HIPAA Compliance Use Case

Overview

HIPAA Compliance helps ensure that all medical records, medical billing, and patient accounts meet certain consistent standards with regard to documentation, handling, and privacy.

Current Situation

Without Network Automation, you would be

- monitoring logins into devices with a syslog server
- Manually managing passwords on devices.
- Performing manual backups of device configuration files.
- Manually modifying configuration files on devices.

Network Automation's Value

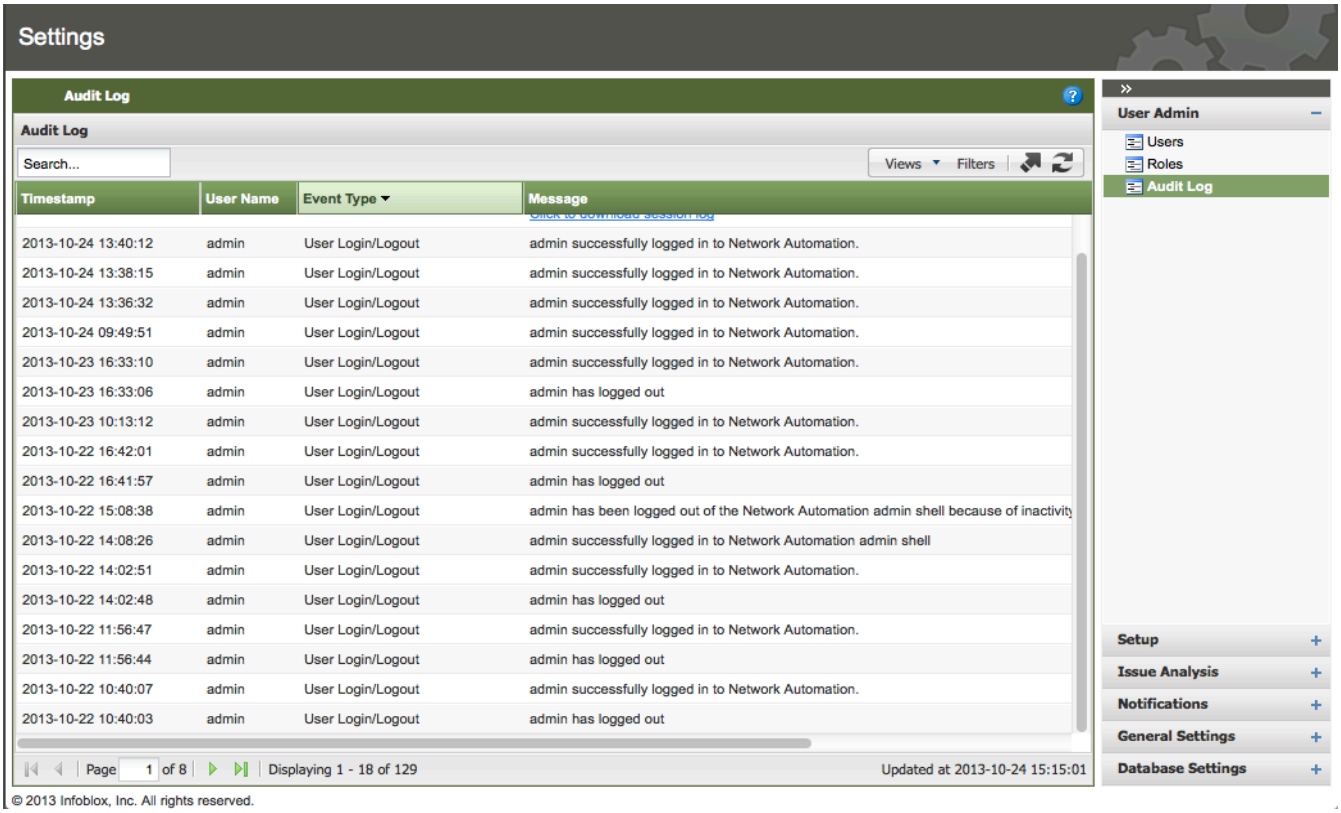
Network Automation can help with HIPAA compliance in the HIPAA Security Standards. Network Automation can help with the following standards:

- 164.308(a)(5) – Security Awareness and Training; Login Monitoring of Network Automation device, Login Monitoring of Managed Devices, and Password Management of network devices with the use of the password change script.
- 164.308(a)(7) – Contingency Plan; Network Automation backup of database and configurations on an adjustable periodic basis.
- 164.312(a)(1) – Access Control; use the ad-hoc script to add or delete users from network devices, enable login timeouts, disable telnet, enable SSH access.

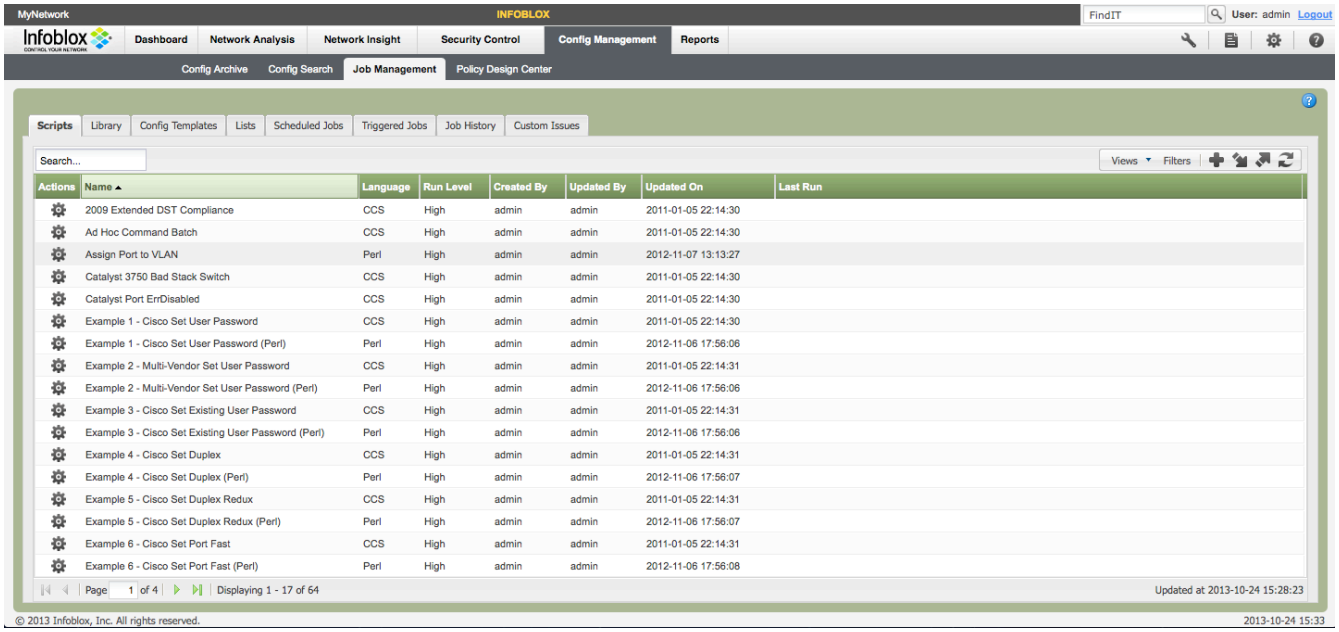
Scripts can be used to implement the HIPAA rules above and a report can be generated for HIPAA audit purposes.

Use Cases

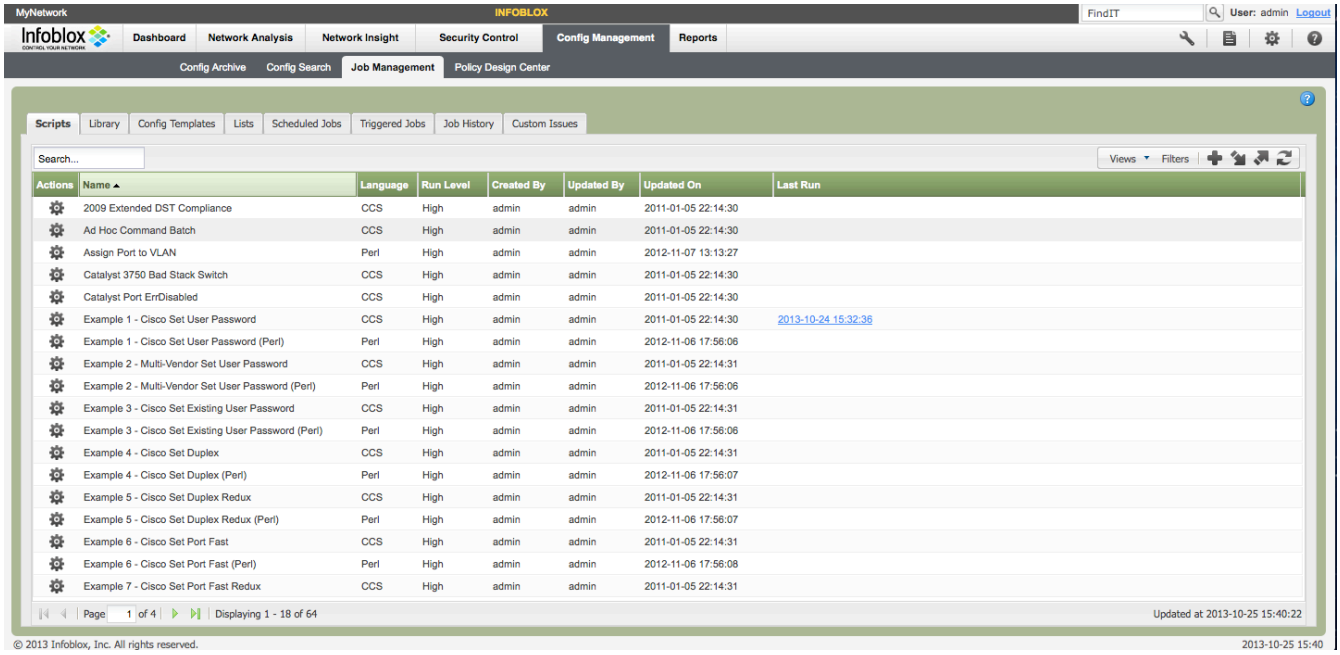
- 164.308(a)(5)) – Security Awareness and Training



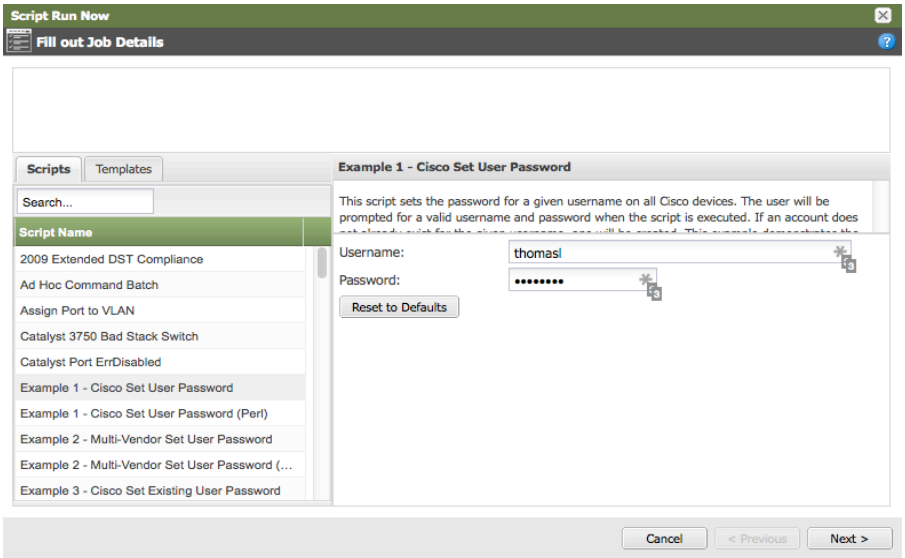
Click on the Settings wheel -> User Admin -> Audit log. You can monitor who is logging into the Network Automation appliance as well as managed network devices when users are using Network Automation's built-in telnet or SSH application. In addition, this information can be exported to a CSV file.



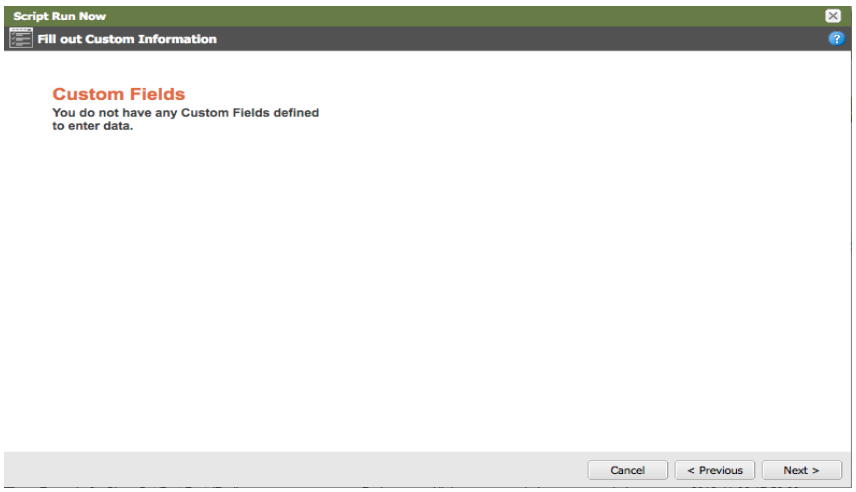
You can manage passwords of network devices with the use of the password change script. Navigate to Config Management -> Job Management -> Scripts. By default, there are seven different scripts that can be used to add usernames and/or modify passwords. These scripts can be copied and modified by the customer to suit their requirements. Below is an example workflow for adding a user and password to a device.



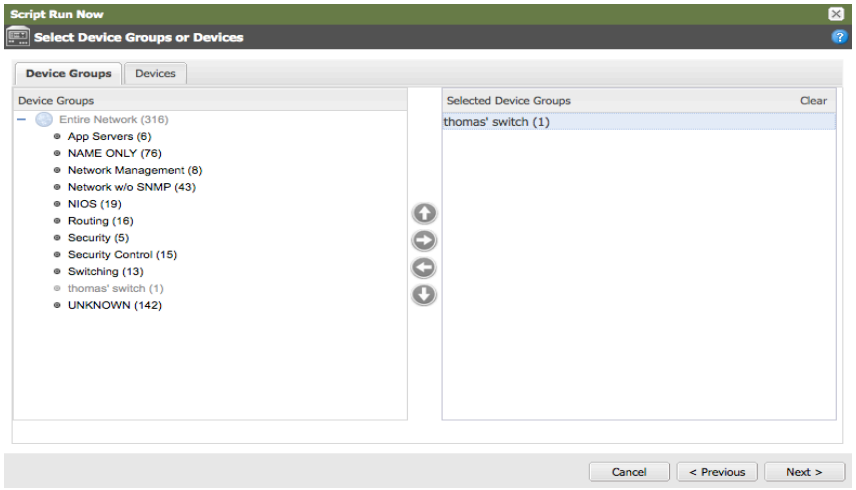
You can assign users to network devices by using the 'Example 1-Cisco Set User Password' script or create your own user addition script. Below is the output of running the script:



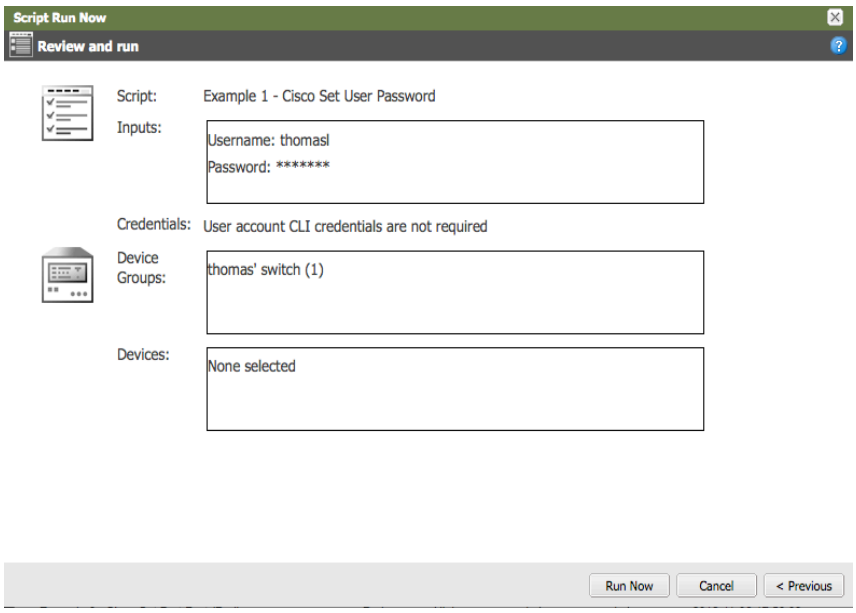
1. Input the username and password on the right side.
2. Click on the Next button.



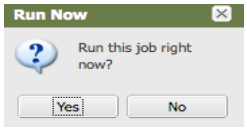
3. Click on the Next button.



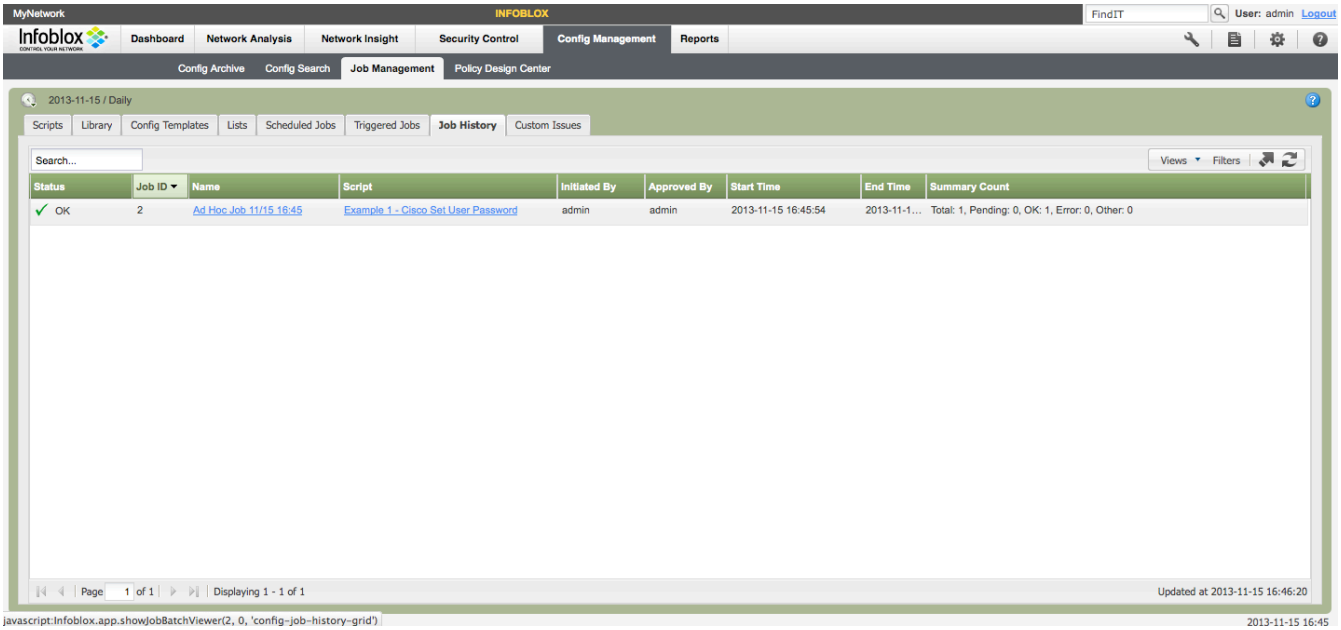
4. Select the device group to run the script on. A device group contains devices that share a common trait such as switches, department, location, etc.
5. Click on the Next button.



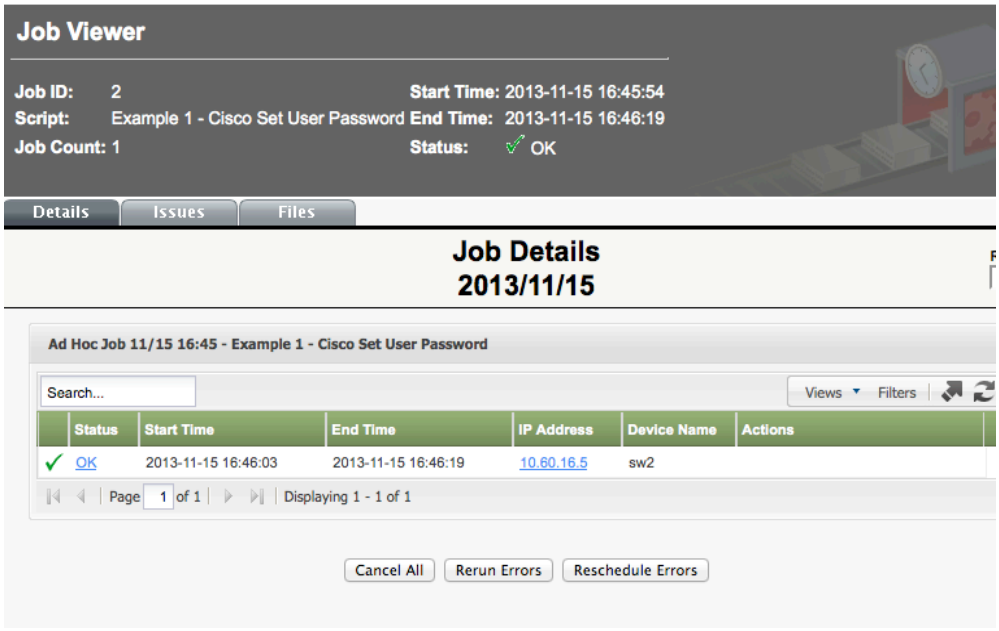
6. Click on the Run Now button if all of the fields look correct.



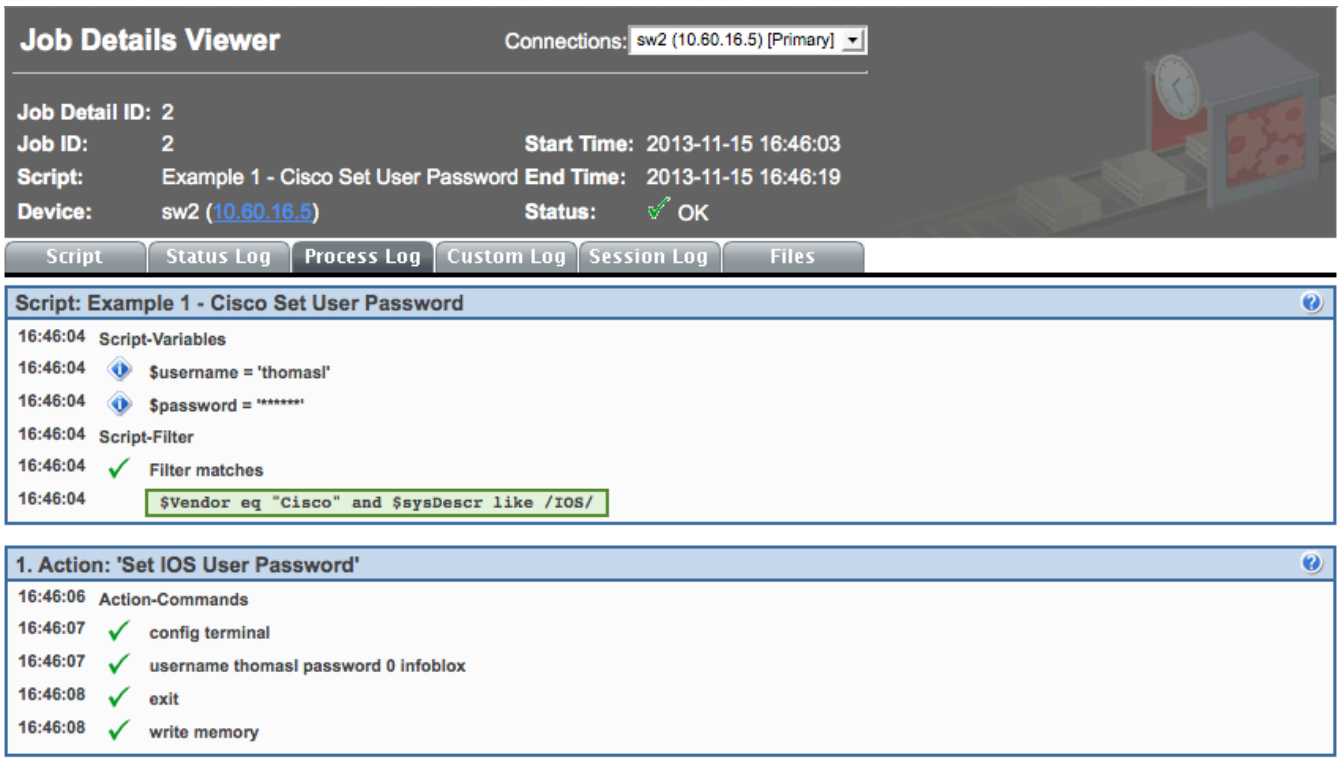
7. Click on the Yes button.



8. The job is now complete. Click on link under the name column to drill down on the details of the job.

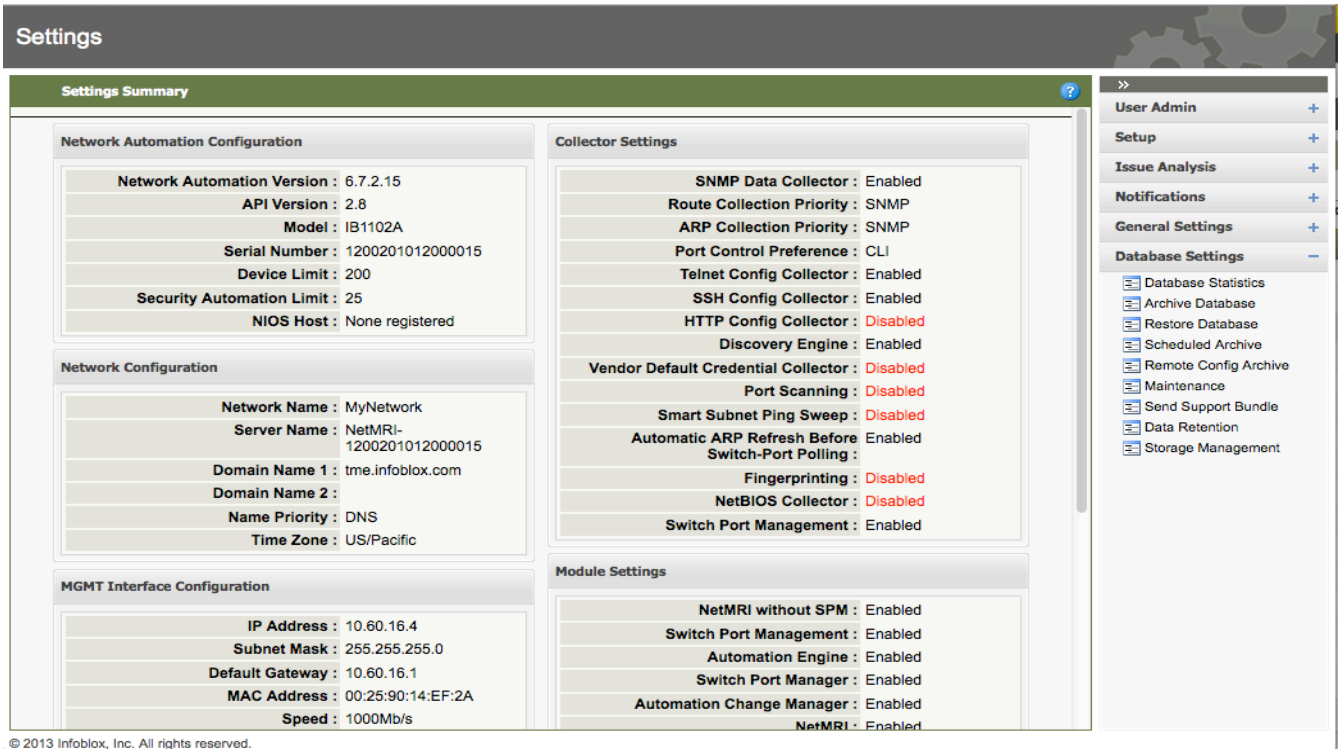


9. Click on the OK button to see the details of the job.



The screen above show the details of the successful running of the job. You can look at the Session Log to see the actual configuration session.

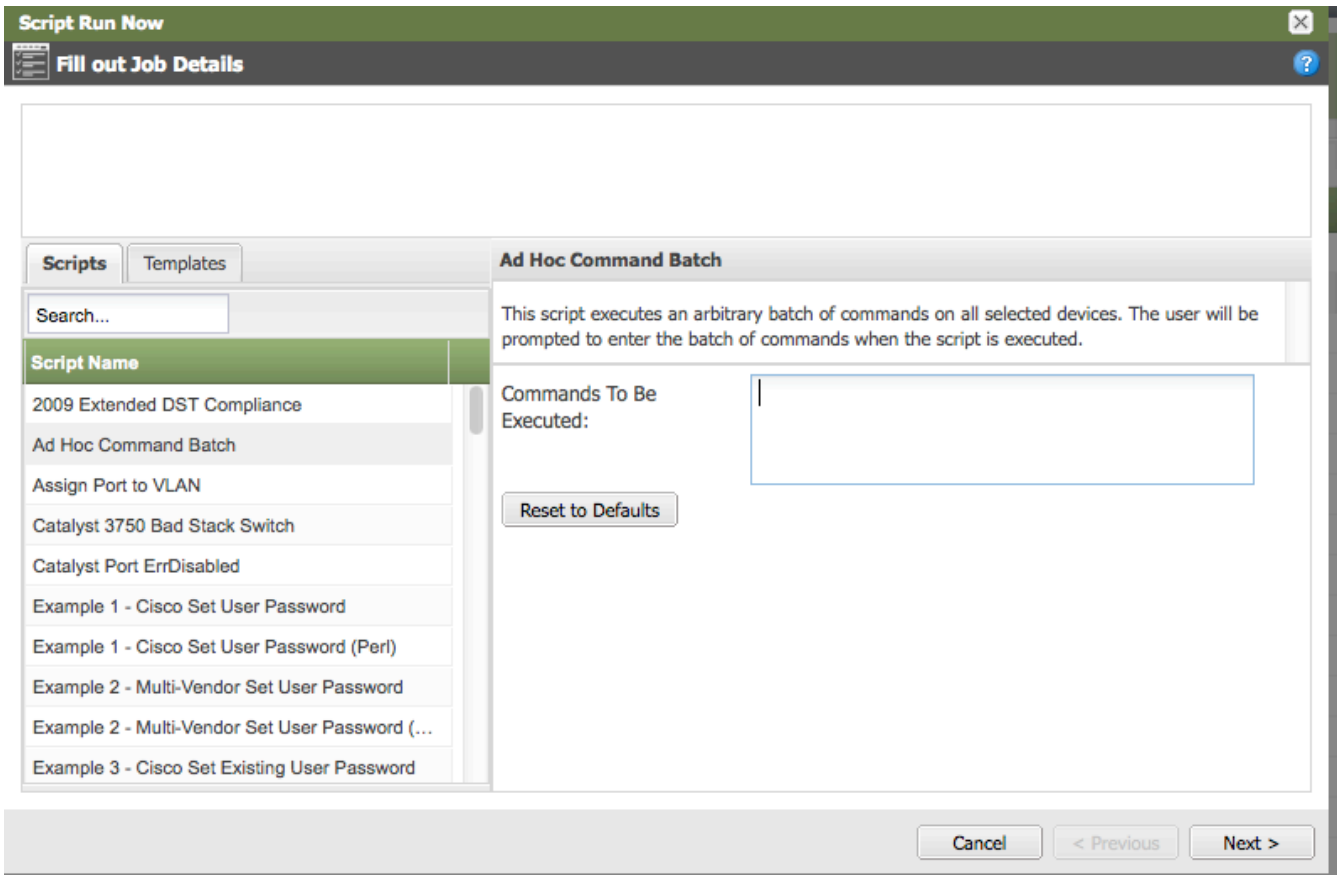
- 164.308(a)(7) – Contingency Plan;



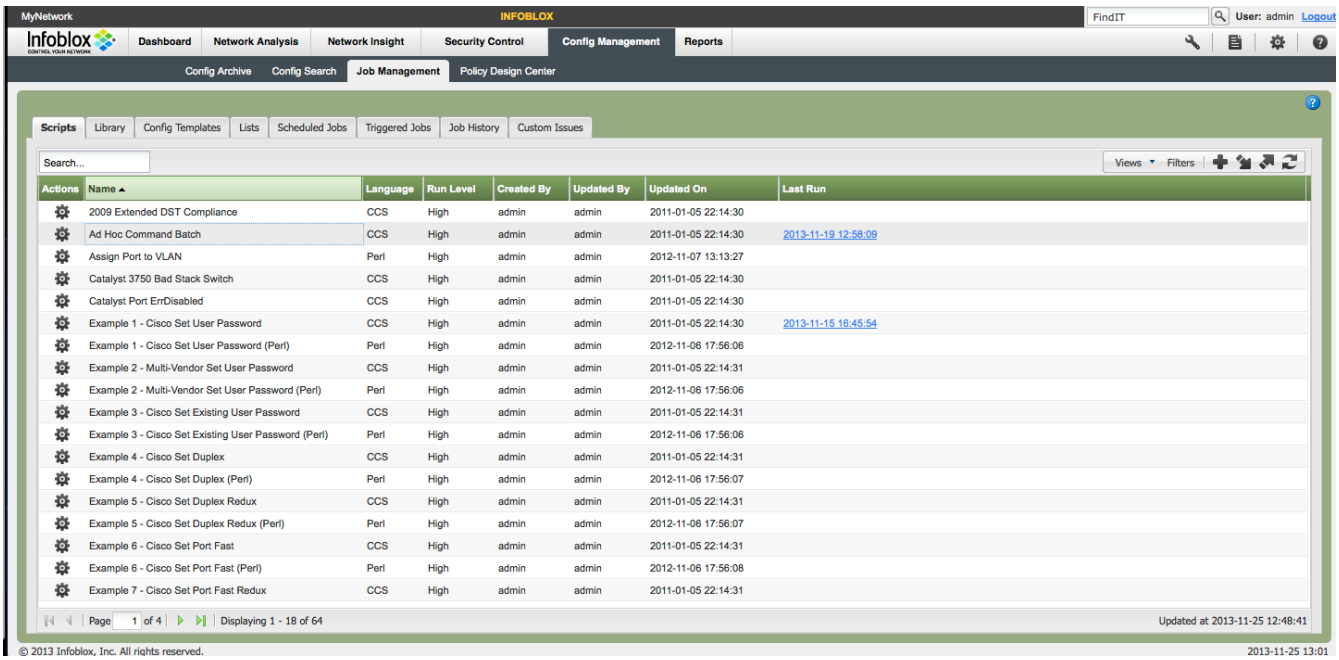
Network Automation backs up the database and configurations on an adjustable periodic basis. Click on the Settings button -> Database Settings. You have a choice of:

- Archive Database – Manually backup the database to a local workstation or remote SCP server.
- Scheduled Archive-Schedule a database backup to up to two remote SCP servers on a one-time, hourly, daily, weekly, or monthly basis.
- Remote Config Archive-Backup the device configuration files on a daily or weekly basis

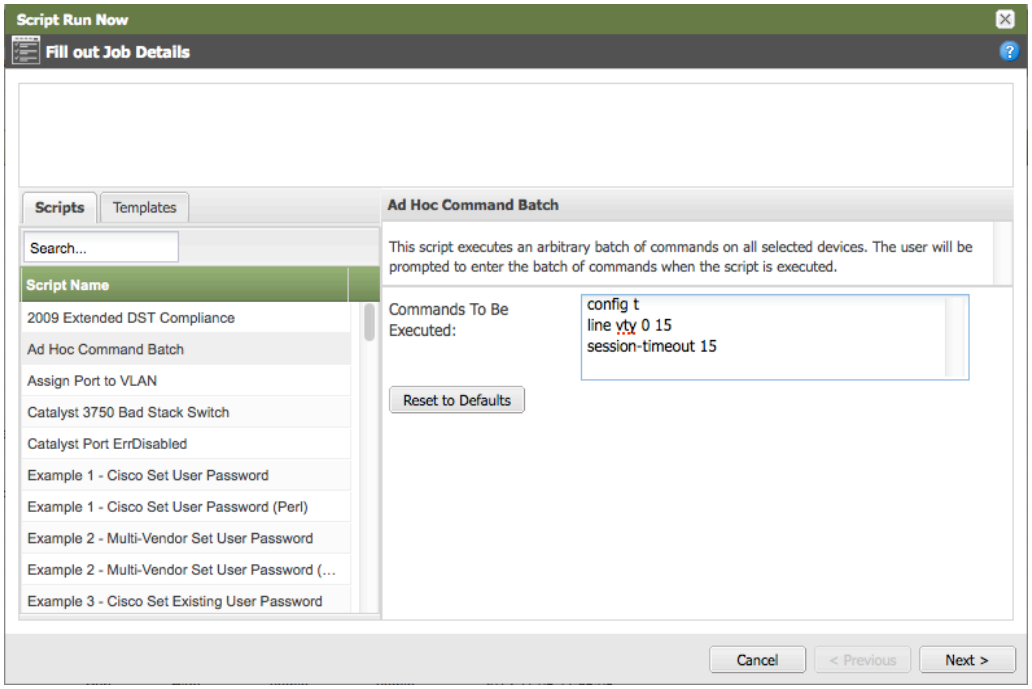
- 164.312(a)(1) – Access Control;



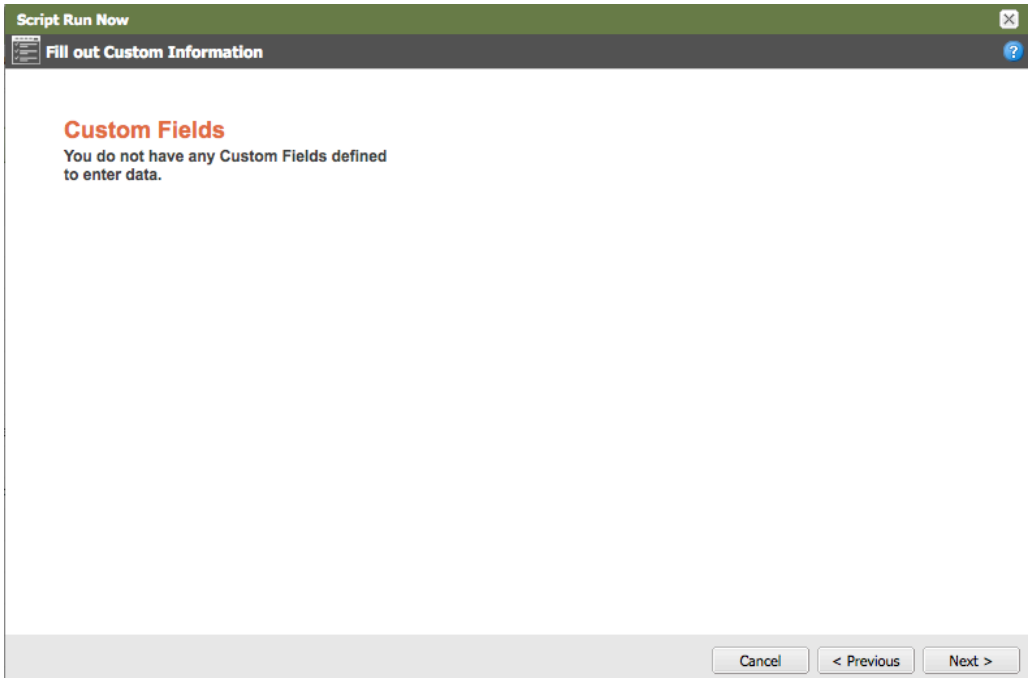
Use the ad-hoc script to add or delete users from network devices, enable login timeouts, disable telnet, and/or enable SSH access. This script can be access by navigating to Config Management -> Job Management -> Scripts -> Ad Hoc Command Batch. Input the commands to add users, delete users, enable login timeouts, disable telnet, or enable SSH access. Below is an example of enabling login timeouts on a device.



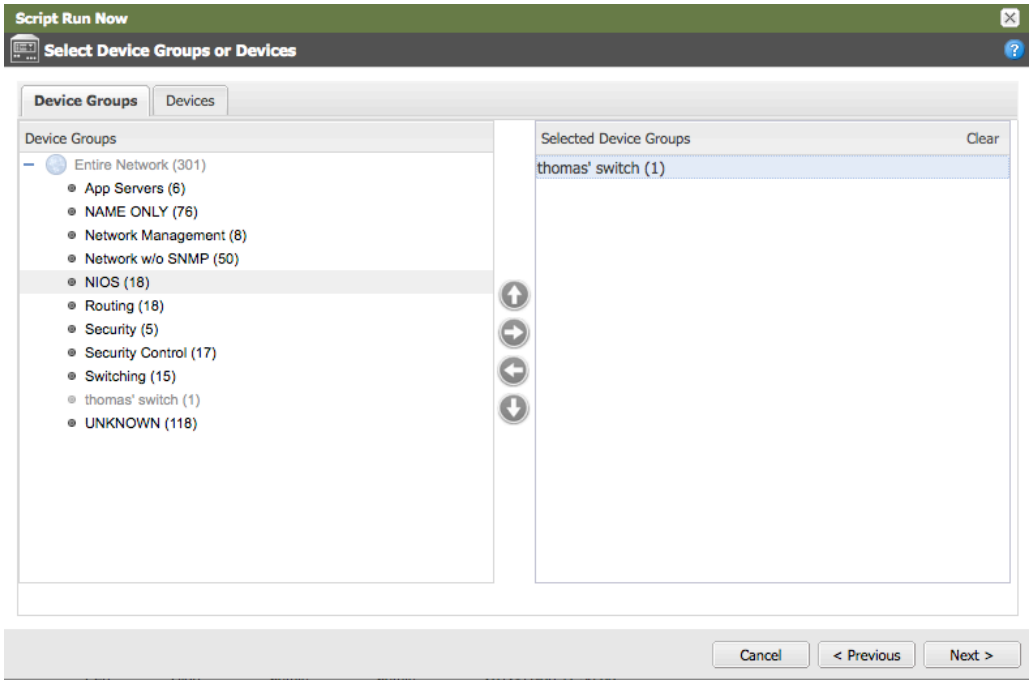
1. Select the Ad Hoc Command Batch script and click on the wheel to run it.



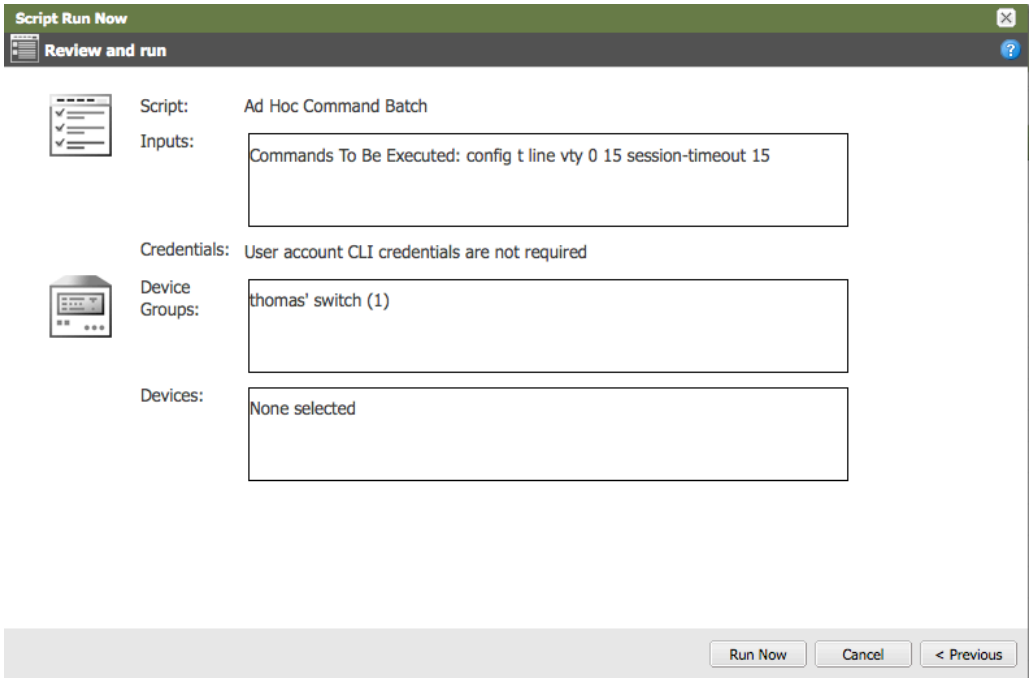
2. Input the commands to be run in the right side box and click on the Next button.



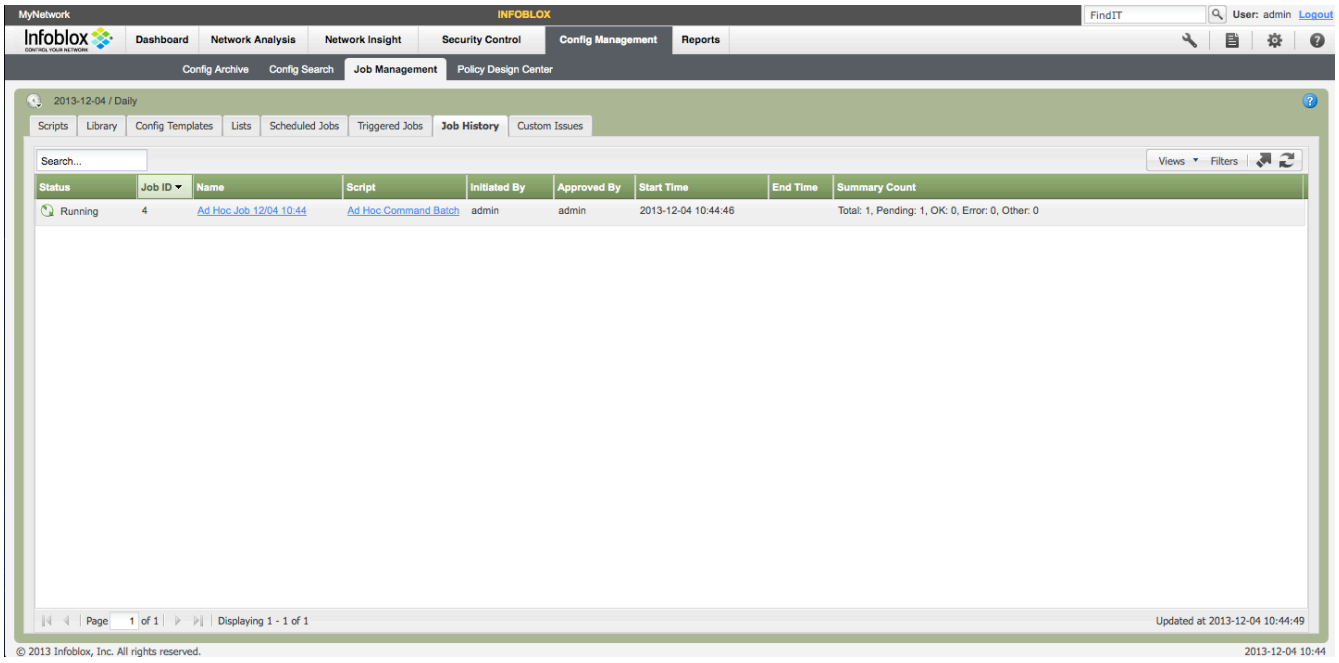
3. Click on the Next button.



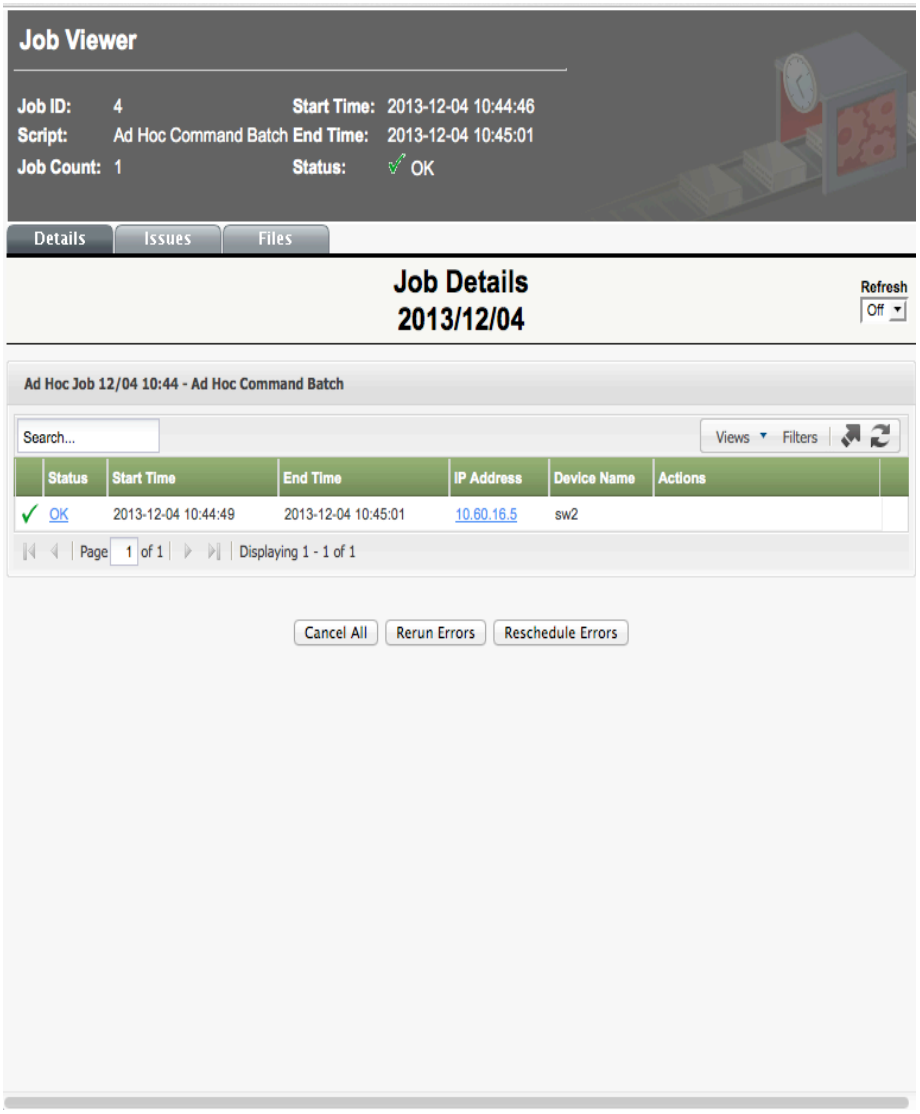
4. Select the device group(s) or devices to run the commands.



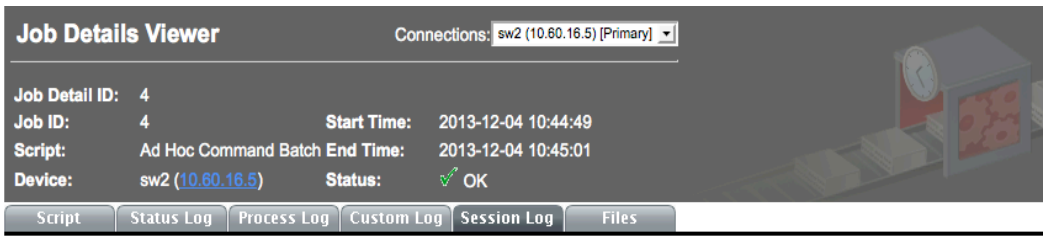
5. This screen gives you the chance to review the details of running the script like the commands and the device group. If everything looks good, click on the Run Now button.



6. You can now click on the name of the job to view the progress.



7. Click on the status link to view the details of the job.

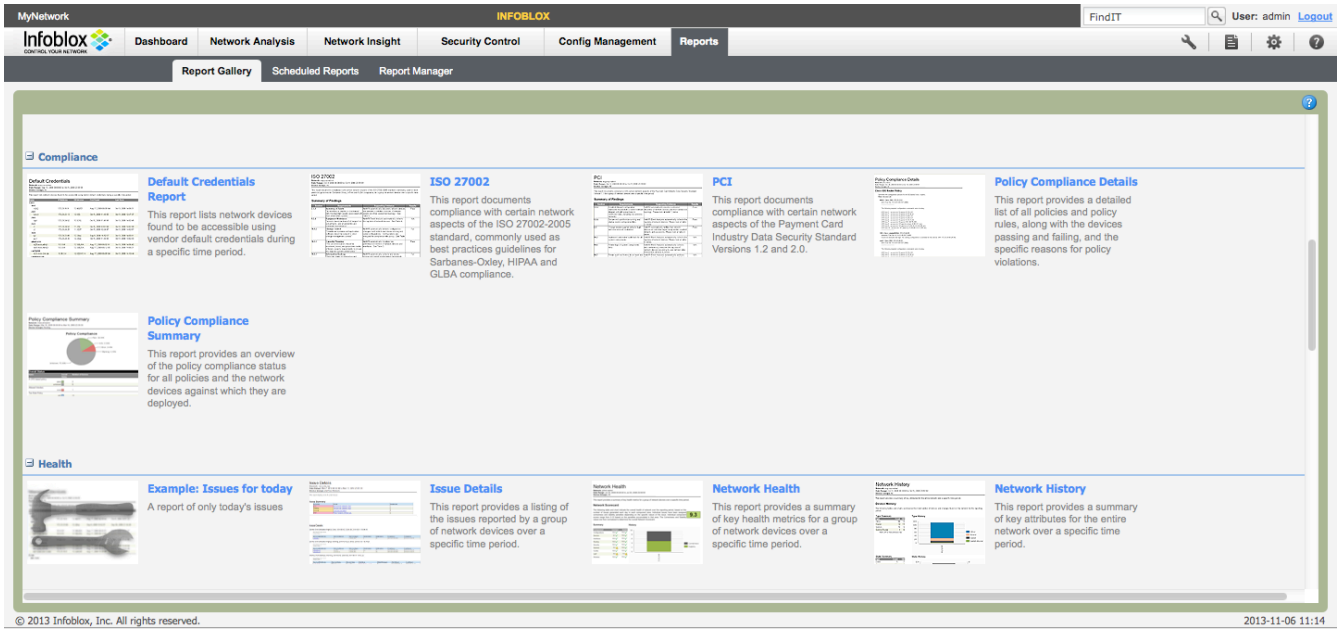



```
Warning: Permanently added '10.60.16.5' (RSA) to the list of known hosts.

Password:

sw2>
sw2>enable
Password:
sw2#
sw2#terminal no monitor
sw2#terminal length 24
sw2#terminal no editing
sw2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
sw2(config)#line vty 0 15
sw2(config-line)#session-timeout 15
sw2(config-line)#

*** Job Completed Successfully ***
```

8. You can click on the Session Log tab to view what Network Automation configured on this switch.

In addition scripts can be created to make the process more automated and customized to your network environment.

- Reports



Navigate to the Reports tab. In the Compliance section, a HIPAA report can be run for yearly audits as well as for checking ongoing compliance.