Philadelphia Stock Exchange

Remote XL & XLE Services
Client Requirements Guide

Version: 1.3
December 1, 2006

Document Revision History

Date	Version	Updated By	Description of Changes
04/18/2006	Draft 0.1	David Marinoff	First Draft
05/08/06	1.0	David Marinoff	Published Document, added IE trusted sites steps
06/08/06	1.1	David Marinoff	Added hostname resolution for RADIANZ clients
06/26/06	1.2	David Marinoff	Edited hostname requirements and general updates from Annette Ward
12/01/06	1.3	Annette Ward	Update document for XLE services and generalize verbage.
01/08/07	1.3	Annette Ward	Edited page numbering

Table of Contents

1.0 Executive Summary

The Philadelphia Stock Exchange (PHLX) is providing remote access to some of its XL Service Desk applications and XLE Broker Cross system. For remote clients to connect to these services they must support certain networking and client workstation requirements. This document outlines the requirements for: network connectivity, hostname resolution, firewall ports, and client workstations.

PHLX is using a number of technologies including Citrix Presentation Server, Citrix Web Interface, and Citrix Secure Gateway to provide clients access to PHLX applications remotely. By utilizing these technologies the communications between the remote client and PHLX will minimize bandwidth and complexity for the clients, while providing a secure and stable solution.

Clients will utilize Internet Explorer (IE) to connect to a webpage for authentication, download a client plug-in, and to open their applications. All traffic will be encrypted by SSL.

1.1 Intended Audience

This document is written for the technical support personnel of the client firm who will be providing network, firewall, and workstation services to the end user. This document is not a step-by-step guide on how to configure these requirements, it is assumed the people providing technical support at the client firms have the technical acumen to configure their systems.

2.0 Network Requirements

To connect to PHLX Services remotely, three network requirements must be fulfilled: the clients must have network connectivity to PHLX through private lines, XLServiceDesk.phlx.com must resolve to an IP via the client's hostname resolution, and there must be ports opened in the client's firewall for the applications.

2.1 Network Connectivity Requirements

Connectivity for PHLX Services is achieved through private communication lines between the client and PHLX. No traffic is sent over the Internet and all routing must go over the private lines.

The client firm must traverse the private communications lines to the IP address 12.41.5.17 (or 67.56.201.153 for RADIANZ clients) to access the PHLX applications remotely. If the traffic is routed to the Internet versus over the private lines the connection will fail.

It may be necessary to NAT on the client's network to access the PHLX systems. NAT'ing is fully supported for the Citrix Secure Gateway solution.

Clients will be utilizing HTTP and HTTPS for communication protocols. Each client should adjust their IE and proxy server configurations appropriately for their environment so that traffic is routed over the private lines for the IP address above, not the Internet

2.2 Hostname Resolution Requirements

The client must resolve the hostname xlservicedesk.phlx.com to the correct IP address. For clients that connect into the PHLX private lines the IP address is 12.41.5.17. For clients connecting into the PHLX over the RADIANZ network the IP address is 67.56.201.153. PHLX does not publish this DNS record in their public DNS due to the requirement that all traffic must route over the private lines.

The firm cannot add a DNS zone in their DNS as their DNS servers would be authoritative for PHLX and this will cause issues with other PHLX services and e-mail. Host files must be used.

The remote applications solution uses an SSL connection via a web browser that requires the proper hostname be used due to the nature of SSL. Attempting to connect to the IP address will result in a failed connection.

2.3 Firewall Port Requirements

PHLX remote services utilize HTTP and HTTPS for communication, ports 80 and 443 respectively. Although only port 443 is required, both ports are recommended between the client and PHLX's IP of 12.41.5.17 (xlservicedesk.phlx.com). The PHLX Firewall Team will open the ports between the client and 12.41.5.17 (or 67.56.201.153 for RADIANZ clients) as part of the initial connection request.

Clients will connect to https://xlservicedesk.phlx.com from within a web browser. It is anticipated that many clients may omit the "s" in https and type http. A redirect from http://xlservicedesk.phlx.com is included as a courtesy and to minimize support calls. This redirect will only occur if clients are able to use port 80 to the PHLX systems.

3.0 Workstation Requirements

The following are requirements for the end user's workstation: Windows 2000 or XP Operating System, Internet Explorer, and administrative privileges on their workstation to install the Citrix client.

3.1 Operating System Requirements

End user workstations must be Windows 2000 or Windows XP 32 bit. Operating Systems that are not supported are: Windows 9x, 64 bit Windows XP, Linux, etc.

3.2 Internet Explorer Requirements

Internet Explorer 5.x or 6.x (any service pack level) is required for the remote PHLX services. IE 7.0 beta, Opera, Firefox, Netscape, etc. will not be supported.

https://xlservicedesk.phlx.com must be added to the trusted sites IE security settings for the plug-in to download. To configure the trusted sites:

- Within IE go to Tools – Internet Options – Security tab
- Click on trusted sites
- Click on the sites button
- Add https://xlservicedesk.phlx.com to the zone and click add
- Click OK to accept the change and OK to close the windows settings windows
- Close IE and re-open IE window and to re-establish connection to the site
- The plug-in will now download

3.3 Administrative Privileges Requirements

The first time a user connects to the webpage they will be prompted to install the client. Administrative privileges are required on the workstation during the initial install of the Citrix web client. After the client is initially installed, administrative privileges are no longer required.