

Remote Access

Terms & Conditions of Service

Produced By:	System Support
Reviewed By:	Leonard Veenendaal Technical Services Manager
Team:	ICT Technical Services
Date:	April 2009
Version	2.1
www.cceducation.net Resource ID:	4264

Contents

Introduction	3
Solution Outline	3
Scope	3
Technical Support.....	3
Roles and Responsibilities	3
CCC.....	3
School Utilising Remote Access	4
Charges	4
Enhancements to the service	4
Appendix A: - Detailed Technical Specification	5
Authentication.....	5
Students.....	5
Staff.....	5
Active Directory Authentication:	5
Types of Access	6
Web Access	6
Thin Client Access.....	6
Appendix B: Diagram showing remote access traffic	7

Introduction

Following a lengthy pilot of various methods of providing schools remote access to their local systems via the CCN network, a solution has been implemented based on the findings of these pilots and input from schools. The system provides Staff and Students access to resources within schools, it also provides Staff access to Centrally Hosted MIS which sits within the core infrastructure of CCN. The system provides varying levels of security dependant on the type of user requesting access. The following document outlines the scope of the project, roles and responsibilities, and details the way in which it has been implemented technically.

Solution Outline

A similar mechanism to the schools MTA service is being utilised to provide remote access. This involves locating an SSL Explorer Server (see <http://www.3sp.com> for details of this product) along with an authentication server on DMZs in the E2BN/CCN networks. Requests to school based web/application servers and centrally Hosted MIS are relayed by the SSL Explorer Server. (See *Appendix A* for Detailed Technical Specification).

Scope

- Remote Access for Staff and Students in the context of this project includes Microsoft Remote Desktop, Citrix Java Client, and Web based access. All other forms of access may be considered following a change request; however they are not covered by the current implementation.
- Initial setup costs for remote access are in the year's current SLA. There is a one off cost for all types of remote access.
- A school signing up to a remote access SLA may request access to as many resources as they like, however once this initial list of resources has been setup any subsequent requests to add additional resources will be subject to a change request process and a £50 charge to cover Education ICT Service costs.

Technical Support

As this is a Production Service, standard Education ICT Service support procedures apply.

Schools are responsible for providing 1st Line technical support for any problems arising from accessing the remote support solution

Education ICT Service cannot take calls from students either in school or from home; students must log issues with the school ICT Team.

Technical Support for any issues relating to remote access via SSL explorer should be logged via the Education ICT Service Helpline either via email helpdesk@ict.cambsed.net or by calling 08450 450973.

Roles and Responsibilities

CCC

For the duration of the provision of the remote access service to school systems, CCC, through the Education ICT Service, undertake to:

- Provide hardware, software and expertise to manage remote access based support issues at no additional cost to the school.
- Provide capacity and oversee the scaling of the systems required to maintain quality of service to end users.
- Publish monthly statistics on usage of the system for all schools.

School Utilising Remote Access

For the duration of the provision of the remote access service, the school undertake to:

- Take responsibility for all local server configuration work required and to absorb any financial implications.
- Ensure that all school systems and infrastructure are configured in a manner that is in line with the technical and security standards laid down by the ICT Service and Cambridgeshire County Council Audit & Information Governance teams.
- Ensure that security best practise (as advised by the ICT Service) is maintained in relation to the authentication of remote access users and local server configuration
- Ensure that student accounts are not used by staff to obtain remote access to any school systems.
- Ensure that no student account is able to access ANY sensitive information including but not limited to MIS, Financial data, personal details of staff/students.
- Bear the responsibility and cost of any local software or other licenses required to make use of services provided through the remote access system
- Take responsibility for the consequences of any inappropriate use of the system
- Provide information on request about users of the system (e.g. complete list of usernames including third parties)
- Accept that the school may be subject to unannounced audit visits at any point during the period of service delivery to ensure that security best practise is being followed.

Both CCC and the school retain the right to terminate the remote access service immediately if it is deemed that there is an unacceptable security risk either to the school ICT infrastructure or the CCN network as a result of the service activities; or because bandwidth demands of the Schools Access are leading to a significant deterioration in the quality of other services.

Charges

Use of the remote access system is a chargeable service. The ICT Service will notify schools of the charges each year through its normal Service Level Agreement process. Schools subscribe to the service annually from April to the following March. Should a school fail to pay its subscription by the end of May in any year, the ICT Service retains the right to withdraw the service.

Enhancements to the service

Schools may submit change requests for new features of the remote access system. The ICT Service will do its best to accommodate such requests within the budgets available. However, the ICT Service does not guarantee to implement any such requests. It will consider them in the light of affordability, technical feasibility, effects on other users and the priority accorded to them by all users of the service.

Appendix A: - Detailed Technical Specification

Access to schools systems such as Remote Desktop, Citrix, OWA and CMIS via e-Portal is granted by having requests sent to the SSL Explorer Server, the SSL Explorer Server then requests the user to authenticate to gain access to the network, once the user has successfully authenticated the request is passed on to either the Remote Desktop, Citrix, OWA or e-Portal applications, where the user would once again authenticate to gain access to the application, data from the school server is then be passed back to the client.

At the school a web/application server must be configured to host any services that the school wishes to access, SSL Explorer is located on a DMZ at the E2Bn firewall and configured to publish the school web/application server.

Centrally Hosted MIS is located in the CCN core infrastructure and is managed by the Education ICT Service.

Authentication

The method of authentication to internal resources varies dependant on the type of user requesting access, which in turn dictates the type of resources available to the user. Users are split into two groups Students and Staff:

Students

Student access is based on the assumption that no student will ever have access to any **“Sensitive personal data”** (as defined in the Data Protection act 1998) during a remote access session. Therefore single factor authentication has been deemed adequate for student access. Students must supply a username and password, which is verified against Microsoft Active Directory in order to gain access.

Staff

Staff access is based on the assumption that all staff may access **“Sensitive personal data”** (as defined in the Data Protection act 1998) during a remote access session. With this in mind a second factor of authentication has been added to increase security of information. This second factor of authentication is provided in the form of a key fob, which generates a **“one time only”** password. This password along with a 4 digit PIN must be entered in addition to the network username and password. If the user does not know the username, password, PIN and be have possession of the key fob assigned to that user, at the time they attempt to logon, it is not possible to gain access.

3rd party

Schools may wish to give 3rd party access to external companies and support agencies to allow access to, but not limited to CCTV systems, management of wireless networks and photocopy/print devices. All 3rd party access it based on 2 factor authentication as described above.

Active Directory Authentication:

Users currently authenticate against a central Active Directory managed by the Education ICT Service. This directory is populated with unique user accounts which are either manually created as part of the Centrally Hosted MIS project, or synchronised with the schools local Active Directory via Microsoft Identity Integration Server (MIIS). Future developments will involve authenticating users directly against their local directory servers with the use of Forest Trusts or sub domains.

Schools using MIIS to synchronise accounts, each have one of two groups assigned to their users to distinguish between staff and students. Based on this group membership SSL Explorer prompts them for either single factor or two-factor authentication. The group membership is assigned centrally, however this is based

on the Organisational Unit (OU) the user exists in within the schools Active Directory. Schools are responsible for ensuring the consistency of this information and would be accountable for a user being placed in an incorrect OU for their role i.e. a staff user in a student OU or student user in staff OU.

Types of Access

Two types of remote access are currently implemented, these are web access and thin client access:

Web Access

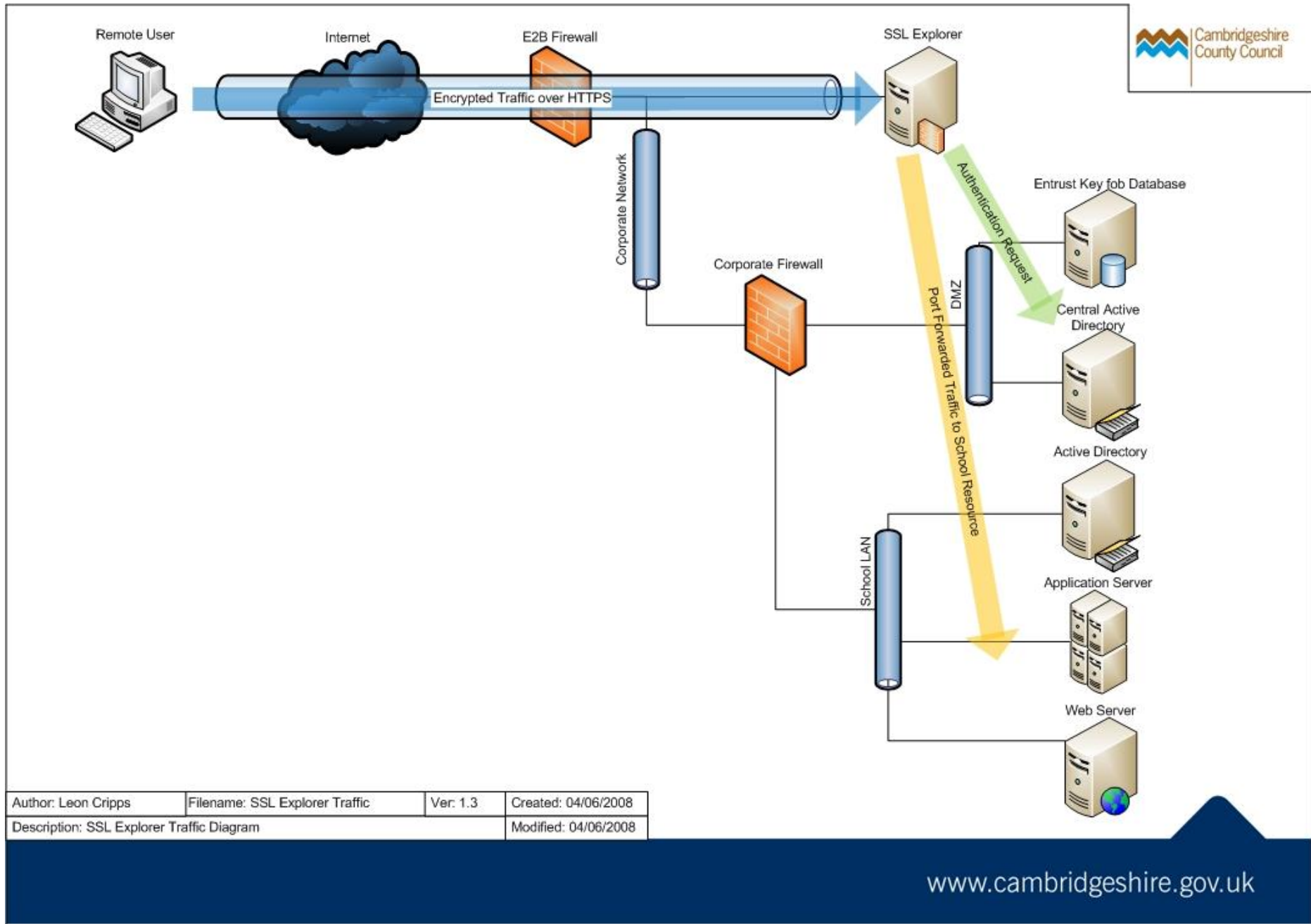
Remote access to web pages hosted within schools is dealt with using a method known as “**reverse proxy**”. As the name implies this means that all requests coming from the Internet, addressed to a school’s Web server, are routed through SSL Explorer, which then makes the request itself to the web server. This has several key benefits:

1. Whether the school web server is set up to use HTTP or HTTPS, requests from the end user to SSL Explorer across the Internet are encrypted.
2. There is no direct access from the Internet to a School’s web server, preventing malicious attacks on school servers through obfuscation or other means.
3. Access to applications can be fully audited and access monitored via warnings and alerts

Thin Client Access

Remote access to thin client software such as Microsoft Remote Desktop and Citrix Java Client are dealt with using a method known as “**SSL VPN**”. The SSL VPN functionality is provided by the *SSL Explorer Agent*. This Agent is a Java application that works in conjunction with your SSL-Explorer session to provide SSL-tunnelling and application launching facilities provided by the SSL-Explorer server. The Agent is launched by a small Java applet placed on all pages that require access to the VPN client. You only need to launch the client once per SSL-Explorer session.

The SSL Explorer Agent opens an SSL VPN tunnel between the local loopback address (127.0.0.1) on the client machine and the SSL Explorer Server over port 443. This is done to ensure no one can spoof the client IP address and maliciously gain access to the SSL VPN tunnel. Once established a random port between 1024 and 65535 is used to connect to the thin client application. The tunnel terminates at the SSL Explorer server, which then port forwards traffic to the thin client server within the school or in the case of Centrally Hosted MIS within the CCN core. Again no direct connection is made between the client machine and the school’s system, traffic is reverse-proxied.



Appendix B: Diagram showing remote access traffic