Install Ironwood's Network Automation Assistant

To install Ironwood's NAA, follow the steps described in "Ironwood NAA Installation and Upgrade Guide".

Login NAA GUI

To login to NAA GUI.

https://<ip address>
or
https://127.0.0.1:8443 if you are logging in from your own laptop to your own VM

user: admin
password: admin

Provide Default User and Password

Default User name

1) Go to
   Settings > Edit Devices > General tab

2) Enter the "Default User" name

3) Be sure the "Default Password Handle Name" is "default_pwd"

Password Handlers hide the passwords from being visible

1) Go to
   Settings > Edit Devices > Password Handler tab

2) Find the "default_pwd" entry and enter the password

Add new Devices

A Device Set is a group of similar devices that share the same attributes such as vender OS, login credentials, standard templates, etc.
Once the Device Set is created, individual devices can be added under it easily.

1) Go to
   Settings > Edit Devices > Devices tab

2) Expand the Assistance menu
   Device Entry > SET Header > Set Name = CISCO_ROUTERS (or whatever name)
   [Optional] Others > OS Type (default Cisco IOS)
   [Optional] Others > Login User (default to the Default User)
   [Optional] Others > Password Handle (default to the Default Password Handle)

3) Click down Convert

4) Cut and Paste the converted text into the text area

5) In the text area, enter the Device IP inside the Device SET

6) Click Save

For Example:

SET=CISCO_ROUTERS
1.1.1.1
1.1.1.2
1.1.1.3

Run a Quick Test

To test if a device is accessible, run a quick test

1) Go to
Run Audit > Run Audit Now > General Audit > Audit

2) Check to see if the new device shows up
Compliance > View Report

Define Commands to watch for Changes

NAA detects any changes you want to watch for.

1) Go to
Data Gathering > Edit Collector

2) Enter commands in the text area of the pre-defined categories.
The commands must start with
cmd: <CLI command>
Optionally, if you need to parse the command output by unix shell, add %sh%.
cmd: <CLI command> %sh% <shell command>

For example:

cmd: show version %sh% grep version

Setup Audit Rules and Standards

To conduct an Audit, Rules and Standards must be defined and assigned to the Device Set.

Create Rule

1) Go to
Compliance > Edit Rules > Manage Rules tab

2) Enter new Rule name and hit Create

3) Go to
Compliance > Edit Rules > Edit Rule tab

4) Find the newly create Rule in the dropdown list

5) In the text area, enter rule commands

6) Click Save

For example:

```
#  - Timezone should be UTC and the Year starts with 20..
# ----------------------
cmd: show clock
<time> UTC <day> <m> <d> [/^20/]
```

Please click Help at the bottom panel to see how to create Rules or click on some existing sample rules.

Create Standard

1) Go to
Compliance > Edit Standards > Manage Standard tab

2) Enter new Standard name and hit Create

3) Go to
Compliance > Edit Standards > Edit Standard tab

4) Find the newly created Standard in the dropdown list

5) Select Rule to Apply from the dropdown list

6) Click Add Rule to one of the listed Categories (Software/Hardware, Security, Config, Operation, Health)

7) Click Save

Assign Standard to Device

1) Go to
Settings > Edit Devices > Devices

2) Expand the Assistance menu
Device Entry > SET Header > Set Name = CISCO_ROUTERS (or whatever name)
Standards > Standard Set = Cisco_IOS_Standard (as an example)

3) Click down Convert

4) Cut and Paste the converted text into the text area

5) In the text area, enter the Device IP inside the Device SET

6) Click Save

For example,

SET=CISCO_ROUTERS,,,,,,,,,Cisco_IOS_Standard-SWHW.std|Cisco_IOS_Standard-CFG.std|Cisco_IOS_Standard-OPS.std|Cisco_IOS_Standard-HTH.std|Cisco_IOS_Standard-SEC.std
1.1.1.1
1.1.1.2
1.1.1.3

Schedule Audits

To schedule audits.

1) Go to
   Run Audit > Schedule Audits

2) Select Hour/Minute/Day/Month

3) Click Save