



Managing SSH Devices with Cisco Defense Orchestrator

- [Managing SSH Devices with Cisco Defense Orchestrator, on page i](#)

Managing SSH Devices with Cisco Defense Orchestrator

Cisco Defense Orchestrator (CDO) allows you to manage devices through SSH. These are the features we support for those devices:

- [Onboard a SSH Device](#). You can use the username and password of a highly privileged user stored on the SSH device to onboard the device.
- [Viewing the device configuration](#). You can view the device configuration file.
- [Review policy and configuration changes from device](#). When you read the configuration file from the SSH device, it will be saved in CDO's database.
- [Out-of-band change detection](#). When you enable Conflict Detection, CDO checks the device every 10 minutes for changes to the device's configuration. If there is a change, the device's status will change to Conflict Detected and you will be able to resolve the conflict.
- [Command line interface support](#). You can issue all SSH device commands to the device through CDO's command line interface.
- Individual CLI commands and groups of commands can be turned into editable and reusable "[macros](#)." You can use the system-defined macros provided by CDO and create your own macros for tasks you perform often.
- [Detect and manage SSH fingerprint changes](#). If any credentials or properties of the device change, and that causes a change to the SSH fingerprint, CDO detects that change and gives you a chance to review and accept the new fingerprint.
- [Change Log](#). The change log captures all the commands you issue to the SSH device.

