SEC DATAPOWER INSTALLATION

DataPower Installation and Configuration for Prod Environment

Abstract

This document covers DataPower installations.

Cihan Seçinti

Table of Contents

Glossary

DP	DataPower

Endpoints and Credentials:

DataPower:

Endpoint: https://172.17.18.241:9090/
Username: admin

Endpoint: https://172.17.18.242:9090/
Username: admin

Endpoint: https://172.17.18.243:9090/
Username: admin

DataPower Installation for DEV environment

Deploy and Configure DataPower on VMware Console

Gateway component doesn’t use an ISO file it should be configured by using its console. You may follow the below commands:

1. Power on machine.
2. When you get prompted for login, type 'admin'.
3. For password type ‘admin’.
4. Press Enter after the ATTENTION message
5. Enable Secure Backup mode? Yes/No **Yes** and then confirm with **Yes**
6. After Common criteria compatibility mode, Type: **No**
7. You'll be forced to change the admin password. Change it to a common password and DO NOT LOSE THIS PASSWORD. The only recovery for this password is to re-deploy image.
8. Use Installation Wizard prompt, Type: **y**
9. Do you want to configure network interfaces? Type: **y**
10. Do you have this information? Type: **y**
11. Do you want to configure the eth0 interface? Type: **y**
12. Do you want to enable DHCP? Type: **n**
13. Enter the IP address for interface in CIDR notation: Type: ***172.17.18.241/28***
14. Enter the IP Address for default IPv4 gateway: Type: ***172.17.18.254***
15. Do you want to configure the eth1 interface? Type: **y**
16. Do you want to enable DHCP? Type: **n**
17. Enter the IP address for interface in CIDR notation: Type: ***172.17.17.225/25***
18. Enter the IP Address for default IPv4 gateway: Type:
19. Enter **n** for question to configure eth2 and eh3 interfaces.
20. Do you want to configure network services? Type: **y**
21. Do you want to configure DNS? Type: **y**
22. Enter the DNS server ip: Type: **172.17.24.193**

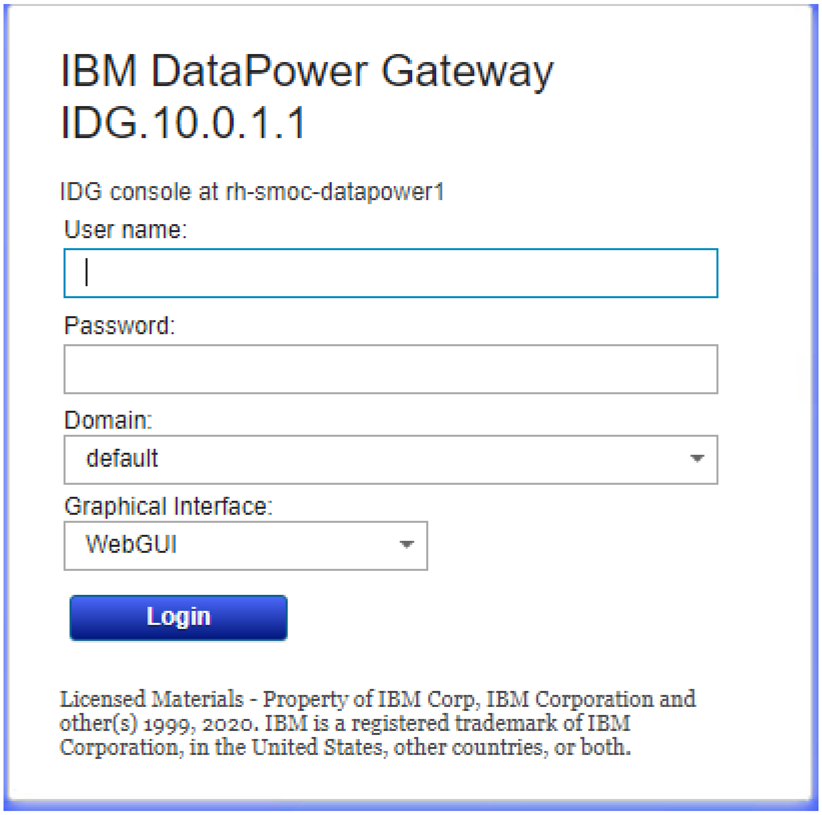
    Note: also, you may configure dns server after the installation via Web Client
23. Do you want to define unique system identifier for the appliance? Type: **y**

    Note: Give any appropriate unique system identifier **rh-smoc-datapower1**
24. Do you want to configure remote management access? Type: **y**
25. This configuration requires the IP address of the local interface that manage the appliance.
26. Do you have this information? Type: **y**
27. Do you want to enable SSH? Type: **y**
28. Enter the local IP address [0 for all]: Type: ***Press Enter***
29. Enter the port number [22]: Type: **22**
30. Do you want to enable WebGUI access? Type: **y**

31. Enter the local IP address [0 for all]: Type: ***Press Enter***
32. Enter the port number [9090]: Type: ***9090***
33. Do you want to configure a user account that can reset passwords [y]: Type: **y**
    Note: This is optional, but you can provide username and password (keep note of this detail)
34. Do you want to configure the hard disk array? Type: **y**
35. Do you want to continue? [y]: Type: **y**
36. Enter name for the file system [ondisk]: Type: **ondisk**
37. Do you want to review the current configuration? [y]: Type: **y**
38. Do you want to save current configuration? [y]: Type: **y**
39. Overwrite previously saved configuration? [y/n]: Type: **y**
40. And now everything should be set, and you can get to web interface.

First Configurations on WebGUI:

1. Enter https://172.17.18.241:9090/ *on your browser.*
2. Accept license and terms and wait for reboot.
3. If your firmware version is not same with the API Connect components, please check the next chapter for firmware upgrade before continuing.
4. Login to gateway server with using admin and your defined admin password. Select WebGUI as "Graphical Interface".



IBM DataPower Gateway
IDG.10.0.1.1

IDG console at rh-smoc-datapower1

User name:

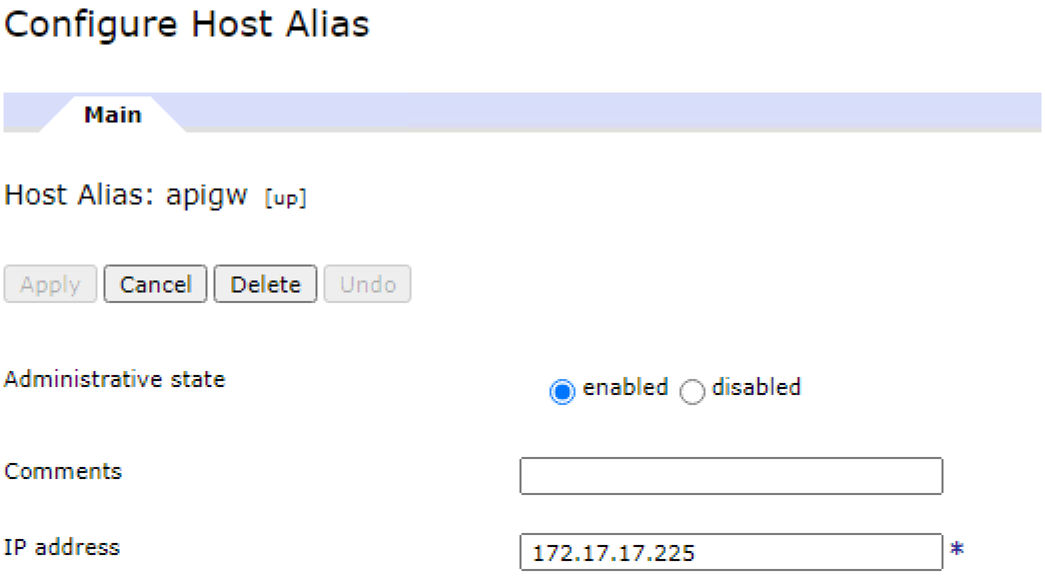
Password:

Domain: default

Graphical Interface: WebGUI

Licensed Materials - Property of IBM Corp, IBM Corporation and other(s) 1999, 2020. IBM is a registered trademark of IBM Corporation, in the United States, other countries, or both.

5. Navigate Network→Interface→Host Alias or search for host alias on the left search pane.
6. Press “Add” button and enter a name and gateway IP address. (**172.17.17.225**)



Configure Host Alias

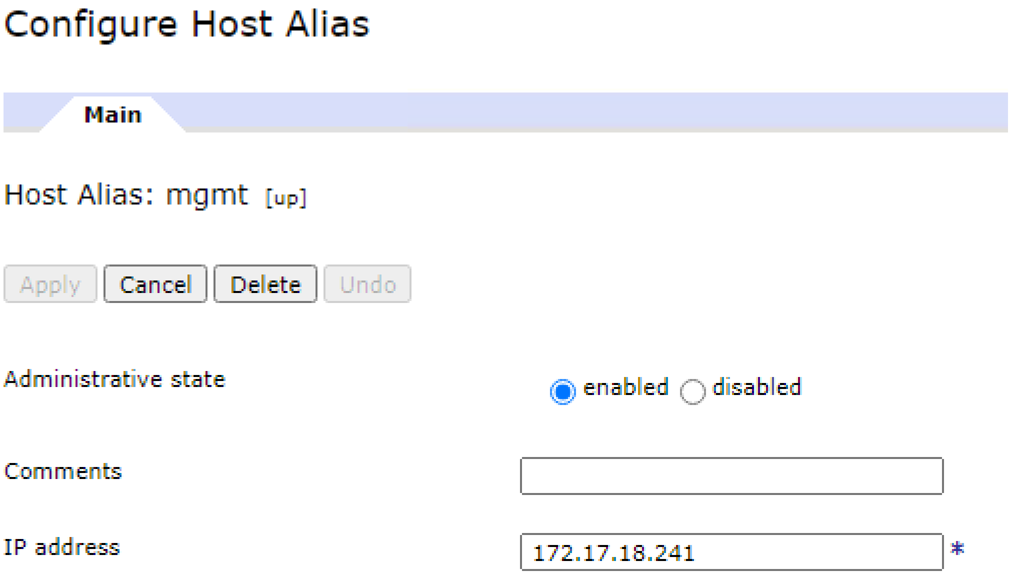
Host Alias: apigw [up]

Administrative state ● enabled ○ disabled

Comments

IP address 172.17.17.225 *

7. Go back and press “Add” button again and enter a name and management IP address. (**172.17.18.241**)



Configure Host Alias

Host Alias: mgmt [up]

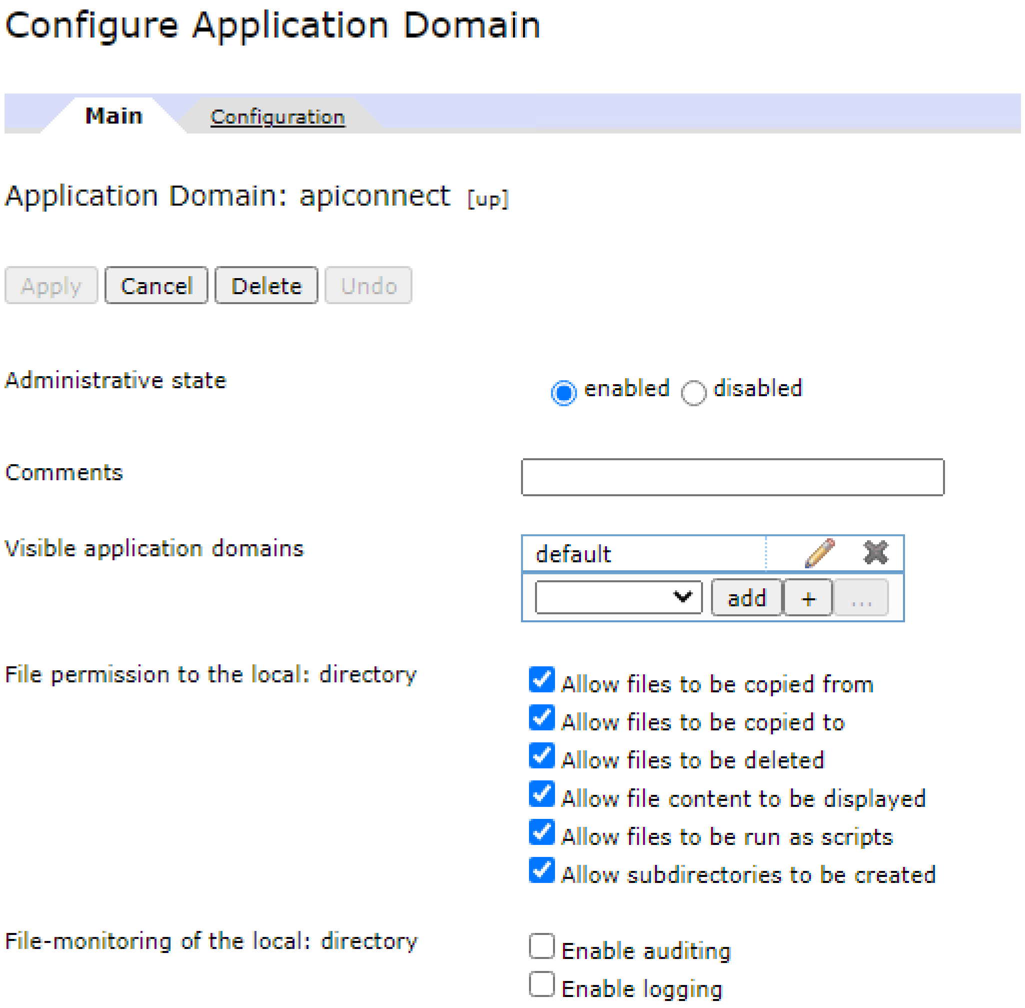
Administrative state ● enabled ○ disabled

Comments

IP address 172.17.18.241 *

8. Navigate to Administration→Configuration→Application Domain or search for application domain.

9. Press "Add" button and give a name. (**apiconnect**)



Configure Application Domain

Application Domain: apiconnect [up]

Administrative state ● enabled ○ disabled

Comments

Visible application domains: default

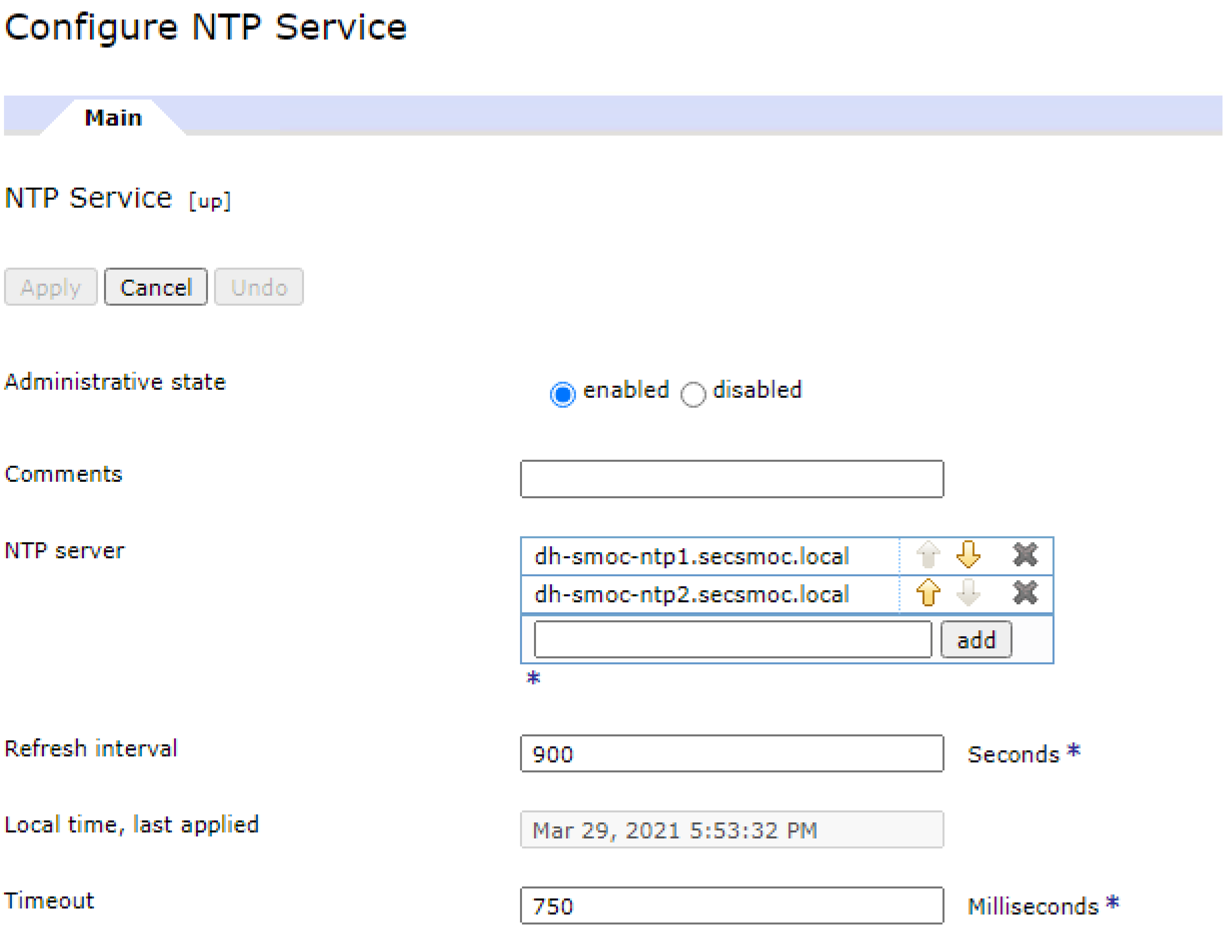
File permission to the local: directory

☑ Allow files to be copied from
☑ Allow files to be copied to
☑ Allow files to be deleted
☑ Allow file content to be displayed
☑ Allow files to be run as scripts
☑ Allow subdirectories to be created

File-monitoring of the local: directory

□ Enable auditing
□ Enable logging

10. Navigate to Network→Interface→NTP Service or search for NTP service.
11. Add NTP Server and set the administrative state "enabled". Development environment NTP server address are "**dh-smoc-ntp1.secsmoc.local**" and "**dh-smoc-ntp2.secsmoc.local**".



Configure NTP Service

NTP Service [up]

Administrative state ● enabled ○ disabled

Comments

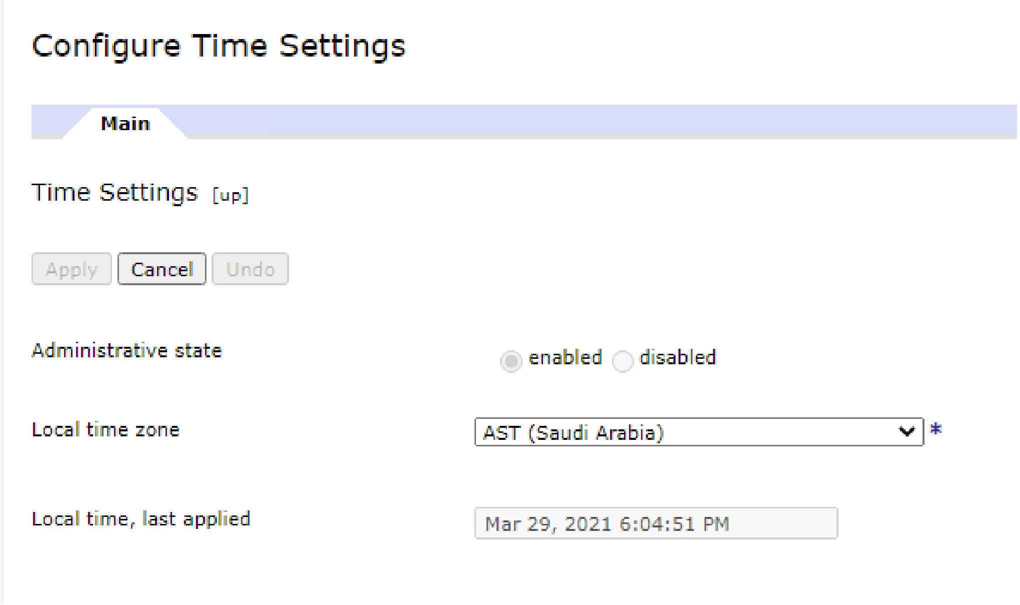
NTP server dh-smoc-ntp1.secsmoc.local
dh-smoc-ntp2.secsmoc.local

Refresh interval 900 Seconds *

Local time, last applied Mar 29, 2021 5:53:32 PM

Timeout 750 Milliseconds *

12. Navigate to Administration→Device→Time settings or search for time settings.
13. Configure the appropriate time zone. (**AST (Saudi Arabia)**)



Configure Time Settings

Time Settings [up]

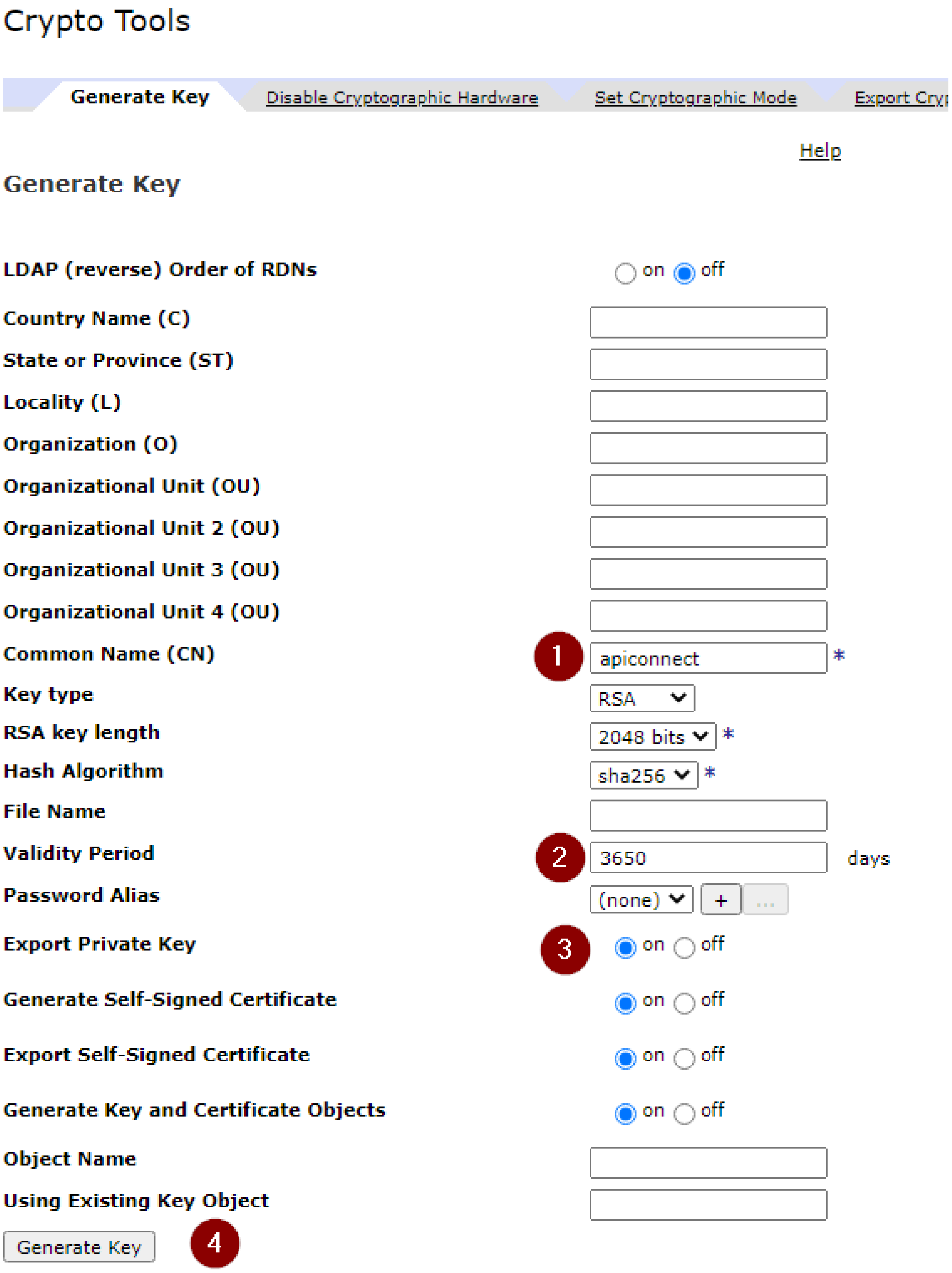
Administrative state ● enabled ○ disabled

Local time zone AST (Saudi Arabia) *

Local time, last applied Mar 29, 2021 6:04:51 PM

API Connect Related Configurations on WebGUI:

1. Navigate to Administrator→Miscellaneous→Crypto Tools or search for crypto tools.
2. Create new one by entering “Common Name” you may also enter the other information, but the rest is optional. You may consider changing “Validity Period”. (Optional) Select “on” for “Export Private Key“and download private key and public cert from file management to store them.



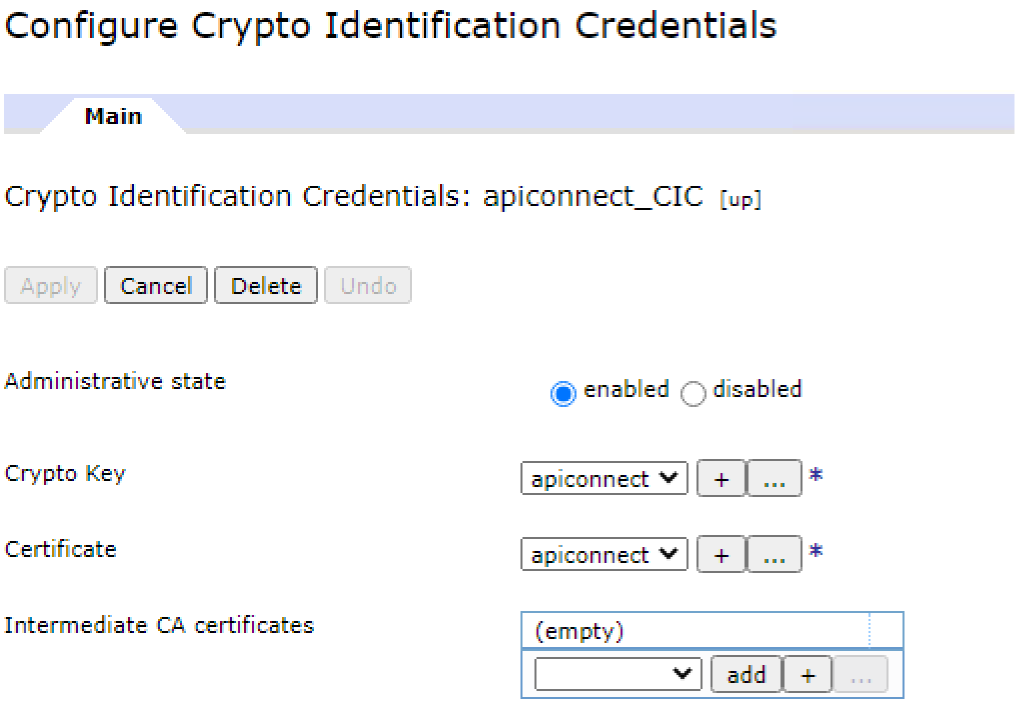
Crypto Tools

Generate Key

LDAP (reverse) Order of RDNs	○ on ● off
Country Name (C)	
State or Province (ST)	
Locality (L)	
Organization (O)	
Organizational Unit (OU)	
Organizational Unit 2 (OU)	
Organizational Unit 3 (OU)	
Organizational Unit 4 (OU)	
Common Name (CN)	apiconnect *
Key type	RSA
RSA key length	2048 bits *
Hash Algorithm	sha256 *
File Name	
Validity Period	3650 days
Password Alias	(none) + ...
Export Private Key	● on ○ off
Generate Self-Signed Certificate	● on ○ off
Export Self-Signed Certificate	● on ○ off
Generate Key and Certificate Objects	● on ○ off
Object Name	
Using Existing Key Object	

Generate Key

3. Navigate to Objects→Crypto Configuration→Crypto Identification Credentials or search for identification credentials.
4. Press “Add” button, give a name and select automatically created Crypto Key and Certificate after usage of Crypto Tools.



Configure Crypto Identification Credentials

Crypto Identification Credentials: apiconnect_CIC [up]

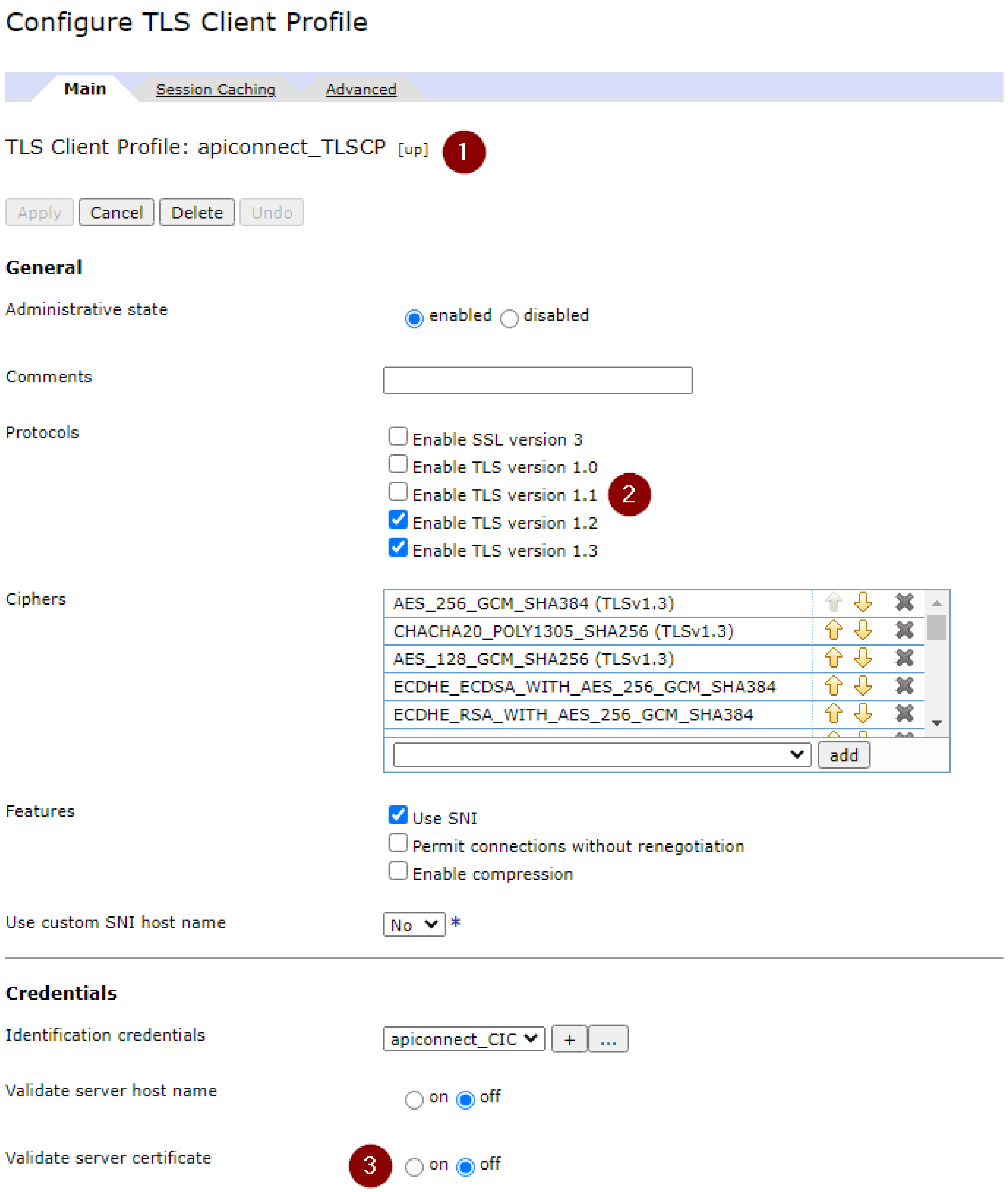
Administrative state ● enabled ○ disabled

Crypto Key apiconnect *

Certificate apiconnect *

Intermediate CA certificates (empty)

5. Navigate to Objects→Crypto Configuration→TLS Client Profile or search for client profile.
6. Press “Add” button, give a name, select defined identification credential in step 4 and check “off” for “Validate server certificate”. (Optional) For security reasons, TLS version 1.0 and 1.1 may be disabled.



Configure TLS Client Profile

TLS Client Profile: apiconnect_TLSCP [up] 1

General

Administrative state ● enabled ○ disabled

Comments

Protocols
□ Enable SSL version 3
□ Enable TLS version 1.0
□ Enable TLS version 1.1 2
☑ Enable TLS version 1.2
☑ Enable TLS version 1.3

Ciphers
AES_256_GCM_SHA384 (TLSv1.3)
CHACHA20_POLY1305_SHA256 (TLSv1.3)
AES_128_GCM_SHA256 (TLSv1.3)
ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
ECDHE_RSA_WITH_AES_256_GCM_SHA384

Features
☑ Use SNI
□ Permit connections without renegotiation
□ Enable compression

Use custom SNI host name No *

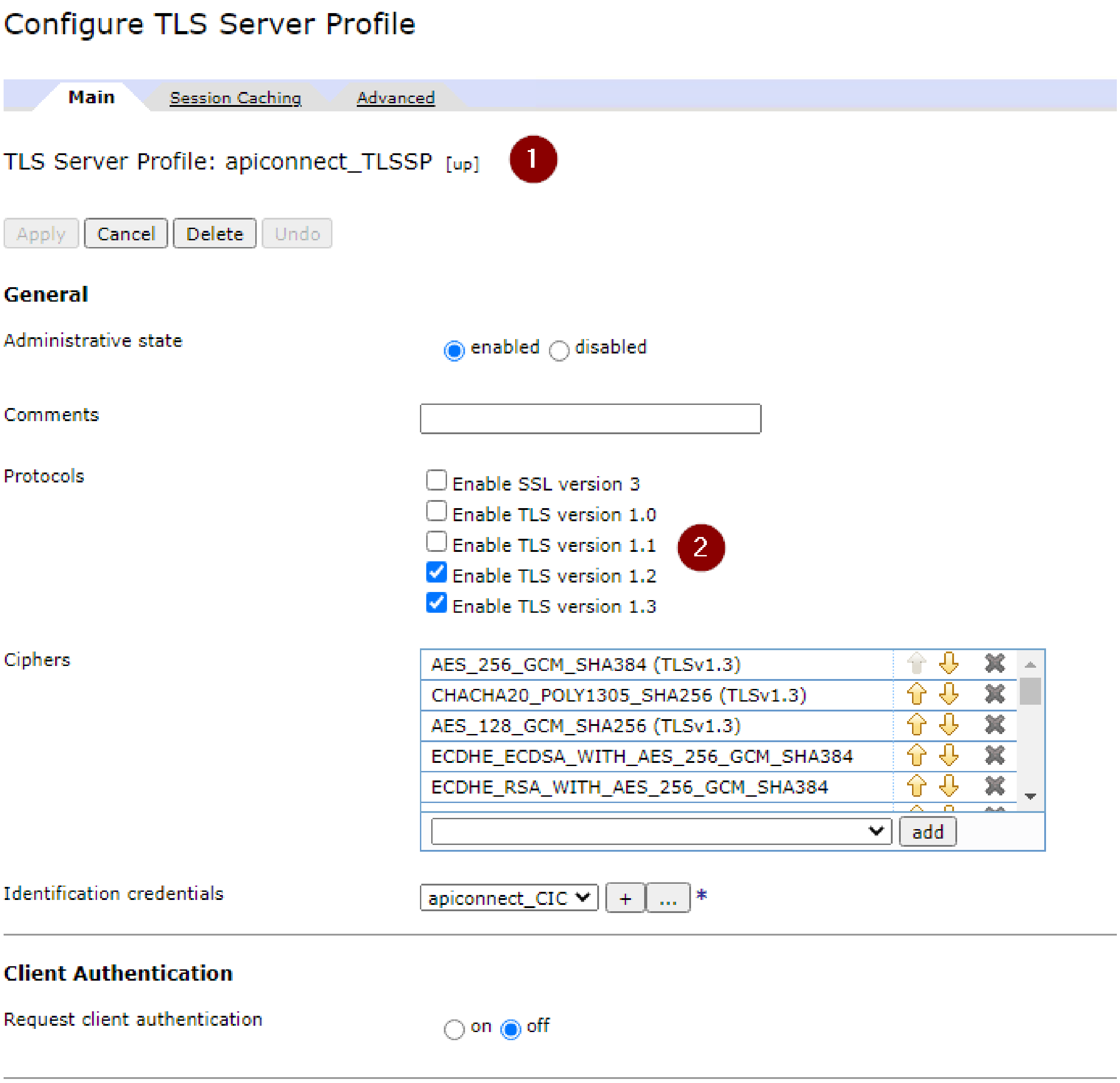
Credentials

Identification credentials apiconnect_CIC

Validate server host name ○ on ● off

Validate server certificate 3 ○ on ● off

7. Navigate to Objects→Crypto Configuration→TLS Server Profile or search for server profile.
8. Press “Add” button, give a name and select identification credential which was defined in step 4. (Optional) For security reasons, TLS version 1.0 and 1.1 may be disabled.



Configure TLS Server Profile

TLS Server Profile: apiconnect_TLSSP [up]

General

Administrative state ● enabled ○ disabled

Comments

Protocols

- ☐ Enable SSL version 3
- ☐ Enable TLS version 1.0
- ☐ Enable TLS version 1.1
- ☑ Enable TLS version 1.2
- ☑ Enable TLS version 1.3

Ciphers

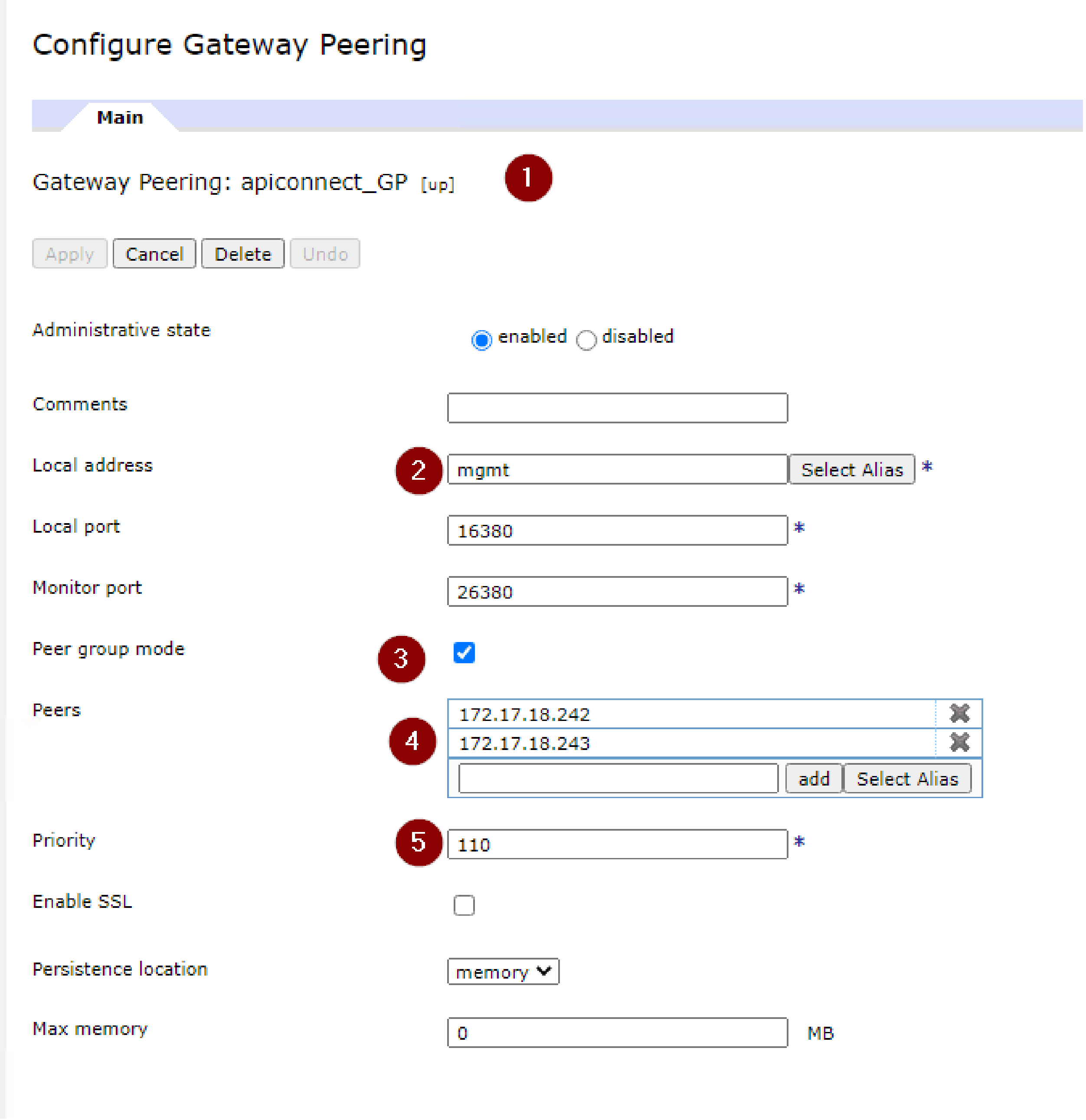
- AES_256_GCM_SHA384 (TLSv1.3)
- CHACHA20_POLY1305_SHA256 (TLSv1.3)
- AES_128_GCM_SHA256 (TLSv1.3)
- ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- ECDHE_RSA_WITH_AES_256_GCM_SHA384

Identification credentials apiconnect_CIC *

Client Authentication

Request client authentication ○ on ● off

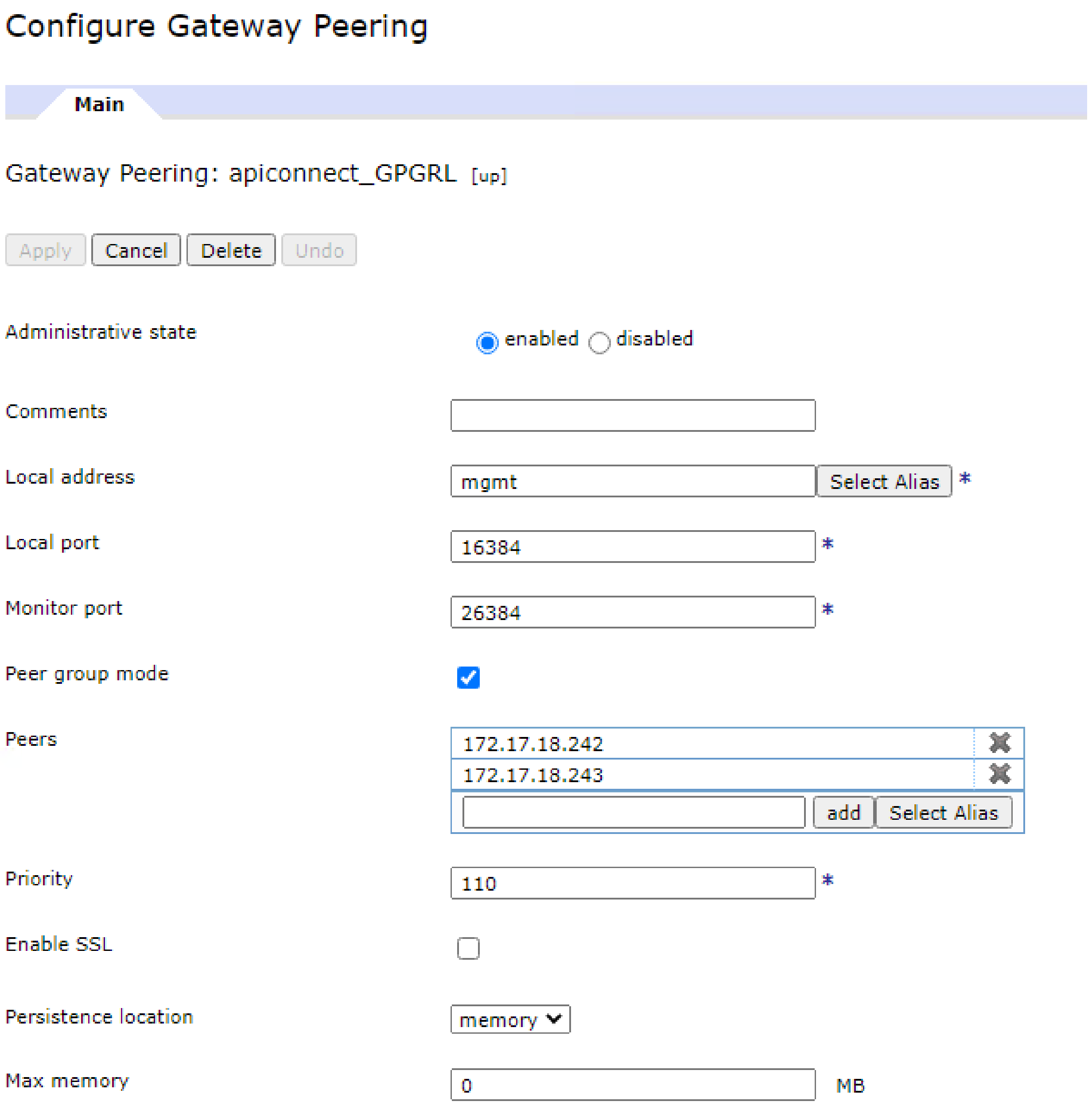
9. Navigate to Objects→Service Configuration→Gateway Peering or search for gateway peering.
10. Press “Add” button, select local address as defined host alias in section “First Configurations on WebGUI”. Uncheck “Enable SSL”.
11. In v10.0.1.1 there are 5 different gateway peering option in the gateway peering manager, IBM recommends creating a new object for each.



Configure Gateway Peering

Gateway Peering: apiconnect_GP [up]

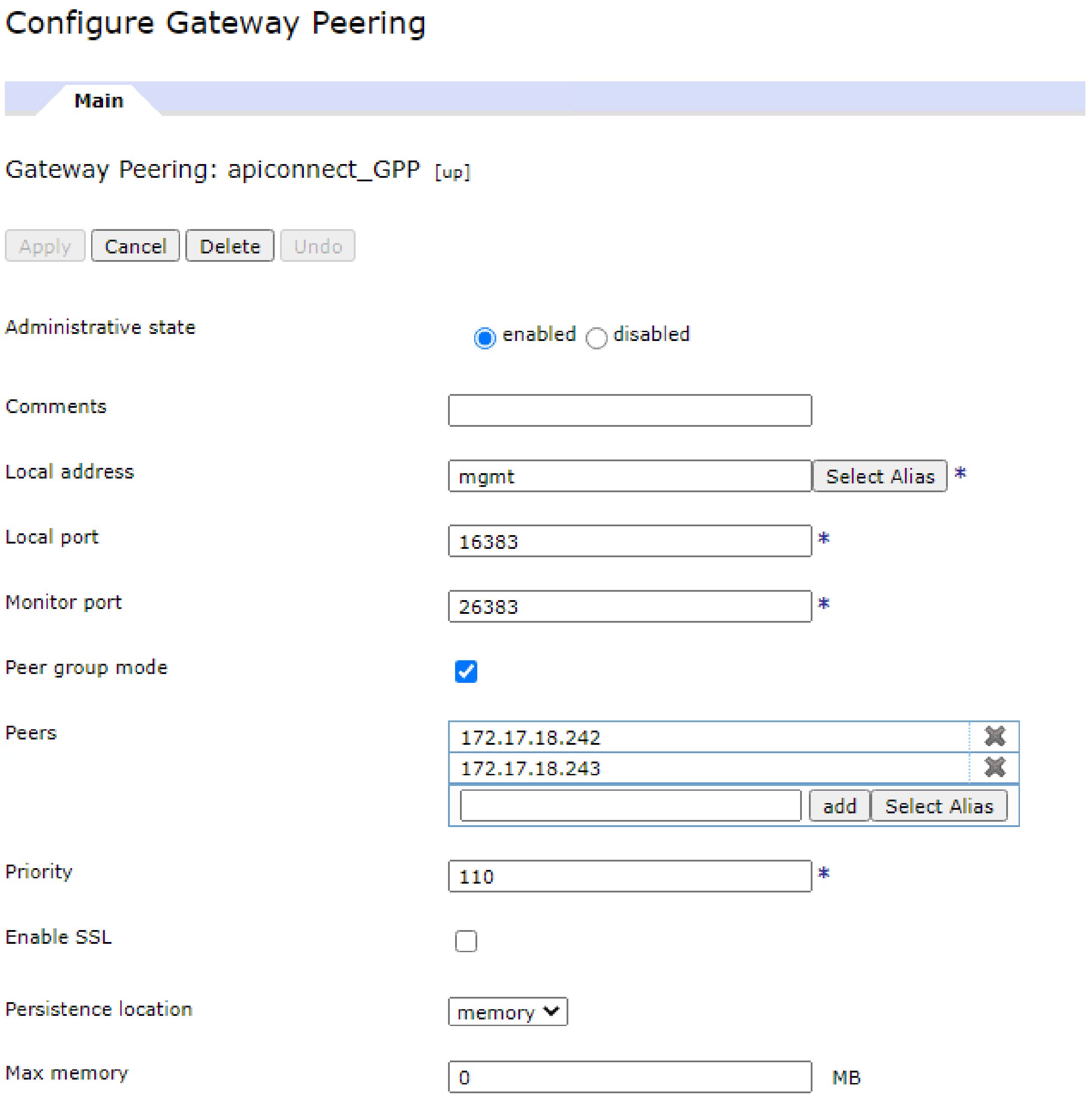
Administrative state	● enabled ○ disabled
Comments	
Local address	mgmt *
Local port	16380 *
Monitor port	26380 *
Peer group mode	☑
Peers	172.17.18.242 172.17.18.243
Priority	110 *
Enable SSL	□
Persistence location	memory
Max memory	0 MB



Configure Gateway Peering

Gateway Peering: apiconnect_GPGRL [up]

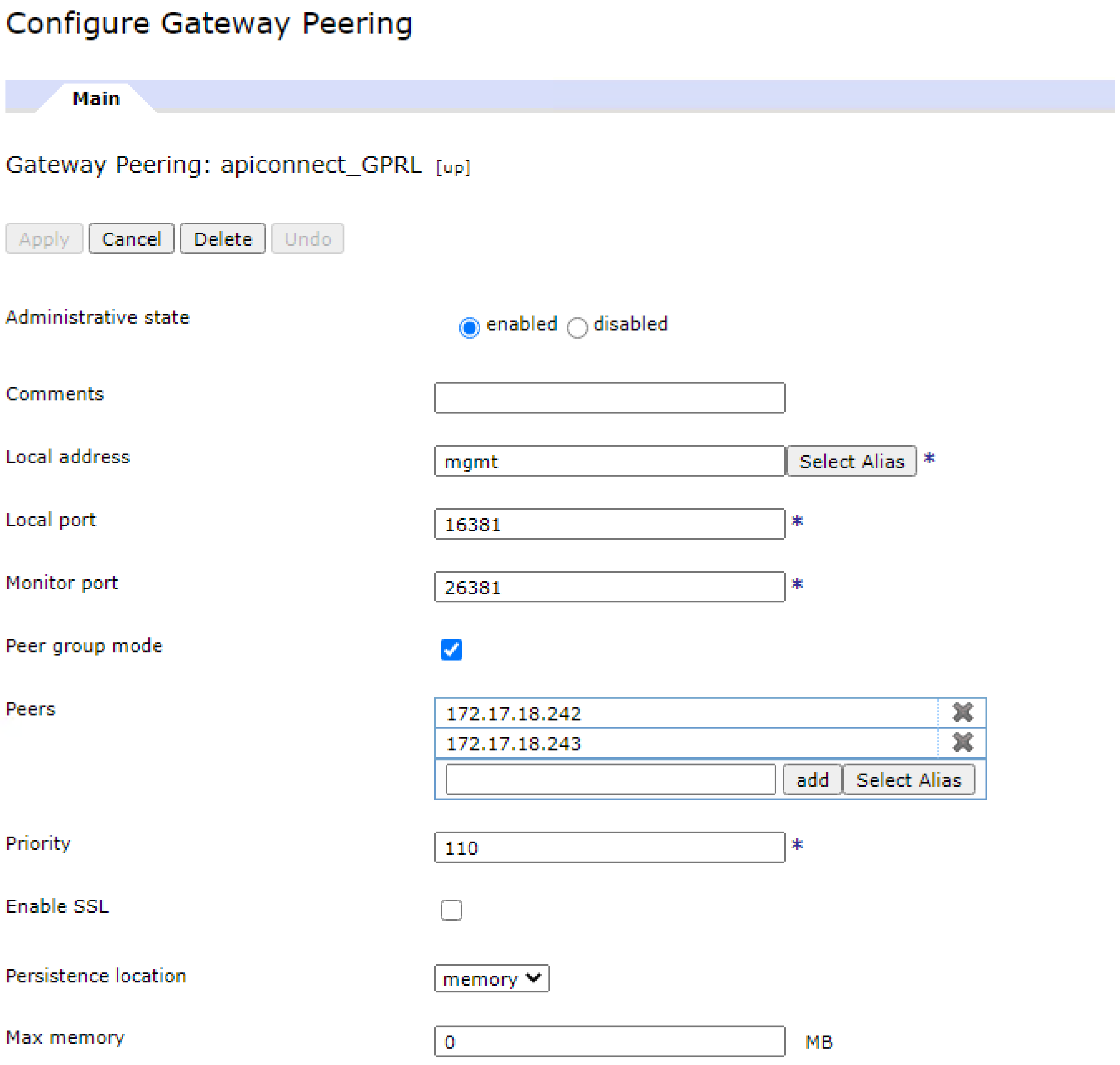
Administrative state	● enabled ○ disabled
Comments	
Local address	mgmt *
Local port	16384 *
Monitor port	26384 *
Peer group mode	☑
Peers	172.17.18.242 172.17.18.243
Priority	110 *
Enable SSL	□
Persistence location	memory
Max memory	0 MB



Configure Gateway Peering

Gateway Peering: apiconnect_GPP [up]

Administrative state	● enabled ○ disabled
Comments	
Local address	mgmt *
Local port	16383 *
Monitor port	26383 *
Peer group mode	☑
Peers	172.17.18.242 ☒ 172.17.18.243 ☒
Priority	110 *
Enable SSL	□
Persistence location	memory
Max memory	0 MB

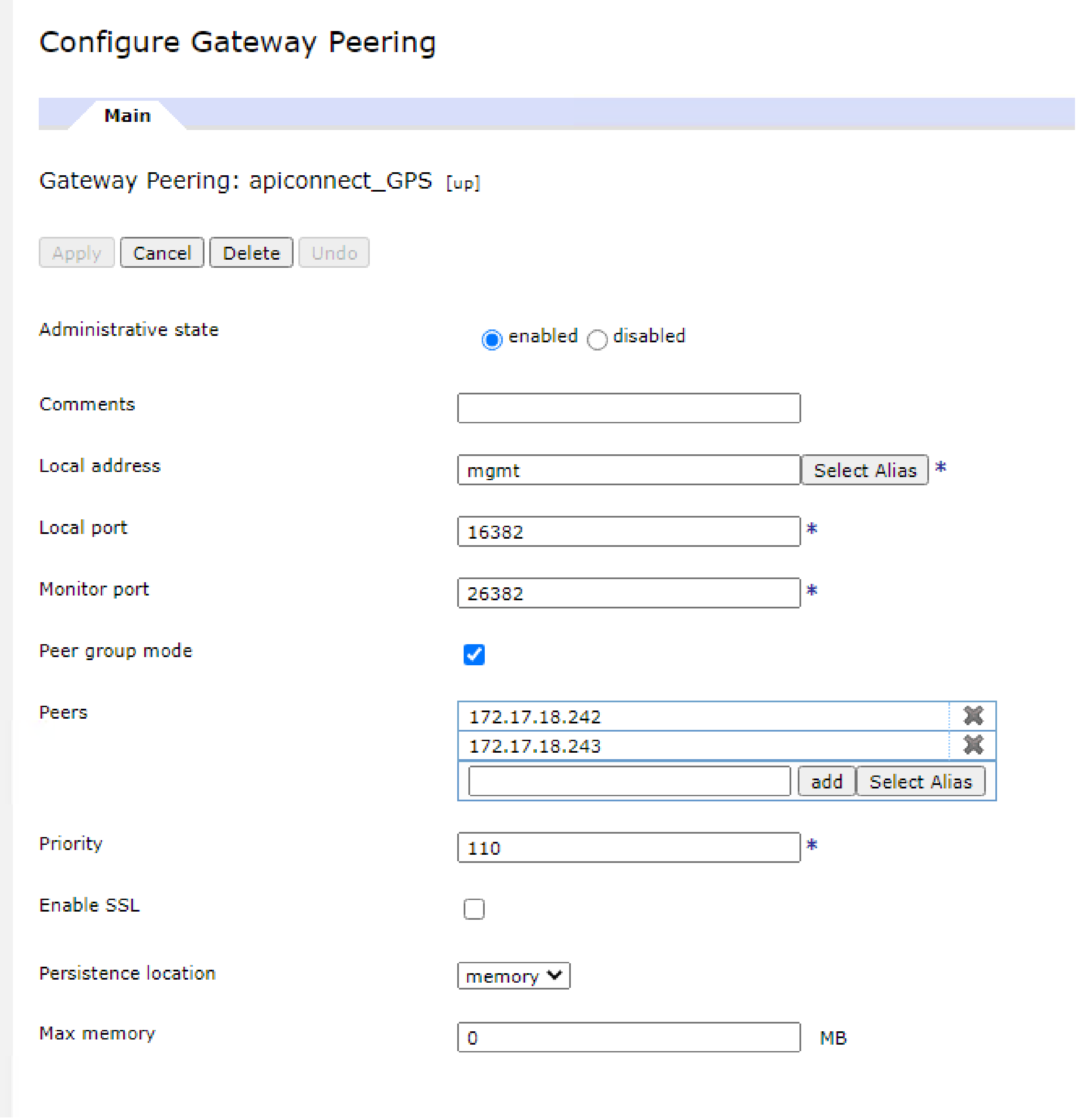


Configure Gateway Peering

Main

Gateway Peering: apiconnect_GPRL [up]

Administrative state	● enabled ○ disabled
Comments	
Local address	mgmt Select Alias *
Local port	16381 *
Monitor port	26381 *
Peer group mode	☑
Peers	172.17.18.242 ✖ 172.17.18.243 ✖ add Select Alias
Priority	110 *
Enable SSL	□
Persistence location	memory
Max memory	0 MB

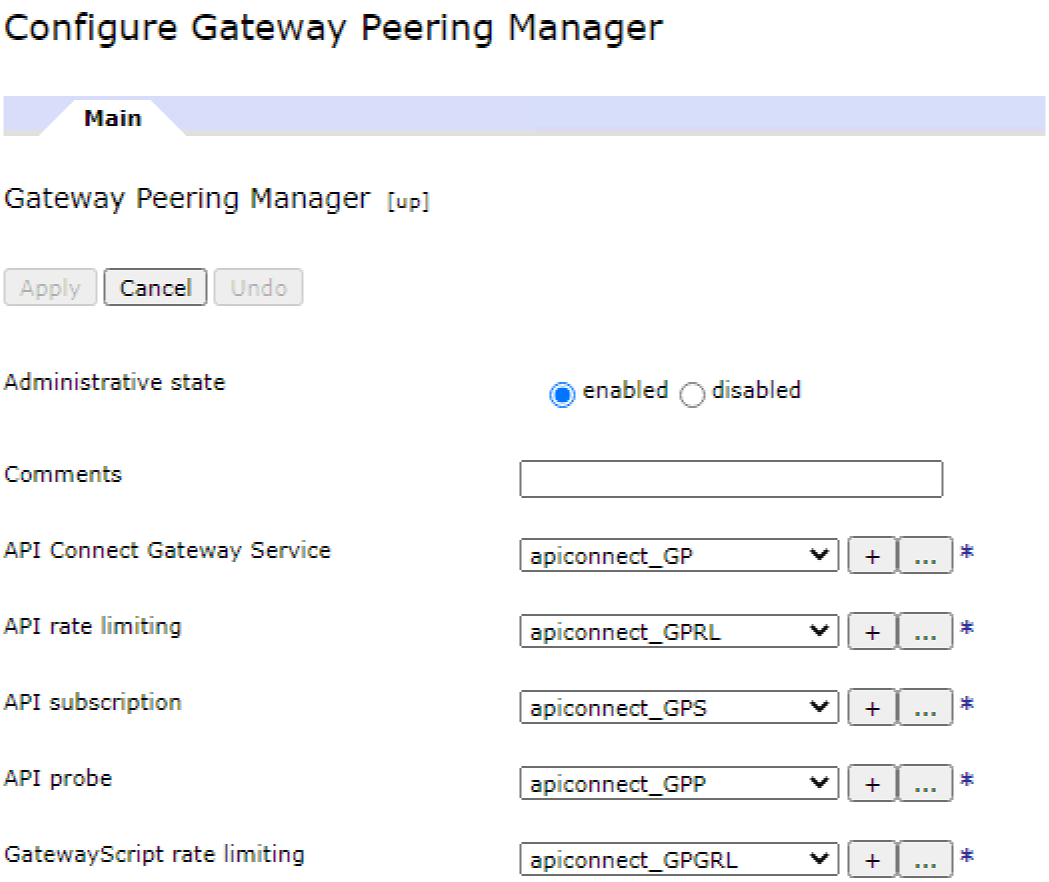


Configure Gateway Peering

Gateway Peering: apiconnect_GPS [up]

Administrative state	● enabled ○ disabled
Comments	
Local address	mgmt [Select Alias] *
Local port	16382 *
Monitor port	26382 *
Peer group mode	☑
Peers	172.17.18.242 172.17.18.243 [add] [Select Alias]
Priority	110 *
Enable SSL	□
Persistence location	memory
Max memory	0 MB

12. Navigate to Objects→ Configuration Management → Gateway Peering Management or search for Peering Manager.
13. Select defined peering group for API Connect Gateway Service, Rate Limit and Subscription, Probe, Gateway Script rate Limit. Check administrative state “enabled” and click apply.

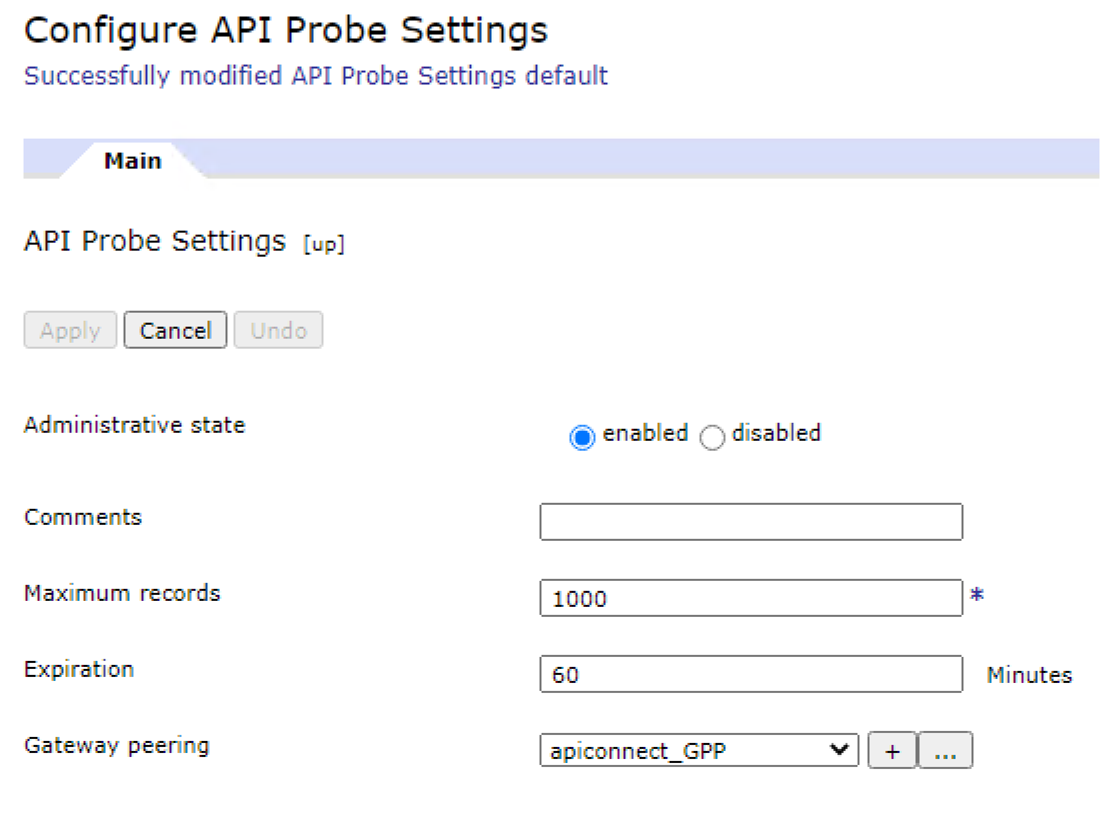


Configure Gateway Peering Manager

Gateway Peering Manager [up]

Administrative state	● enabled ○ disabled
Comments	
API Connect Gateway Service	apiconnect_GP *
API rate limiting	apiconnect_GPRL *
API subscription	apiconnect_GPS *
API probe	apiconnect_GPP *
GatewayScript rate limiting	apiconnect_GPGRL *

14. Navigate to Objects→Configuration Management→API Probe Setting or search for API probe.



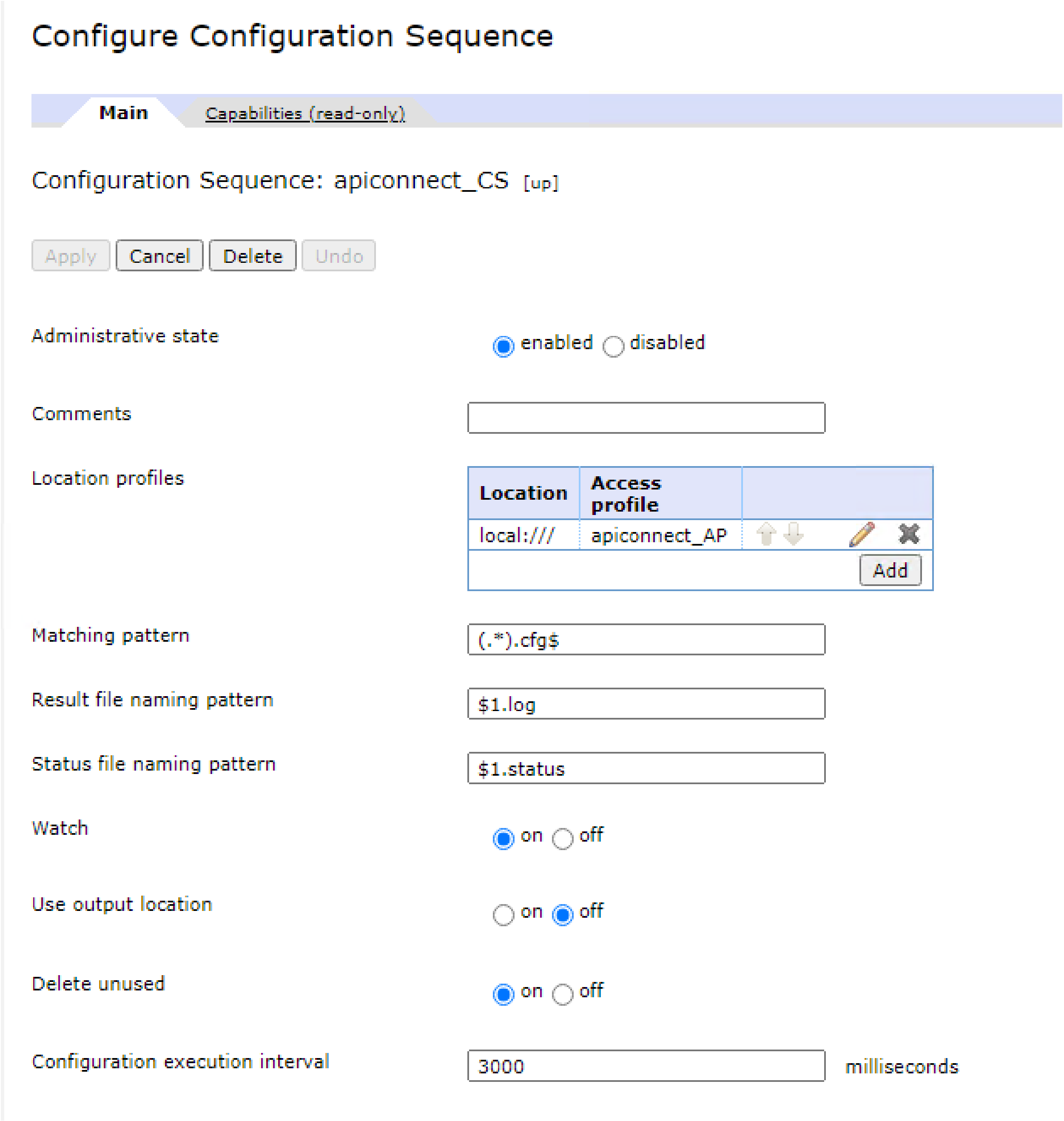
Configure API Probe Settings

Successfully modified API Probe Settings default

API Probe Settings [up]

Administrative state	● enabled ○ disabled
Comments	
Maximum records	1000 *
Expiration	60 Minutes
Gateway peering	apiconnect_GPP

15. Navigate to Objects→Configuration Management→Configuration Sequence or search for configuration sequence.
16. Press “Add” button and define location profiles as shown in the figure:



Configure Configuration Sequence

Configuration Sequence: apiconnect_CS [up]

Administrative state ● enabled ○ disabled

Comments

Location profiles

Location	Access profile
local:///	apiconnect_AP

Matching pattern (.*).cfg$

Result file naming pattern $1.log

Status file naming pattern $1.status

Watch ● on ○ off

Use output location ○ on ● off

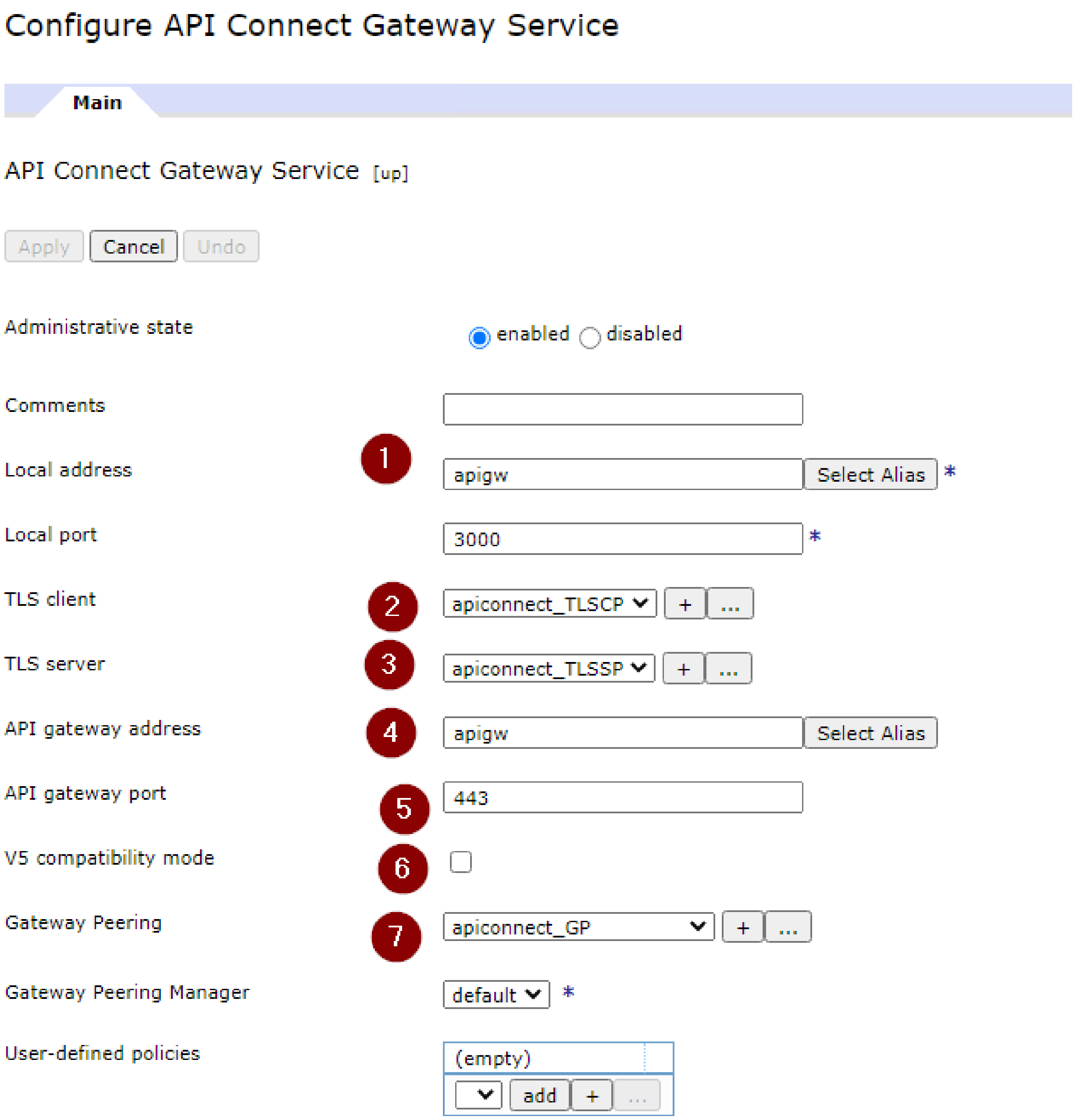
Delete unused ● on ○ off

Configuration execution interval 3000 milliseconds

17. Navigate to Objects→Service Configuration→ API Connect Gateway Service or search for API Connect.
18. Select defined host alias in section "First Configurations on WebGUI", defined TLS client in step 6, defined TLS server in step 8, defined gateway peering in step 10 and uncheck "V5 compatibility mode"

    Note: You may change the API gateway port to 443 if nothing listens this port.

    For difference between V5 compatibility and Gateway please check this link: https://www.ibm.com/support/knowledgecenter/en/SSMNED_2018/com.ibm.apic.overview.doc/rapic_gateway_types.html



Configure API Connect Gateway Service

Main

API Connect Gateway Service [up]

Apply | Cancel | Undo

Administrative state	● enabled ○ disabled
Comments	
Local address	apigw [Select Alias] *
Local port	3000 *
TLS client	apiconnect_TLSCP [+] [...]
TLS server	apiconnect_TLSSP [+] [...]
API gateway address	apigw [Select Alias]
API gateway port	443
V5 compatibility mode	□
Gateway Peering	apiconnect_GP [+] [...]
Gateway Peering Manager	default *
User-defined policies	(empty) [add] [+] [...]

Upgrading Firmware

1. Download the same firmware version with API Connect components. **(10.0.1.1)**
2. Click “System Control” at the home page.
3. Upload .scyrpt4 file and press “Boot Image” button.

References and Links

You may find useful links below:

1. DataPower VMware deployment: https://www.ibm.com/support/knowledgecenter/SSMNED_v10/com.ibm.apic.install.doc/tapic_install_datapower_gateway.html