Lumos PenCS Network Configuration Guide

General Practice Privacy Preserved Linkage

June 2020 – Version 1.3

Overview

Lumos is a state-wide program led by the NSW Ministry of Health in partnership with Primary Health Networks (PHNs) and the Centre for Health Record Linkage (CHeReL). Lumos links general practice data to many health system data collections, shedding light on patient journeys across the healthcare continuum.

The purpose of this document is to provide IT support staff with information to configure GP networks to support the Lumos data extraction from GP practice management systems.

Network Protocols

Host	NAT/Proxy Support
HTTPS	NAT or HTTP Proxy
FTPS	NAT or HTTP Proxy

Network Configuration

Network address translation (NAT)

Outbound Traffic Destination Ports

When Network address translation (NAT) is configured it allows outbound traffic to make connections to the internet without new network configurations. If certain destination ports are filtered there must be provisions made to allow connections to the destination hostnames/ports.

Host	Protocol/Port	Usage	Normal Port State
authentigate.cherel.org.au	TCP 443	HTTPS	Open
csu.cherel.org.au	TCP 991	Implicit FTPS Control	Open
csu.cherel.org.au	TCP 3000 - 3010	Implicit FTPS Data	Closed – Opened Using Control Port

When adding network rules, please ensure that the hostname is used instead of a statically defined IP address, as it could change in the future.

DNS Resolutions

Records should be able to be resolved against public nameservers and return public IP addresses.

Host
authentigate.cherel.org.au
csu.cherel.org.au

Optional HTTP Proxy for Implicit FTPS

Support for HTTP 1.1 proxies is supported by the data extraction process (CAT4). This configuration is pulled from the CAT4 scheduler configuration in the format of “<Hostname>:<Port>”.

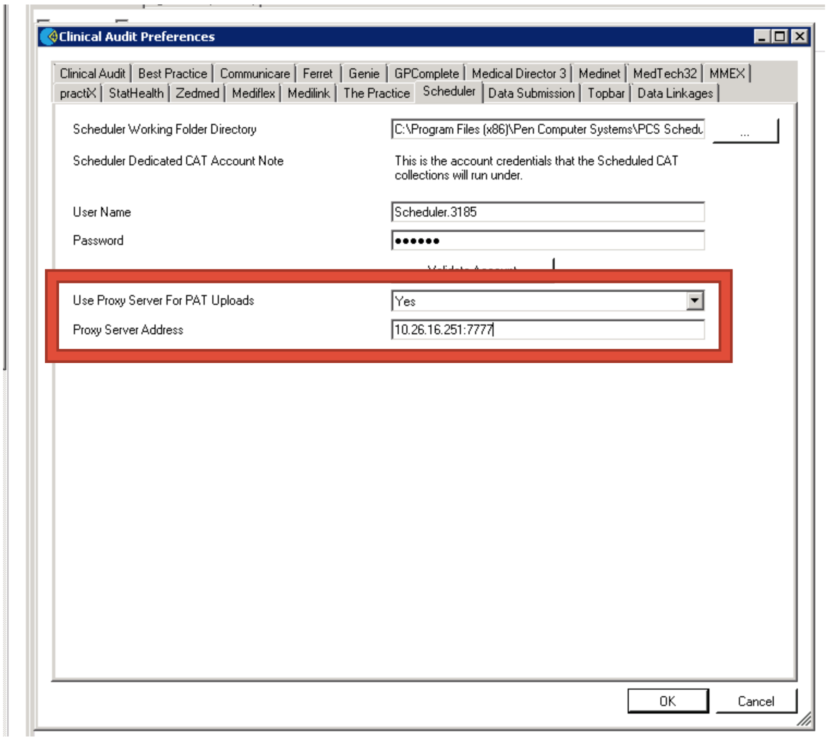
Support for outbound connections needs to include the following protocols and ports.

Host	Protocol/Port	Usage	Normal Port State
authentigate.cherel.org.au	TCP 443	HTTPS	Open
csu.cherel.org.au	TCP 991	Implicit FTPS Control	Open
csu.cherel.org.au	TCP 3000 - 3010	Implicit FTPS Data	Closed – Controlled Using Control Port

When adding exceptions, please ensure that the hostname is used over a statically defined IP address, as it could change in the future.

Setting Scheduler HTTP Proxy (PenCS)

Proxy Server Address is set under the Scheduler Tab in the Clinical Audit Preferences. The format for the Proxy Server Address is “<Hostname>:<Port>”.



Scheduler Working Folder Directory: C:\Program Files (x86)\Pen Computer Systems\PCS Schedu

Scheduler Dedicated CAT Account Note: This is the account credentials that the Scheduled CAT collections will run under.

User Name: Scheduler.3185

Password: ••••••

Use Proxy Server For PAT Uploads: Yes

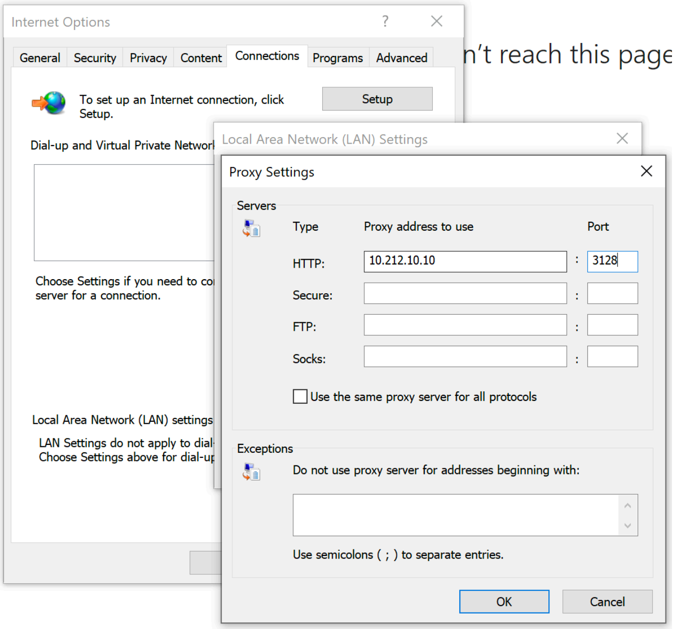
Proxy Server Address: 10.26.16.251:7777

Setting API HTTP Proxy

Calls to the Authentigate API can be setup to proxy through HTTP/Socks proxy by setting it globally within Internet Options > LAN settings > Use proxy server for your LAN. Any exceptions need to be also entered as this configuration impacts all requests from the server.

Intercepting TLS/HTTPS Certificates

HTTP proxy servers that intercept TLS traffic and decrypt communications are supported as long as the certificate authority is located within the local windows certificate manage in the trusted roots folder. Certificate pinning isn’t implemented between Authentigate and the CAT4 application.



To set up an Internet connection, click Setup.

Dial-up and Virtual Private Networ

Choose Settings if you need to co server for a connection.

Local Area Network (LAN) settings

LAN Settings do not apply to dial Choose Settings above for dial-up

HTTP: 10.212.10.10 : 3128

Secure: :

FTP: :

Socks: :

□ Use the same proxy server for all protocols

Exceptions

Do not use proxy server for addresses beginning with:

Use semicolons (;) to separate entries.

SOCKS Proxy Support

SOCKS4/SOCKS5 is not supported at this time within the data extraction process using CAT4.

Operating System/TCP Requirements

When making a TLS handshake it should be done using Transport Layer Security (TLS) 1.2. This applies to both the Authentigate portal and FTPS connections. Older TLS protocols are not supported and are generally considered legacy by the industry. The table below references the actions required to support TLS 1.2 within the Windows security subsystem (SChannel) based on the version currently in-service by the data custodian.

Operating System	Action
Windows XP Windows Server 2003 Windows Small Business Server 2003 Windows Small Business Server 2003 R2	**Not supported** Microsoft is no longer supporting this operating system as of April 2014
Windows Vista Windows Server 2008 SP2 Windows Small Business Server 2008	**Supported with Windows updates and registry changes** Microsoft KB4019276 must be installed for TLS 1.2 support https://support.microsoft.com/en-us/help/4019276/update-to-add-support-for-tls-1-1-and-tls-1-2-in-windows Microsoft no longer supporting this operating system as of April 2017
Windows 7 Windows Server 2008 R2 Windows Small Business Server 2011	**Supported with Windows updates and registry changes** Microsoft KB3140245 must be installed for TLS 1.2 support https://support.microsoft.com/en-ph/help/3140245/update-to-enable-tls-1-1-and-tls-1-2-as-a-default-secure-protocols-in Microsoft is no longer supporting this operating system as of January 2020
Windows 8 & 8.1 Windows 10 Windows Server 2012+ (Including Essentials)	**Supported** No Action Required