Technical Support Guide

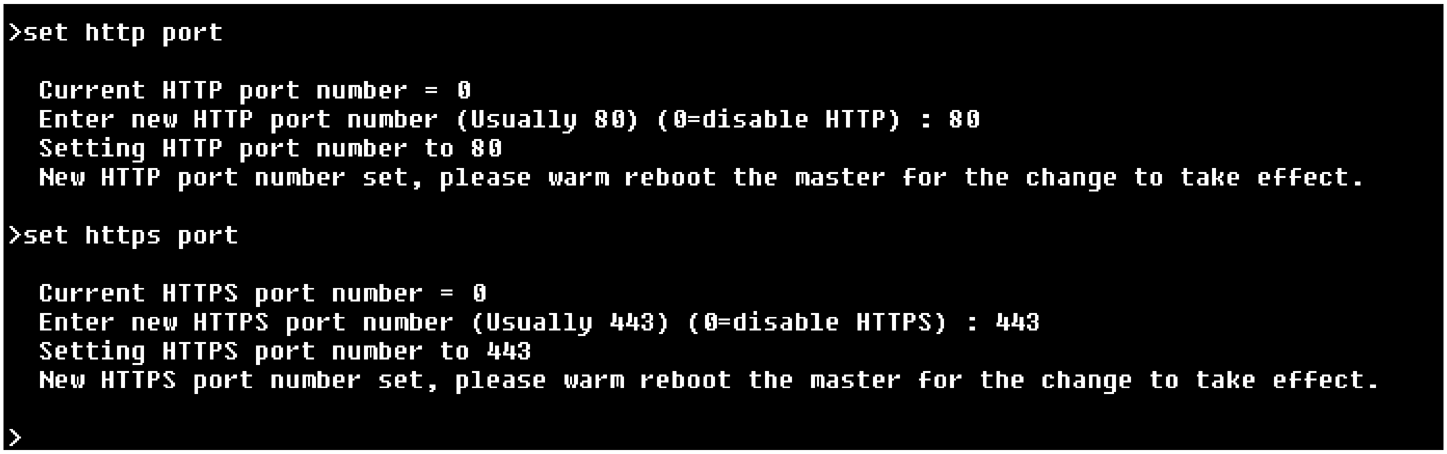
v1.0

7-Jun-21

Enable Server Ports via Telnet or SSH on NX Controllers

If HTTP/HTTPS/Telnet/SSH/FTP has been disabled using the web console and you need to re-enable from telnet or SSH there will be 2 separate settings for each protocol that need to be altered, the port number and the enable/disable flag.

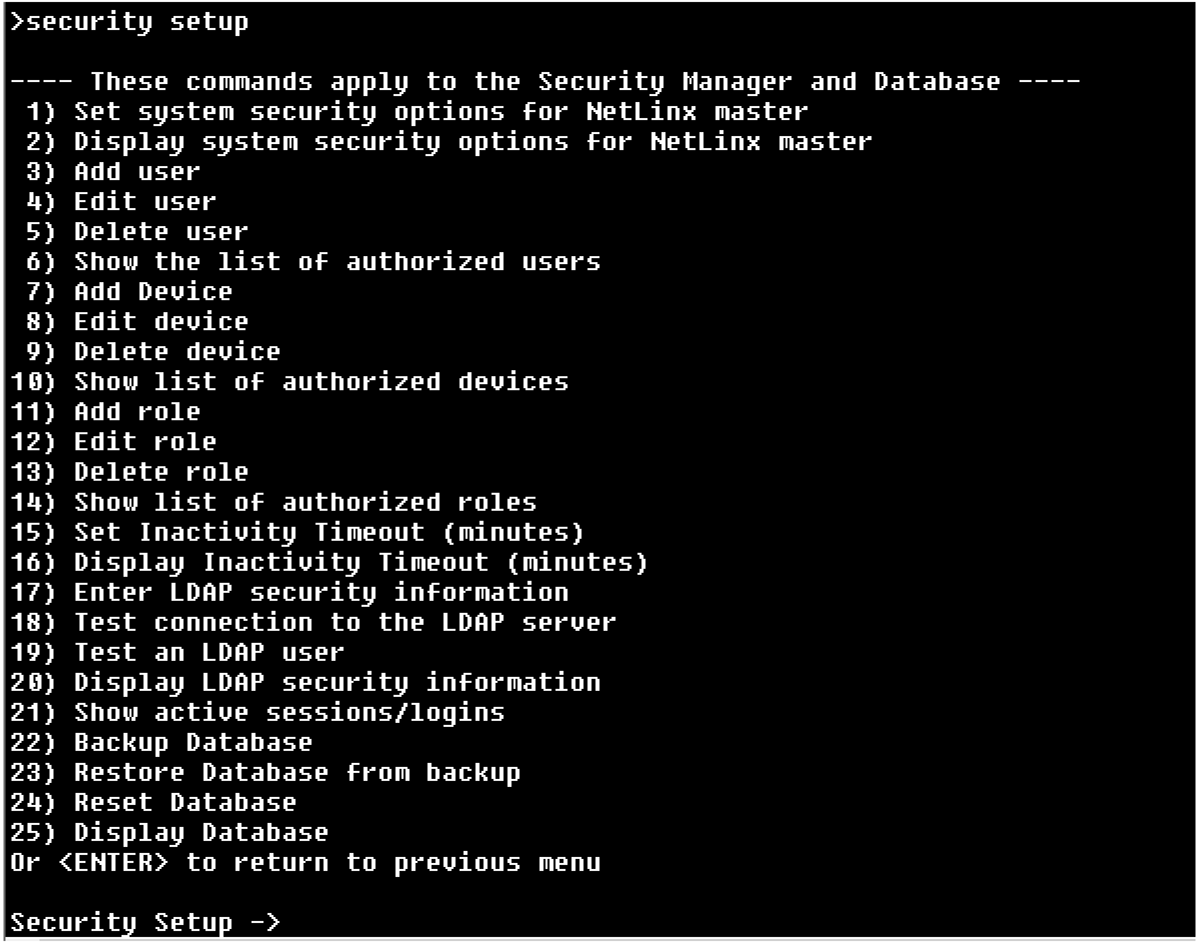
The first step will be the step that most people are familiar with and it is to set the ports using the 'SET HTTP PORT' 'SET HTTPS PORT' 'SET TELNET PORT' 'SET SSH PORT' or 'SET FTP PORT' telnet commands and entering your desired port number when prompted.



```
>set http port

  Current HTTP port number = 0
  Enter new HTTP port number (Usually 80) (0=disable HTTP) : 80
  Setting HTTP port number to 80
  New HTTP port number set, please warm reboot the master for the change to take effect.

>set https port

  Current HTTPS port number = 0
  Enter new HTTPS port number (Usually 443) (0=disable HTTPS) : 443
  Setting HTTPS port number to 443
  New HTTPS port number set, please warm reboot the master for the change to take effect.

>
```

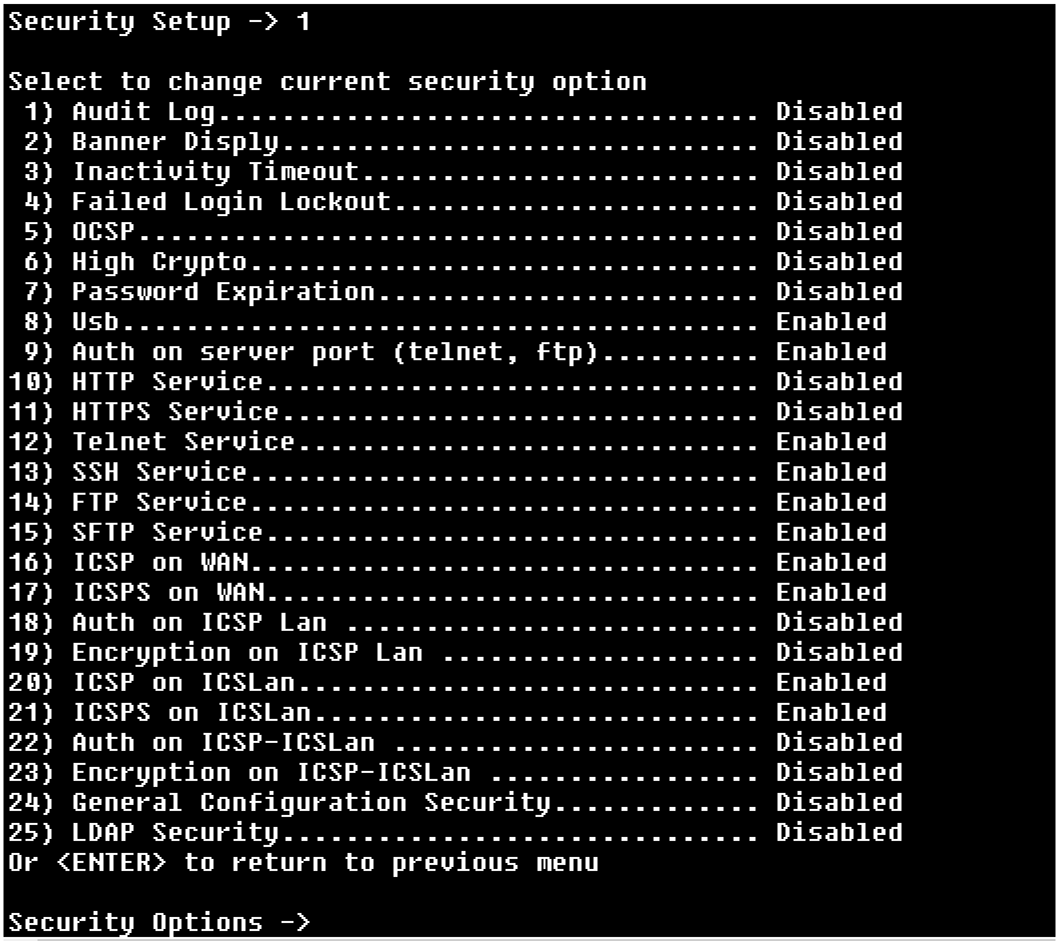
For step 2 you must go into the security setup menu, the system security options submenu, and enable the communications protocol that you are working on.

1. SECURITY SETUP - This will enter the security setup menu and give you a list of options to selection from.



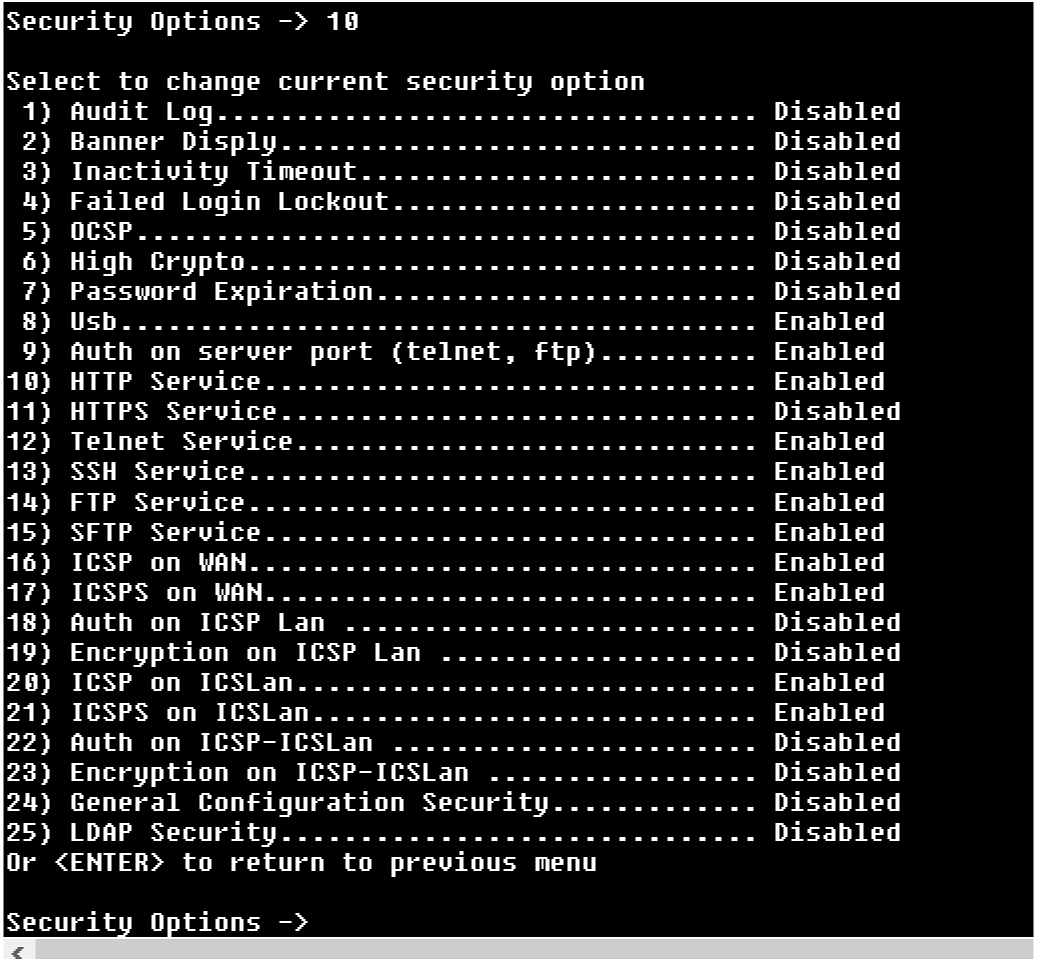
```
>security setup

---- These commands apply to the Security Manager and Database ----
 1) Set system security options for NetLinx master
 2) Display system security options for NetLinx master
 3) Add user
 4) Edit user
 5) Delete user
 6) Show the list of authorized users
 7) Add Device
 8) Edit device
 9) Delete device
10) Show list of authorized devices
11) Add role
12) Edit role
13) Delete role
14) Show list of authorized roles
15) Set Inactivity Timeout (minutes)
16) Display Inactivity Timeout (minutes)
17) Enter LDAP security information
18) Test connection to the LDAP server
19) Test an LDAP user
20) Display LDAP security information
21) Show active sessions/logins
22) Backup Database
23) Restore Database from backup
24) Reset Database
25) Display Database
Or <ENTER> to return to previous menu

Security Setup ->
```

2. At the Security Setup -> prompt enter 1 to enter the submenu “Set system security options for Netlinx Master”.



```
Security Setup -> 1

Select to change current security option
 1) Audit Log.................................. Disabled
 2) Banner Disply.............................. Disabled
 3) Inactivity Timeout......................... Disabled
 4) Failed Login Lockout....................... Disabled
 5) OCSP....................................... Disabled
 6) High Crypto................................ Disabled
 7) Password Expiration........................ Disabled
 8) Usb........................................ Enabled
 9) Auth on server port (telnet, ftp).......... Enabled
10) HTTP Service............................... Disabled
11) HTTPS Service.............................. Disabled
12) Telnet Service............................. Enabled
13) SSH Service................................ Enabled
14) FTP Service................................ Enabled
15) SFTP Service............................... Enabled
16) ICSP on WAN................................ Enabled
17) ICSPS on WAN............................... Enabled
18) Auth on ICSP Lan .......................... Disabled
19) Encryption on ICSP Lan .................... Disabled
20) ICSP on ICSLan............................. Enabled
21) ICSPS on ICSLan............................ Enabled
22) Auth on ICSP-ICSLan ....................... Disabled
23) Encryption on ICSP-ICSLan ................. Disabled
24) General Configuration Security............. Disabled
25) LDAP Security.............................. Disabled
Or <ENTER> to return to previous menu

Security Options ->
```

3. You should now see a list of security options and each option should show enabled or disabled next to it. Enter option 10 for HTTP, 11 for HTTPS, 12 for Telnet Service, 13 for SSH Service, and 14 for FTP Service at the Security Options -> prompt to toggle the options enabled/disable status.



```
Security Options -> 10

Select to change current security option
 1) Audit Log.................................. Disabled
 2) Banner Disply.............................. Disabled
 3) Inactivity Timeout......................... Disabled
 4) Failed Login Lockout....................... Disabled
 5) OCSP....................................... Disabled
 6) High Crypto................................ Disabled
 7) Password Expiration........................ Disabled
 8) Usb........................................ Enabled
 9) Auth on server port (telnet, ftp).......... Enabled
10) HTTP Service............................... Enabled
11) HTTPS Service.............................. Disabled
12) Telnet Service............................. Enabled
13) SSH Service................................ Enabled
14) FTP Service................................ Enabled
15) SFTP Service............................... Enabled
16) ICSP on WAN................................ Enabled
17) ICSPS on WAN............................... Enabled
18) Auth on ICSP Lan .......................... Disabled
19) Encryption on ICSP Lan .................... Disabled
20) ICSP on ICSLan............................. Enabled
21) ICSPS on ICSLan............................ Enabled
22) Auth on ICSP-ICSLan ....................... Disabled
23) Encryption on ICSP-ICSLan ................. Disabled
24) General Configuration Security............. Disabled
25) LDAP Security.............................. Disabled
Or <ENTER> to return to previous menu

Security Options ->
```

4. Press ESC twice to return to the root telnet menu.
5. Enter the command REBOOT to reboot the controller and after it reboots you should have access to the HTTP/HTTPS/Telnet/SSH/FTP web server again.