Acellus Set-up Technical Note

Setting Up Acellus Teacher Administration

The Acellus Learning System has been designed to provide a reliable resource to store student progress information. Every effort has been made to make the system fault tolerant and effective. To prevent tampering with student databases, the system is protected with GoldKey security.

All student data is stored at the International Academy of Science data center. Acellus courses are delivered over the Internet and do not require a local server. If the number of simultaneous users exceeds the local Internet connectivity, a local Media server can be installed at the school. The local Media server is used to deliver video and other multimedia to students over the local network, but student data is still stored at the central data center where it can be backed-up and protected. Schools with local Media servers also have a reduced license fee per student.

Troubleshooting Acellus Teacher Sign In

To sign into Acellus, teachers will need to authenticate using a GoldKey Token. To do this successfully, a teacher will need access to servers in the following IP ranges over **ports 80 and 443**:

12.171.56.0/25 (255.255.255.128) — Primary range used for administration.
12.154.57.0/25 (255.255.255.128) — Back-up range used for system fail over.
172.85.76.0/22 (255.255.252.0) — Back-up range used for system fail over.

If a teacher is not able to sign into Acellus or create a Gold Identity account, they may see one of the following messages:

> Connecting to server GoldKeyVault.com ...
>
> Failed to communicate with GoldKeyVault server. The server connection timed out. Please check your connectivity and try again later.

These symptoms indicate that the GoldKeyVault software cannot communicate over port 443 with IP addresses in the ranges listed above. The problem with the outbound connection may be caused by any of the following.

Network Firewall / Proxy Filter

Many networks utilize a proxy server to analyze and filter web content. Please make sure that your network firewall and proxy filter are configured to allow outgoing traffic to the IP ranges listed above.

Such proxy servers should be configured to allow all traffic to goldkeyvault.com. This will allow the GoldKeyVault application to perform the authentication that is necessary in order for you to sign in to Acellus.

Proxy settings on the Client Computers

Unless your network is using a transparent proxy, proxy settings must be configured on each client computer. In Windows, your proxy settings can be configured by opening Internet Explorer and selecting Tools -> Internet Options -> Connections -> LAN Settings.

To add exceptions for your proxy server, click on the Advanced button in the Proxy Server section and enter the following list in the Exceptions section:

acellus.com;

*.acellus.com;

goldkey.com;

*.goldkey.com;

goldkeyid.com;

*.goldkeyid.com;

goldidentity.com;

*.goldidentity.com;

goldkeyvault.com

Windows Firewall

The Windows Firewall can be configured to block outgoing connections by default. When computers are configured in this way, outgoing connections that do not match an explicit rule will be denied. Outgoing rules should be enabled to allow outgoing traffic to the IP ranges listed above, over ports 80 and 443. In some cases, you may also need to specifically allow outbound traffic from the GoldKeyVault application.

The Windows firewall for each client can be configured using an Active Directory group policy, or through the Windows Firewall with Advanced Security on each client.

Opening Windows Firewall Configuration using Active Directory

Log in to your Active Directory controller and open Group Policy Management from under Administrative Tools. From the tree on the left, find the domain you would like to modify and expand Group Policy Objects. Then, right-click on the Default Domain Policy and click Edit, and then select Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Windows Firewall with Advanced Security -> Windows Firewall with Advanced Security -> Outbound Rules.

Note: *It may take a while for the new group policy settings to propagate to client workstations. To force an update on a workstation after you have changed the policy settings, log in as an administrator on the workstation, open the command prompt and run the gpupdate command.*

Opening Windows Firewall Configuration on the Workstation

From a client computer, open Control Panel and select System and Security -> Windows Firewall and click on Advanced Settings. You may also search for Windows Firewall with Advanced Security in the Start menu.

Creating a New Rule in the Windows Firewall

Once you have progressed to this point, the firewall configuration is the same whether you are managing it through Active Directory or on the client workstation itself.

Click on Outbound Rules and select New Rule from the Action menu. When you are asked to select the type of rule you would like to create, select Custom and click Next -> Next -> Next. On the Scope screen, choose to specify the list of remote IP addresses. For each of the IP ranges listed above, click on Add, enter the range into the IP or Subnet field, and click on OK.

Finally, click on Next -> Allow the connection -> Next -> Next, specify the name of the rule as “Unblock Acellus,” and click Finish.

For technical assistance, please call your Acellus Coordinator or Technical Support at (877) 411-1138 (toll free) or (816) 229-3800.