

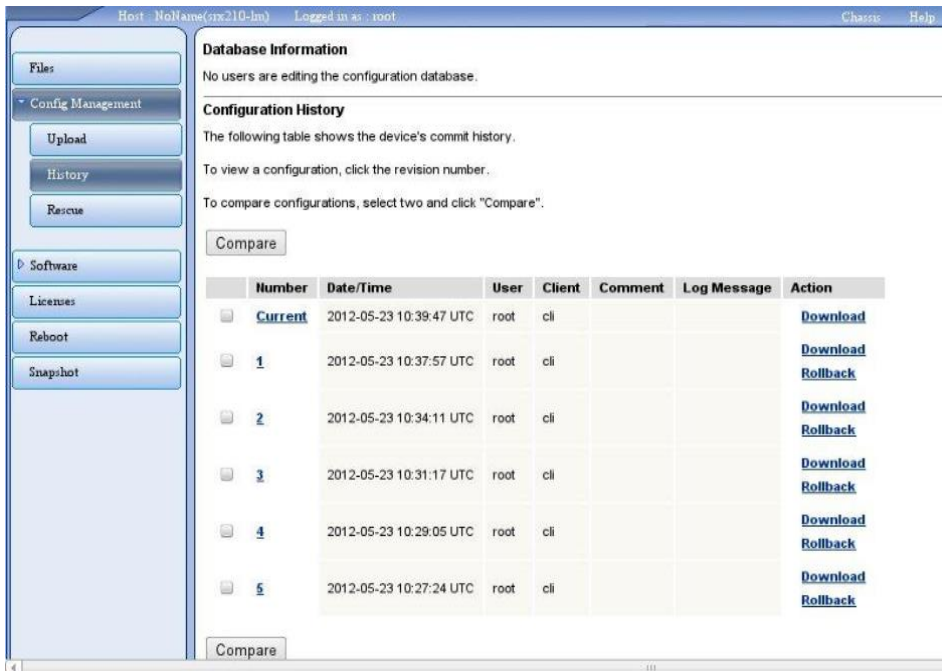
Juniper JunOS Devices (SRX, SSG, E, EX, J, M, MX, T Series Devices)

There are several different methods of extracting the configuration from your Juniper JunOS device and this guide outlines three different methods.

Using HTTP(S)

We would recommend using HTTPS rather than HTTP for transferring your devices configuration as the latter provides no encryption. The procedure for getting the configuration from the device using HTTP(S) is as follows:

1. Using your favorite web browser, connect to the HTTP(S) service provided by your Juniper JunOS device for remote management. You can do this by entering "https://" (recommended) or "http://" followed by your devices IP address.
2. Logon using your administration username and password.
3. Select the "Maintain" tab at the top of the view, and then select the "Config Management" tab on the right and then "History".
4. Click the "Download" button of the "Current" configuration in the number column to save the configuration to a local file



Host: NoName(mrx210-lm) Logged in as: root

Database Information
No users are editing the configuration database.

Configuration History
The following table shows the device's commit history.
To view a configuration, click the revision number.
To compare configurations, select two and click "Compare".

Compare

Number	Date/Time	User	Client	Comment	Log Message	Action
Current	2012-05-23 10:39:47 UTC	root	cli			Download
1	2012-05-23 10:37:57 UTC	root	cli			Download Rollback
2	2012-05-23 10:34:11 UTC	root	cli			Download Rollback
3	2012-05-23 10:31:17 UTC	root	cli			Download Rollback
4	2012-05-23 10:29:05 UTC	root	cli			Download Rollback
5	2012-05-23 10:27:24 UTC	root	cli			Download Rollback

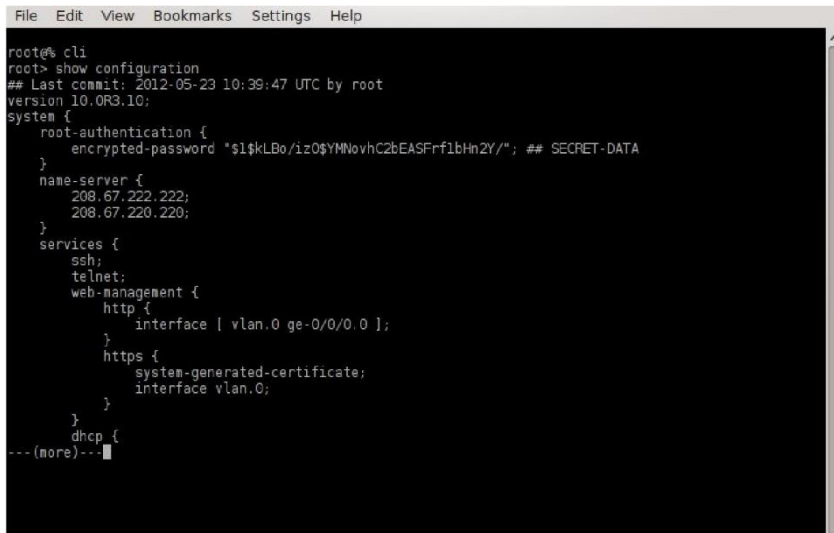
Compare

Using SSH, Telnet or the Console

For this procedure you will be using the Command Line Interface (CLI) of your Juniper JunOS 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 Juniper JunOS using your favorite SSH client, Telnet or a direct console connection.
2. Logon using your administration authentication credentials.
3. Execute the following command:

```
cli  
show configuration | no-more
```

A screenshot of a terminal window with a menu bar (File, Edit, View, Bookmarks, Settings, Help) and a dark background. The terminal text shows a user at the root prompt entering 'cli' and then 'show configuration'. The output displays system configuration details including authentication, name-server, services (ssh, telnet, web-management), and dhcp. The output is truncated with '---(more)---' at the end.

```
File Edit View Bookmarks Settings Help  
root% cli  
root> show configuration  
## Last commit: 2012-05-23 10:39:47 UTC by root  
version 10.0R3.10;  
system {  
  root-authentication {  
    encrypted-password "$1$kLBo/iz0$YMNvvhC2bEASFr1bHn2Y/"; ## SECRET-DATA  
  }  
  name-server {  
    208.67.222.222;  
    208.67.220.220;  
  }  
  services {  
    ssh;  
    telnet;  
    web-management {  
      http {  
        interface | vlan.0 ge-0/0/0.0 ;  
      }  
      https {  
        system-generated-certificate;  
        interface vlan.0;  
      }  
    }  
    dhcp {  
---(more)---
```