

SOPHOS

Security made simple.



Pocket Guide

Disable Telnet and HTTP behavior

For Customers with Sophos Firewall

Document Date: November 2016

Contents

| | |
|--|----|
| Overview..... | 3 |
| Fresh Installation / Factory Reset | 3 |
| <i>HTTP service</i> | 3 |
| <i>Telnet Service</i> | 4 |
| <i>Behavior List</i> | 5 |
| v15 to v16 Migration | 5 |
| <i>Device Access and Admin Port Settings: HTTP</i> | 5 |
| <i>Device Access Settings: Telnet</i> | 8 |
| Migration Behavior during Deployment: HTTP | 9 |
| Migration Behavior during Deployment: Telnet..... | 9 |
| Copyright Notice..... | 10 |

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**

| Zone | Admin Services | | | Authentication Services | | | |
|------|-------------------------------------|--------------------------|-------------------------------------|--------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| | HTTPS | Telnet | SSH | NTLM | Captive Portal | Radius SSO | Client Authentication |
| LAN | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| WAN | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| DMZ | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| VPN | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| WiFi | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

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

Local Service ACL Exception Rule

Licensing | **Device Access** | Admin Settings | Central Management | Time

Rule Name *

Rule Position

Description

IP Family IPv4 IPv6

Source Zone

Network / Host *

Services *

- HTTPS
- Telnet
- SSH
- Web Proxy
- DNS
- Ping/Ping6

Apply 2 selected items

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

Admin Port Settings

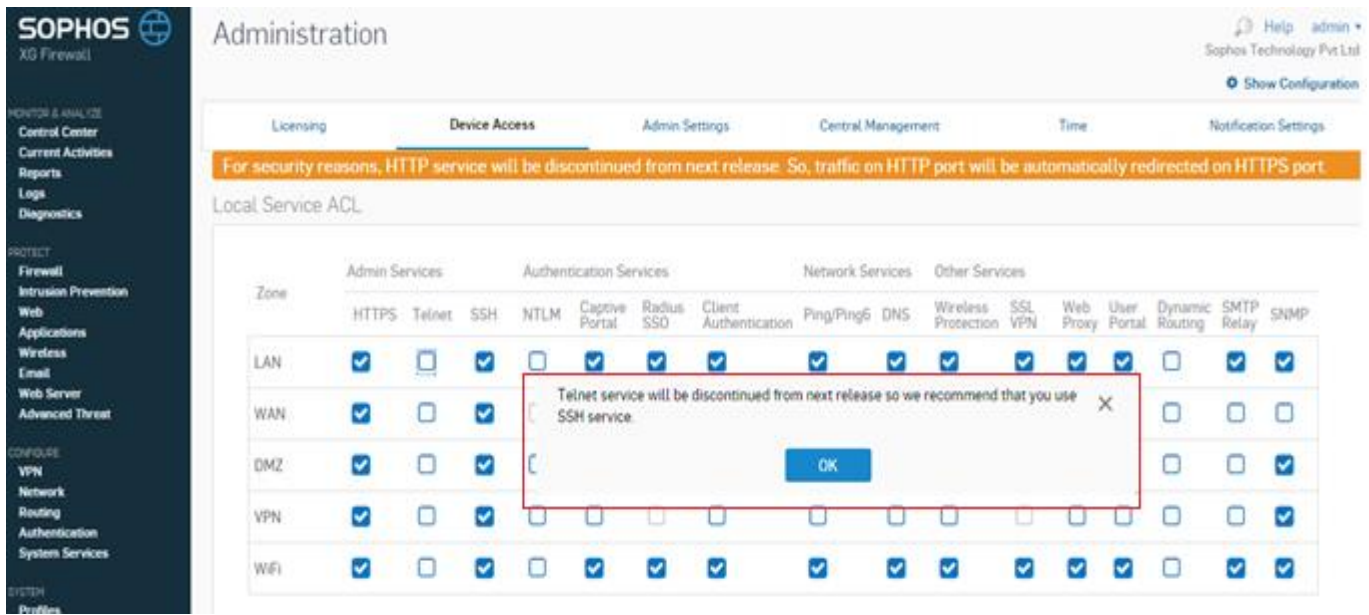
Admin Console HTTPS Port *

User Portal HTTPS Port *

Certificate *

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):

System > Administration > Device Access Help admin ▾
Sophos Technology Pvt Ltd

Local Service ACL

| Zone | Admin Services | | | | Authentication Services | | | | Network Services | | Other Services | | | | |
|------|-------------------------------------|-------------------------------------|--------------------------|-------------------------------------|--------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|--------------------------|
| | HTTP | HTTPS | Telnet | SSH | NTLM | Captive Portal | Radius SSO | Client Authentication | Ping/Ping6 | DNS | Wireless Protection | SSL VPN | Web Proxy | User Portal | Dynamic Routing |
| LAN | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| WAN | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| DMZ | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| VPN | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| WiFi | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |

System > Administration > Settings Help admin ▾
Sophos Technology Pvt Ltd

Admin Console Settings

Admin Port Settings

Admin Console HTTP Port *

Admin Console HTTPS Port *

User Portal HTTPS Port *

Certificate * (The above selected certificate will also be used for My Account & Captive Portal)

Device Access and Admin Port Settings in v16:

The screenshot shows the 'Administration' page in the Sophos Firewall console. A warning banner at the top states: "For security reasons, HTTP service will be discontinued from next release. So, traffic on HTTP port will be automatically redirected on HTTPS port." Below this, the 'Local Service ACL' table is displayed. The table has columns for 'Zone' and various services: Admin Services (HTTPS, Telnet, SSH), Authentication Services (NTLM, Captive Portal, Radius SSO, Client Authentication), Network Services (Ping/Ping6, DNS), and Other Services (Wireless Protection, SSL VPN, Web Proxy, User Portal, Dynamic Routing, SMTP Relay, SNMP). The LAN zone has checkboxes checked for HTTPS, SSH, Captive Portal, Radius SSO, Client Authentication, Ping/Ping6, DNS, and Wireless Protection. Other zones (WAN, DMZ, VPN, WiFi) have different combinations of services checked.

The screenshot shows the 'Admin Port Settings' configuration page. It includes input fields for 'Admin Console HTTP Port *' (set to 80), 'Admin Console HTTPS Port *' (set to 4444), and 'User Portal HTTPS Port *' (set to 443). A 'Certificate *' dropdown is set to 'ApplianceCertificate'. A red box highlights the 'Admin Console HTTP Port *' field and the text below it: "Access of Admin Console on HTTP port is not supported. Traffic on HTTP port will be automatically redirected on HTTPS port." An 'Apply' button is at the bottom left.

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:

The screenshot shows the 'Device Access' configuration page for v15. Under 'Local Service ACL', a table lists services for various zones. Telnet is enabled (checked) for all zones: LAN, WAN, DMZ, VPN, and WiFi.

| Zone | Admin Services | | Authentication Services | | | | Network Services | | Other Services | | | | | | |
|------|-------------------------------------|-------------------------------------|-------------------------------------|--------------------------|--------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|--------------------------|
| | HTTP | HTTPS | Telnet | SSH | NTLM | Captive Portal | Radius SSO | Client Authentication | Ping/Ping6 | DNS | Wireless Protection | SSL VPN | Web Proxy | User Portal | Dynamic Routing |
| LAN | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| WAN | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| DMZ | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| VPN | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| WiFi | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |

Telnet Service Message in v16:

The screenshot shows the 'Administration' page for v16. A warning message is displayed: "For security reasons, HTTP service will be discontinued from next release. So, traffic on HTTP port will be automatically redirected on HTTPS port." Below this, a dialog box is shown with the message: "Telnet service will be discontinued from next release so we recommend that you use SSH service." The dialog box has an 'OK' button.

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

Copyright 2015-2016 Sophos Limited. All rights reserved.

Sophos is a registered trademark of Sophos Limited and Sophos Group. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the license terms or you otherwise have the prior permission in writing of the copyright owner.