Installing the RM SafetyNet Certificate – Managed Apple OS X and IOS

Contents

Introduction

This document describes how to deploy the RM SafetyNet certificate to managed Apple OS X and IOS clients in a managed Apple OS X network, and how to reconfigure the proxy server settings (if required).

If your RM SafetyNet devices use 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

- You must have an Apple OS X server network to manage multiple OS X clients using Apple Remote Desktop and Apple Profile Manager. Standalone devices can be configured using the "manual method" sections of this document.
- You must have Apple Profile Manager or Apple Configurator to manage multiple IOS devices. Standalone devices can be configured using the "manual method" sections of this document.
- The Apple OS X server and clients must be running OS X 10.8.4 or later
- IOS devices must be running IOS version 7 or later
- You must have an administrator account for the local Apple network
- You must be using one of the following browsers:
  - Safari
  - Google Chrome (OS X only, Google Chrome is not supported for RM SafetyNet connections on IOS devices)

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.

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

Current proxy address	New proxy address	Port number
staffproxy.segfl.ifl.net	sslfilter.staffproxy.segfl.ifl.net	8080
staffproxy.slc.ifl.net	sslfilter.staffproxy.slc.ifl.net	8080
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 or device type (e.g. iPhone iPad) on the network for testing purposes
- Ensure all servers and stations are up to date in terms of software deployment and that no restarts are pending
- 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.

Downtime Requirements

In most cases no server downtime is expected during the certificate deployment or proxy server setting process.

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

Downloading the Certificate and OSX Installer

1. Browse to http://www.rm.com/googlessl
2. Under **Managed IOS & Mac**, click the **Certificate** link and save the file in a temporary location.
3. Under **Managed IOS & Mac,** click the **OSX Installer** link and save the file in a temporary location.

(Here you can also download a PDF copy of these instructions.)

Deploying the Certificate

Apple OS X

Follow the procedure below for the method which is most suitable for your network and OS X devices.

Apple Profile Manager method

For Apple Networks using Profile Manager to manage OS X stations only

1. Logon to an Apple OS X client on the same subnet as the Apple Server as an administrator
2. Launch **Safari** and browse to the URL of your Profile Manager web interface (https://{your appleserver FQDN}/Profilemanager)
3. Login to **Profile Manager** as an administrator
4. From the **Library** list, select the device group corresponding to the stations on your network e.g. **Student Desktops**
5. Click the **Settings** tab and click **Edit**
6. Select **Certificates** in the left hand pane and then **Configure**
7. Click **Add Certificate** and browse to the location of the previously downloaded RM SafetyNet certificate, then click **Choose**. This should populate the **Certificate Name** field
8. Click **OK** then **Save**
9. Repeat steps 5 to 9 for each **device group** under the **Device Group** node in the **Library**
10. Repeat steps 5 to 8 for each **user group** under the **Groups** node in the **Library**
11. Restart each OS X device that is currently being managed by Apple Profile Manager

Apple Remote Desktop (ARD) method

For Apple Networks using Apple Remote Desktop to manage OS X stations only

1. Logon to the **Apple Remote Desktop Server** as an administrator
2. **Ctrl-Click** or **right-click** the previously downloaded **RMEducationCANew_mpkg.zip** file and select **Open**
3. If prompted with an "Are you sure you want to open it" dialog box, click **Open**
4. Launch **Remote Desktop** from **Applications** and login to the application as an administrator
5. Select the **Install** icon at the top of the window

6. Drag and drop the previously downloaded **RMEducationCANew.mpkg** file into the **Packages** window
7. Click **Save** and enter **RM SafetyNet Certificate New Install** in the **Save As:** field and click **Save**
8. Right-click (or Ctrl-click) the new **RM SafetyNet Certificate New Install** package in the left hand pane and select the **Edit Task...**
9. With the **Install Packages** windows still open, select **All Computers** in the **Remote Desktop** window
10. Select the computers you wish to deploy the package to (you should ensure that these stations are powered on and not currently in use), and drag them into the bottom area of the **Install Packages** window (you may need to rearrange the window locations on screen to achieve this)

Note: It is advised that you test the deployment to a single station before adding multiple stations to the task

11. Once you have added all computers that require the package, select **Install**

Manual install method

A manual method that will work for all OS X stations

1. Logon to the Apple station as an administrator
2. **Ctrl-Click** or **right-click** the previously downloaded **RMEducationCANew_mpkg.zip** file and select **Open**
3. If prompted with an "Are you sure you want to open it" dialog box, click **Open**
4. This should extract **RMEducationCANew.mpkg** to the **Downloads** folder
5. Double-click **RMEducationCANew.mpkg**
6. Click **Continue** > **Install**, then enter your administrator password
7. At **The installation was successful** message click **Close**

Apple IOS

Follow the procedure below for the method which is most suitable for your network and IOS devices.

Apple Profile Manager method

For Apple Networks using Profile Manager to manage IOS devices only

1. Logon to an Apple OS X client on the same subnet as the Apple Server as an administrator

2. Launch **Safari** and browse to the URL of your Profile Manager web interface (https://{your appleserver FQDN}/Profilemanager)
3. Login to **Profile Manager** as an administrator
4. From the **Library** list, select **Device Groups** and the device group corresponding to the stations on your network e.g. **Student iPads**
5. Click the **Settings** tab and click **Edit**
6. Select **Certificates** in the left hand pane and then **Configure**
7. Click **Add Certificate** and browse to the location of the previously downloaded RM SafetyNet certificate, then click **Choose**
8. Note: this should populate the **Certificate Name** field
9. Click **OK** then **Save**
10. Repeat steps 5 to 9 or each **device group** under the **Device Group** node in the **Library**
11. Repeat steps 5 to 9 for each **User Group** under the **Groups** node in the **Library**
12. These settings will be pushed to your previously enrolled IOS devices

Apple Configurator method

For Apple Networks using Apple Configurator to manage IOS devices only

1. Logon to the Apple Configurator station as an administrator
2. Launch **Apple Configurator 2** from the **Applications** folder
3. Connect an IOS device via USB
4. Select **File** then **New Profile**
5. Under the **General** section, enter **RM SafetyNet Certificate 2016 Install** as the name and "**a profile to install the RM SafetyNet certificate**" in the Description field
6. Select **Certificates** from the **left hand** pane
7. Click **Configure**, then browse to the location of the previously downloaded RM SafetyNet certificate, then click **Open**
8. Click **File** then **Save**. Save the profile in an appropriate location with the name **RM SafetyNet Certificate Install Profile**
9. Right-click or Ctrl-click the connected iOS device and select **Add** then **Profiles**
10. Browse to the location of the profile saved in step 8 and click **Add**
11. Follow the prompts in Configurator to install the profile

Note: Unsupervised devices will require intervention on the device itself. Supervised devices should install the profile silently.

Manual install method

A manual method that will work for all IOS devices

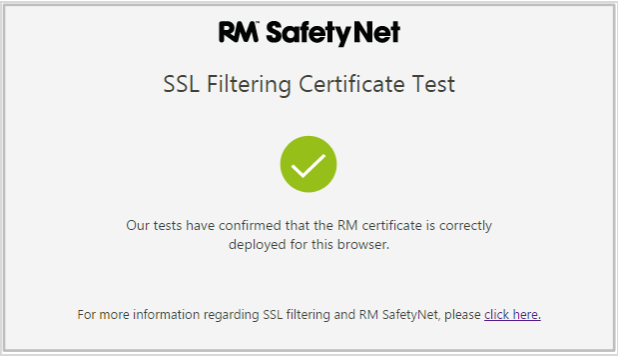
1. Logon to the device
2. Ensure the device is connected to your wireless network
3. Launch Safari and browse to the following URL

   http://www.rm.com/googlessl
4. Under **iPhone & iPad stand-alone**, click the **Certificate** link and save the file in a temporary location.
5. Select **Install** and enter the **passcode** for the device
6. Select **Install**, **Install**, **Done**
7. Repeat the process for any IOS devices that require the certificate to be installed

Checking the Certificate is deployed

Method for all OS X stations and IOS devices

To check that the certificate is deployed to the station or device, open an internet browser and go to http://certificatecheck.rm.com .



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

Deploying Proxy Server Settings

*Only follow this section if the network is currently using a **non-transparent proxy.***

Apple OS X

Follow the procedure below for the method which is most suitable for your network and OS X devices.

Apple Profile Manager method

For Apple Networks using Profile Manager to manage OS X stations only

1. Logon to an Apple OS X client on the same subnet as the Apple Server as an administrator
2. Launch **Safari** and browse to the URL of your Profile Manager web interface (https://{your appleserver FQDN}/Profilemanager)
3. Login to **Profile Manager** as an administrator
4. From the **Library** list, select **Device Groups** and the device group corresponding to the stations on your network e.g. **Student Desktops**
5. Click the **Settings** tab and click **Edit**
6. Select **Network** in the left hand pane and then **Configure**

Note: Only follow the next step if the fields are already populated in the Proxy Server section. If no details are present move onto the next device group.

Note: pay particular attention at this point if you are using a separate proxy for Staff. This must be changed to reflect the new value for the Staff proxy, otherwise your users will receive a different filtering experience than they are accustomed to. For guidance on this, please contact RM support.

7. Under the **Proxy Setup** section, amend the existing details to reflect the new RM SafetyNet proxy server details
8. Click **OK** then **Save**
9. Repeat steps 5 to 8 or each **device group** under the **Device Group** node in the **Library**
10. Repeat steps 5 to 8 for each **User Group** under the **Groups** node in the **Library**

Apple Remote Desktop method

For Apple Networks using Apple Remote Desktop to manage OS X stations only

If your site currently uses Apple Remote Desktop to deploy the proxy server settings, then you must edit the UNIX commands or ARD packages that are currently being used to distribute the proxy server settings, to include the new RM SafetyNet proxy server details.

Please contact your support provider for further assistance with this process.

Manual method

A manual method that will work for all OS X stations

1. Login to the station as a local administrator
2. Launch **System Preferences > Network**
3. Click **Ethernet** or **Wi-fi** (depending on a your network connection) and click **Advanced**
4. Select **Proxies** and amend any **ticked** item in the **Select a protocol to configure** section to reflect the new RM SafetyNet Proxy details

Apple IOS

Follow the procedure below for the method which is most suitable for your network and IOS devices.

Apple Profile Manager method

For Apple Networks using Profile Manager to manage IOS devices only

1. Logon to an Apple OS X client on the same subnet as the Apple Server as an administrator
2. Launch **Safari** and browse to the URL of your Profile Manager web interface (https://{your appleserver FQDN}/Profilemanager)
3. Login to **Profile Manager** as an administrator
4. From the **Library** list, select **Device Groups** and the device group corresponding to the stations on your network e.g. **Student Desktops**
5. Click the **Settings** tab and click **Edit**
6. Select **Network** in the left hand pane and then **Configure**

Note: Only follow the next step if the fields are already populated in the Proxy Server section. If no details are present move onto the next device group.

Note: pay particular attention at this point if you are using a separate proxy for Staff. This must be changed to reflect the new value for the Staff proxy, otherwise your users will receive a different filtering experience than they are accustomed to. For guidance on this, please contact RM support.

---

7. Under the **Proxy Setup** section, amend the existing details to reflect the new RM SafetyNet proxy server details
8. Click **OK** then **Save**
9. Repeat steps 5 to 8 or each **device group** under the **Device Group** node in the **Library**
10. Repeat steps 5 to 8 for each **User Group** under the **Groups** node in the **Library**

11. These settings will be pushed to your previously enrolled IOS devices

Apple Configurator method

For Apple Networks using Apple Configurator to manage IOS devices only

1. Logon to the Apple Configurator station as an administrator
2. Launch **Apple Configurator** from the **Applications** folder
3. Connect an IOS device via USB
4. Select **Settings** > **Wi-Fi**, then click **Configure settings**...

Note: Only follow the next step if the fields are already populated in the Proxy Server section. If no proxy server settings are configured here, then click **Cancel** *and do not proceed.*

Note: pay particular attention at this point if you are using a separate proxy for Staff. This must be changed to reflect the new value for the Staff proxy, otherwise your users will receive a different filtering experience than they are accustomed to. For guidance on this, please contact RM support.

5. Under the **Proxy Setup** section, amend the existing details to reflect the new RM SafetyNet proxy server details
6. Click **Save**
7. Redeploy the profile to your IOS devices using your usual method in Apple Configurator

Manual method

A manual method that will work for all IOS devices

1. Logon to the device
2. Locate and launch the **Settings** app
3. Select **Wi-fi** then your **Wi-fi network** name (this should be **ticked**)
4. Under **HTTP proxy**, update the settings with the details of your new RM SafetyNet proxy server

Checking SSL Interception is active

Note: this test will only work once you have deployed the certificate and your device is configured to use the SSL filtering proxy servers

Apple OS X

1. Launch Safari and browse to https://www.google.com
2. Select the padlock in the address bar and click **Show Certificate**
3. Click Certificates and ensure that the **Issue by** field displays **RM Education**

Note: If you receive any security messages or the certificate is not signed by RM Education, please contact RM support for guidance.

Apple iOS

Note: it is not possible to view the SSL certificate that is presented to the device using Safari on iOS. The steps below will verify the certificate details in the Google Chrome app., which must be deployed separately to the device

1. Locate and launch the **Chrome** app
2. Browse to https://www.google.com
3. Select the padlock in the address bar and ensure that **RM SafetyNet Filtering** or **RM Education** is displayed in the text box

Note: If you receive any security messages or the certificate is not signed by RM Education, please contact RM support for guidance.