Proxy Settings Guide

For Intralinks Users and IT Professionals

Intralinks 24x7x365 support US: + (1) 212 543 7800 UK: +44 (0)20 7623 8500.
See Intralinks login page for other national numbers

Introduction

This document shows you how to address proxy and firewall issues at your site as you prepare to install Intralinks Designer, Multi-file Download and other Intralinks applications.

To use these products, you must be able to establish a secure Internet connection to Intralinks' servers. Intralinks uses HTTPS, a secure Internet protocol, to protect and encrypt sensitive data transmitted over the World Wide Web.

IT departments in many organizations have a defined list of websites that have been approved for passing directly through the proxy server. This is often referred to as a white list. To ensure that Intralinks users in your organization can access the services they use, please add the following sites to the proxy server's white list. This will resolve most Internet access issues for Intralinks applications. Your organization's network team can help you whitelist the Intralinks URLs.

https://via.intralinks.com
https://sync.intralinks.com
https://push.intralinks.com
https://services.intralinks.com
https://downloads.intralinkscontent.com
https://webservices.intralinks.com
https://api.intralinks.com
https://irm.intralinks.com
https://courier.intralinks.com
https://debtspace.intralinks.com

Connection failures

If your organization has firewall rules or proxy settings in place, users may receive error messages, such as "Connection Failed Using Proxy," when they attempt to launch an Intralinks application. This error indicates that your organization's IT team may need to configure the proxy settings referenced in the Intralinks **Proxy.config** configuration file, located in each user's Application Data folder, or provide employees with the information they need to log in using a proxy server.

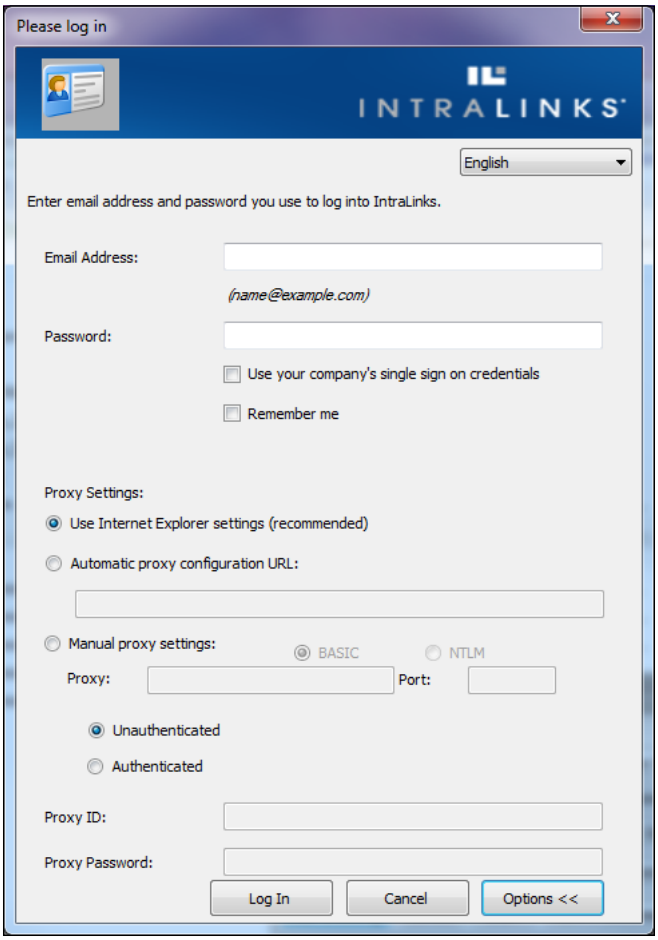
You or your organization's IT team may need to modify other settings in the configuration file, as well. These are described in the next sections.

Configuring proxy settings

You have two options for setting proxy information: You can provide users with the proxy settings so that they can enter the information themselves when they log into Intralinks applications, or you can update the configuration file for these products and distribute the updated file to the employees who need them.

Providing proxy settings to users

When users log into installed applications like Intralinks Courier and Intralinks Designer, they can click an **Options** button in the login window to display the fields needed to enter proxy details. When they log into the same application again in the future, their previous entries will appear by default and do not need to be changed unless your organization makes changes to its proxy server. Users will have to enter proxy settings separately for each Intralinks application.



The Intralinks Designer login screen, with proxy settings displayed.

If you use this option, you must provide users with the following proxy information:

If you use your computer's system settings If you want for the Intralinks application to use the proxy settings specified in your computer's system settings, ask users to mark the **Use Internet Explorer settings (recommended)** option. No additional entries are required.

If you use a Proxy Automatic Configuration file You must provide users with the address for Proxy Automatic Configuration (PAC) file (for example, `http://proxy.Intralinks.com/pacfile.pac`). When users log in, they should select the **Automatic proxy configuration URL** option and enter the address for the PAC file in the field that appears below the option. No additional entries are required.

If you use manual proxy settings You must provide users with the following information:

- Authentication type — BASIC or NTLM
- The IP address for the proxy, (for example, `192.192.192.192`)
- The port used for the proxy (for example, `8080`)
- The proxy ID and password (if the proxy is authenticated)

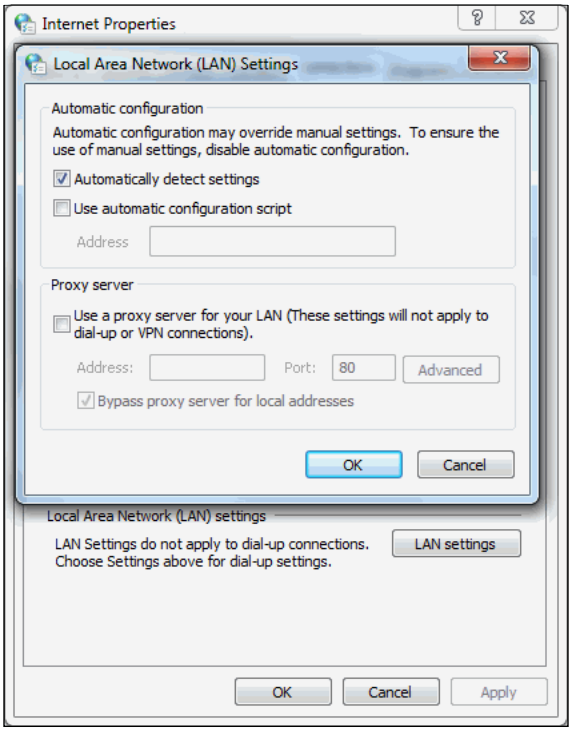
Users should enter these values in the appropriate fields in the **Manual proxy settings** section of the login window.

Configuring the Proxy.config file

You can use Notepad to edit the **Proxy.config** configuration file.

Proxy settings are accessed from the Windows Control Panel.

1. Click on the **Start** button and select **Control Panel**.
2. Select **Internet Options**.
3. Click the **Connections** tab.
4. Click **LAN Settings**. The **Local Area Network (LAN) Settings** dialog box appears.



The Local Area Network (LAN) Settings screen.

The following options appear in the **Local Area Network (LAN) Settings** dialog box:

- **Automatically detect settings**: If you use this option, no action is required.
- **Use automatic configuration script**: If a Proxy Automatic Configuration (PAC) file is being used, update the **PACFileURL** value for the following statement in the Proxy.config file:

  ```
  <add key="PACFileURL" value=""/>
  ```

  To do this, highlight and copy the URL from the **Address** field in the **Local Area Network (LAN) Settings** dialog box to the PACFileURL section of the configuration file, as shown in the following example:

```
<add key=”PACFileURL”
value=”http://proxy.Intralinks.com/pacfile.pac”/>
```

- **Use a proxy server for your LAN**: If you select this option, update the **ProxyIp** value in the configuration file, shown below:

  ```
  <add key=”ProxyIp” value=”http://Address:Port
  Number”/>
  ```

  To update the setting, enter the address from the **Address** field in the **Local Area Network (LAN) Settings** dialog box, followed by a colon (:), and then by the port number, as shown below:

  ```
  <add key=”ProxyIp”
  value=”http://192.192.192.192:8080”/>
  ```

  where the address is `192.192.192.192` and the port number is `8080`.

Intralinks' support of proxy authentication

Intralinks supports network credentials for proxy authentication, as well as proxy credentials for proxy authentication. You can specify the credentials you are using in the in the Proxy.config file, as shown in the following example:

```
<add key="AuthenticationType" value="NETWORKCREDS" />
<add key="AuthenticationType" value="" />
<add key="AuthenticationType" value="PROXYCREDS" />
```

If the AuthenticationType is “NETWORKCREDS” or is blank, Intralinks applications will log into Proxy Server with Credential Type of **Network/default Credentials**.

If the AuthenticationType is “PROXYCREDS”, Intralinks Designer will log into Proxy Server with Credential Type of **Proxy Credentials**, and the Intralinks applications' login window will display these additional populated fields: domain, user ID, and password.

Intralinks Designer supports NTLM, BASIC, Digest and Kerberos proxy authentication. You specify the one you are using in the following entry in the Proxy.config configuration file, repeated here to show each value you can use.

```
<add key="ProxyAuthenticationTypes" value="Basic" />
<add key="ProxyAuthenticationTypes" value="NTLM" />
<add key="ProxyAuthenticationTypes" value="Digest" />
<add key="ProxyAuthenticationTypes" value="Kerberos" />
```

If the ProxyAuthentication value is incorrect, upon login your Intralinks applications will use the default Internet Explorer proxy settings for the authentication type NETWORKCREDS.

Intralinks applications do not support Active Directory (AD) proxy authentication. If AD proxy authentication is being used, whitelist the Intralinks URLs, as described in the introduction to this document, so that Intralinks Designer and other Intralinks applications can bypass AD proxy authentication.

For additional assistance

If you need additional assistance, contact an Intralinks customer service representative. Contact information is listed on the title page of this document.