

Check points if you using a proxy environment.

Determine if the issue is due to your network

Many company deploy additional network features to enhance security, such as proxy servers, web security servers or firewalls. These can sometimes interfere to sign-in of ARGOS RPA service cloud.

To determine if the network you're connected to is causing issues with using ARGOS RPA service cloud , try to connect on a device outside of your company network such like a home pc or a mobile device (Except corporate WiFi environment). If you are able to successfully connect & sign-in to "<https://rpa.argos-labs.com>", your company network is likely the reason why you cannot connect or sign-in to ARGOS RPA service cloud.

Issues due to firewall

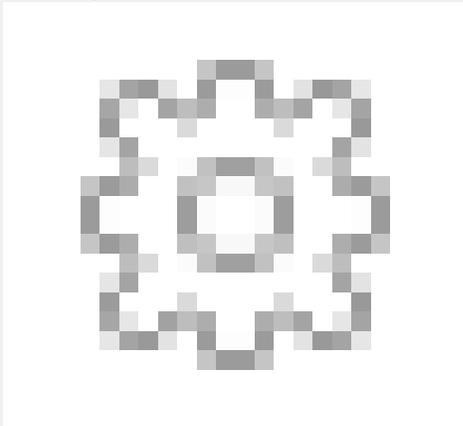
ARGOS RPA uses AWS and AWS CDN network, so your firewall must be openly configured for "*.argos-labs.com" domains (or IP address) and 80/TCP, 443/TCP ports. Because the IP addresses of AWS and AWS CDN is changeable things, we suggest to use 'domain based policy'. If your device does not support 'domain based policy', you can use "AWS IP range" instead.

See <https://ip-ranges.amazonaws.com/ip-ranges.json> for more details.

Issues due to proxy

#1. How to find out whether you are using a proxy or not

1. Run 'Internet Explorer'
2. Click a cog icon(

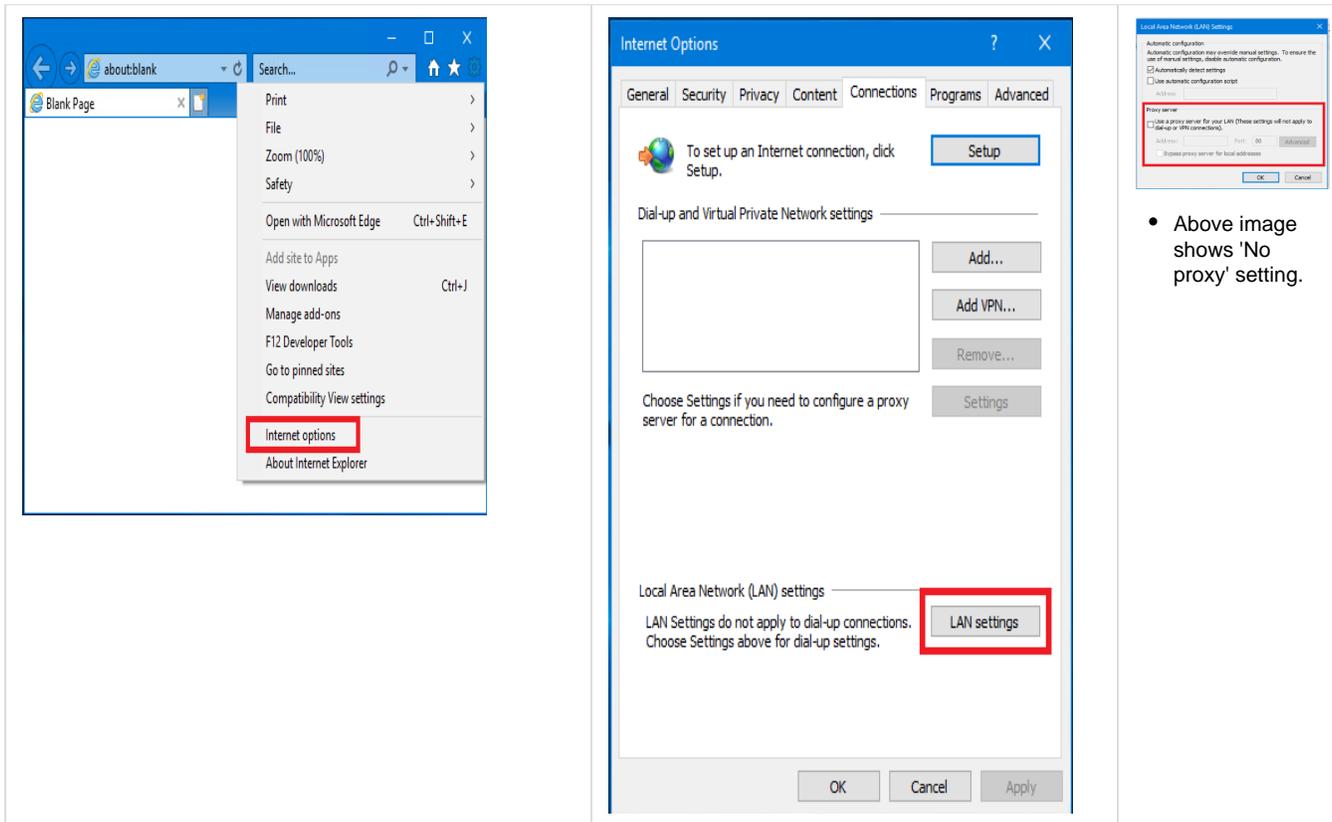


3. Select "Internet options"

4. Choose "Connections" tab

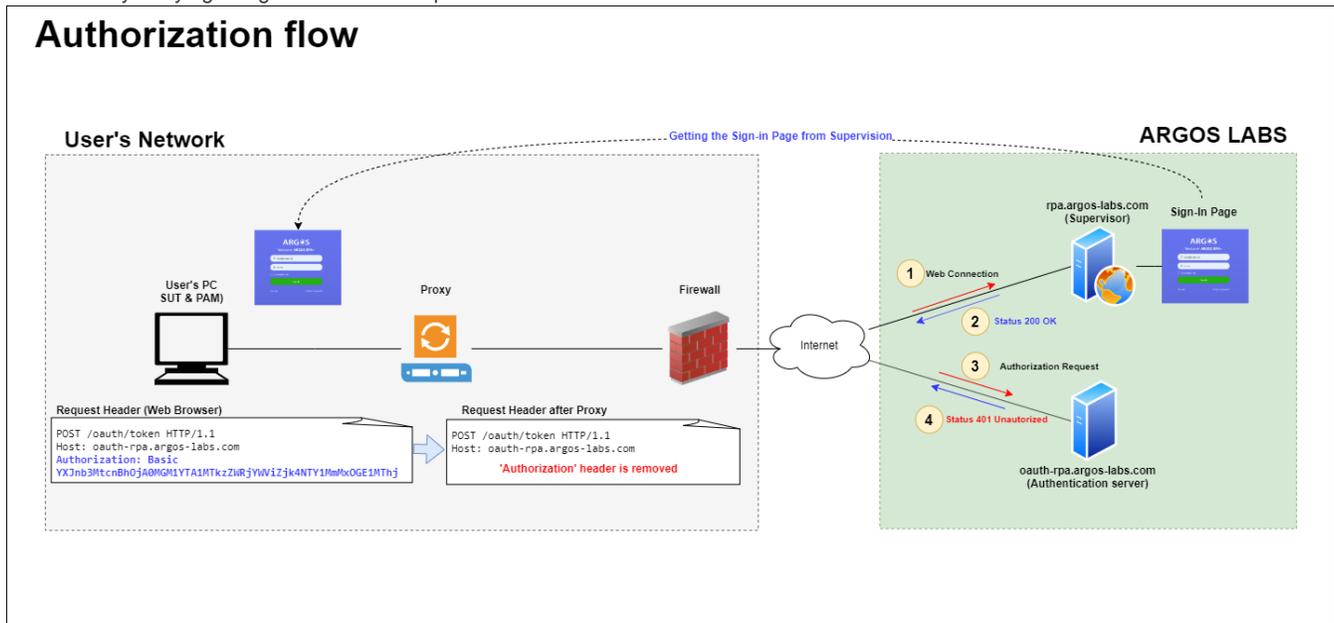
5. Click "LAN settings"

6. Check out "Proxy server" session



#2. issues due to proxy

STU and Supervisor uses an "Authorization" header when making requests to authentication service. Some proxies, such as **ProxySG** (by Symantec), strip an authorization header information by default for security. When the authentication service of ARGOS RPA does not see the authorization header, the session cannot be established successfully and you will get '**401 Unauthorized Error**' from the authentication server when you trying to sign-in to STU or Supervisor.



To resolve this issue, we recommend working with your IT team to allow the authorization header through your proxy. The configuration details may differ depending on the device you are using. For example configuration, read "**Allow ProxySG to always forward server authorization upstream**".