# LGfL Security Guidance

# June 2016



---

## 1. Introduction

The London Grid for Learning Trust takes its responsibilities for the security of the private network and its users very seriously by determining policy and ensuring that appointed suppliers implement this policy.

The policy acknowledges that web-based remote access products could bypass LGfL's core firewall and usage policy rules. These have been divided into 3 categories within the LGfL 2.0 network.

## 2. Remote Access Categories

LGfL has three categories for Remote Access services that connected schools use across the LGfL 2.0/TRUSTnet infrastructure.

Category 1 tools are USO-authenticated, ensuring that remote access facilities can be routinely provisioned (and more importantly, automatically removed when a user leaves an establishment), due to being linked to LGfL USO. Services benefitting from this include RAv3 (Cisco SSL VPN services), CentraStage, LogMeIn Rescue Enterprise (LGfL USO Edition), and a Remote Desktop Gateway to support schools' 'Terminal Servers'.

Category 2 tools are everything else (bar category 3 tools) as they are not USO-integrated and therefore their manually-created accounts represent a clear risk to the school, due to the need for additional manual intervention if a user leaves.

Category 3 tools are services that are, from time to time, classified as introducing significant security concern and therefore will not be permitted.

### Category 1

Category 1 tools (RAV3, CentraStage and LogMeIn Rescue Enterprise) are, by default, allowed access to the LGfL 2.0 network and once commissioned require no further requests or support cases to enable their use.

These products, combined with LGfL USO, allow a granular approach to permissions, so that any abuse that is identified can be managed without disturbing the use of services for other users.

Category 1 tools RAv3 and CentraStage are provided free for use by subscribing schools and their support partners, in order to establish secure remote access and device management.

LGfL strongly recommends the adoption of RAv3 and CentraStage or another Category 1 tool. LGfL's policy is for all users to migrate over time to Category 1 tools. LGfL is committed to working with Remote Access application suppliers to add more tools to Category 1.

LogMeIn Rescue Enterprise, authenticated by LGfL USO and OTP tags, is a Category 1 tool, but the technician providing support must have a valid subscription to LogMeIn Rescue Enterprise.

### Category 2

Products in this category set provide the ability to gain access to services located in school from the Internet.

It should be noted that allowing such proxy avoidance services to run circumnavigates the filtering system in place across LGfL 2.0. LGfL and its agents are unable to offer support on the use or mis-use of products in this category set.

These tools do not make use of LGfL USO, permissions are 'on for all' and any management of abuse will impact on all users of these services. This category of tools can be authorised for an establishment by the Head Teacher. To do this the Head Teacher should visit…

https://support.lgfl.org.uk/secure/myacc/ht/declarations.aspx

…to confirm agreement and understanding of the risks and issues relating to using this category set.

Due to the increased risks involved with the use of tools in this category, the school will need OTP (One Time Password) second factor authentication tags for all Nominated Contacts and the Head Teacher.

These tags can be purchased at:

https://shop.atomwide.com/ProductDetail.aspx?id=135&cat=7

LGfL recognises that users and their support agents have existing tools and methods. LGfL does not wish to ban all remote access products, and will always attempt to allow users to employ tools with which they are familiar until such time as any tool is objectively assessed to be inappropriate for use on the LGfL 2.0 network.

For this reason it is not possible to publish a comprehensive list of 'allowed' and 'disallowed' products; security requires more than a good product, it also requires good practice. Products will be deemed as acceptable by LGfL until otherwise known to be a threat to security.

## Category 3

The products in this category are not permitted on LGfL 2.0, as they do not offer appropriate granular control or reporting, so any abuse would be impossible to contain or act against. This will have an un-predictable effect on other LGfL users. Products in this category may circumnavigate firewalling and security.

The blocking of Category 3 products is also designed to ensure safety and security of pupils and staff. For example a third-party support provider using a Category 3 classified product with a number of schools had a staff member who was arrested on child-related charges and subsequently bailed, but their access to the PCs used by children on a daily basis remained open and un-monitored by any appropriate authority.

LGfL's Support of remote access products is limited to those in Category 1.

The LGfL Technical Steering Board:

- strongly recommends the use of just products located in Category 1
- encourages schools NOT to use products in category 2 or 3
- permits the use of products in category 2, but with the explicit permission of the Head Teacher who additionally takes on the ownership of the risk
- does not permit products in category 3

## 3. RAv3

The LGfL 2.0 service includes a remote access system called RAv3 (LGfL Remote Access v3). This is a Cisco-based encrypted solution that allows specified users IP-level access to a school's network in an auditable way. The RAv3 service must be enabled by the Head Teacher who, under the Data Protection Act 1998, is responsible for the security of the school's data.

The RAv3 service can offer specified USO account holders a range of access options, from full access to anything on the school's local network, to a limited remote view of a single desktop. In this way, an IT Manager can have complete network access and a Bursar can just remotely access their school office workstation from home.

Further details on how to set up and configure this service is available here:

https://support.lgfl.org.uk/secure/guide/WebGuide/Help.html?ras_user_guide.html

The Head Teacher must activate the RAv3 product by visiting the page of the LGfL Support Site linked below and approving its use, thus releasing the service for configuration by the school's Nominated Contact:

https://support.lgfl.org.uk/secure/ras/resources.aspx

Processes that can be successfully run over the RAv3 connection include:

1.Microsoft Remote Desktop services function over the RAv3 connection and, once enabled on the target workstation, terminal services, or other servers (in Admin connection mode), allow users to interact much as if they were actually sitting in front of that device at the school.

Further details can be found here:

https://support.lgfl.org.uk/secure/guide/WebGuide/Help.html?ras_user_guide.html

Client software for this is typically included in the operating system (OS) for both Windows PCs and Mac OS devices, while a range of compatible 'apps' for such devices as iPads and iPhones is available from third party vendors.

2. Windows 'shares' (CIFS) can be 'mapped' directly to users via RAv3, offering simple file-level access to the user's home area or shared resources on network servers or workstations.

3. Microsoft Remote Assistance functions over the RAv3 connection. Once enabled on the target workstation, it will allow a remote user to 'take over' the workstation so that the user on the target workstation can see what is happening on that machine. Using this mode of connection, the remote user can demonstrate a process to, or have their activity 'witnessed' by, a local user who is sitting in front of the device. This offers an ideal scenario for support and/or one-to-one training.

Client software for this is typically included in the OS for Windows PCs.

4. Full VPN functionality can be enabled for those users who require an IP-encrypted tunnel between the remote machine and their establishment's network – the freely available Cisco AnyConnect (or mobile equivalent) client will allow this. The service delivers an encrypted SSL IP level 'tunnel' between the local and remote systems via RAv3. Further details can be found here:

https://support.lgfl.org.uk/secure/guide/WebGuide/Help.html?ras_user_guide.html

5. VNC connections can be established over a RAv3 connection, in a secure setup with traceability, which will provide access to a remote desktop. There are many variants of VNC for client machines, all of which are compatible with RAv3 and provide a wide range of remote access solutions; some are available for free download. Further details can be found here:

https://support.lgfl.org.uk/secure/guide/WebGuide/Help.html?ras_vnc.html

## 4. CentraStage / Autotask

The LGfL 2.0 service now includes a licence for CentraStage OnDemand to facilitate formal remote network support. .

All LGfL 2.0 customers will be able to install CentraStage on Windows devices (with Mac OS X and iOS support to follow) at no additional charge. The OnDemand service provides secure, audited remote access into every device, from anywhere, as well as providing a complete hardware and software inventory of a school network. CentraStage will integrate with LGfL USO accounts that are enabled for use with a USO-OTP tag. The remote support capability includes:

Remote screen share and RDP access
Remote command line
Remote task manager
Remote Windows service management
Remote event log viewer
Remote registry editor
File transfer

An upgrade licence to the CentraStage IT Management suite is available to provide a complete and automated remote management system for use by third party support companies allowing unattended access to remote devices for remote upgrade, maintenance etc. Traceability of access is maintained for security purposes.

CentraStage IT Management on LGfL 2.0 is a hosted IT management solution, bringing centralised visibility, control and automation to IT support in schools.

As an enhancement to the standard CentraStage platform provided by LGfL, the fully-featured version is available as an upgrade to LGfL customers and their IT support organisations. For further information see:

http://services.lgfl.net/

When used to the fullest extent, CentraStage delivers:

- Audit/asset management – know what you've got out there in schools, and what you are supporting.
- Monitoring – know what's gone wrong, and potentially what is about to go wrong. Reduce downtime, and improve device availability and performance.
- Deployment – deploy software, drivers, updates, etc., centrally out to schools. Keep your environment secure, patched and stable.
- Remote support – audited, integrated remote diagnostics and support into any device from any network.
- Reporting – report on your supported assets, the health of your estate, your activity levels. Keep yourselves and your customers informed.

The CentraStage product from LGfL has been configured to allow access to USO users who have a valid OTP tag associated with their account. Tags are available from the shop site:

https://shop.atomwide.com/ProductDetail.aspx?id=135&cat=7

To enable CentraStage for your school your Nominated Contact must raise a support case via:

https://support.lgfl.org.uk/

## 5. LogMeIn Rescue Enterprise (LGfL authenticated version)

LGfL has worked with LogMeIn to arrange that LogMeIn Rescue Enterprise is able to authenticate users using LGfL USO, and can therefore be placed in Category 1. This service requires second factor authentication by OTP tag.

Other LogMeIn products such as LogMeIn Central, and the free versions of LogMeIn, can be accessed under Category 2

LGfL's LogMeIn Rescue Enterprise solution delivers full traceability, and supports granular per-school control over users' access. In the interests of control and accountability, this option remains strongly advised for all schools making use of the LogMeIn services.

## 6. Hosted WebEx Conferencing

LGfL now provides a centrally hosted and managed WebEx facility that allows schools to organise their own online conferences and meetings which include live video and screensharing. As the server is hosted within the core of the network, web filtering settings will not need to be adjusted to use this functionality. Users with many different types of devices are capable of participating in WebEx meetings from any location.

The service is available to all staff in LGfL-subscribing schools. Meeting requests must be submitted to the LGfL Service Desk with details of time, date, meeting duration and email addresses of everyone involved. Meetings will be organised on the school's behalf but delegate responses must be managed by the school. Instructions will be provided when a meeting is requested.

## 7. Other

In the interests of sound security policies, requests made for the opening of firewall ports should be kept to the minimum required to permit the intended applications to function, and limit port access to the specific IP address range which is necessary.

LGfL does routine intrusion detection checks.

Many otherwise adequate security tools can be rendered insecure by poor practice, and LGfL strongly encourages all concerned to observe sensible security arrangements, such as two-factor authentication, and absolute secrecy with respect to passwords. Any school-selected security tool should be fully described in the school's own security policy. To illustrate this, an 'industry strength' router can be rendered completely insecure if installed and left to run with the as-supplied default username and password.

## 8. RD Gateway Servers

LGfL provides a secure RD (Remote Desktop) gateway by exposing the encrypted port 443 to the Internet. The service provides an initial layer of authentication against the user's USO credentials and, when successfully authenticated, the user is passed onto a school's own locally-hosted Microsoft server running a target RD session. At this point, local authentication will be needed.

The service is available to both staff and pupils alike, and the USO system provides a granular level of control over access, so for example Year 7 and 8 students and staff can be granted access and all other users denied access.

This service is delivered in a resilient manner.

Inbound access to the LGfL 2.0 network over tcp port 3389 is not allowed as a result of the availability of this service.

Schools not wishing to use this centrally-provided service can install their own RD Gateway Server and expose it to the Internet on tcp port 443 by raising a MIP support case on the LGfL USO Support Site.

## 9. Category 2 - Head Teacher's Declaration

This declaration

https://support.lgfl.org.uk/secure/myacc/ht/declarations.aspx

is visible on the support site but only to Head Teachers, and is used to gain consent from a Head Teacher to the release of Category 2 remote access services into their school.

For the Head Teacher to be able to accept this statement online, the Head Teacher must be using an OTP second factor authentication tag.

*I have read and understand the security policy operated by LGfL across the LGfL / TRUSTnet network available to me on this page.*

*I acknowledge that LGfL provide a number of remote access products incorporating a high degree of security and traceability.*

*There are remote access products that I wish my school to make use of that fall into Category 2 of the remote access software definitions.*

*I wish my establishment to make use of these products.*

*I acknowledge that this imposes an increased level of risk to both my establishment and the LGfL WAN as a whole and agree that myself and the Nominated Contacts within my establishment will make use of OTP 2nd Factor authentication to protect the data held by my establishment, and LGfL and its agents.*

*I hereby confirm my agreement to take full and sole responsibility for any issues arising from the use or deployment of any remote access products enabled Category 2 within, or from, my school.*