

# Nipper – Big IP F5 v11.x.x Devices

---

*Multiple Award Winning Security Software*

## **Titania Nipper Version 2.6.2** **Published November 2019**

© Titania Limited 2019. All Rights Reserved

This document is intended to provide advice and assistance for the installation and running of Nipper software. While Titania takes care to ensure that all the information included in this document is accurate and relevant, customers are advised to seek further assistance from our support staff if required.

No part of this documentation may be copied or otherwise duplicated on any medium without prior written consent of Titania Limited, publisher of this work.

The use of Nipper software is subject to the acceptance of the license agreement.

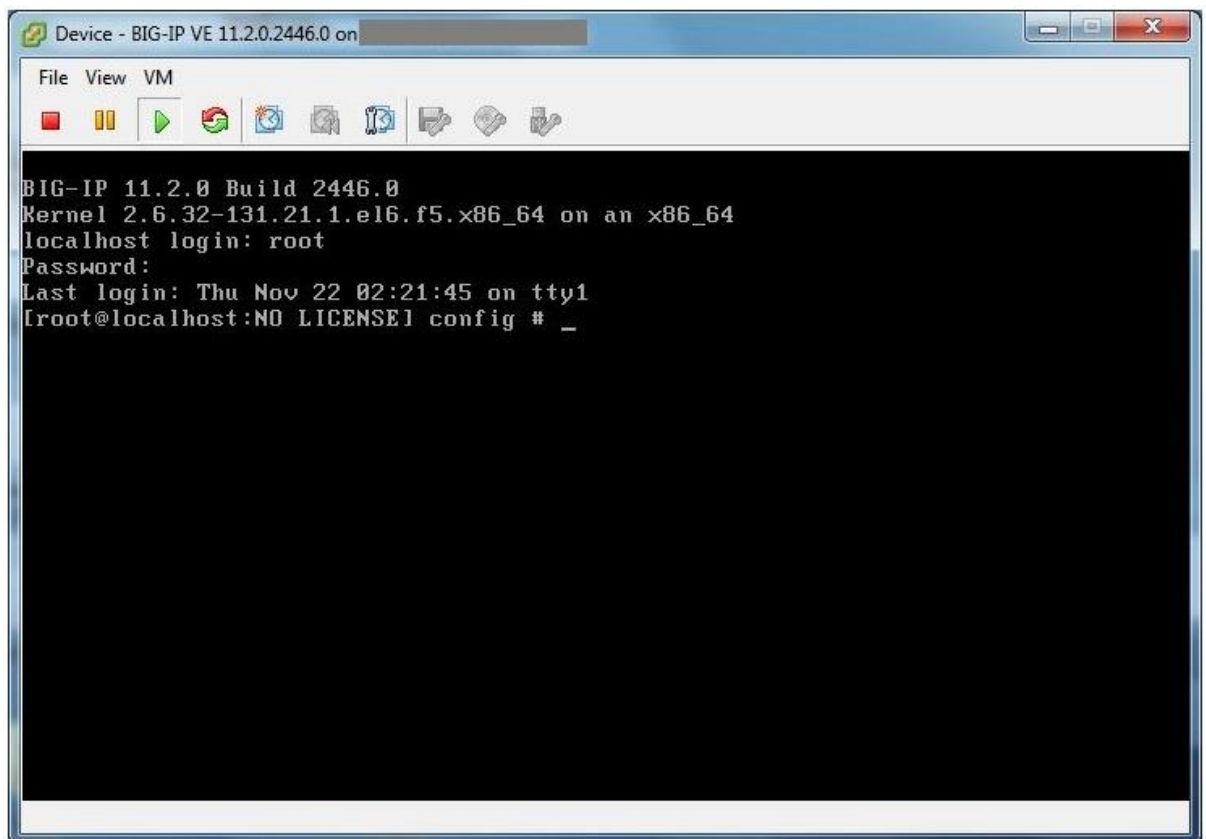
Titania Limited  
Security House  
Barbourne Road  
Worcester  
WR1 1RS

Telephone: (+44)1905 888 785  
Technical Support: [Support@titania.com](mailto:Support@titania.com)  
Licensing: [Enquiries@titania.com](mailto:Enquiries@titania.com)  
Nipper Support: <https://www.titania.com/support/nipper-support/>

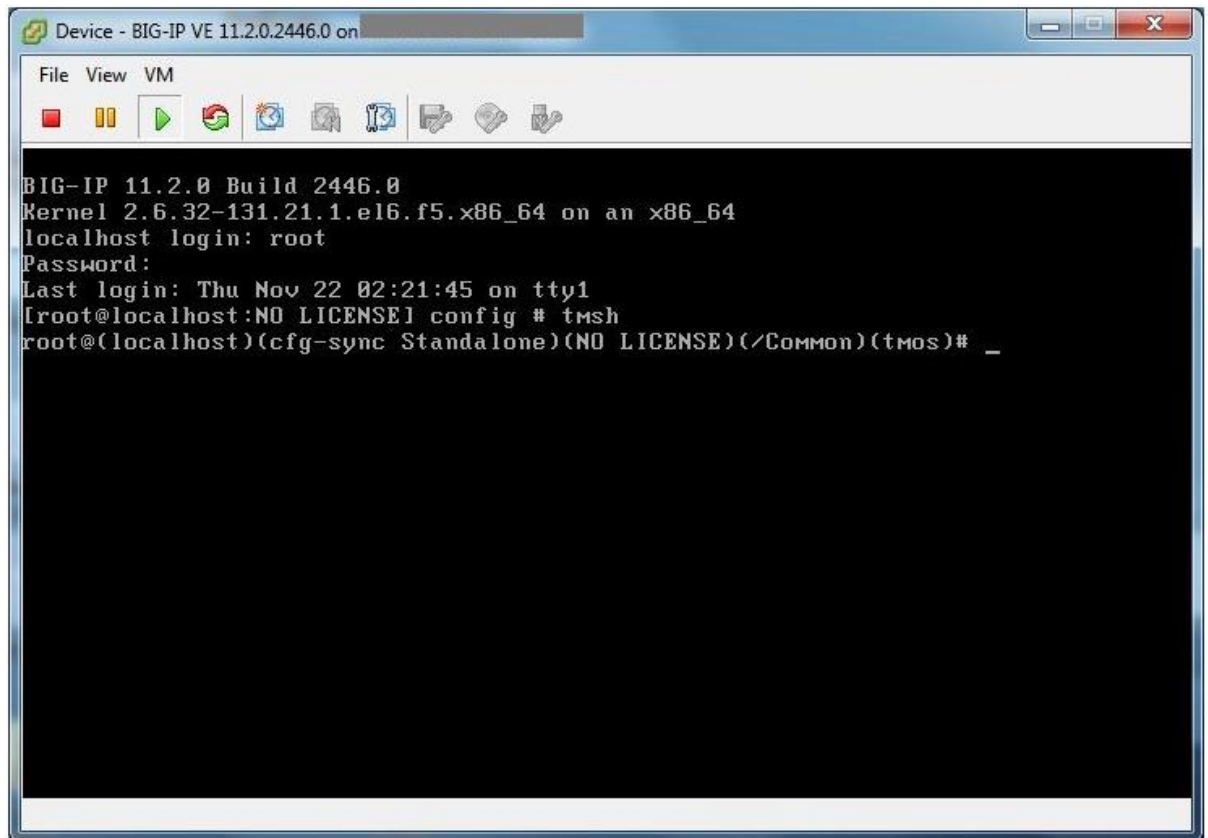
## Using SSH, Telnet or direct console connection

For this procedure you will be using the Command Line Interface (CLI) of your Big IP F5 device using an SSH client (such as OpenSSH or Putty), Telnet or through the console port. We would recommend using either SSH (for remote connections) or using a direct connection to the console port. Telnet provides no encryption of the communications and therefore your authentication credentials and configuration would be vulnerable if a malicious user were to monitor your connection.

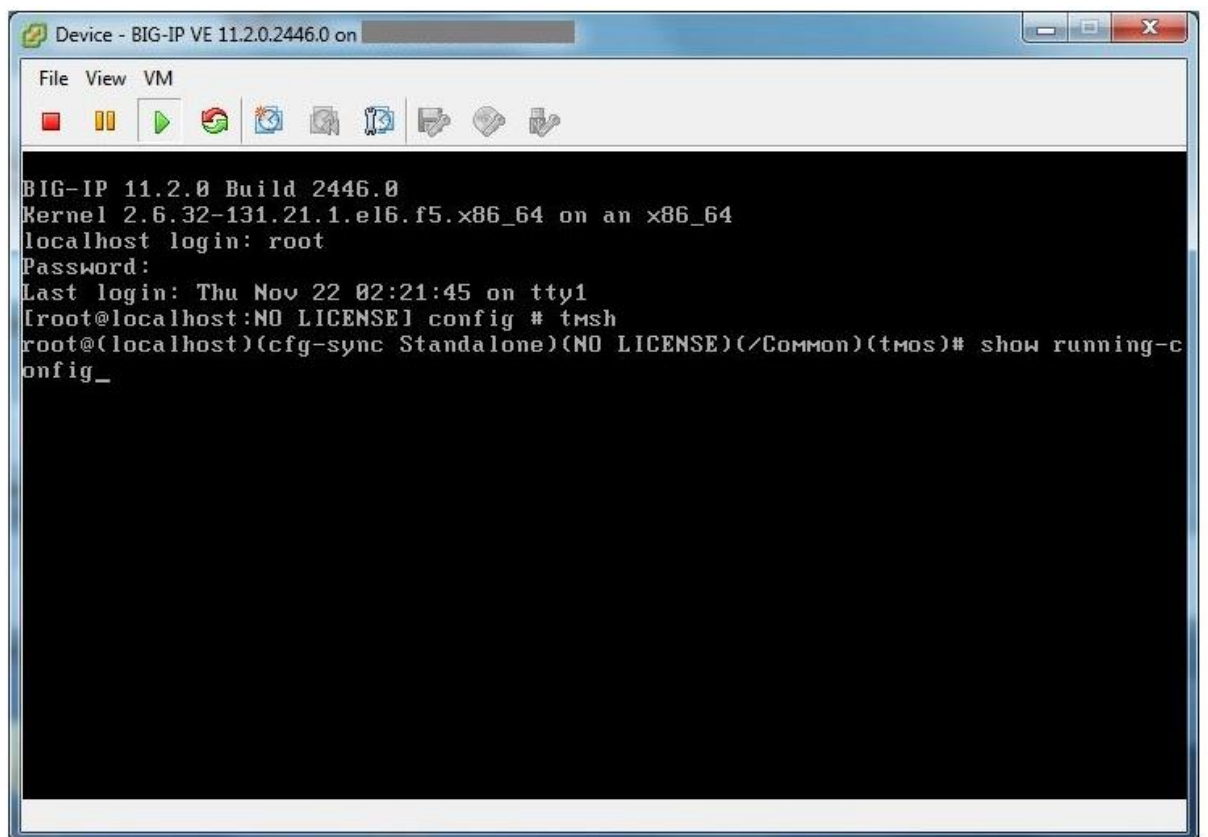
1. Connect to the Big IP F5 using your favourite SSH client, Telnet or a direct console connection.
2. Certain Big IP devices will be capable of dual booting so make sure that you have selected the correct version for the following instructions.
3. Logon using your administration authentication credentials.



4. Enter the command **tmsh**



5. Next enter the command **show running-config**



6. Capture the output (using cut and paste, for example).

```
Device - BIG-IP VE 11.2.0.2446.0 on [redacted]
File View VM
[Icons: Run, Stop, Pause, Play, Reset, Undo, Redo, Copy, Paste, Print, Full Screen, Help]

auth password-policy { }
auth remote-role { }
auth remote-user { }
auth source { }
auth user admin {
    description "Admin User"
    encrypted-password "$1$salt$IEd.dPRrJY41NYnnaBENQ1"
    partition COMMON
    partition-access all
    role admin
    shell none
}
cli global-settings {
    audit enabled
}
cli preference {
    alias-path { /COMMON }
    prompt { host user status current-folder config-sync-status }
}
cm cert dtca-bundle.crt {
    certificate-key-size 2048
    checksum SHA1:1220:951b780ac9c8637e8869e0ad4d2bf44a07d100ce
    create-time 2012-09-20:01:39:05
    created-by %devmgmt
}
---(less 9%)---
```

7. Save the captured output to a text file on your local machine.
8. This text file will be readable by Nipper Studio.