**WildFly 36 — Enable HTTPS (localhost) on Windows**

*Working guide for jBPM/KIE deployments using Undertow + Elytron*

## Assumptions

* OS: Windows
* WildFly: 36.0.0.Final
* WildFly home (adjust as needed): %WILDFLY\_HOME% = C:\wildfly-36.0.0.Final\wildfly-36.0.0.Final
* Goal: Application HTTPS on 8443 (localhost), optional HTTP→HTTPS redirect, optional Management HTTPS (9993).

## 1) Generate a localhost certificate (with SAN)

SAN is required by modern browsers. Generate a self‑signed keystore named server.jks inside the WildFly standalone configuration folder.

cd C:\wildfly-36.0.0.Final\wildfly-36.0.0.Final\standalone\configuration

keytool -genkeypair -alias wildfly -keyalg RSA -keysize 2048 -validity 825 ^  
 -keystore server.jks -storepass changeit -keypass changeit ^  
 -dname "CN=localhost, OU=IT, O=Peraton, L=Chicago, ST=Illinois, C=US" ^  
 -ext "SAN=dns:localhost,ip:127.0.0.1"

## 2) Start the server (bind interfaces)

Bind to all interfaces during setup. For localhost‑only hardening later, use 127.0.0.1 for both binds.

"%WILDFLY\_HOME%\bin\standalone.bat" -b 0.0.0.0 -bmanagement 0.0.0.0

## 3) Configure Elytron (keystore → key‑manager → SSL context)

Create the Elytron objects that point to server.jks.

"%WILDFLY\_HOME%\bin\jboss-cli.bat" --connect

/subsystem=elytron/key-store=serverKS:add(path=server.jks,relative-to=jboss.server.config.dir,type=JKS,credential-reference={clear-text=changeit})  
/subsystem=elytron/key-manager=serverKM:add(key-store=serverKS,credential-reference={clear-text=changeit})  
/subsystem=elytron/server-ssl-context=serverSSL:add(key-manager=serverKM,protocols=["TLSv1.3","TLSv1.2"])

## 4) Point the existing Undertow HTTPS listener to serverSSL

WildFly already has an HTTPS listener named 'https'. Switch it to the new Elytron SSL context.

/subsystem=undertow/server=default-server/https-listener=https:write-attribute(name=ssl-context,value=serverSSL)

:shutdown(restart=true)

## 5) Test HTTPS

Confirm the welcome page (or your app) over TLS.

curl -vk https://localhost:8443/

## 6) (Optional) Redirect HTTP 8080 → HTTPS 8443

Discover the actual HTTP listener name and set redirect. Common names include 'default' or 'http'.

/subsystem=undertow/server=default-server:read-children-names(child-type=http-listener)  
/subsystem=undertow/server=default-server/http-listener=<NAME>:write-attribute(name=redirect-socket,value=https)

:shutdown(restart=true)

## 7) (Optional) Enable Management Console over HTTPS (9993)

Reuse the same SSL context for the management interface.

/core-service=management/management-interface=http-interface:write-attribute(name=ssl-context,value=serverSSL)  
/core-service=management/management-interface=http-interface:write-attribute(name=secure-socket-binding,value=management-https)

:shutdown(restart=true)

# URLs:  
# HTTP management: http://localhost:9990/console  
# HTTPS management: https://localhost:9993/console

## Verification commands

# Verify Elytron keystore exists  
/subsystem=elytron/key-store=serverKS:read-resource  
  
# Verify HTTPS listener configuration  
/subsystem=undertow/server=default-server/https-listener=https:read-resource  
  
# Verify HTTP listeners and redirect  
/subsystem=undertow/server=default-server:read-children-resources(child-type=http-listener)  
  
# Verify socket bindings  
/socket-binding-group=standard-sockets/socket-binding=https:read-resource  
/socket-binding-group=standard-sockets/socket-binding=http:read-resource

## Troubleshooting

* Duplicate resource (WFLYCTL0212) — The resource already exists; use write-attribute instead of add. Idempotent commands may print this during re-runs.
* Browser CN/SAN errors — Regenerate the keystore with SAN as shown in Step 1 (must include dns:localhost and ip:127.0.0.1).
* Keystore not found — Confirm server.jks is in %WILDFLY\_HOME%\standalone\configuration and the Elytron key-store uses relative-to=jboss.server.config.dir.
* Windows firewall blocks 8443/9993 — Add inbound rules or test locally on the machine. For remote access, open the ports.
* Only allow loopback — Start with: standalone.bat -b 127.0.0.1 -bmanagement 127.0.0.1

## Appendix: ready‑to‑run CLI scripts

enable-https-localhost.cli

# enable-https-localhost.cli  
batch  
/subsystem=elytron/key-store=serverKS:add(path=server.jks,relative-to=jboss.server.config.dir,type=JKS,credential-reference={clear-text=changeit})  
/subsystem=elytron/key-manager=serverKM:add(key-store=serverKS,credential-reference={clear-text=changeit})  
/subsystem=elytron/server-ssl-context=serverSSL:add(key-manager=serverKM,protocols=["TLSv1.3","TLSv1.2"])  
/subsystem=undertow/server=default-server/https-listener=https:write-attribute(name=ssl-context,value=serverSSL)  
run-batch  
:shutdown(restart=true)

enable-mgmt-https.cli

# enable-mgmt-https.cli  
batch  
/core-service=management/management-interface=http-interface:write-attribute(name=ssl-context,value=serverSSL)  
/core-service=management/management-interface=http-interface:write-attribute(name=secure-socket-binding,value=management-https)  
run-batch  
:shutdown(restart=true)

## jBPM / KIE Notes

* If exposing KIE Server/Business Central over HTTPS, update org.kie.server.location and any controller URLs to https://localhost:8443/...
* If SSO/Keycloak is used, add the HTTPS redirect URI(s) for your apps to avoid login loops.

Result:

1) WildFly Welcome / Apps — http 8080 → https 8443 (if redirect enabled)

2) Management Console — http 9990 → https 9993 (if management HTTPS enabled)