Agent Firewall Allowlisting Rules

Refer to this document for a list of addresses to optimize Automox agent functionality as well as addresses needed to patch Microsoft OS versions from Windows update.

Network and firewall requirements for running the Automox agent

If your organization has egress filtering on the firewall, you will need to allow access to the following hostnames / IP addresses for the Automox agent to communicate with the cloud platform. All agent communications take place over port 443 (https).

Agent access to the Automox platform, and some third-party patches:

- api.automox.com

Agent access to content uploaded for use with Worklets and Required Software Policies:

- automox-policy-files.s3.us-west-2.amazonaws.com

**Note:** The platform-IP addresses are subject to change. Add the hostnames to your list of trusted sites, if possible, or regularly check for the latest IPs assigned to the platform.

- Recommended approach using URL:
  - Allow traffic on port 443 outbound to api.automox.com
- Alternative approach using IP addresses:
  - Check for current IP addresses by running the following command:

  ```
  nslookup api.automox.com
  ```

Proxy and Firewall Considerations

Windows

See [Windows Update troubleshooting: Issues related to HTTP/Proxy](#)

You might choose to apply a rule to permit HTTP RANGE requests for the following URLs:

- *.download.windowsupdate.com
- *.dl.delivery.mp.microsoft.com
- *.delivery.mp.microsoft.com

Firewall
<table>
<thead>
<tr>
<th>Protocol</th>
<th>Endpoint URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS 1.2</td>
<td>*.prod.do.dsp.mp.microsoft.com</td>
</tr>
<tr>
<td>HTTP</td>
<td>emdl.ws.microsoft.com</td>
</tr>
<tr>
<td>HTTP</td>
<td>*.dl.delivery.mp.microsoft.com</td>
</tr>
<tr>
<td>HTTP</td>
<td>*.windowsupdate.com</td>
</tr>
<tr>
<td>HTTPS</td>
<td>*.delivery.mp.microsoft.com</td>
</tr>
<tr>
<td>TLS 1.2</td>
<td>*.update.microsoft.com</td>
</tr>
<tr>
<td>TLS 1.2</td>
<td>tsfe.trafficshaping dsp.mp.microsoft.com</td>
</tr>
</tbody>
</table>

**Note:** Make sure to not use HTTPS for those endpoints that specify HTTP, and vice versa. The connection will fail.

**Note:** When leveraging split-tunneling with a VPN, make sure to include these endpoints in your list of sites with direct access to the internet.

**Microsoft Windows 10 Connection Points**

Microsoft provides a complete list of connection points per Windows 10 feature version. Here is a link to the connection point document for Windows 10 version 20H2 (refer to the links on the left for other feature versions).

https://docs.microsoft.com/en-us/windows/privacy/manage-windows-20h2-endpoints

**macOS**

See Use Apple products on enterprise networks.