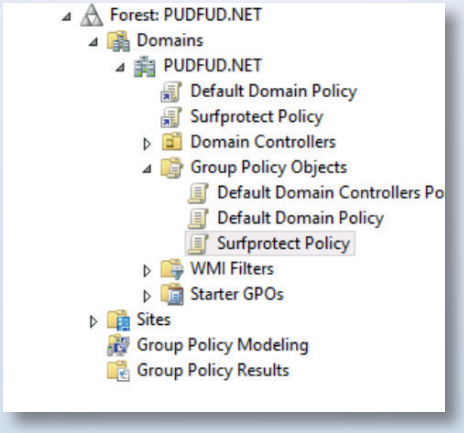
SurfProtect Quantum Certificate Setup

SurfProtect's cloud-based HTTPS filtering feature requires that all devices on your network trust Exa Education. This document provides guidance to enable this across your network, however, should you require any additional help then please do not hesitate to contact our dedicated support team on **0345 145 1234** or by emailing **helpdesk@exa.net.uk**

A certificate published by Exa Education needs to be installed on each device within your network. This can be done on a per machine basis, however we have detailed how to deploy the necessary certificate using various management tools below.

Deployment with Active Directory

1. Download your SurfProtect Quantum certificate at **www.exa.is/certificate**
2. Once you are logged into your active directory server, go to **Start > Administrative Tools > Group Policy Management**
3. Identify the Group Policy Object that you wish to edit (optionally, you may wish to create a new Group Policy Object to define all surfprotect settings in one place)
4. Right click the newly created Group Policy Object and select **edit**
5. Navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies**
6. Right click on the folder **Trusted Root Certification Authorities** and select **Import**
7. Follow the steps in the **Certificate Import Wizard**, providing the location of the certificate downloaded from the SurfProtect panel when prompted for a file to import.



exa education

Version 2.0

Deployment with Google Admin Console (GSuite)

1. Download your SurfProtect Quantum certificate at **www.exa.is/certificate**
2. Log into the admin panel at **https://admin.google.com**
3. Navigate to Device Management
4. In the **DEVICE SETTINGS** menu on the left, select Network
5. Select **Certificate > ADD CERTIFICATE**
6. Navigate to the previously downloaded certificate
7. Ensure that the option labelled Use this certificate as an HTTPS certificate authority is checked
8. Click **Save**

Individual Windows Machine Installation

1. Download your SurfProtect Quantum certificate at **www.exa.is/certificate**
2. Click the **Windows Start Button** and type '*mmc*' into the search bar to locate and run the Microsoft Management Console
3. Navigate to the **File** menu > **Add/Remove Snap-in**
4. From the **Available snap-ins** pane, select **Certificates** and then click on the button labelled **Add**
5. In the **Certificates snap-in** wizard, select **computer account** or **local computer** when prompted for which context the snap-in should manage certificate for.
6. Click **Finish** to close the wizard and **OK** to close the snap-ins window
7. In the console tree, double-click on **Certificates**
8. Right-click the **Trusted Root Certification Authorities** and click **import**
9. Follow the steps in the **Certificate Import Wizard**, providing the location of the certificate downloaded from the SurfProtect panel when prompted for a file to import

Individual Mac OS X Installation

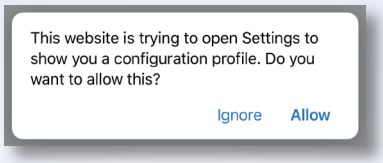
1. Download your SurfProtect Quantum certificate at **www.exa.is/certificate**
2. Launch **Keychain Access**
3. From the **Keychain Access** toolbar, select **File > Import Items**
4. Provide the location of the downloaded certificate when prompted for a file location and click **Open**
5. Double-click on the newly imported certificate, labelled **Exa Networks Ltd CA**
6. In the **Trust** section of the newly opened window, set the value in the dropdown labelled **Secure Sockets Layer (SSL)** to **Always Trust**
7. Close the current window to apply changes
8. Enter your system password when prompted and click on **Update Settings**

Individual Chromebook Installation

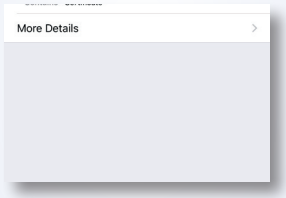
1. Download your SurfProtect Quantum certificate at **www.exa.is/certificate**
2. Scroll to the bottom of your Chromebook's **Settings** page and click on **Show advanced settings**
3. Under the **HTTPS/SSL** section, click on **Manage certificates**
4. Navigate to the **Authorities** tab in the **Certificate Manager** and click **Import**
5. Select the certificate from your **Downloads** location and click on **Open**

Individual iOS Installation

1. Navigate to **exa.is/certificate**
2. Tap **Allow** on the pop-up



3. On the following screen tap **Install** (if using iOS 12.x, you can find this in **Settings > Profile Downloaded**)



4. Input your **Passcode** if prompted
5. Confirm by tapping **Install**
6. Return to **Settings** and follow: **General > About > Certificate Trust Settings** and Enable **'Exa Networks Ltd Root CA'** by tapping the slider.

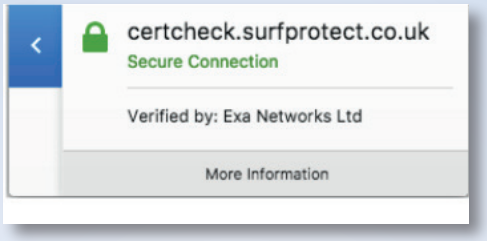
Individual Android Version 7 Installation

1. Navigate to **www.exa.is/certificate**
2. This will prompt a download, click **open**
3. Input your **Passcode** when prompted
4. Set the Certificate name then choose credential use as **VPN and Apps** option.
5. Tap **OK**, this will then install and become a user certificate.

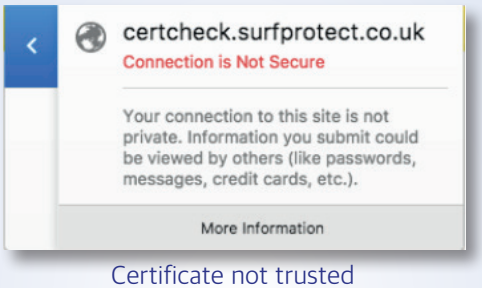
Installation Verification

You can check whether the certificate is being successfully trusted by visiting the SurfProtect Certificate Status page at **http://certcheck.surfprotect.co.uk**

This page will automatically detect the location you're browsing from so it can present a certificate signed by the authority you've trusted during negotiation of the secure HTTPS connection. If your browser shows that the connection is safe then this validation serves as proof that the service certificate is trusted.



Certificate successfully trusted



Certificate not trusted

If you don't already have SurfProtect configured to transparently decrypt all web traffic you can test decryption by configuring your browser to use **proxy.quantum.exa-networks.co.uk** on port 3128.

SurfProtect Quantum AD Configuration

SurfProtect Quantum integrates with Active Directory to provide 'per user' policy filtering and reporting. To achieve this, your AD data needs to be imported to SurfProtect. This document provides guidance on this process, however, should you require any additional help then please do not hesitate to contact our dedicated Technical Support team on **0345 145 1234** or by emailing **support@exa.net.uk**

IMPORTANT: If you do not want to enact the AD integration feature of SurfProtect Quantum, or do not have an AD server, you do not need to perform the following steps.

This will prevent these devices accessing any website belonging to a restricted SurfProtect category, or any website that you have added to your blocked list.

Why synchronise your Active Directory data with SurfProtect?

Individual users are represented in Active Directory by a unique user account and by membership to an arbitrary number of group accounts.

With Active Directory integration enabled, SurfProtect can apply different filtering policies to unique users as well as group accounts.

SurfProtect also uses the information from the data synchronisation to display the real names of your users to enrich the data provided by our data analytics panel.

Steps

1. Download the SurfProtect Quantum configuration script at **www.exa.is/installing**
2. Right click on the downloaded file and select '**Run with Powershell**'
   NOTE: **This script must be run directly on your Active Directory domain server in order to perform all necessary configuration.**
3. Select '**Open**' in the security dialogue box that appears.
4. Follow the commands on screen, the script should complete in a matter of minutes.
5. Please call our Technical Support team on **0345 145 1234** once these steps have been performed.

Single Sign-On

Single sign-on (also known as SSO) is an authentication service that allows a user to access multiple applications with one set of login credentials (e.g. username and password), often without the need to retype these details once they have logged in to the computer.

Why is SSO important for SurfProtect?

SurfProtect communicates with popular SSO schemes in order to obtain information about which user is accessing a web page or other resource hosted on a website. This information is used both to provide granular filtering control, and to ensure that the logs and reports available with SurfProtect Analytics clearly identify which user accessed or requested which online content.

Windows Active Directory

SSO is achieved with Active Directory by requesting a user's information from the web browser whenever a web resource is requested by a machine in your school's local domain.

Running the above script will establish trust between your school's domain controller and our proxy servers. This means that when a user requests access to a website, the web browser will be able to communicate with the domain controller to identify the individual and provide SurfProtect with trusted proof of who that person is. As a result, SurfProtect can then filter the web request according to that individual's filtering profile, and record their online activity.

As SSO requires direct authentication against our proxy servers, Active Directory SSO requires web browsers to be configured with explicit proxy settings. Fortunately, these settings can be pushed to all Windows devices by creating a Group Policy Object; using this mechanism also helps to prevent settings from being manually changed by students.

Mixed Environments

If your school uses devices outside of your AD domain, such as iPads and Chromebooks, which are not managed as part of your local domain, individual user filtering and identification will not be possible.

These devices will still receive transparent SurfProtect filtering when connected to your school's network, however user identity information and profile matching will not be enacted and web logs will not be populated with user or machine identities.

Depending on your school's mobile device and guest internet policies, it may be that you wish to always prevent unlogged internet access from being performed. If this is the case, you can disable non-authenticated filtering in the SurfProtect panel. In doing this, students or visitors attempting to access the school's internet service on a mobile device will be presented with a screen which advises that they are unable to do so and must instead login to a configured machine.