SSL Remote Access Service - Minimum Device Standards

Version 2.4

Table of Contents

1. Overview 1
2. Operating System 1
3. Web Browser 2
4. Personal Firewall 2
5. Anti-virus Solution 3
5.1. HSC/GP Users 3
5.2. All Other Users 3
6. Modem/Router 4
7. Remote Desktop Requirement For HSC/GP staff 4
8. Reporting problems 4

1. Overview

This document replaces all variations of existing HSC SSL Remote Access Service – Minimum Device Standards documents

To use this service the device must meet the following minimum standards otherwise connection may be refused. It is the user's responsibility to ensure that the device is configured to these standards and address any issues that may occur in achieving them.

The sections below give details of the supported versions of the operating system, web browser, firewall and anti-virus. BSO are reliant on the latest releases of these components being verified and added to the approved list by the manufacturer of the appliance used to provide the HSC SSL Remote Access Service. Therefore there may be a delay in a new version being released and it being approved for SSL Remote Access.

2. Operating System

The acceptable operating systems on non-corporate devices are:

Microsoft Windows 8.1 (32 & 64 bit versions)
Microsoft Windows 10 (32 & 64 bit versions)*

***NOTE:** Windows 10 is **NOT** available for use by the Special Nurse Organ Donation Team.

The operating system must be a legitimate licensed copy and have all available critical security patches applied.

When using **Windows 8.1** to make a connection to the HSC network you will require at least **Power User** rights on the device. This is required to install the ActiveX controls and plugins needed to make the solution work.

With **Windows 10** a standard user account has the appropriate rights to install the Active X controls and plugins.

Apple operating systems are not currently supported as they will not allow the security restrictions which are implemented by this service.

3. Web Browser

Microsoft Internet Explorer 11 is the recommended web browser for this service.

Mozilla Firefox, Google Chrome and Microsoft Edge browsers are not recommended by the BSO-ITS Security Team as they may generate errors which prevent the login sequence.

All available critical security patches must be applied.

4. Personal Firewall

A list of personal firewalls that are approved on the non-corporate device can be found at:

http://www.opswat.com/products/oesis-framework/supported-applications

The personal firewall must be active before the connection is made. If not, the connection will be blocked.

Other firewalls may work but have not been verified.

NOTE: Bar Library, PARS and HPRM users - this check will be bypassed if you provide BSO with a static public IP address which you will use to access the service.

NOTE: Personal firewall is not checked for Ophthalmology, Dental and Pharmacy users.

5. Anti-virus Solution

Please note that Sophos Anti-Virus now provide a free of charge anti-virus solution for any non-business related PCs, i.e. a home PCs. You can manage up to 10 devices with your Sophos Dashboard. For more information on how to download this and install it see the **Sophos Anti-Virus – For Home Use** document for details.

Note: The BSO-ITS Security Team recommend the use of Sophos Anti-Virus when using HSC SSL Remote Access Service as it provided the best performance of those tested.

The following section shows the accepted anti-viruses for specific users:

5.1. HSC/GP Users

The following anti-virus solutions are approved on the non-corporate device:

ESET NOD32 (any version) [†]
AVG 2013 or later (including free editions) [†]
Sophos v10 or later
Symantec Norton Antivirus, Norton Internet Security, or Norton 360
Windows Defender

The anti-virus solution must be active and up to date (i.e. not allowed to go more than 3 days without an update) before making a connection. If not, the connection will be blocked.

Other AV solutions **will not** work as they do not comply with all the security requirements for this service.

5.2. All Other Users

Any anti-virus solution can be used.

The anti-virus solution must be active and up to date (i.e. not allowed to go more than 3 days without an update) before making a connection. If not, the connection will be blocked.

NOTE: Bar Library, PARS and HPRM users - this check will be bypassed if you provide BSO with a static public IP address which you will use to access the service.

[†] Performance with this AV program may be slow.

6. Modem/Router

Use of a wireless router is acceptable as all traffic is encrypted until it reaches the SSL Remote Access Gateway.

7. Remote Desktop Requirement For HSC/GP staff

This service is only available to HSC and GP staff if they are making a remote desktop connection from a non-corporate (home) PC onto a corporate PC (HSC provided). The corporate PC must not be in use by anyone else at the time of the connection and will not be available to anyone else during the remote session.

The BSO ITS Security Team need to pre-configure your remote access to allow the connection to the HSC PC and up to 2 PCs can be configured. Any changes to which corporate PC you connect to, needs to be requested via the BSO Service Desk with a standard service level agreement's response time.

Where the corporate PC is a laptop or tablet, HSC and GP staff should follow the guidance on how to secure portable devices as per the **Use of ICT Equipment** policy.

8. Reporting problems

If you are experiencing issues or have any queries about the SSL Remote Access Service you should contact the **BSO ICT Service Desk**. The Service Desk is available from Monday to Friday (excluding public holidays) from 8.30 – 17.00.

The contact details for the ICT Service Desk are:

Telephone: 028 9536 2400
E-mail: supportteam@hscni.net

Please record the **session reference number** as shown in Figure 1 and details of any error messages that are displayed and how far you get in the connection process before the error appears. This greatly helps the IT teams when investigating the problem.

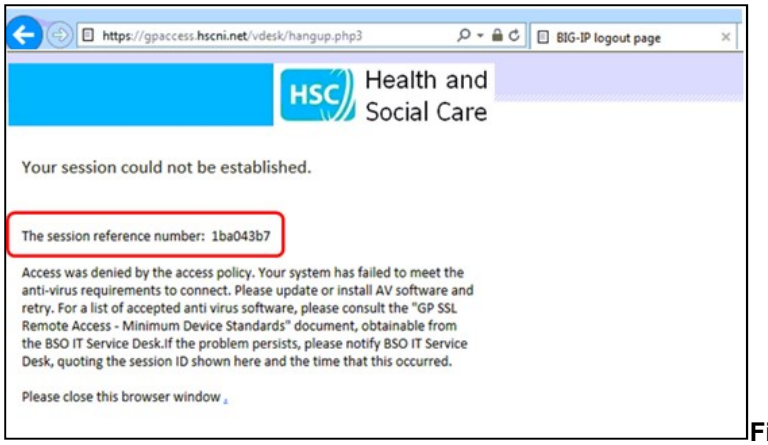
https://gpaccess.hscni.net/vdesk/hangup.php3
BIG-IP logout page
HSC
Health and
Social Care
Your session could not be established.
The session reference number: 1ba043b7
Access was denied by the access policy. Your system has failed to meet the anti-virus requirements to connect. Please update or install AV software and retry. For a list of accepted anti virus software, please consult the "GP SSL Remote Access - Minimum Device Standards" document, obtainable from the BSO IT Service Desk.If the problem persists, please notify BSO IT Service Desk, quoting the session ID shown here and the time that this occurred.
Please close this browser window

Figure 1