Configure Wildfly using https when redirecting

When using a load balancer or other reverse proxy in the following way, Wildfly may redirect requests by using an incorrect URI scheme:

- The reverse proxy terminates TLS sessions
- Non-TLS connections (HTTP instead of HTTPS) are used between the proxy and CustomerID

With this configuration, Widfly may use HTTP instead of HTTPS in redirects. In this case you can, for example, go to the CustomerID login screen and authenticate, but you cannot see the CustomerID main page after authentication.

For configuring Wildfly always to use HTTPS in redirects, you can use the following configurations:

- In Wildfly configuration, set **proxy-address-forwarding** for the http-listener:

  Wildfly standalone.xml or domain.xml

  ```
  <server name="default-server">
      <http-listener name="default" socket-binding="http" redirect-socket="https" proxy-address-
  forwarding="true" enable-http2="true"/>
      <https-listener name="default-https" socket-binding="https" security-realm="UndertowRealm"/>
      <host name="default-host" alias="localhost,login.example.com,localhost">
          <location name="/" handler="welcome-content"/>
          <http-invoker security-realm="ApplicationRealm"/>
          <filter-ref name="server-header"/>
          <filter-ref name="x-powered-by-header"/>
      </host>
  </server>
  ```

- In the reverse proxy configuration, add X-Forwarded-Proto header to the requests forwarded to CustomerID. For example, haproxy can be configured as follows. Please see the documentation of your proxy for a similar configuration in your environment.

  haproxy.cfg

  ```
  frontend https-in
      reqadd X-Forwarded-Proto:\ https if { ssl_fc }
  ```