



# Glow Firewall Requirements

Date: September 2007

Author: Glow Team

Ref: GC112  
(version: 2.3)

## Firewall Requirements

This document is intended for the person or team responsible for the firewalls within a local authority. Where the local authority is intending to use particular services, please review this latest version to ensure that the relevant configurations are in place.

Some Glow components require that specific ports, other than port 80, must be open on local authority and school firewalls which are on the path between the client workstation and the Glow datacentre.

All Glow services are hosted in the datacentre on a specific range of IP addresses. Therefore, firewall rules need only be set for these addresses.

*Note: This revised document includes ports and the associated IP range for each service provided: Information is listed in Table 1 over.*

*A choice can therefore be made whether to restrict the opening of ports to each service being used or to open for the entire range as noted below.*

### Glow Datacentre range:

IP Range - 212.219.20.0

Netmask - 255.255.255.0

IP Range - 212.219.21.0

Netmask - 255.255.255.192

All TCP ports are **outbound** to the datacentre only, however for components where a secondary data stream is in place, the firewall will either have to understand the protocols concerned and provide full stateful inspection, or permit the inbound secondary data streams from the data centre.

Further information regarding this is noted in the table 1 over:

Application	Firewall Port(s) TCP	Firewall Port(s) UDP	Public IP addresses of service	Client Station Application Pre-requisites*	Additional Notes
Portal	80 and 443		212.219.20.1 and 212.219.20.2 212.219.20.81 and 212.219.20.82	Supported browser	
Glow Meet <sup>1</sup>	443	Destination Ports: 52000-52999 Source Ports: 50000-50999	212.219.20.36 to 212.219.20.38 inclusive	Java Runtime Environment with WebStart or Marratech Software and Java Runtime Environment	
Web Hosting	80 443 21 (FTP) 35000 to 35500		212.219.20.49 to 212.219.20.60 inclusive		Glow will be using FTP-TLS, so a suitable FTP client is required to upload and download files. WebDAV may also be used for this purpose.  TCP 35000 to 35500 are passive FTPS data channels.

<sup>1</sup> We advise that you may (depending on the type of firewall in your infrastructure) need to configure the source and destination ports for Glow Meet connections as follows:

Protocol	Source Port	Destination Port	Destination IP Range
UDP	50000-50999	52000-52999	212.219.20.36

Video Streaming <sup>2</sup>	80 and 443 21(FTP) 8000 35000 to 35500 554 1755 7070	554 1755 34445 to 34459  1024 to 5000 6970 to 32000	212.219.20.33 and 212.219.20.34	A suitable media player is required depending upon the file format(s) being viewed. No guarantees are implied however.	TCP 35000 to 35500 are passive FTPS data channels.  TCP 8000 – Essential port for streaming of content. Additional support for Flip4Mac streaming of Microsoft format files  TCP 554, 1755 and 7070 are control channels.  UDP 1024-5000 - MMS Data  UDP 6970-32000 - RTSP Data (i.e. Real and QuickTime)  UDP 34445-34459 - Client replies to Server (i.e. UDP resends etc)  UDP 1755 - Data resend requests by MMS  UDP 554 - Proxy Server Requests
Mailing Lists <sup>3</sup>	Same as portal		212.219.20.39 to 212.219.20.42 inclusive		

<sup>2</sup> Ports required for MMS and RTSP streaming.

<sup>3</sup> Contained within portal – assumption that authorities already allow sending and receiving of email so SMTP (TCP25) not specified

Glow Chat	80, 443 and 563		212.219.20.43 and 212.219.20.44	Java Runtime Environment	
Secure File Transfer (Securenet)	80 and 443		212.219.20.4	Java Runtime Environment	
Glow Mail <sup>4, 5</sup>	443 993(IMAPs) <sup>6</sup> 995(POP3s)		212.219.20.17 to 212.219.20.19 inclusive and 212.219.20.21		Assumption being that authorities are already sending/receiving email
Virtual Learning Environment	Same as Portal		212.219.20.7 and 212.219.20.8		
Glow Messenger	Same as Portal  5060 5061 5062		212.219.20.10 and 212.219.20.11		TCP 5060 – Used for SIP  TCP 5061 – Used for SIP-TLS  TCP 5062 – Used for address book functionality

Table 1

\*Further information and other recommendations can be found in the Client Requirements document. Details on how to get this are noted at the end of this document.

<sup>4</sup> Using an email rich client will be feasible within Glow, if an authority would like to complement the existing web based version. It is worth noting that the protocols that will be used are IMAP4s and POP3s for this traffic.

<sup>5</sup> If a rich client is used for Glow Mail, mail will be sent on via an authorities own SMTP server. Therefore, no firewall changes will have to be made out to the Glow datacentre for this port. This is also true of home users whereby SMTP traffic will have to be routed out via the end user's ISP SMTP server.

<sup>6</sup> IMAPs and POP3s service are not yet available at the time of release of this document. It is anticipated that these will be available by the end of October 2007. Further information may be obtained from your Glow Technical Contact.

## Other Technical Considerations

### Blocking the word 'Chat'

During the pilot phase it was noted that the configuration of some filtering systems to block the word 'chat' caused the Glow Chat application to fail or work incorrectly. Testing has shown that filtering can prevent certain functionality of Glow from working. It may be necessary to bring forward further recommendations of this type.

### Consistency of client IP address

During the pilot phase of Glow an issue was encountered where a chain of proxies between the client browser and the Glow system caused the public IP address of the client session to change during the session. This invalidated the Glow session cookie and caused the session to fail. A re-authentication screen was then generated with the prompt "NetPoint Basic over LDAP".

The session cookie is the mechanism by which a current session is identified by the Glow Authentication system. It is essential that the IP address of the client remains unchanged throughout a session.

## Further Considerations

Additional port requirements may be added as development continues with Glow applications – information in this context will be made available as necessary. Furthermore, the list of ports requirements may be reduced in the future.

Finally, the JANET Videoconferencing Service (JVCS) is the only available route for existing H.320 or H.323 video conferencing endpoints to interoperate with the Glow Meet service. It is expected that port requirements are already in place to allow H.323 VC endpoint to connect to JVCS across authorities so therefore no changes for Glow will have to be made.

If there are issues regarding this or any other firewall related queries, please contact Glow Support using the details below.

Email: [glowsupport@rm.com](mailto:glowsupport@rm.com)  
Tel: 0845 130 2213

Further information is provided as part of the Client Requirements and Network Bandwidth Requirements documents. These are available to download from the LTS website (<http://www.glowscotland.org.uk/training/toolkit/technical.asp>) or are available on request by emailing [glowsupport@rm.com](mailto:glowsupport@rm.com)