SurfProtect® Quantum Setup Guide

Located entirely in the cloud, SurfProtect Quantum performs network-level filtering, This means that all traffic on your school's internet connection is filtered, regardless of the machine or device used to access it. As a result, you do not need to install any hardware on your school's premises* - instead, you can be assured that you are receiving industry-leading protection, without having to configure and maintain an on-site device!

Providing categorised, age-appropriate filtering, BYOD protection, search term filtering, safeguarding support, subscription to the IWF and Home Office Terrorism Watch List, all with the flexibility to create the exact level of filtering you want for your school, you can be assured that SurfProtect Quantum protects your staff and students from the many dangers present online - and that you are in accordance with the current framework.

Below we have detailed many of the features you will receive with SurfProtect Quantum.

Filtering	
HTTP filtering	✓
HTTPS decryption	✓
Intercept BYOD	✓
Realtime classification	✓

Encrypted Websites	
Enforce Google SafeSearch	✓
Keyword filtering	✓
Restricted YouTube	✓

Identification	
External IP	✓
Username	✓
Groups	✓
Full IPv6 support	✓

Single Sign-on	
Active Directory	✓

Logs	
Downloadable logs of all filtered traffic	✓
Includes all search queries	✓
Indicate user	✓

Analytics	
Analytics dashboard	✓
Search query report	✓

Administration	
Centralised control panel	✓
Single sign-on authentication	✓

In order to receive completely cloud-based filtering, there are a few things to do on your network which enable us to perform AD integration and HTTPS filtering on your school's internet connection.

Please complete the following steps to allow these features of your filtering service to be enacted. If you require help at any point, please do not hesitate to contact our dedicated support team on **0345 145 1234** or by emailing **support@exa.net.uk**.

exa education
Internet & Filtering for Schools

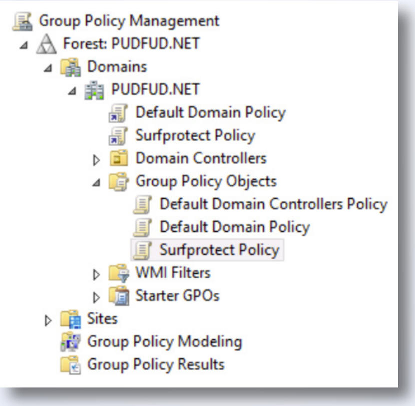
*If you are an external SurfProtect Quantum customer and do not wish to deploy the proxy to each device, you will require a firewall as this enables us to implement DNAT rules to force your internet connection to SurfProtect Quantum for filtering to be performed.

Certificate Setup

SurfProtect Quantum’s HTTPS filtering feature requires that all devices on your network trust Exa Education. In order to do this, 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. Log into the SurfProtect panel at **panel.surfprotect.co.uk**
2. Navigate to the downloads page via **Tools > Downloads**
3. Download the file labelled **surfprotect authority certificate**
4. Logged into you active directory server, go to **Start > Administrative Tools > Group Policy Management**
5. 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)
6. Right click the newly created Group Policy Object and select **edit**
7. Navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies**



8. Right click on the folder **Trusted Root Certification Authorities** and select **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.

Deployment with Goodle Admin Console (GSuite)

G Suite

1. Log into the SurfProtect panel at **panel.surfprotect.co.uk**
2. Navigate to the downloads page via **Tools > Downloads**
3. Download the file labelled **SurfProtect Authority Certificate**
4. Log into the admin panel at **https://admin.google.com**
5. Navigate to Device Management
6. In the **DEVICE SETTINGS** menu on the left, select Network
7. Select **Certificate > ADD CERTIFICATE**
8. Navigate to the previously downloaded certificate
9. Ensure that the option labelled Use this certificate as an HTTPS certificate authority is checked
10. Click **Save**

Individual Windows Machine Installation

1. Log into the SurfProtect panel at **panel.surfprotect.co.uk**
2. Navigate to the downloads page via **Tools > Downloads**
3. Download the file labelled **SurfProtect Authority Certificate**
4. Click the **Windows Start Button** and type ‘*mmc*’ into the search bar to locate and run the Microsoft Management Console
5. Navigate to the **File** menu > **Add/Remove Snap-in**
6. From the **Available snap-ins** pane, select **Certificates** and then click on the button labelled **Add**
7. In the **Certificates snap-in** wizard, select **computer account** or **local computer** when prompted for which context the snap-in should manage certificate for.
8. Click **Finish** to close the wizard and **OK** to close the snap-ins window
9. In the console tree, double-click on **Certificates**
10. Right-click the **Trusted Root Certification Authorities** and click **import**
11. 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. Log into the SurfProtect panel at **panel.surfprotect.co.uk**
2. Navigate to the downloads page via **Tools > Downloads**
3. Download the file labelled **SurfProtect Authority Certificate**
4. Launch **Keychain Access**
5. From the **Keychain Access** toolbar, select **File > Import Items**
6. Provide the location of the downloaded certificate when prompted for a file location and click **Open**
7. Double-click on the newly imported certificate, labelled **Exa Networks Ltd CA**
8. In the **Trust** section of the newly opened window, set the value in the dropdown labelled **Secure Sockets Layer (SSL)** to **Always Trust**
9. Close the current window to apply changes
10. Enter your system password when prompted and click on **Update Settings**

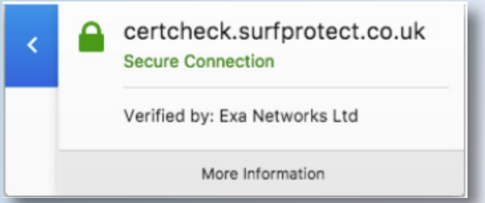
Individual Chromebook Installation

1. Log into the SurfProtect panel at **panel.surfprotect.co.uk**
2. Navigate to the downloads page via **Tools > Downloads**
3. Download the file labelled **SurfProtect Authority Certificate**
4. Scroll to the bottom of your chromebook’s **Settings** page and click on **Show advanced settings**
5. Under the **HTTPS/SSL** section, click on **Manage certificates**
6. Navigate to the **Authorities** tab in the **Certificate Manager** and click **Import**
7. Select the certificate from your **Downloads** location and click on **Open**

Installation Verification

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

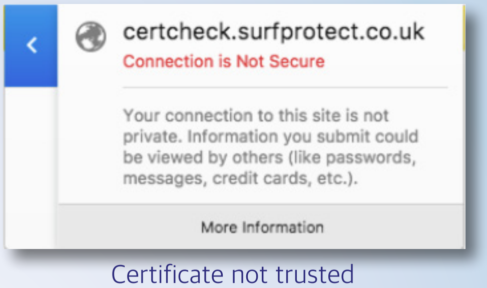
This page will automatically detect the location you're browsing from so it can present a certificate signed by the authority you've trusted during negotiation of the secure HTTPS connection. If your browser shows that the connection is safe then this validation serves as proof that the service certificate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


certcheck.surfprotect.co.uk

Secure Connection

Verified by: Exa Networks Ltd

Certificate successfully trusted


certcheck.surfprotect.co.uk

Connection is Not Secure

Your connection to this site is not private. Information you submit could be viewed by others (like passwords, messages, credit cards, etc.).

Certificate not trusted

If you don't already have SurfProtect configured to transparently decrypt all web traffic then you can test decryption by configuring your browser to use **proxy.quantum.exa-networks.co.uk** on port 3128. This proxy service is configured to always decrypt HTTPS traffic, regardless of your settings for transparent interception.

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 part of the document provides guidance on this process.

There are two possible methods to perform the import; Method 1 is a quicker process, however in some circumstances it may not work successfully and you will be presented with an error message. If this occurs, please use Method 2. Both Methods 1 & 2 have the same final steps. As always, if you require assistance at any point, please don't hesitate to get in touch.

Steps - Method 1

1. Log into your SurfProtect panel at **https://surfprotectpanel.exa.net.uk/** and click on the link '**AD configuration script**' under the Downloads section located in the left hand side navigation bar.
2. Right click on the downloaded file and select '**Run as Administrator**'.
   NOTE: **This script must be run directly on your Active Directory domain server in order to perform all necessary configuration. The installation script must also be run with administrative privileges and the PowerShell execution policy on your domain controller must permit the execution of scripts.**
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.

Steps - Method 2

1. Login to your SurfProtect panel at **https://surfprotectpanel.exa.net.uk/** and click on the link '**AD configuration script**' under the Downloads section located in the left hand side navigation bar.
2. Right click on the PowerShell application and '**Run as Administrator**'.
   NOTE: **This script must be run directly on your Active Directory domain server in order to perform all necessary configuration. The installation script must also be run with administrative privileges and the PowerShell execution policy on your domain controller must permit the execution of scripts.**
3. In the PowerShell window, change directory to the location where the installation script is stored (e.g.: cd ~\Downloads)
4. Invoke the installation process with: **powershell.exe -ExecutionPolicy Unrestricted -f "Quantum AD installer.ps1"**
5. Press **Enter** when prompted to begin installation.

Final Steps - Methods 1 & 2

1. Once the script has been run successfully, you will need to copy the created .ldif file and email it to **support@exa.net.uk**. This file can be found at **C:\Program Files\SurfProtect\Data\Users.ldif** A member of our team will then confirm when this has been uploaded. Please do not perform the next step until you have received this confirmation.
2. In order for SurfProtect integration with Active Directory SSO to function, your operating system or web browser must be configured to use the SurfProtect AD proxy service below.

Proxy Address: ad.quantum.exa-networks.co.uk
Proxy Port: 3128

The service on this hostname is dedicated specifically to Active Directory.

Important Information

Application Control

During the early release phase of SurfProtect Quantum, you may experience a slight interruption to the functionality of some applications used by your school.

This is because many apps now use HTTPS to communicate and, in some cases, use outdated forms of the security protocol which are not compatible with SurfProtect Quantum. As a result, in order to allow these apps to be effectively filtered by SurfProtect Quantum, our team must perform manual diagnostics to resolve the issue and enable your school to continue using the application.

Your feedback during this time is incredibly beneficial as it enables us to quickly identify and support these apps, so if you come across an app which does not work as expected please don't hesitate to let our team know. We have already implemented resolutions for a number of commonly-used applications, such as DropBox.

This list will continue to grow throughout the early release period and is automatically applied to all SurfProtect Quantum customers, so you don't have to worry about performing manual updates to receive the latest development.

Please note, by enabling these older technology-based apps to work we can no longer decrypt the information that they transfer across your connection. Therefore, use of that particular app may go against your school's e-safety policy. For example, it is not possible to decrypt or log any traffic that is used by the Capita SIMS app.

If you have a query or concern about a specific app used by your school, please get in touch on **0345 145 1234** or **support@exa.net.uk**.

BYOD Filtering

Please note that if your school uses devices, 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 SurfProtect Quantum 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.