

Elluminate Live! Access Guide

This guide is provided to Elluminate *Live!* users to assist them to make a successful connection to an Elluminate *Live!* session through a proxy firewall. In some cases settings discussed in this document are controlled by the user's System Administrator. If this is the case, intervention by that System Administrator will be required.

This document contains the information on:

- Launching Elluminate Live!
- Configuring Proxy Settings
 - Step 1: Gathering Proxy Information
 - Windows
 - Solaris
 - Mac
 - Step 2: Entering Proxy Information into Java Web Start
 - Step 3: Entering Proxy Information into Elluminate Live!
 - Configuration Difficulties
- System Administrator Information

Launching Elluminate Live!

The Elluminate *Live!* eLearning and Web Conferencing solution is launched when a user clicks on a link in an Internet browser or email. Clicking the link downloads a small Java Network Launching Protocol (JNLP) file containing the information necessary to connect to an Elluminate *Live!* session. Java Web Start launches, reads the information in the JNLP file, ensures that the proper Java Resource (JAR) files are in place, and makes the connection to the Elluminate *Live!* server.

Java Web Start detects the proxy settings used by the default Internet browser on the connecting system, and uses the same settings during the connection process. Java Web Start supports most proxy configuration scripts and can detect proxy settings in most environments. If Java Web Start cannot detect the proxy settings, it will prompt to specify them. In this case it will be necessary to manually configure Java Web Start's proxy settings in order to launch Elluminate *Live!*. Java Web Start will also prompt for username and password should it encounter an authenticating proxy.

Configuring Proxy Settings

STEP 1: (Gathering Proxy Information)

Windows

1. Click on the **Start** menu and select **Control Panel** (Start \rightarrow Settings \rightarrow Control Panel)

- 2. Open your Internet Options control
- 3. Select the Connections tab
- 4. Click on LAN Settings...



5. If 'Use a proxy server for your LAN' is checked, record the information listed beside Address and Port. If proxy Address and Port number information is not available or not present, contact your System Administrator.

Local Area Network (LAN) Settings	? ×
Automatic configuration Automatic configuration may override manual settings. To ensure use of manual settings, disable automatic configuration.	the
Automatically detect settings	
Use automatic configuration script	
Address	
Proxy server	
Use a proxy server for your LAN (These settings will not apply dial-up or VPN connections).	to
Address: 255.255.1.1 Port: 8080 Advanced.	
Bypass proxy server for local addresses	
OK Canc	el

6. If 'Use a proxy server for your LAN' is checked, but the Address or Port is null, click the Advanced button and record the information next to HTTP (or Gateway). If proxy Address and Port or not present, contact your System Administrator.

Proxy Set	tings		? ×
⊂Servers			
<u>_</u>	Туре	Proxy address to use	Port
<u>¢</u>	HTTP:	255.255.1.1	: 8080
	Secure:	255.255.1.2	: 8080
	FTP:	255.255.1.1	: 8080
	Gopher:	255.255.1.1	: 8080
	Socks:		:
	🔲 Use the sa	ame proxy server for all protoco	ls
Exceptio	Do not use pr	oxy server for addresses beginr is (;) to separate entries.	ning with:
		ОК	Cancel

Apple Mac OS X

- 1. Open your System Preferences
- Select Network
 Select your connection device from the Show drop-down box

L	ocation: Automatic	
	Show: Built-in Ethernet	
TCP/	IP PPPoE AppleTalk Proxies Ethernet)
Configure IPv4:	Manually	
IP Address:	192.168.100.102	
Subnet Mask:	255.255.255.0	
Router:	192.168.100.1	
DNS Servers:	192.168.1.11 192.168.1.12	
Search Domains:	corp.elluminate.com	(Optional)
IPv6 Address:		
	Configure IPv6	?

4. Select the **Proxies** tab

00	Network
Show All	Q
Location: Auton	natic
Show: Built-	in Ethernet
	AppleTalk Proving Ethernet
	Appletaik Proxies Ethernet
Configure Proxies: Man	ually
Select a proxy server to configure:	Web Proxy Server
FTP Proxy	255.255.255.0 : 8080
Web Proxy (HTTP)	
Secure Web Proxy (HTTPS)	Hoxy server requires password
Streaming Proxy (RTSP)	Set Password
Exclude simple hostnames	
Bypass proxy settings for these Hos	sts & Domains:
🗹 Use	e Passive FTP Mode (PASV)
n	
Click the lock to prevent further cha	anges. Assist me Apply Now

5. Copy down the information in the Address and Port fields from either Web Proxy or Secure Web Proxy

If this information is not available or not present on your computer, you will need to contact your System Administrator for assistance.

Solaris

Mozilla

- 1. Open Mozilla
- 2. Select **Options** from the **Tools** menu
- 3. Select the Advanced button and then select the Netwok tab
- 4. Select the Settings button in the Connection area

Options							×	
†		0	3	6		<u></u>		
Main	Tabs	Content	Feeds	Privacy	Security	Advanced		_
General	Network L	Jpdate Enci	ryption					
-						6		Select Settings Button
Conne	ection						5	
Config	gure how F	iretox conne	ects to the	Internet		S <u>e</u> tting:	5	
⊂ Cache								
Use u	pto 50	MB of s	pace for th	e cache		Clear N	ow	
				ОК	Car		Help	

5. Record the address and port numbers listed under Manual proxy configuration

С	onnection Settings			×		
ſ	- Configure Proxies to a	Access the Internet				
	Direct connection to the Internet					
	 Auto-detect pro> 	y settings for this net <u>w</u> ork				
	⊙ <u>M</u> anual proxy co	nfiguration:				
	HTTP Proxy:	255.255.255.0	<u>P</u> ort:	8080		
		Use this proxy server for all p	rotocols			
	<u>S</u> SL Proxy:		Port:	0		
	ETP Proxy:		Po <u>r</u> t:	0		
	<u>G</u> opher Proxy:		Port:	0		
	SO <u>C</u> KS Host:		Por <u>t</u> :	0		
	<u>N</u> o Proxy for:	localhost, 127.0.0.1				
		Example: .mozilla.org, .net.nz, 19	2.168.1.	0/24		
	O Automatic proxy	configuration URL:				
	Reload					
,						
		OK Cance		Help		

Netscape

- Open Netscape
 Select Preferences from the Edit menu
- 3. Expand the **Advanced** menu and select **Proxies**
- Click the View button beside Manual Proxy Information
 Record the address and port numbers listed beside HTTP Proxy and Security Proxy

Step 2: (Entering Proxy Information into Java)

Windows

Open Java Application Manager

- Click on the Start menu and select Control Panel (Start → Settings → Control Panel)
- 2. Select Java



3. From the General tab, select the Network Settings button



4. In the pop-up, click the button to **Use proxy server**. Then enter the information you copied before into the Address and Port boxes.

Network Settings	×
Network Proxy Settings	
Override browser proxy settings.	
O Use browser settings	
 Use proxy server 	
Address: 255.255.1.1 Port: 3081 Advanced]
Bypass proxy server for local addresses	
 Use automatic proxy configuration script 	
Script location:	
O Direct connection	
OK Cance	:

Apple Mac OS X

Please proceed to Step 3.

Solaris

Open Java Application Manager

- Solaris: Open a Terminal window and type javaws.
 From the General tab, select the Network Settings button



3. In the pop-up, click the button to **Use proxy server**. Then enter the information you copied before into the Address and Port boxes.

Network Settings	×
Network Proxy Settings	
Override browser proxy settings.	
O Use browser settings	
 Use proxy server 	
Address: 255.255.1.1 Port: 3081 Advanced	
Bypass proxy server for local addresses	
O Use automatic proxy configuration script	
Script location;	
O Direct connection	
OK Cance	el

STEP 3: (Entering Proxy Information into Elluminate *Live!*)

The proxy information should pass automatically from Java Web Start to Elluminate *Live!*. If it does not, a Connection Failed error message will appear, and it may be necessary to manually configure the proxy settings in Elluminate *Live!*. In this step, Elluminate *Live!* will be manually configured to use a specified address and port number to connect to a proxy.

1. Cancel the authentication process by clicking the **Cancel** button when prompted to try again in the Elluminate *Live!* environment.

Connect	ion failed	×
0	Connection failed. Direct call to EL02.ELLUMINATE.COM:2187 failed. Operation timed out: connect Direct call to EL02.ELLUMINATE.COM:80 failed. java.io.IOException: Server is not a JINX server HTTP/1.0 400 Bad Request Try again? OK Cancel	

- 2. Select Tools (on a Mac, select the "Elluminate Live!" menu)
- 3. Select Preferences
- 4. Select General
- 5. Select Proxy Settings

- 6. In the Method field, select 'HTTP Proxy Server'.
- 7. Enter the proxy address recorded in the step above into the **Server** field, and the port number into the **Port** field.

Preferences		E
Application Sharing Filtered Keys Hosting Options Remote Control Simulated Keys Audio Level Control Mute Sound Sample Rate Silence Suppression Froxy Settings Profile My Profile My Profile Session Connection Video Frame Rate Window Settings Whiteboard StarOffice Installation	Method: HTTP Proxy Server Server: 255.255.1.1 Port: 8080	
Restore Defaults 🔻	OK Apply Cancel	

8. Select Apply

- 9. Select Ok
- 10. Select Join Session from the Session menu.
- 11. If this fails, go back to step 6 and select 'HTTPS Proxy Server'.

© Preferences	Σ	(
Application Sharing Filtered Keys Hosting Options Remote Control Simulated Keys Level Control Mute Sound Sample Rate Silence Suppression General Hot Keys Proxy Settings Profile My Profile My Profile Session Connection Frame Rate Window Settings Whiteboard StarOffice Installation	Method: HTTPS Proxy Server Server: 255.255.1.1 Port: 8080	
Restore Defaults 🔻	OK Apply Cancel	

Configuration Difficulties If a connection still cannot be established to the session, contact your System Administrator. Further configuration may be required to allow connection to an Elluminate *Live!* session.

System Administrator Information:

What are we trying to do:

The Elluminate *Live!* eLearning and Web Conferencing solution is launched when a user clicks on a link in an Internet browser or email. Clicking the link downloads a small Java Network Launching Protocol (JNLP) file containing the information necessary to connect to an Elluminate *Live!* session. Java Web Start launches, reads the information in the JNLP file, ensures that the proper Java Resource (JAR) files are in place, and makes the connection to the Elluminate *Live!* server.

Java Web Start detects the proxy settings used by the default Internet browser on the connecting system, and uses the same settings during the connection process. Java Web Start supports most proxy configuration scripts and can detect proxy settings in most environments. If Java Web Start cannot detect the proxy settings, it will prompt to specify them. In this case it will be necessary to manually configure Java Web Start's proxy settings in order to launch Elluminate *Live!*. Java Web Start will also prompt for username and password should it encounter an authenticating proxy.

Addresses, Ports and Protocols

If a user is attempting connection to a session running on one of Elluminate's servers, it will be made to one of the following servers:

Since Elluminate uses dynamic server assignment, it is not possible to state in advance precisely which server will host a session. This means the IP Address is known only when the session actually starts. As a result, please ensure firewalls (and proxy systems) allow access to the entire set of Elluminate hosts in the domain **elluminate.com** and to the following IP Address ranges:

- 216.220.49.208 with netmask 255.255.255.240 (in CIDR notation: 216.220.49.208/28)
- 65.110.166.160 with netmask 255.255.255.224 (in CIDR notation: 65.110.166.160/27)
- 74.200.25.224 with netmask 255.255.255.224 (in CIDR notation 74.200.25.224/27)

Enabling access to both of the address blocks listed will reduce the impact of any configuration changes that Elluminate might make.

Elluminate *Live!* connects on one of two ports 2187 or 80 for unencrypted sessions; when session encryption is used, port 443 is used instead of 2187. We need to establish a connection on one of these two ports. Once this connection has been made it will remain open and transfer all communication which is a proprietary protocol called the Collaborative Communication Framework (CCF), which is layered on a TCP transport protocol.

Firewall and web content filters must allow the download of both JNLP files (or content types) and JAVA application archive (JAR) files. The desktop client system must be configured to allow the download, installation, and execution of JAVA network applications. In addition, the end user must have these permission.

Please Note:

- Only authorized clients may connect to an Elluminate *Live!* Server
- The connection is always initiated from the client
- After connecting, only the Elluminate *Live!* server will send data to the client

For more information, and access to a 24-hour Configuration Room which you may use to test a system's ability to login to an Elluminate *Live!* session, visit www.elluminate.com/support.

If you have any further questions, please contact us for support. Thank you.