Managing IOS Devices with Cisco Defense Orchestrator

Managing IOS Devices with CDO

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

- Onboard Devices and Services. You can use the username and password of a highly privileged user stored on the IOS device to onboard the device.
- View a Device's Configuration File. You can view the device configuration file.
- Read Changes from Cisco IOS or SSH to CDO. When you check for changes in the configuration file from the Cisco IOS device, it will be saved in CDO's database.
- Out-of-Band Changes on Devices. 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.
- CDO Command Line Interface. You can issue all IOS 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.
- Manage Change Logs in CDO. The change log captures all the commands you issue to the IOS device.

Managing IOS Devices with Cisco Defense Orchestrator