SOPHOS
Security made simple.

PocketGuide

Disable Telnet and HTTP behavior

For Customers with Sophos Firewall
Document Date: November 2016

Contents

Overview

If HTTP is enabled in v15, for admin port, HTTP services will be redirected to HTTPS. In v16, HTTP service is removed.
Telnet services will be discontinued from next release, with a warning message to use SSH instead of Telnet. The message shown is “Telnet service will be discontinued from next release so we recommend that you use SSH service".

Fresh Installation / Factory Reset

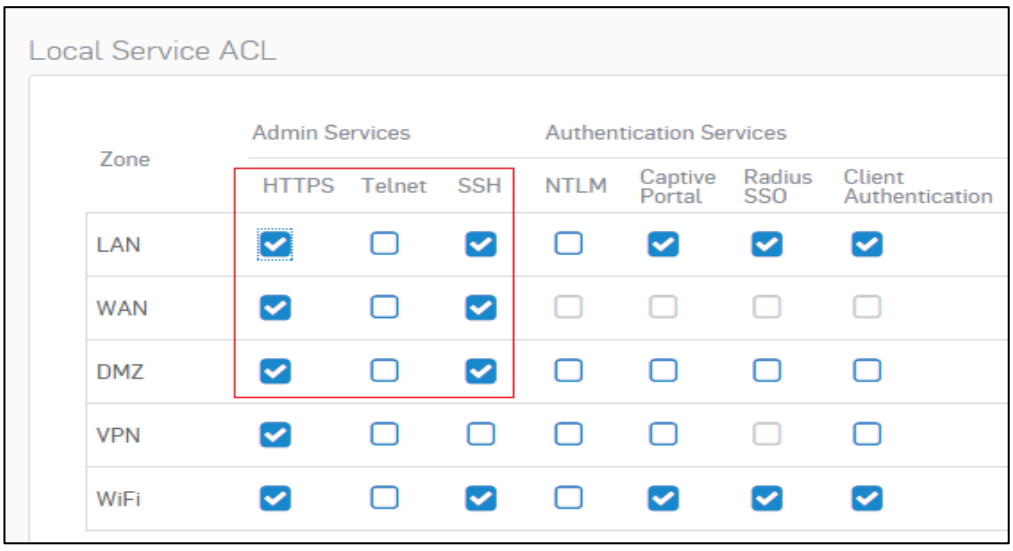
For Fresh Installation / Factory reset / RESET -3 ad Wizard in Copernicus v16, http service is removed from device access, admin port setting, zone and local service ACL exception rule.

Telnet service would be available in device access, zone and local service ACL exception rule but once you try to enable in v16 it would give you message "Telnet service will be discontinued from next release so we recommend that you use SSH service".

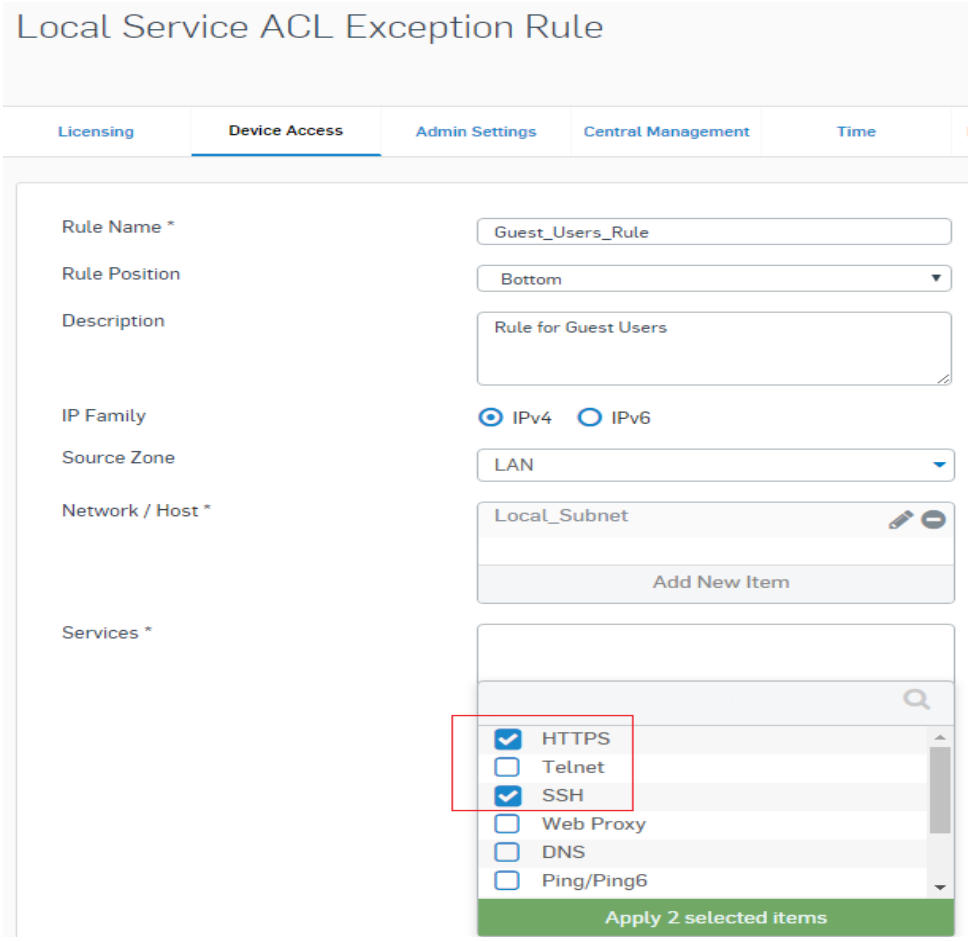
HTTP service

HTTP service option removed from following in v16:

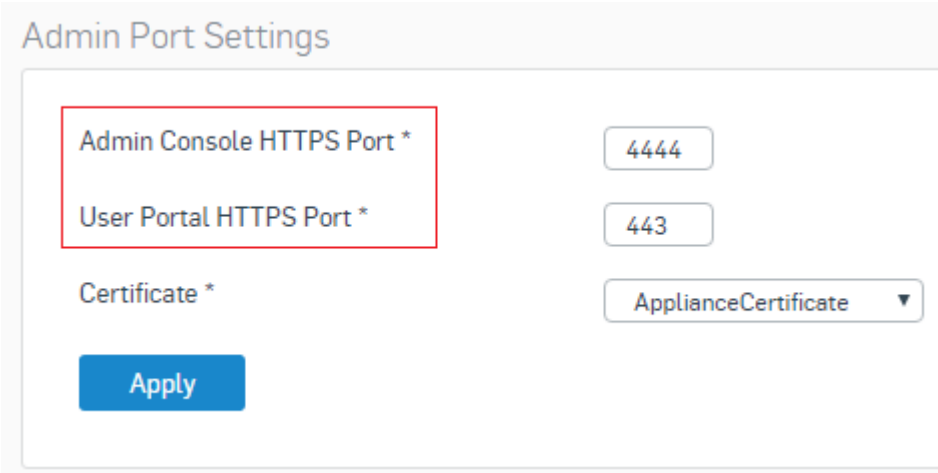
- **System>Administration> Device Access > Zone**



- **System>Administration> Device Access > Local Service ACL Exception Rule**

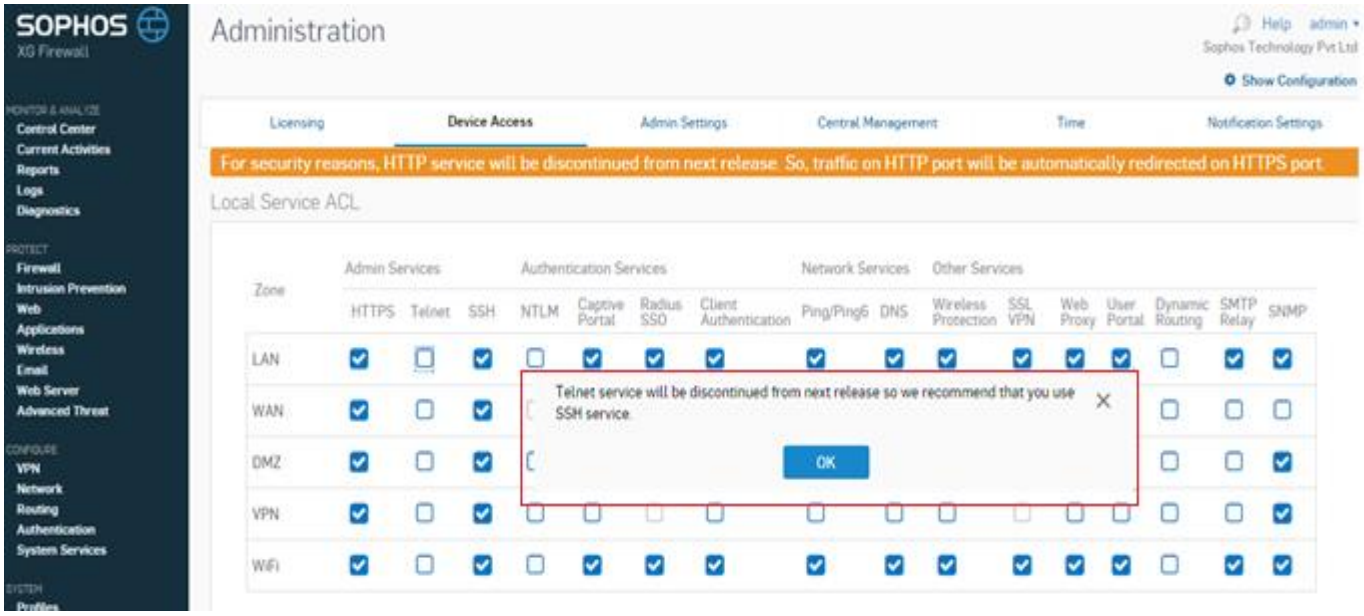


- **System>Administration> Admin Settings>Admin Port Settings**



Telnet Service

Telnet service would be available in the pages listed above. However, it gives a warning message as shown below:



Behavior List

Fresh Installation/Factory Reset/RESET-3/Wizard	Device Access	Admin Port setting	Zone	Local Service ACL Exception Rule
HTTP	NA	NA	NA	NA
HTTPS	Yes	Yes	Yes	Yes
Telnet	Yes	NA	Yes	Yes
SSH	Yes	NA	Yes	Yes

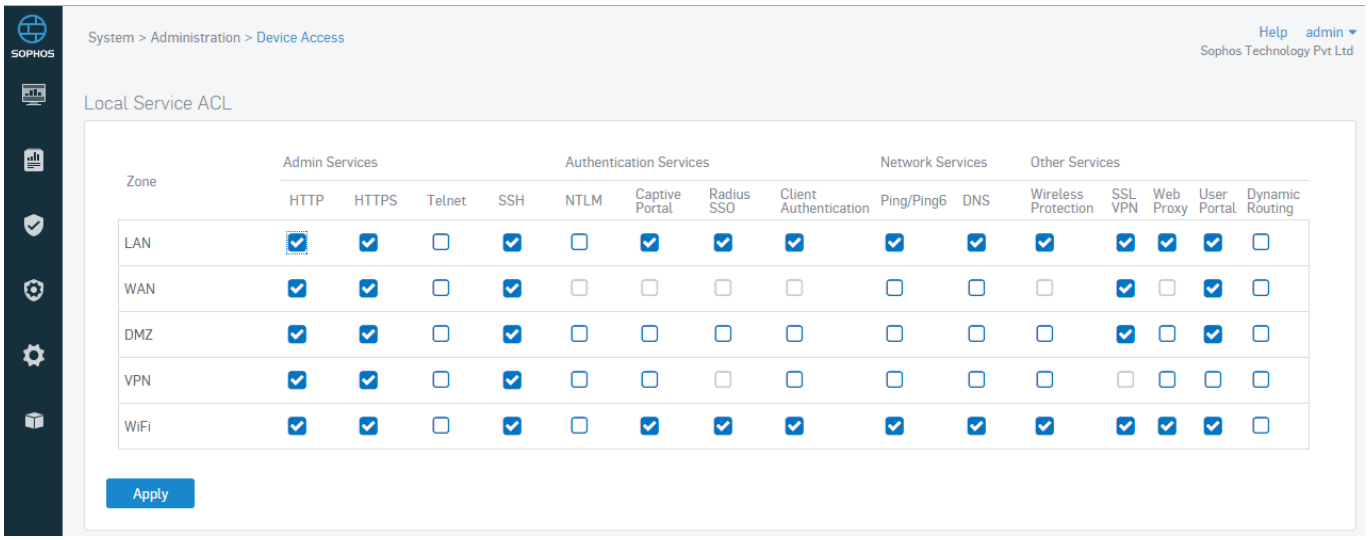
v15 to v16 Migration

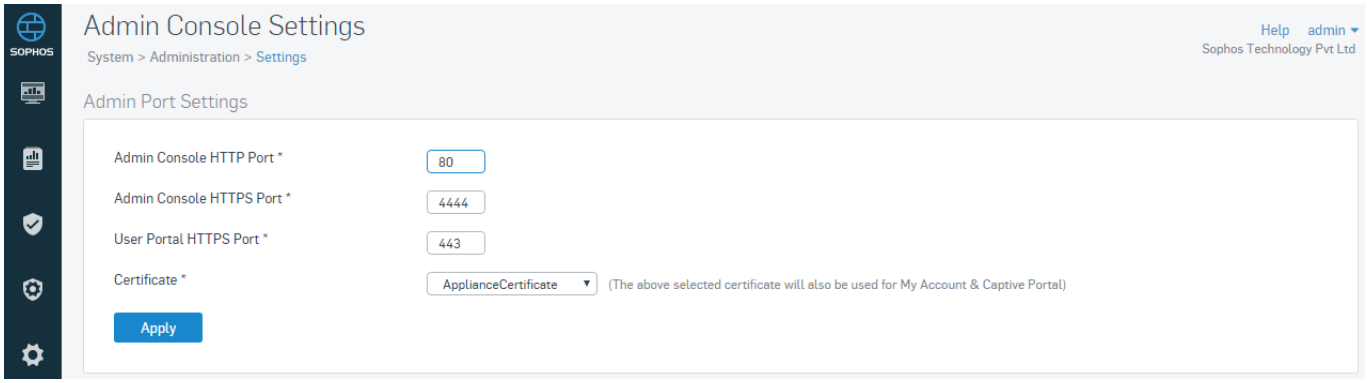
Device Access and Admin Port Settings: HTTP

The following will be version 15 to version 16 migration behavior for HTTP:

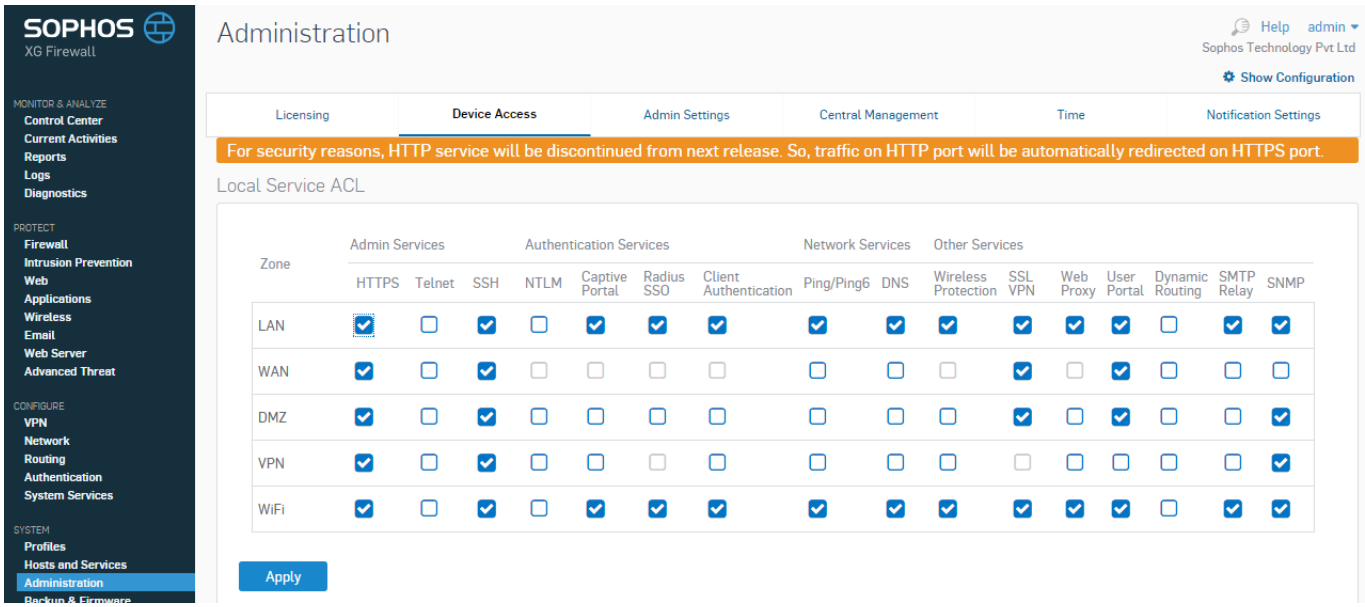
- If HTTP enabled in v15, after migration to v16, HTTP request will be redirected to HTTPS
- If HTTP is not enabled in v15, after migration to v16, HTTP request will **not** be redirected to HTTPS

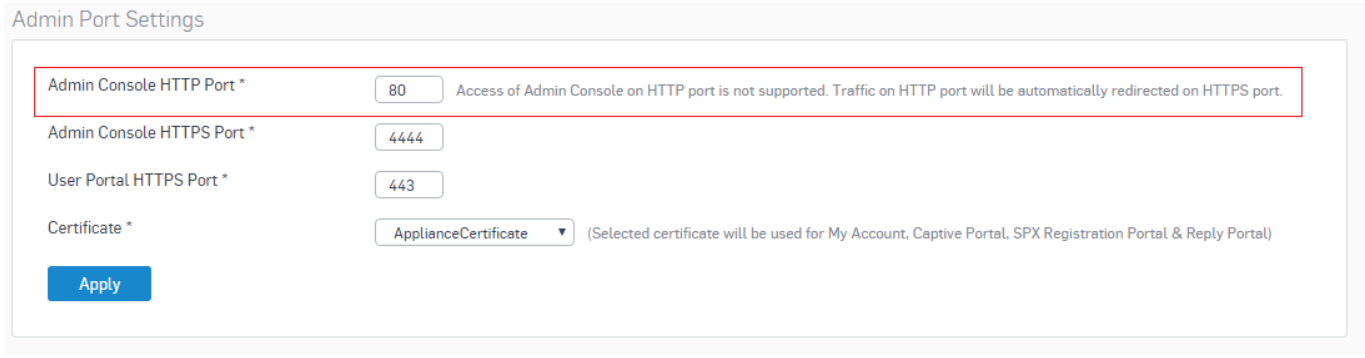
Device Access and Admin Port Settings in v15 (HTTP Enabled):





Device Access and Admin Port Settings in v16:





Local ACL Rule Exception: HTTP

The following will be version 15 to version 16 migration behavior for Local ACL Rule:

- Local ACL rule for HTTP created with 'DROP' action would be deleted during v15 to v16 migration
- Local ACL rule for HTTP created with Accept would be converted with HTTPs in v15 to v16 migration

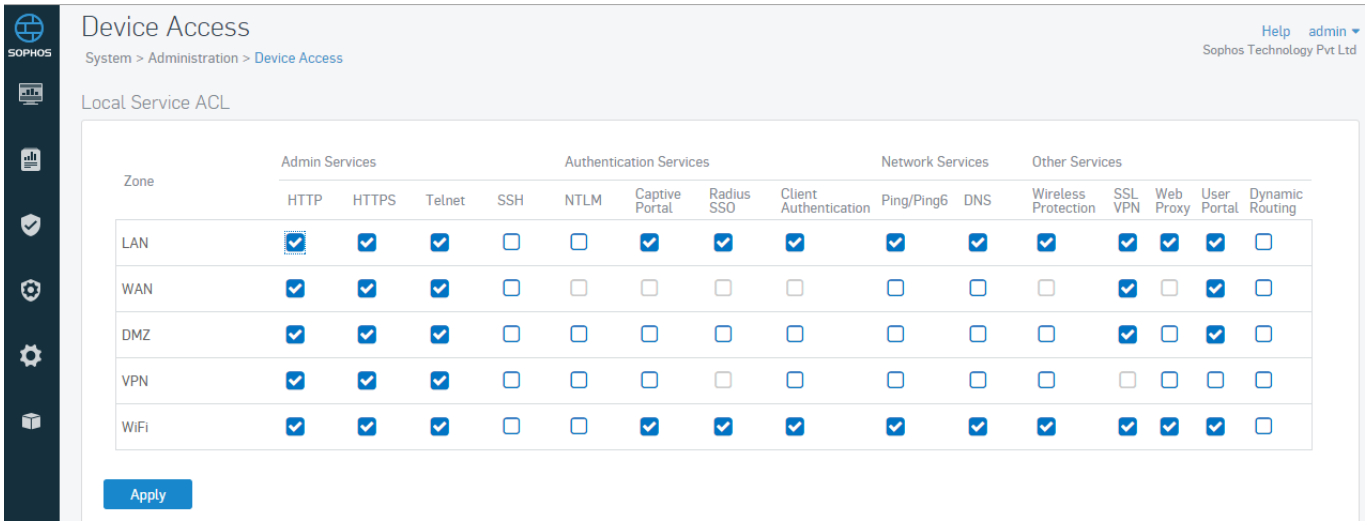
Local ACL Rules - LAN/WAN/DMZ/VPN/Wi-Fi/Custom to Local Zone **for HTTP:**

Rules Details	In V15	After Migration to V16
Rule1	Drop HTTP	Rule is deleted
Rule2	Allow HTTP	Allow HTTPS
Rule3	Allow HTTPS ,SSH	Allow HTTPS , SSH
Rule4	Allow HTTP, HTTPS, SSH	Allow HTTPS, SSH
Rule5	Drop HTTP, HTTPS, SSH	Drop HTTPS, SSH
Rule6	Allow HTTP, SSH	Allow HTTPS , SSH

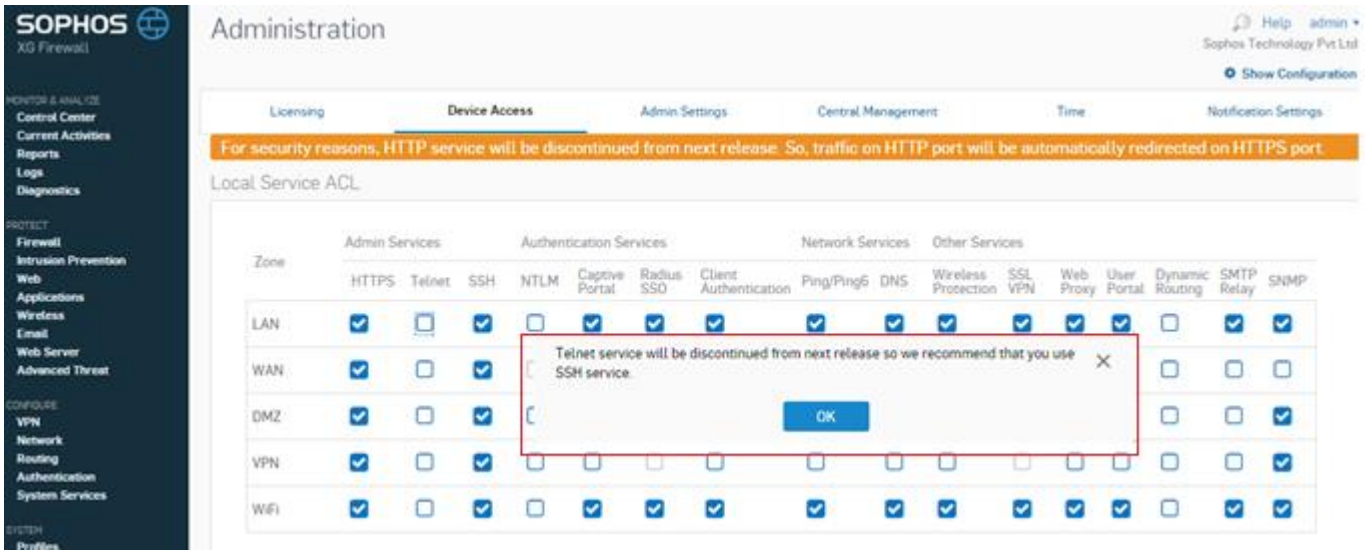
Device Access Settings: Telnet

Telnet service would be available in device access, zone and local service ACL exception rule but once you try to enable in v16 it would give you message "Telnet service will be discontinued from next release so we recommend that you use SSH service".

Telnet Enabled in v15:



Telnet Service Message in v16:



Local ACL Rules- LAN/WAN/DMZ/VPN/Wifi/Custom to Local Zone for Telnet:

Rules Details	In V15	After Migration to V16
Rule1	Drop Telnet	Drop Telnet
Rule2	Allow Telnet	Allow SSH
Rule3	Allow HTTPS ,SSH	Allow HTTPS , SSH
Rule4	Allow Telnet, HTTPS, SSH	Allow HTTPS, SSH
Rule5	Drop Telnet, HTTPS, SSH	Drop Telnet, HTTPS, SSH
Rule6	Allow HTTPS, Telnet	Allow HTTPS , SSH

Migration Behavior during Deployment: HTTP

E: Enabled, D: Disabled, A: Available, NA: Not Available

V15					After Migration to V16				
Services	**Device Access-HTTP**	**Device Access-HTTPS**	**Admin Port setting**	**Zone**	**HTTP to HTTPS Redirection**	**Device Access-HTTP**	**Device Access-HTTPS**	**Admin Port setting**	**Zone**
HTTP	E	E	Yes-Default/Custom	A	Work	NA-With Notification	Yes	Yes with Notification	NA
HTTP	E	D	Yes-Default/Custom	A	Work	NA-With Notification	Yes	Yes with Notification	NA
HTTP	D	E	Yes-Default/Custom	A	Won't work	NA-without notification	Yes	NA	NA
HTTPS	No Behaviour change directly to HTTPS and in above scenario.				No Behaviour change directly to HTTPS. It would react as per HTTP Configuration in previous version like above scenario.				

Migration Behavior during Deployment: Telnet

E: Enabled, D: Disabled, A: Available, NA: Not Available

V15				After Migration to V16		
Services	**Device Access-Telnet**	**Device Access-SSH**	**Zone**	**Device Access-Telnet**	**Device Access-SSH**	**Zone**
Telnet	E	E	A	Disabled but Available for configuration with warning message	E	Disabled but Available for configuration with warning message
Telnet	E	D	A	Disabled but Available for configuration with warning message	E	Disabled but Available for configuration with warning message

V15				After Migration to V16		
Telnet	D	E	A	Disabled but Available for configuration with warning message	E	Disabled but Available for configuration with warning message
Telnet	D	D	A	Disabled but Available for configuration with warning message	Disabled but Available to configure	Disabled but Available for configuration with warning message

Copyright Notice