

Appendix A - Deployment Security Checklist

This checklist is intended as a guide for site administrators. It may not be an exhaustive list of issues (this will vary depending on the site security policy, for example), but should be of assistance as a starting point.

Task	Note
Plan deployment topology for H.323 equipment.	
Check H.323 capabilities of the site firewall.	
Establish security policy for H.323 equipment and implement on site firewall.	
Determine if an H.323 proxy is to be used for either policy or technical reasons (e.g. is NAT used inside the site for H.323 terminal addresses?).	
Establish access methods for the H.323 terminal location, whether by lock and key, or under supervision.	
Prevent H.323 terminal users from altering configuration settings on the terminal during a session.	
Run port scanner against site's H.323 equipment to understand open services, and remove unnecessary services.	
Turn off gatekeeper IP multicast discovery if not used (where gatekeeper deployed).	

Ensure topology from campus border router and from any management stations to the H.323 terminal is run over dedicated connections or switched Ethernet paths.	
Check and change default user names and passwords on H.323 equipment.	
Schedule checks for software and firmware updates, and subscribe to appropriate security-related mailing lists for your H.323 equipment.	
Use source IP addresses to control participants that can connect to MCU devices (Janet Videoconferencing service connects out to participants from the MCUs).	

Source URL: <https://community-stg.jisc.ac.uk/library/janet-services-documentation/appendix-deployment-security-checklist>