based filtering you are currently using *userproxy.luton.ifl.net* for all users.

Your new value for all proxy changes will be *sslfilter.userproxy.luton.ifl.net*.

The port number will be 8080.

If you are not sure which proxy server to use on your network, please contact RM support for guidance and **do not proceed** with the installation.

Before you start

For best practice we recommend you complete these tasks before you start the installation:

- Make a full backup of all servers on the network. Verify the backups by restoring some files from the backup to a test folder on your server.
- Ensure you have access to a sample test client of each operating system variant on the network for testing purposes.
- Ensure all servers and stations are up to date in terms of software deployment and Windows Updates, and that no restarts are pending, as this could affect the certificate deployment.
- If non-transparent proxy mode is used on your network, make sure you have your new RM SafetyNet proxy server details handy (see previous section). If you are not sure about your new proxy server settings, contact RM Support.

Server downtime

In most cases no server downtime is expected during the certificate deployment or proxy server setting process. An exception to this is for Windows Server 2003 servers, which will require a restart if you have not yet installed the SHA256 Hotfix (see **Appendix II: SHA256 Hotfix for Windows Server 2003 networks**).

All network computers should be restarted to deploy the RM SafetyNet certificate. For various reasons some computers may require multiple restarts to apply the GPO.

If you follow the process correctly, internet access for users will be unaffected.

Deploying the certificate

On Windows Active Directory networks you can deploy the RM SafetyNet SSL certificate centrally, by creating and deploying a Group Policy Object (GPO).

Note Where GPO deployment is not possible, for example on non-domain-joined computers, you can install the certificate manually on each Windows computer. Illustrated instructions are provided in a separate guide, *Installing the RM SafetyNet Certificate on your Windows computer*, which you can download from <http://www.rm.com/googlessl>.

Create a Windows Group Policy Object

We provide a script to automate the creation of a new Group Policy Object which will be used to deploy the certificate. You only need to create the GPO once on your network.

1. Log on to a domain controller as an **administrator**.
(On a CC4 network, log on to the CC4 First server.)
1. Browse to <http://www.rm.com/googlessl>
Under **Managed Windows**, click the **GPO script & certificate** link.
(Here you can also download a PDF copy of these instructions.)
2. Save the **RM SafetyNet SSL Certificate (SHA-384) Deployment** zip file in a temporary location on the server and extract the contents.
3. Browse to the location of the files and double-click
RM SafetyNet SSL Certificate (SHA-384) Deployment.vbs
4. Click OK, OK.
5. If prompted with an **Open file Security Warning** dialog box, click **Run**.
6. **Wait** until you see the message “The GPO has been successfully created”. Click **OK**.

If the procedure is not successful and you see an error message, you can create the GPO manually (see **Appendix I: Creating the GPO manually**).

Deploying the certificate to servers

To deploy the certificate to all your network servers, do the following at each server:

1. Log on to the server as an administrator.
2. Ensure all internet browsers are closed.
3. To launch the command prompt, click **Start** and **Run**, type **cmd** and press **Return**.
4. In the window type **gpupdate /force** and press **Return**.
5. To check that the certificate has been deployed, open a browser and go to <http://certificatecheck.rm.com>.



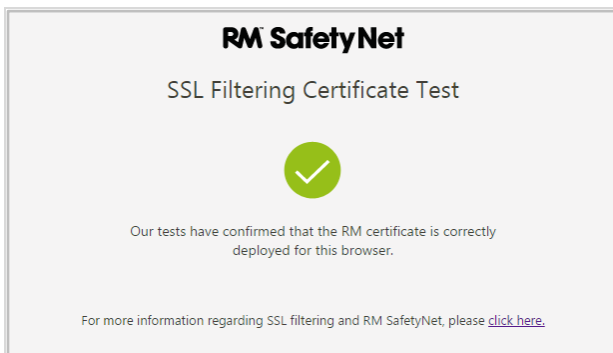
If your browser passes the test, this server has the certificate correctly installed.

If it fails the check, you may get some useful diagnostic information by running `gpupdate /force` (see above). If you need further help, contact RM Support.

Deploying the certificate to computers by GPO

To deploy the certificate by GPO to all your managed Windows network computers, do the following at each computer:

1. To deploy the GPO, restart the computer.
2. To check that the certificate has deployed, open an internet browser and go to <http://certificatecheck.rm.com>.



If your browser passes the test, this computer has the certificate correctly installed.

Installing the RM SafetyNet Certificate – Managed Windows

If it fails the check, you may get some useful diagnostic information by running `gpupdate /force` (see above). If you need further help, contact RM Support.

If necessary you can install the certificate manually on each Windows computer (see below).

Installing the certificate manually

The RM SafetyNet certificate can be installed manually on non-domain-joined Windows devices if required. Fully illustrated instructions are given in a separate guide, *Installing the RM SafetyNet Certificate - Windows stand-alone*, which you can download from <http://www.rm.com/googlessl>.

Deploying proxy server settings

- If your network is currently using a **transparent proxy**, contact **RM Support** to request that RM's Internet Hosting Group (IHG) switch over your entire network to the Google SSL filtering proxy servers. Do not follow the instructions in the rest of this section.
- If your network is currently using a **non-transparent proxy**, follow the instructions below.

Separate instructions are provided for CC4 networks, Ranger networks and other Windows Server networks: choose the one that applies to your network.

CC4 networks

1. Log on to the **CC4 First Server** as an administrator.
2. Open the RM Management Console (RMMC) and log in as **systemadmin** or equivalent.
3. In the left-hand pane, expand **Registry Policies**, **User Policies**, and select **Guest**.
4. In the Categories list, select **Proxy Server**.
 - If the **Connect to the Internet via a proxy server** box is ticked, click the plus + icon to the left of the box. Replace the current **proxy address** and **port** with the new RM SafetyNet proxy details. Click **Save**.
 - If the **Connect to the Internet via a proxy server** box is not ticked, go to the next step.
5. Repeat steps 3–4 for your other user policies as required (e.g., RM Explorer, Staff, Standard, and any custom user policies). Don't forget to **Save** each amendment you make.

Note If you are using a separate proxy for Staff, take care to reflect the new value for the Staff proxy, otherwise your users will experience unexpected filtering behaviour. If you need further guidance on this, please contact RM Support.

6. Repeat steps 3–5 for all user policies in the Global folder. Don't forget to **Save** each amendment you make.

Ranger networks

1. Log on to the **Ranger Administration server** as an administrator.
2. Open the **Ranger Administrator** console.
3. In the left-hand pane, expand **Security, Groups**, and select **RangerManagers**.
4. In the right-hand pane, select the **Internet** tab.
 - If any proxy settings are displayed, replace the current **Proxy server address** and **Proxy server port** with the new RM SafetyNet proxy details. Click **Apply**.
 - If there are no current proxy settings, **do not enter** any details. Go to the next step.
5. Repeat steps 3 to 4 for the following groups:
 - RangerStaffUsers
 - RangerSecureUsers
 - Domain admins

Don't forget to **Apply** each amendment you make.

Note If you are using a separate proxy for Staff, take care to reflect the new value for the Staff proxy, otherwise your users will experience unexpected filtering behaviour. If you need further guidance on this, please contact RM Support.

Other Windows Server networks

Only follow this section if you have a 'vanilla' Windows Server network, not a CC4 or Ranger network.

Proxy server settings can be delivered to clients in various ways, depending on the operating systems and IE browser versions in use. The possible methods include:

- Group Policy Preferences (Registry Settings)
- Group Policy Preferences (Internet Settings import)
- Custom logon scripts

- Internet Explorer Maintenance GPO settings (IEM) (*XP and IE 8 only*)
- Manual settings on each computer
- A combination of the above.

If you know what mechanism you are currently using to deliver proxy server settings, follow the relevant section below.

If you are unsure how you are delivering proxy server settings to clients, please contact RM Support.

Group Policy Preferences (Registry Settings) and Scripts

1. Log on to a domain controller as an administrator.
2. Launch the **Group Policy Management Console**, following the appropriate instructions for your server operating system:
Windows Server 2003 and 2008R2
Click **Start > Administrative Tools > Group Policy Management**.
Windows Server 2012, 2012R2 and 2016
Click the **Start** button, type **gpmc.msc** and press **Return**.
3. In the left-hand pane, expand **Forest > Domains > {Your Domain} > Group Policy Objects**.
4. For each GPO, check the following locations in the Group Policy Management Editor for any settings that relate to proxy servers:
 - *User Configuration | Preferences | Windows Settings | Registry*
 - *Computer Configuration | Preferences | Windows Settings | Registry*
5. In particular, search for anything that is setting the following registry keys:
 - *HKCU\Software\Microsoft\Windows\CurrentVersion\InternetSettings\ProxyEnable*
 - *HKCU\Software\Microsoft\Windows\CurrentVersion\InternetSettings\ProxyServer*
 - *HKCU\Software\Microsoft\Windows\CurrentVersion\InternetSettings\ProxyOverride*
6. Check each GPO for the presence of Startup and Shutdown scripts in **Computer Configuration | Policies | Windows Settings | Scripts (Startup/Shutdown)**
7. Check each GPO for the presence of Logon or Logoff scripts in **User Configuration | Policies | Windows Settings | Scripts (Logon/Logoff)**
8. Amend any proxy server values you find, to reflect the new RM SafetyNet proxy details.

Note If you are using a separate proxy for Staff, take care to reflect the new value for the Staff proxy, otherwise your users will experience unexpected filtering behaviour. If you need further guidance on this, please contact RM Support.

Group Policy Preferences (Internet Settings import)

1. Log on to a domain controller as an administrator.
2. Launch the **Group Policy Management Console**, following the appropriate instructions for your server operating system:
Windows Server 2003 and 2008R2
Click **Start > Administrative Tools > Group Policy Management**.
Windows Server 2012, 2012R2 and 2016
Click the **Start** button, type **gpmc.msc** and press **Return**.
3. In the left-hand pane, expand **Forest > Domains > {Your Domain} > Group Policy Objects**.
4. For each GPO, use the **Group Policy Management Editor** to check the location:
User Configuration | Preferences | Control Panel Settings | Internet Settings
5. If there is an entry in the right-hand pane, right-click it and select **Properties**.
6. Amend any proxy details found on the **Connections** tab > **LAN settings** button, to reflect the new RM SafetyNet proxy details.

You can find further guidance on using Group Policy Preferences (GPP) here

- Group Policy Preferences - <https://technet.microsoft.com/en-us/library/dn581922>
- Replacing IEM settings - <http://msdn.microsoft.com/en-us/library/dn338129>

Internet Explorer Maintenance (IEM)

Use this method for Windows XP3 or IE 8 proxy settings only, on Windows Server 2003 or 2008R2.

1. Log on to a domain controller as an administrator.
2. To launch the **Group Policy Management console**, click **Start > Administrative Tools > Group Policy Management**.
3. In the left-hand pane, expand **Forest > Domains > {Your Domain} > Group Policy Objects**.
4. Right-click the GPO responsible for proxy server setting delivery and click **Edit...**
5. Navigate to **User Configuration\Policies\Windows Settings\Internet Explorer Maintenance\Connection\Connection Settings**
6. Double-click **Proxy Settings**.
7. Ensure that **Enable proxy settings** is ticked.
8. Under **Address of proxy**, enter the server and port details to reflect the new RM SafetyNet proxy details.

Note If you are using a separate proxy for Staff, take care to reflect the new value for the Staff proxy, otherwise your users will experience unexpected filtering behaviour. If you need further guidance on this, please contact RM Support.


9. Click OK.

Each user will need to log off and back on again for the new proxy address to be delivered to their computer.

Manual proxy settings on computers

Computer/server-based

These settings will affect all users on this computer or server, and will overwrite any previously set proxy settings. Use this procedure **only if you're sure** you do not set the proxy via any other mechanism above. If you are not sure which process to use, please contact RM Support.

1. Log on to the computer or server as an administrator.
2. Launch Internet Explorer. From the Tools  menu choose Internet options.
3. On the Connections tab, click LAN settings.
4. Ensure the Use a proxy server for your LAN box is ticked, and enter the Address and Port details for your new RMSafetyNet proxy.
5. Ensure the Bypass proxy server for local addresses box is ticked.
6. Click Advanced.
7. Under Exceptions in the Do not use proxy server for addresses beginning with... box, enter the addresses of any sites for which the proxy should be bypassed. Click OK.
8. Click OK and OK.
9. Launch a command prompt as administrator, following the appropriate instructions for your operating system:

Windows Server 2003 / 2008R2, Windows XP / Windows 7

- i. Click Start and type cmd in the Search Programs and files field.
- ii. Right-click the cmd icon and select Run as Administrator.

Windows Server 20012 / 2012R2 / 2016 and Windows 8 / 8.1 / 10


- a) Click the Start button and type cmd
- b) Right-click the Command Prompt icon and choose Run as Administrator. If a User Account Control prompt is displayed, click Yes to continue.

10. Type `Netsh winhttp import proxy source=ie` and press **Return**.
11. Ensure the command returns the details of the proxy and any bypass lists that you configured in steps 4 to 7.

Note If an error message is displayed or nothing is returned after you run the `netsh` command, please contact RM Support.

User-based

Note: these settings will only affect the logged-on user.

1. Log on to the computer or server as an administrator.
2. Launch Internet Explorer. From the **Tools**  menu choose **Internet options**.
3. On the **Connections** tab, click **LAN settings**.
4. Ensure the **Use a proxy server for your LAN** box is ticked, and enter the **Address** and **Port** details for your new RMSafetyNet proxy.
5. Ensure the **Bypass proxy server for local addresses** box is ticked.
6. Click **Advanced**.
7. Under **Exceptions** in the **Do not use proxy server for addresses beginning with...** box, enter the addresses of any sites for which the proxy should be bypassed. Click **OK**.
8. Click **OK** and **OK**.

Checking that SSL interception is active

When you have successfully deployed the certificate and configured your device to use the SSL filtering proxy servers, you can use this test to confirm that the proxy settings are correct and RM SafetyNet is intercepting encrypted Google searches. Follow the instructions for either browser:

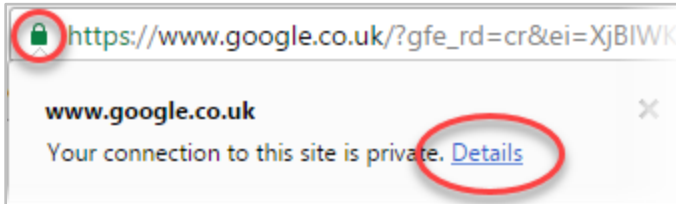
Using Internet Explorer:

1. Browse to <https://www.google.com>
2. Press **Alt-F** and select **Properties**.
3. Click **Certificates**.
4. In the Certificate window, confirm that the **Issue by** field displays **RM SafetyNet Filtering Proxy SHA-384**.

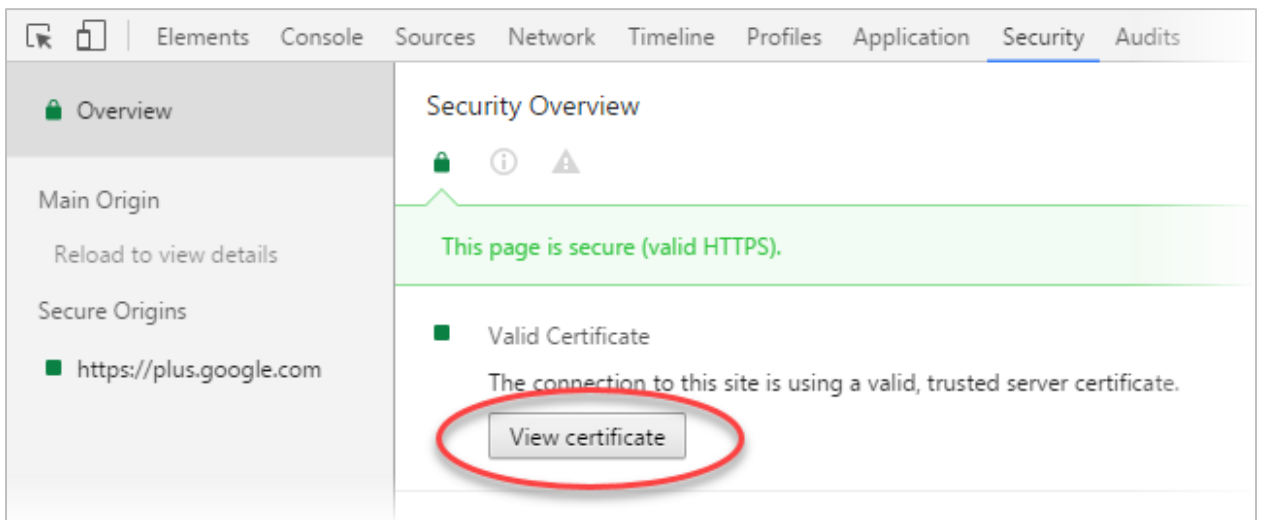
Using Google Chrome:

Installing the RM SafetyNet Certificate – Managed Windows

1. Browse to <https://www.google.com>
2. Click the padlock icon and click **Details**.



3. Click **View certificate**.



4. In the Certificate window, confirm that the **Issued By** field displays **RM SafetyNet Filtering Proxy SHA-384**.

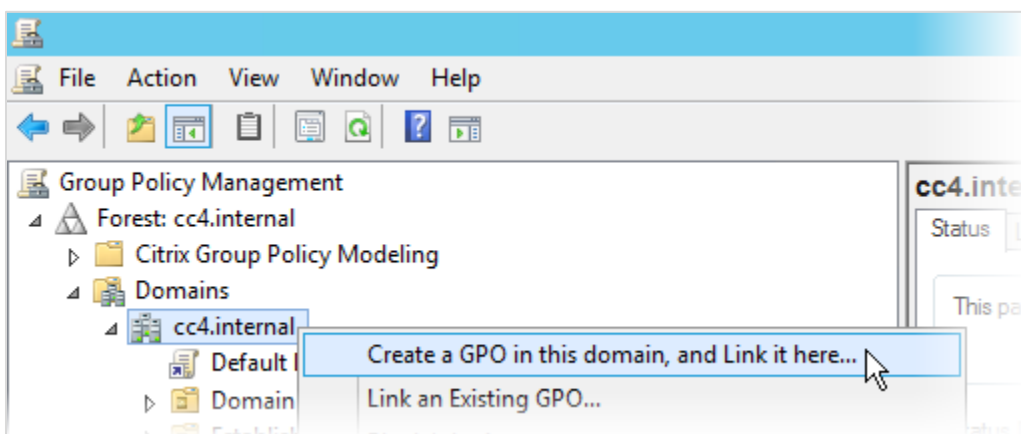
Note If any security messages are displayed, or the certificate is not signed by RM Education Certification Authority, please contact RM Support for guidance.

Appendix I: Creating the GPO manually

If the automatic GPO creation script fails (see page 7), you can manually create the GPO and import the certificate as follows.

This only needs to be completed once on your network. This section will create a new Group Policy Object which will be used to deploy the certificate.

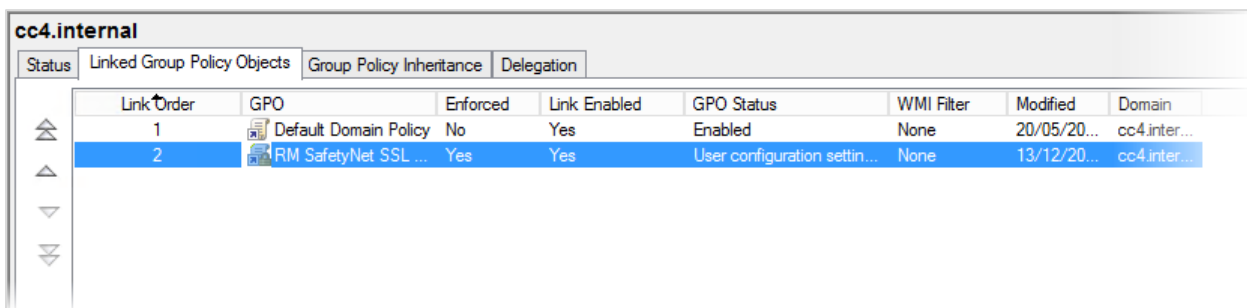
1. Log on to a domain controller as an administrator.
2. Open the Group Policy Management console, following the appropriate instructions for your server operating system:
 - *Windows Server 2003 and 2008R2*
From the **Start** menu choose **Administrative Tools, Group Policy Management**.
 - *Windows Server 2012, 2012R2 and 2016*
Click the **Start** button, type `gpmc.msc` and press **Return**.
3. In the left-hand pane, expand **Forest, Domains**, right-click the domain name and choose **Create a GPO in this domain, and Link it here...**



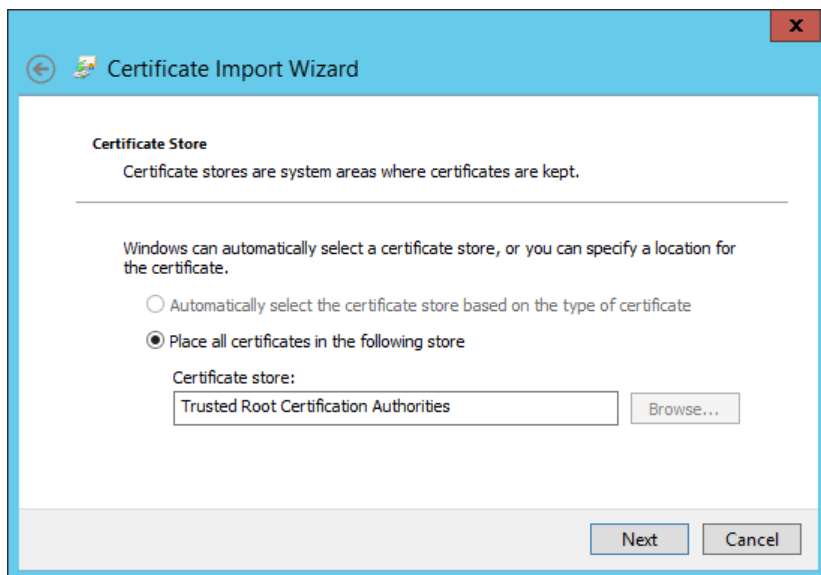
(on Windows Server 2003 this option is named **Create and Link a GPO here...**)

4. In the New GPO window, for Name enter **RM SafetyNet SSL Certificate (SHA-384)** and click **OK**.
5. In the left-hand pane, select the domain name. In the right-hand pane, click the **Linked Group Policy Objects** tab and select **RM SafetyNet SSL Certificate (SHA-384)**. Using the up and down arrows, ensure that it is second in the Link Order.

Installing the RM SafetyNet Certificate – Managed Windows



6. In the left-hand pane, right-click **RM SafetyNet SSL Certificate (SHA-384)** and choose **Edit...**
7. In the left-hand pane of the Group Policy Management Editor, navigate to **Computer Configuration | Policies | Windows Settings | Security Settings | Public Key Policies**
8. Right-click the **Trusted Root Certification Authorities** folder and choose **Import...**
9. In the Certificate Import Wizard, on the Welcome page click **Next**.
10. On the 'File to Import' page, browse to the certificate file. This will be in the same location as the script file you downloaded earlier (see step 2 of Create a Windows Group Policy Object on page 7). Select it and click **Open**.
11. Click **Next**.
12. On the Certificate Store page, ensure that **Place all certificates in the following store** is selected. Click **Next**.

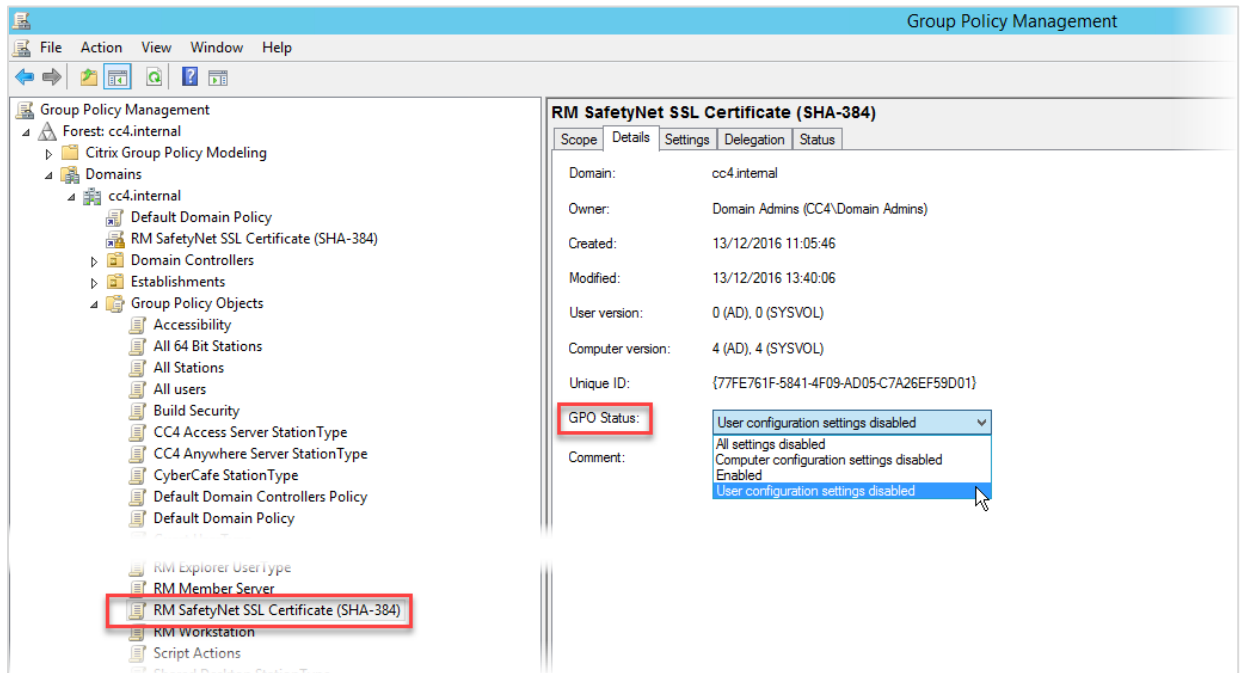


Click **Finish**.

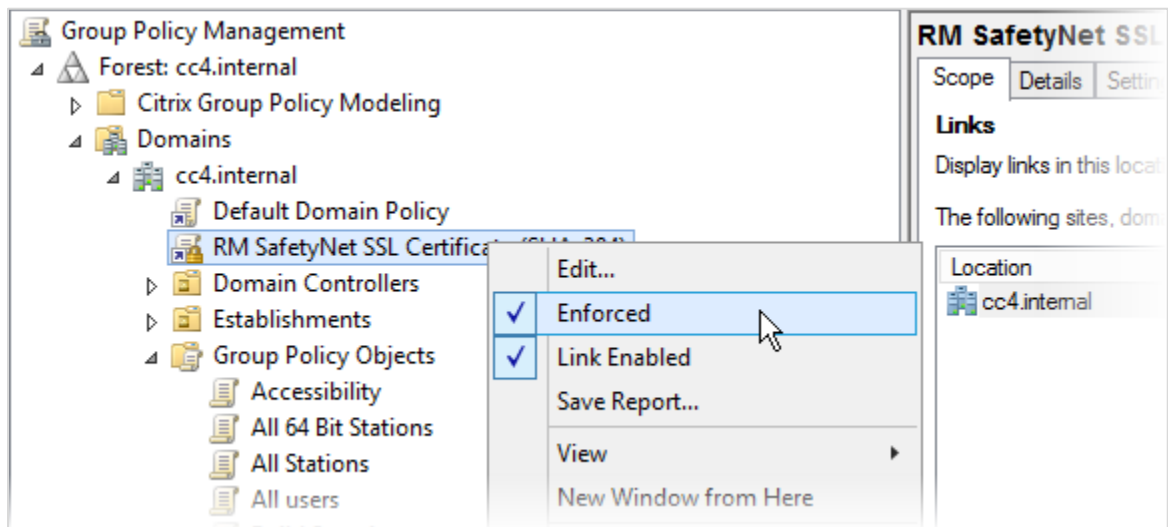
13. At the "import was successful" message, click **OK**.
14. Close the Group Policy Management Editor.

Installing the RM SafetyNet Certificate – Managed Windows

15. Back in the Group Policy Management console, select the newly created GPO in the left-hand pane and click the **Details** tab in the right-hand pane.



16. Change the GPO Status to **User configuration settings disabled**.
To confirm the change click **OK**.
17. In the left-hand pane, under **Forest, Domains, your domain**, right-click **RM SafetyNet SSL Certificate (SHA-384)** and choose **Enforced**.



18. Close the Group Policy Management console, and Administrative Tools (if open).

Appendix II: SHA256 Hotfix for Windows Server 2003 networks

1. Download the following hotfix from the Microsoft website to a temporary folder location on a domain controller.

(Ensure that you download the correct platform (x64 or i386) for your Windows Server 2003 servers. You may need to click the **Show hotfixes for all platforms and languages** link to see downloads for platforms other than x64.)

Applications that use the Cryptography API cannot validate an X.509 certificate in Windows Server 2003 <http://support.microsoft.com/kb/938397/en-gb>

2. Launch the executable file and specify a temporary folder to unzip the files.
3. Browse to the temporary folder and double-click **WindowsServer2003.WindowsXP-KB938397-x64-enu.exe**
or
WindowServer2003-KB938397-x86-ENU.exe
depending on your operating system.
4. Click **Next**, then click **I Agree, Next** and **Finish**. The server restarts.
5. When the server has restarted, log back in as an administrator.
6. From the **Start** menu choose **Control Panel, Add or Remove Programs**.
7. Ensure that the **Show updates** box is ticked. Verify that **Hotfix for Windows Server 2003 (KB938397)** is listed as installed.
8. Repeat this procedure on all Windows Server 2003 servers in the domain. Restart each server after the installation.