Configuring the firewall with a proxy in a DMZ

The following instructions refer to ports 80 and 443 which are standard HTTP ports. The proxy can use other ports, because it is only used by RBA and the OPS instance, and not browsers directly. The customer should change the ports described below to match what their proxy uses.

- If the proxy handles **incoming** connections, the customer should configure the firewall between the DMZ and the internal network to allow inbound connections from the proxy to Prinergy (w.x.y.z) on **port 61235** .
- If the proxy handles **outgoing** connections, and the firewall between the DMZ and the internal network restricts outbound connections, the customer should configure it to allow outbound connections from Prinergy (w.x.y.z) to the proxy on destination **port 80**, or **port 443** if using SSL.
- If the proxy handles outgoing connections, the customer must also add its information to configure `AutomationApp.exe.config` on the Prinergy server. Here is an example configuration entry for the proxy, where `192.168.1.10:3128` is the proxy's address and port on the internal network:

```
<configuration>
...configSections section must come first if present...
  <system.net>
  <defaultProxy>
   <proxy usesystemdefault="false"
    proxyaddress="http://192.168.1.10:3128"
    bypassonlocal="true"
    />
   </defaultProxy>
  </system.net>
  ... other configuration sections ...
<configuration>
```

- For more information, see http://msdn.microsoft.com/en-us/library/kd3cf2ex%28v=VS.90%29.aspx.
- Proxy information can also be configured via **Tools** > **Internet Options** > **Connections** tab, when the araxi user is logged in. Note that configuring a proxy in this way affects all programs running under the araxi user. If a less global effect is desired, set the proxy only for `AutomationApp.exe` as described in the previous step.
- If using SSL, the customer should configure the firewall between the DMZ and the internet to allow inbound connections to their proxy (s.t.u.v) on port 80, or port 443. Once communication between Prinergy and OPS has been proven to work in both directions, the customer should configure the firewall to only accept connections from the OPS server (a.b.c.d).
- If the firewall between the DMZ and the internet restricts outbound connections, it must allow connections from the proxy server (s.t.u.v) to the OPS server (e.f.g.h) on destination port 80 (port 443 if using SSL.)