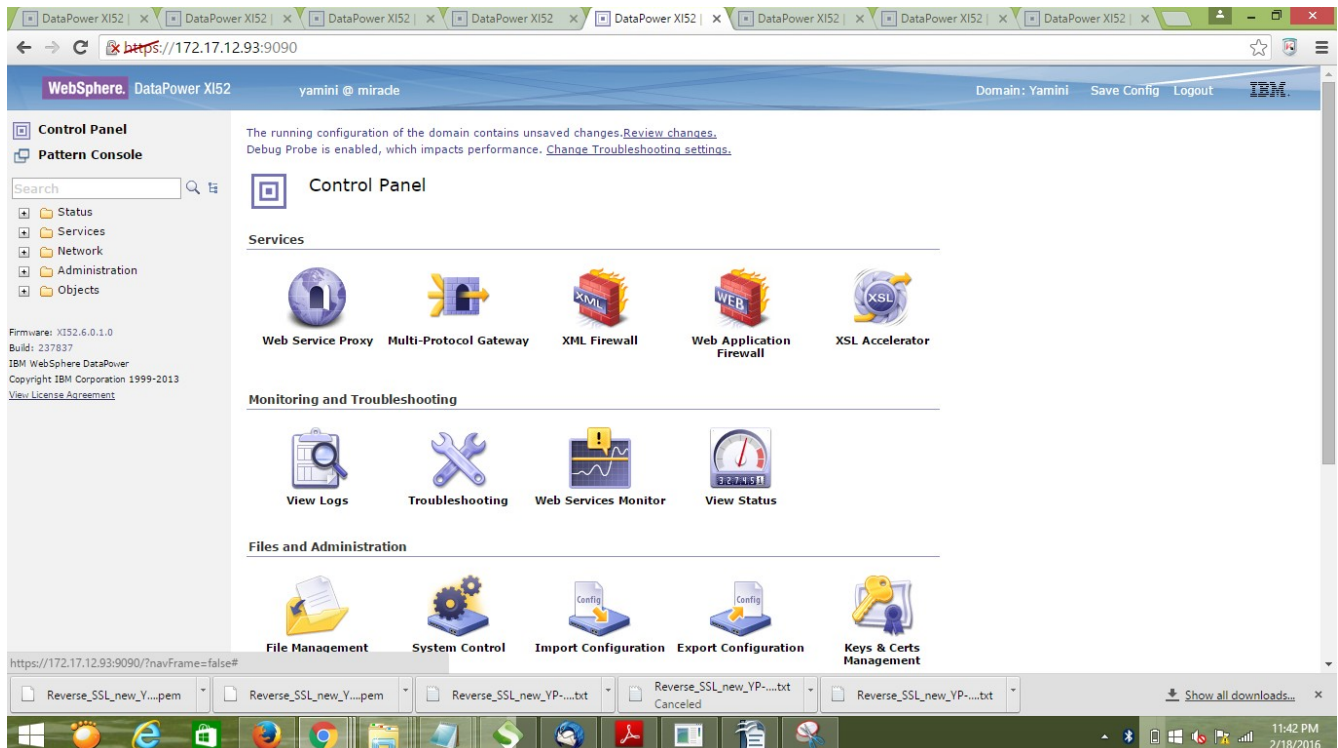


Logging into WebGUI:



Click on the **MPG(Multi-Protocol Gateway)** :



Click on **ADD** button :

The screenshot shows the WebSphere DataPower XI52 Control Panel interface. The main content area is titled 'Configure Multi-Protocol Gateway'. It contains a table with the following columns: Multi-Protocol Gateway Name, Op-State, Logs, Type, Req-Type, Back Side URL, Resp-Type, and Front Protocol. The table lists several gateways, including 'FTP_SERVER', 'mpg_AAA', 'mpg_CallProcessing', 'mpg_Datapower-sdfc-YP', 'MPG_encrypt_decrypt', 'mpg_forward_YP', 'mpg_multiple_destinations_YP', 'mpg_payload', 'mpg_reverse', 'MPG_SIGN_VERIFY', and 'MPG_twoway_YP'. The 'Op-State' column shows the status of each gateway (e.g., 'down', 'up'). The 'Add' button is located at the bottom left of the table.

Multi-Protocol Gateway Name	Op-State	Logs	Type	Req-Type	Back Side URL	Resp-Type	Front Protocol
FTP_SERVER	down		Static Backend	Non-XML	ftp://FTP_MIRACLE:miracle@172.17.12.152:21/OUTPUT	Non-XML	Sample
mpg_AAA	up		Static Backend	SOAP	http://172.17.12.237:2133/	SOAP	http_FSH_AAA_9875
mpg_CallProcessing	up		Static Backend	SOAP	http://172.17.12.237:2133	SOAP	http_CallProcessing_9587
mpg_Datapower-sdfc-YP	down		Dynamic Backend	Non-XML	NA	Non-XML	Http-Datapower-sdfc-yp-1187
MPG_encrypt_decrypt	up		Static Backend	SOAP	http://172.17.12.237:2133/	SOAP	http_encrypt2222_5897
mpg_forward_YP	down		Static Backend	SOAP	https://172.17.12.93:4587	SOAP	http_CallProcessing_9587
mpg_multiple_destinations_YP	up		Dynamic Backend	SOAP	NA	SOAP	http_multiple_destn_8847
mpg_payload	up		Static Backend	SOAP	https://172.17.12.237:2133	SOAP	http_payload_1231
mpg_reverse	up		Static Backend	XML	http://172.17.12.93:8020	XML	https_reverse_YP_4587
MPG_SIGN_VERIFY	up		Static Backend	SOAP	http://172.17.12.237:2133/	SOAP	http_test_8021
MPG_twoway_YP	up		Static Backend	SOAP	https://172.17.12.93:4587	SOAP	https_2way_YP_1002

Click on **Static-Backend** and give the backend URL as HTTP.
Configure the HTTPS FSH.

The screenshot shows the 'Configure Multi-Protocol Gateway' page with the 'General' tab selected. The 'Multi-Protocol Gateway Name' is 'mpg_reverse'. The 'Type' is set to 'static-backend'. The 'Default Backend URL' is 'http://172.17.12.93:8020'. The 'Front Side Protocol' is 'https_reverse_YP_4587 (HTTPS Front Side Handler)'. The 'Add' button is visible next to the 'Front Side Protocol' field.

General Configuration

Multi-Protocol Gateway Name: mpg_reverse

Summary:

Type: ☒ static-backend

XML Manager: default

Multi-Protocol Gateway Policy: policy_reverse_YP

URL Rewrite Policy: (none)

Back side settings: Default Backend URL: http://172.17.12.93:8020

Front side settings: Front Side Protocol: https_reverse_YP_4587 (HTTPS Front Side Handler)

Click on “+” button and configure the **Policy**.

Configure Multi-Protocol Gateway Style Policy

Policy:
 Policy Name: policy_forward_YP
 Apply Policy Cancel Export View Log View Status Close Window

Rule:
 Rule Name: policy_forward_YP_rule_0 Rule Direction: Server to Client
 New Rule Delete Rule

Create rule: Click New, drag action icons onto line. Edit rule: Click on rule, double-click on action.

Filter Sign Verify Validate Encrypt Decrypt Transform Route AAA Results Advanced

ORIGIN SERVER CLIENT

Action: Match
 ALL
 Match Rule:
 Matching Type : url
 URL Match : *
 HTTP Method : default
 Comments : Default Match
 Match with PCRE : off
 Boolean Or Combinations : off

Create Reusable Rule

Order	Rule Name	Direction	Actions
1	policy_forward_YP_rule_req	Client to Server	delete rule
2	policy_forward_YP_rule_0	Server to Client	delete rule

Scroll to top

Click on **New Rule** and set the **Rule Direction** as Client to Server.

Then configure the **Match Action**:

Matching Type: **URL**

URL Match : *

Then click on **Apply Policy**.

Again follow the above process by selecting the Rule Direction as Server to Client.

Set the **Request -Response** type as **XML**:

User Agent settings

Match **Property**

Note: To edit the User Agent, please access via the XML Manager above.

SSL Client Crypto Profile
 (none) + ...

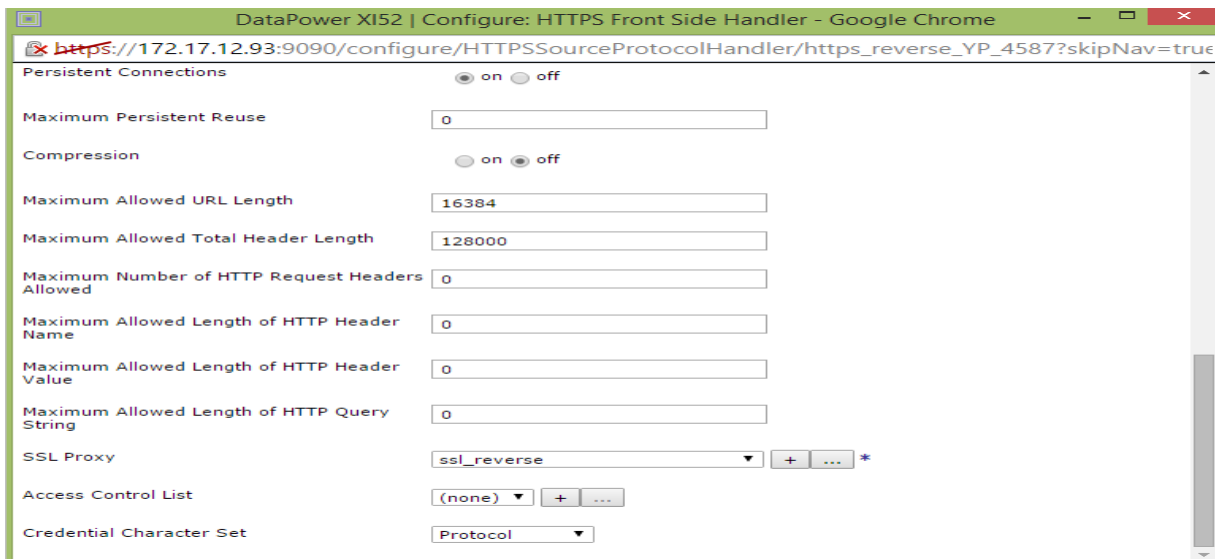
Response Type

☐ JSON
☐ Non-XML
☐ Pass through
☐ SOAP
☒ XML

Request Type

☐ JSON
☐ Non-XML
☐ Pass through
☐ SOAP
☒ XML

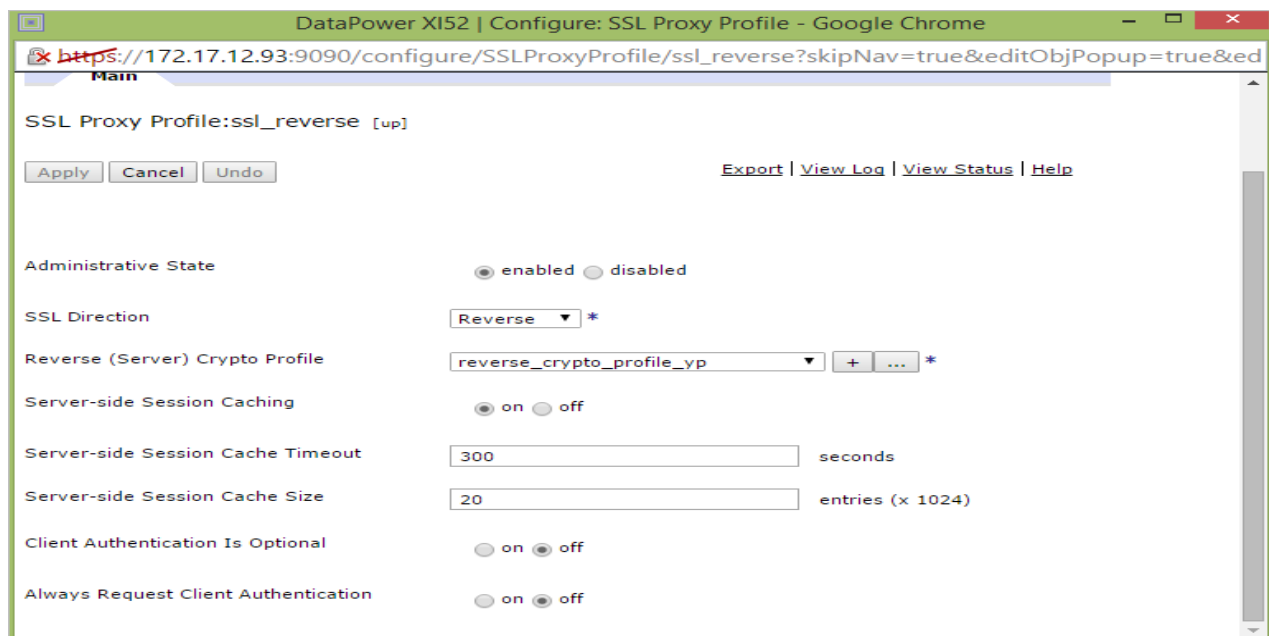
Create a **HTTPS** Front side handler.



The screenshot shows the 'Configure: HTTPS Front Side Handler' page in a Google Chrome browser. The URL bar shows a secure connection to 172.17.12.93:9090. The page contains several configuration fields:

- Persistent Connections:** Radio buttons for 'on' (selected) and 'off'.
- Maximum Persistent Reuse:** Text input field with value '0'.
- Compression:** Radio buttons for 'on' and 'off' (selected).
- Maximum Allowed URL Length:** Text input field with value '16384'.
- Maximum Allowed Total Header Length:** Text input field with value '128000'.
- Maximum Number of HTTP Request Headers Allowed:** Text input field with value '0'.
- Maximum Allowed Length of HTTP Header Name:** Text input field with value '0'.
- Maximum Allowed Length of HTTP Header Value:** Text input field with value '0'.
- Maximum Allowed Length of HTTP Query String:** Text input field with value '0'.
- SSL Proxy:** Dropdown menu showing 'ssl_reverse' with '+' and '...' buttons.
- Access Control List:** Dropdown menu showing '(none)' with '+' and '...' buttons.
- Credential Character Set:** Dropdown menu showing 'Protocol'.

Click on “+” button to create an SSL Proxy.



The screenshot shows the 'Configure: SSL Proxy Profile' page in a Google Chrome browser. The URL bar shows a secure connection to 172.17.12.93:9090. The page title is 'Main'. The configuration is for 'SSL Proxy Profile: ssl_reverse [up]'. There are buttons for 'Apply', 'Cancel', and 'Undo'. On the right, there are links for 'Export', 'View Log', 'View Status', and 'Help'.

The configuration fields are:

- Administrative State:** Radio buttons for 'enabled' (selected) and 'disabled'.
- SSL Direction:** Dropdown menu showing 'Reverse' with an asterisk.
- Reverse (Server) Crypto Profile:** Dropdown menu showing 'reverse_crypto_profile_yp' with '+' and '...' buttons.
- Server-side Session Caching:** Radio buttons for 'on' (selected) and 'off'.
- Server-side Session Cache Timeout:** Text input field with value '300' and unit 'seconds'.
- Server-side Session Cache Size:** Text input field with value '20' and unit 'entries (x 1024)'.
- Client Authentication Is Optional:** Radio buttons for 'on' and 'off' (selected).
- Always Request Client Authentication:** Radio buttons for 'on' and 'off' (selected).

Set the **SSL Direction** as Reverse and configure the **Reverse Crypto Profile** by clicking on “+” button.

https://172.17.12.93:9090/configure/CryptoProfile/reverse_crypto_profile_yp?skipNav=true&editObjPop

Apply Cancel Undo Export View Log View Status Help

Administrative State ☒ enabled ☐ disabled

Identification Credentials crypto_identf_YP + ...

Validation Credentials crypto_valid_YP + ...

Ciphers HIGH:MEDIUM:!aNULL:!eNULL:@ST


Options

- ☒ Enable default settings
- ☒ Disable SSL version 2
- ☐ Disable SSL version 3
- ☐ Disable TLS version 1.0
- ☐ Permit insecure SSL renegotiation to a legacy SSL client
- ☐ Enable compression
- ☐ Disable TLS version 1.1
- ☐ Disable TLS version 1.2

* Send Client CA List ☐ on ☒ off

Now, configure the **identification credentials** by clicking on “+” button and upload the Key and Certificate from the cert:/// folder.

https://172.17.12.93:9090/configure/CryptoidentCred/crypto_identf_YP?skipNav=true&editObjPopup=ti

 **Configure Crypto Identification Credentials**

Main

Crypto Identification Credentials:crypto_identf_YP [up]

Apply Cancel Undo Export View Log View Status Help

Administrative State ☒ enabled ☐ disabled

Crypto Key ssl_crypto_soapui + ... *

Certificate ssl_crypto_soapui + ... *

Intermediate CA Certificate (empty)

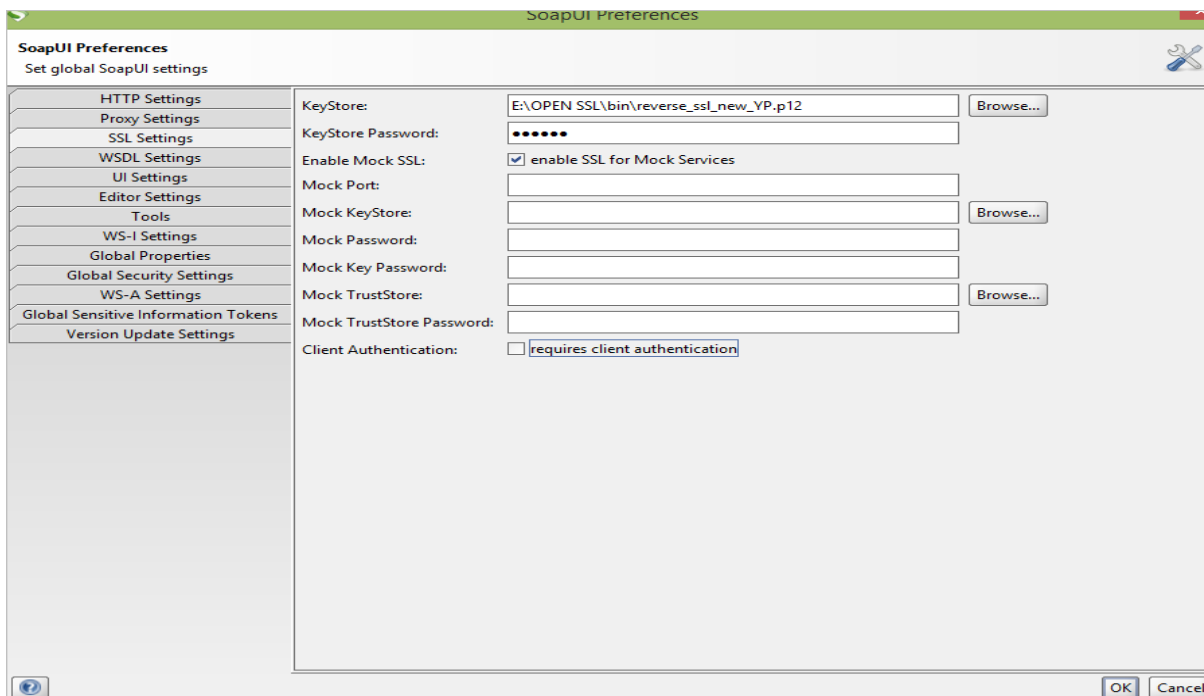
add + ...

Create a **KeyStore**:

Goto SSLProxy Folder and click on **openssl.exe** file which is available in the bin folder.

```
E:\OPEN SSL\bin\openssl.exe
OpenSSL> pkcs12 -export -in key_certify_k-sscert.pem -inkey key_certify_k-private
key.pem -out reverse_ssl_new_YP.p12 -name yamini
Loading 'screen' into random state - done
Enter Export Password:
Verifying - Enter Export Password:
OpenSSL>
```

Add the KeyStore in the SoapUI:



Testing :

Now send the Corresponding request based on the type of the request and the Port on which the service is running.