



# Hardening Guidelines

---

This appendix contains the following section:

- [Hardening Guidelines, page A-1](#)

## Hardening Guidelines

If you consider hardening the system, you should consider the following hardening guidelines:

- Refer to the host platform's hardening guides.

RHEL/CentOS 7.x:

[https://access.redhat.com/documentation/en-US/Red\\_Hat\\_Enterprise\\_Linux/7/pdf/Security\\_Guide/Red\\_Hat\\_Enterprise\\_Linux-7-Security\\_Guide-en-US.pdf](https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/pdf/Security_Guide/Red_Hat_Enterprise_Linux-7-Security_Guide-en-US.pdf)



**Note**

---

The above link references external websites and Cisco is not responsible for keeping it up-to-date. It is provided for reference only. If you find that the content is outdated or if you cannot access the link, please contact the website owner for updated information.

---

- Disable or block the ports that are not used by Cisco Prime Access Registrar. The Prime Access Registrar documentation outlines the default port usage.

For a list of ports used by Prime Access Registrar, see the *"Ports" section in the "Overview" Chapter of the [Cisco Prime Access Registrar 9.1 Reference Guide](#)*. Note that some are defaults and may have been changed during install or configuration.

