

Root Password for the SRX 210 Services Gateway

The root user has complete privileges to configure the SRX 210 services gateway and manage files in the device's file system. Initially, the root password is not defined on the device. To ensure basic security, you must define the root password during initial configuration. If a root password is not defined, you cannot commit configuration settings on the device.



NOTE: If you use a plaintext password, the device displays the password as an encrypted string so that users viewing the configuration cannot see it.

The root password must meet the following conditions:

- Must be at least six characters long.
- Most character classes can be included in a password (alphabetic, numeric, and special characters), except control characters.
- Must contain at least one change of case or character class.

For Common Criteria environments only, the password must be between 10 and 20 characters long and must include at least 3 of the 5 character classes (uppercase letters, lowercase letters, punctuation marks, numbers, and other special characters). Control characters are not recommended. For more information, see the *Secure Configuration Guide for Common Criteria and JUNOS-FIPS*.

- Related Topics**
- SRX 210 Services Gateway Basic Connectivity Overview
 - Device Identification for the SRX 210 Services Gateway
 - Time Zone and System Time for the SRX 210 Services Gateway

