NERC Compliance Use Cases

Overview

For network and IT teams who work in the Energy sector, the North American Energy Reliability Corporation Critical Infrastructure Protection (NERC-CIP) standards provide a thorough guide to electrical generation utilities for maintaining and ensuring the reliability and security of their "cyber assets", usually defined as any electronic device that participates or supports the electric power grid. The standard focuses on best practices such as:

- Identify and document a risk-based assessment methodology to use to identify its critical assets. (CIP-002-3 R1, R3)
- Develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset (with annual approvals). (CIP-002-4 R2, R3)
- Document and implement a security policy that represents management's commitment and ability to secure its critical cyber assets. (CIP-003-3 R1, R4, R5, R6)
- Implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets. (CIP-003-4 R4, R5, R6)
- Implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s). (CIP-005-3a R3.1, R3.2)
- Perform a cyber-vulnerability assessment of the electronic access point to the Electronic Security Perimeter(s) at least annually. (CIP-005-3a R3.1, R3.2 R4.3, R4.4)
- Ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. Display appropriate use banners upon all interactive access attempts. (CIP-005-4a R1, R2)
- Ensure the implementation of a physical security program for the protection of Critical Cyber Assets. (CIP-006-3c)
- Ensure that only those ports and services for normal and emergency operations are enabled. Enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access. (CIP-007-3 R2, R5)
- Ensure identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. (CIP-008-3)
- Ensure that recovery plans are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. (CIP-009-3)

Current Situation with Manual Processes

For many utilities, NERC is a challenge because most teams attempt to maintain compliance via manual documentation and periodic spot checks. Typically, a senior network admin is required for the manual process which can be difficult because they are already busy.

While NERC is listed as a standard, they are typically at a higher-level and it's up to the individual network team to decipher the best practices into actionable items or rules to maintain and prove compliance. So the IT teams must build individual rules, then manually check and re-check and then cobble together the results when audits are required.

Network Automation with Infoblox

Infoblox Network Automation helps ensure that your network assets maintain your desired state for NERC requirements. By leveraging customizable, built-in expertise, you can determine which rules and polices you'd like to follow and the platform does continuous monitoring and single-click reporting for those standards.

Key capabilities tied to NERC include:

- Extensive network discovery and inventory features to identify and track existing and new devices.
- Customizable and extensive reporting for tracking Critical Cyber Assets and current state.
- Robust policy definition and reporting solution that allows creation of specific rules to be applied across single or multiple network devices.

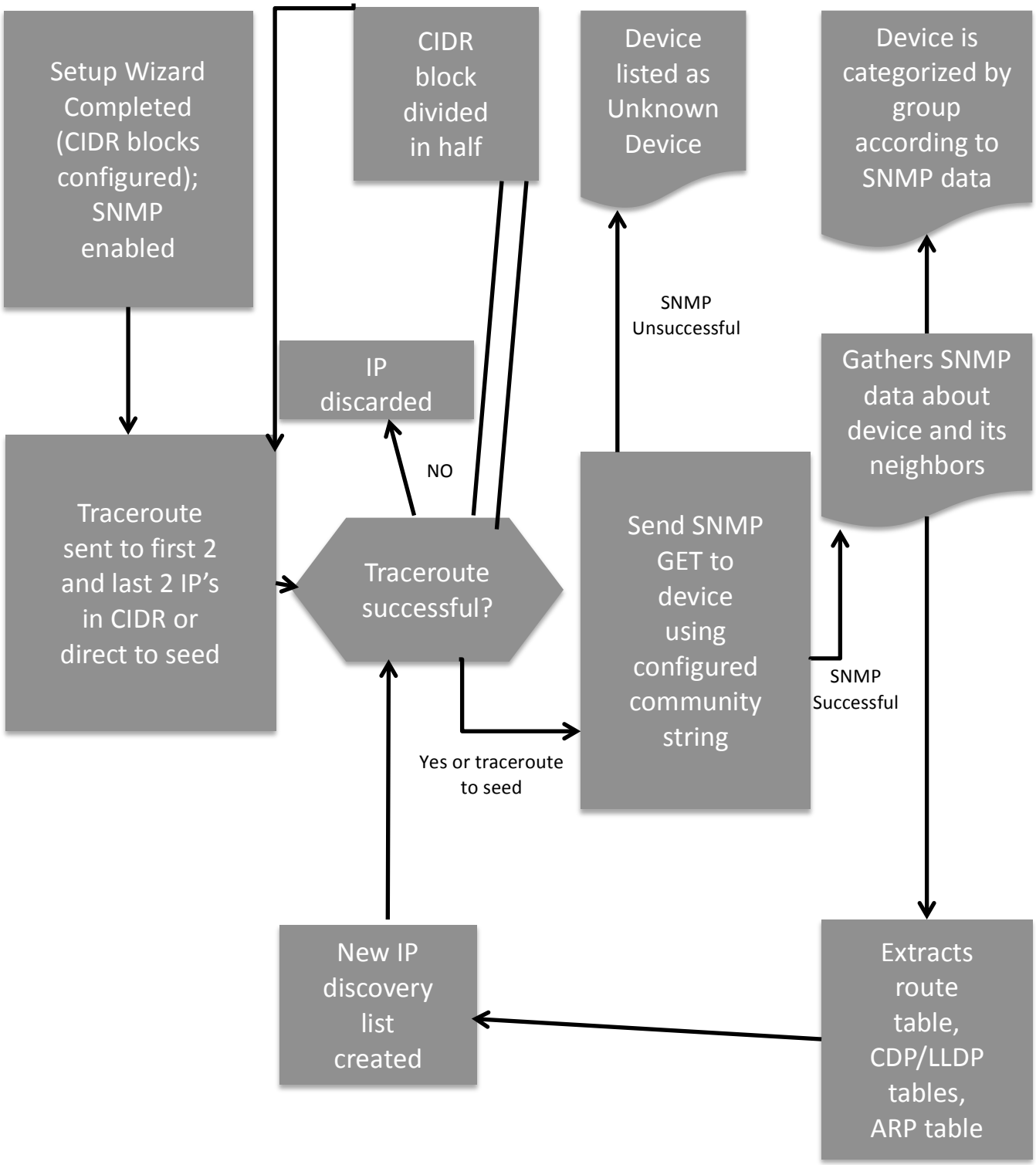
- Network topology diagrams, access control, and change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software.
- Tracking end-hosts connected through switch ports over time for security and auditing requirements.
- Review default accounts, passwords and network management community strings.
- Extensive network infrastructure device grouping and a topological understanding of relationships, ensuring every device can be designated inside or outside a given security perimeter.
- Network configuration modification to display banner messages on network infrastructure devices.
- Simplify management by tracking parameters such as port status to Administratively UP or Administratively DOWN.
- User-based access rights and control for maintaining security for multiple users.

Use Case

This use case document provides a sample of how to create and monitor for NERC compliance mandates. By following the instructions, you can create your own rule and policy for your specific environment. More importantly, you can easily broaden this to include other parameters by using the templates and customization options available within Infoblox Network Automation.

CIP-002-3 R1, R3- Network Automation covers this standard with the following features:

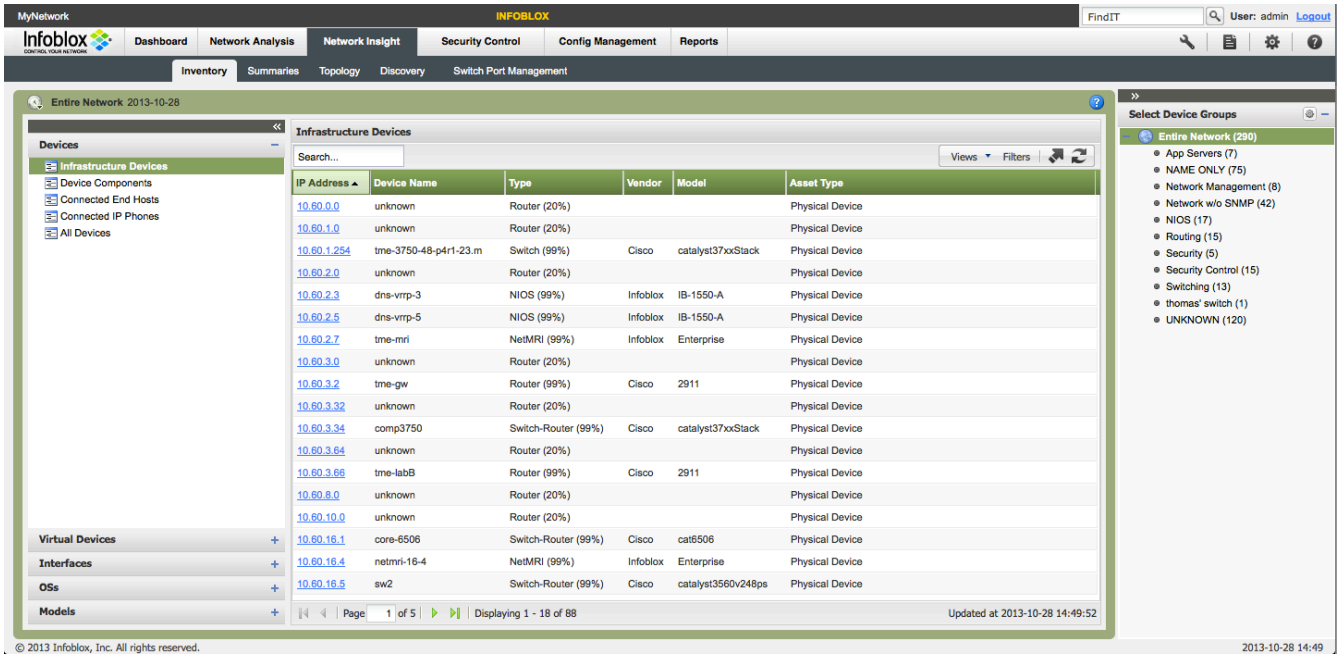
- **Device Discovery**



The diagram above describes how devices are discovered. Discovery is done on a periodic basis to ensure the discovery process updates the inventory without being consuming a large amount of network bandwidth. You enter the subnets, SNMP community strings, and CLI credentials to start the process of device discovery. Network Automation also uses default SNMP community strings and CLI credentials if your SNMP community

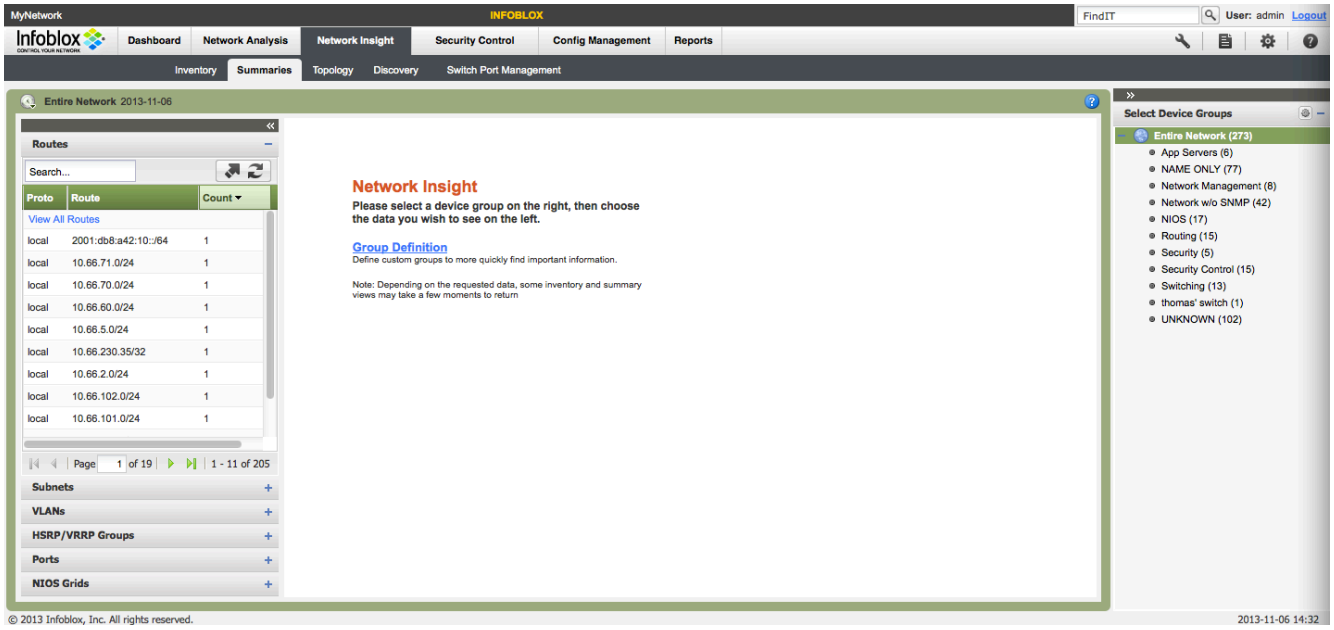
strings and CLI credentials do not work. This will help in discovering devices that you did not know about. Refer to the Network Automation Administrator Guide for more information on the setup wizard.

- **Network insight**



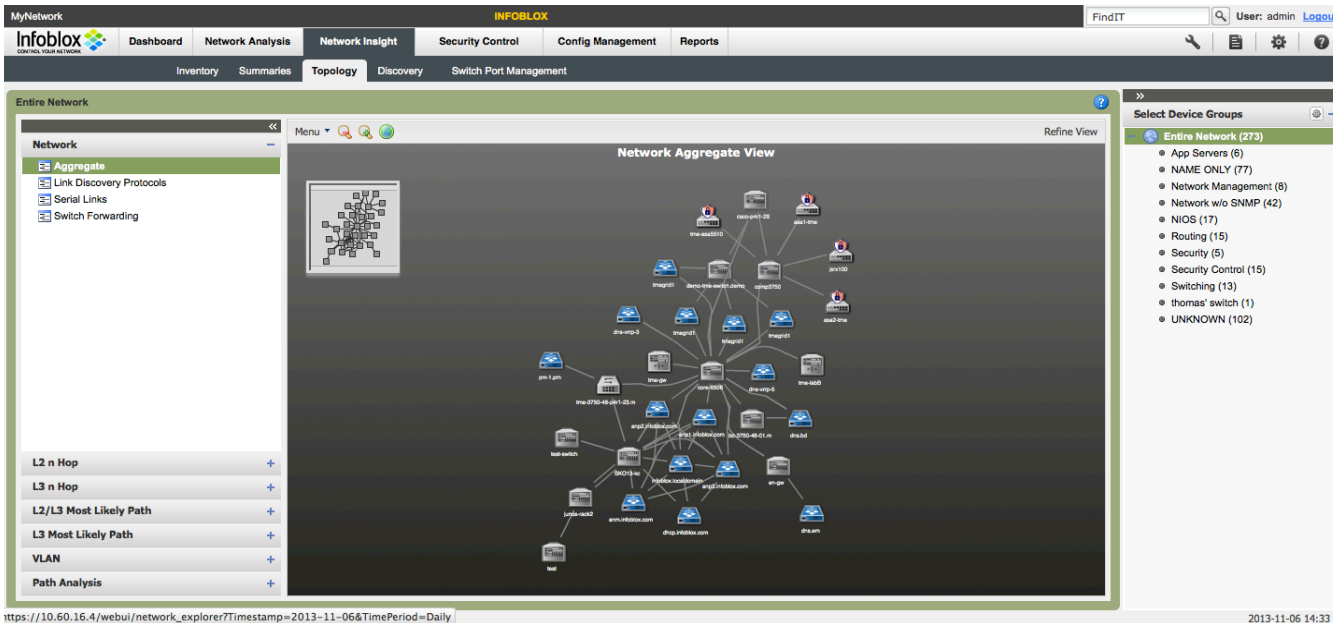
The Network Insight tab shows:

- Inventory of Discovered Devices
  - Devices
    - Infrastructure devices. This includes routers, switches, firewalls, load balancers, etc.
    - Device components like I/O boards in a chassis based device.
    - End hosts
    - IP phones
    - Aggregation of the above.
  - Virtual Devices
  - Interfaces
    - Configuration of - Shows all interfaces being tracked by the appliance, including IP configuration, associated device, VLAN and trunking status, and line speed.
    - Unused Down ports - All interfaces marked administratively “down” (user configured as “off”) and operationally “down” (not physically connected). This helps determine whether devices are not needed or if connections can be consolidated to eliminate unneeded hardware.
    - Unused Up ports- All interfaces that are administratively marked “up” and operationally “down.” The list can help to quickly identify bad device configurations (unused ports should not be administratively “up”), failed or unplugged network cables, and badly allocated devices.
    - Recently changed ports- All interfaces that had status changes within the last hour. On a stable network interface, status should not change often, so the list should small or empty. If there are known connectivity problems, this list helps isolate possible problem sources.
  - Operating Systems- lists operating systems running on devices in the network, including routers, switches, load balancers, Infoblox NIOS systems, and other devices from numerous vendors discovered on the network.
  - Device models-Lists model names of devices in the network.



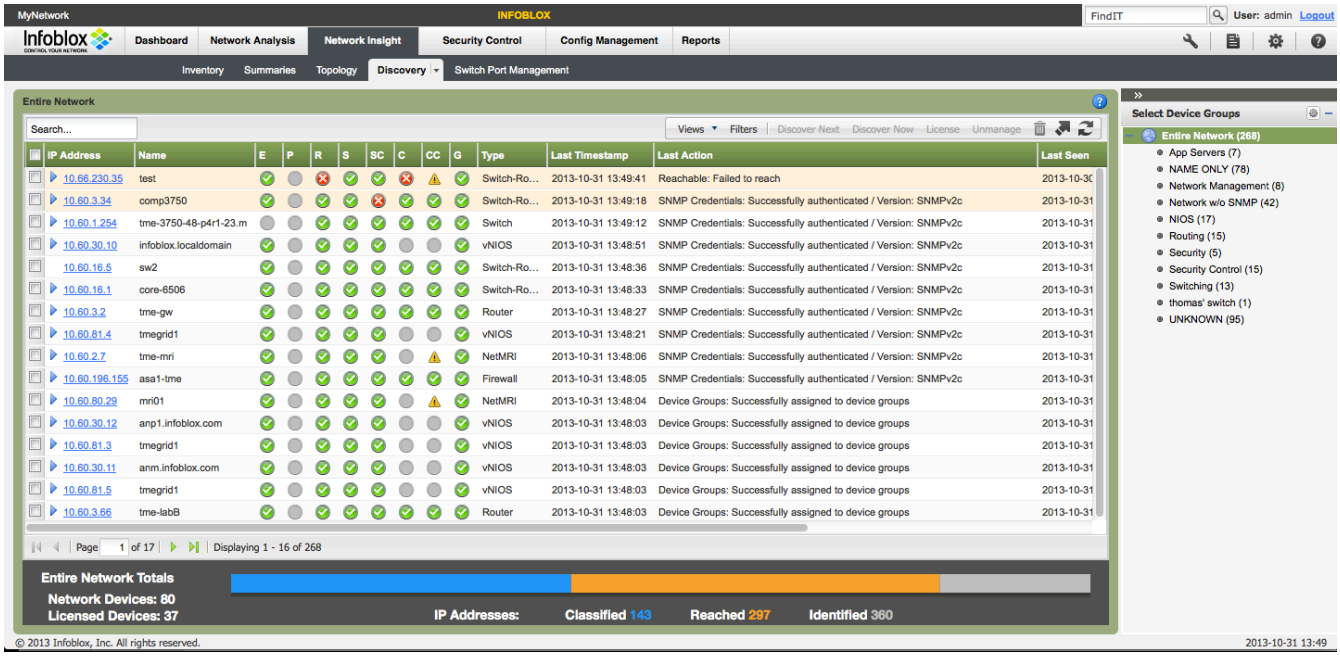
Summaries of

- Routes-lists routes reported by all devices in the network from each of their interfaces during the last network polling cycle by Network Automation.
- Subnets-Subnets are compiled from all router and switch-router devices discovered and catalogued by Network Automation, including any virtual device contexts.
- VLANs-Shows VLANs discovered in the network.
- HSRP/VRRP groups-lists Hot Standby Router Protocol (HSRP) groups and Virtual Router Redundancy Protocol (VRRP) groups found in the network, starting with the Virtual IP address of the group.
- Ports-lists ports found in the network. The list is a superset of ports listed in Switch Port Manager.
- NIOS Grids-lists any Infoblox NIOS Grid Masters found in the network.

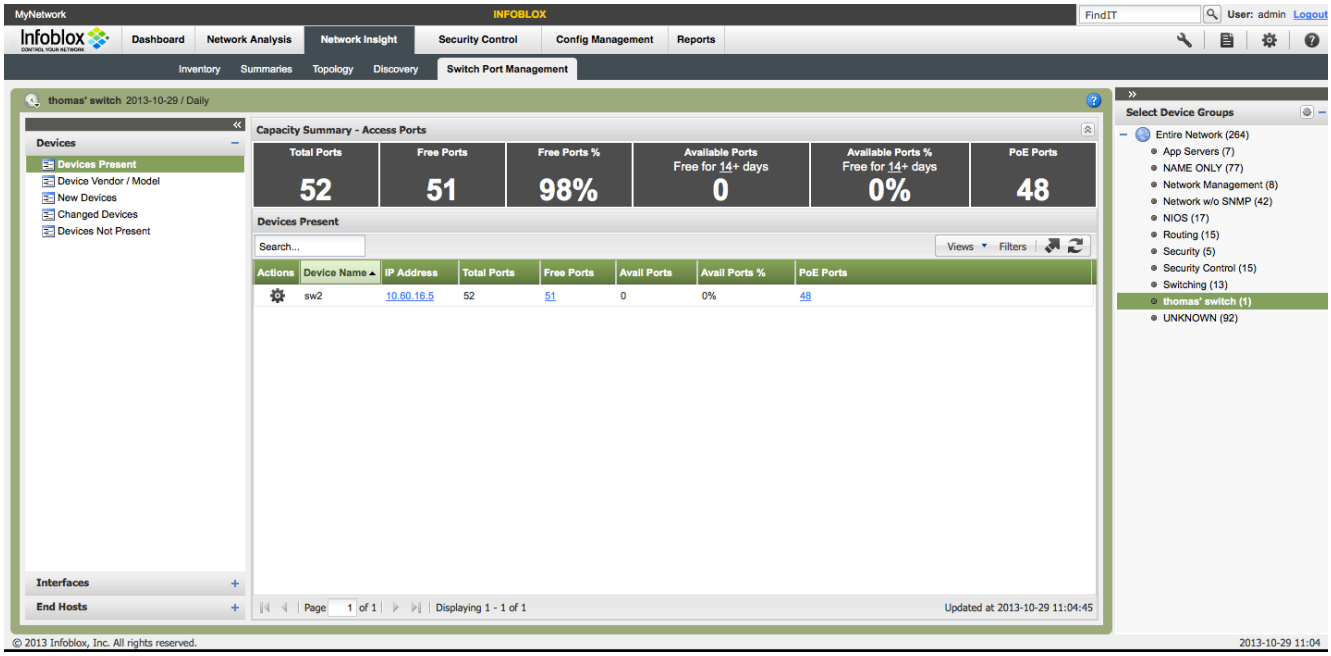


Topology

- Network
  - Aggregate View-combines the Link Discovery Protocols, Serial Links and Switch Forwarding views.
  - Link Discovery Protocol view-shows L2/L3 devices using Link Layer Discovery Protocol (LLDP) or Cisco Discovery Protocol (CDP), and their interconnections.
  - Serial Links view-shows L2/L3 devices connected by serial links.
  - Switch Forwarding view- shows L2/L3 devices using switch forwarding.
- L2 n Hop- shows devices that can be reached from a selected starting device through a chosen number of Layer 2 (actually a hybrid of L1 and L2) connections.
- L3 n Hop - shows all active devices that can be reached from a selected starting device in the network through a chosen number of routed Layer 3 connections.
- L2/L3 Most Likely Path - shows the most likely path traffic would take between two devices, including both Layer 2 and Layer 3 connectivity.
- L3 Most Likely Path - shows the most likely path that routable Layer 3 traffic would take between a source device and a destination device, ignoring Layer 2 connectivity between Layer 3 devices
- VLAN - shows the spanning tree that a given VLAN uses on the network.
- Path Analysis - allows tracing a Layer 3 path across a network of any scale, subject only to the restriction that Network Automation must discover and manage both the source and destination devices.



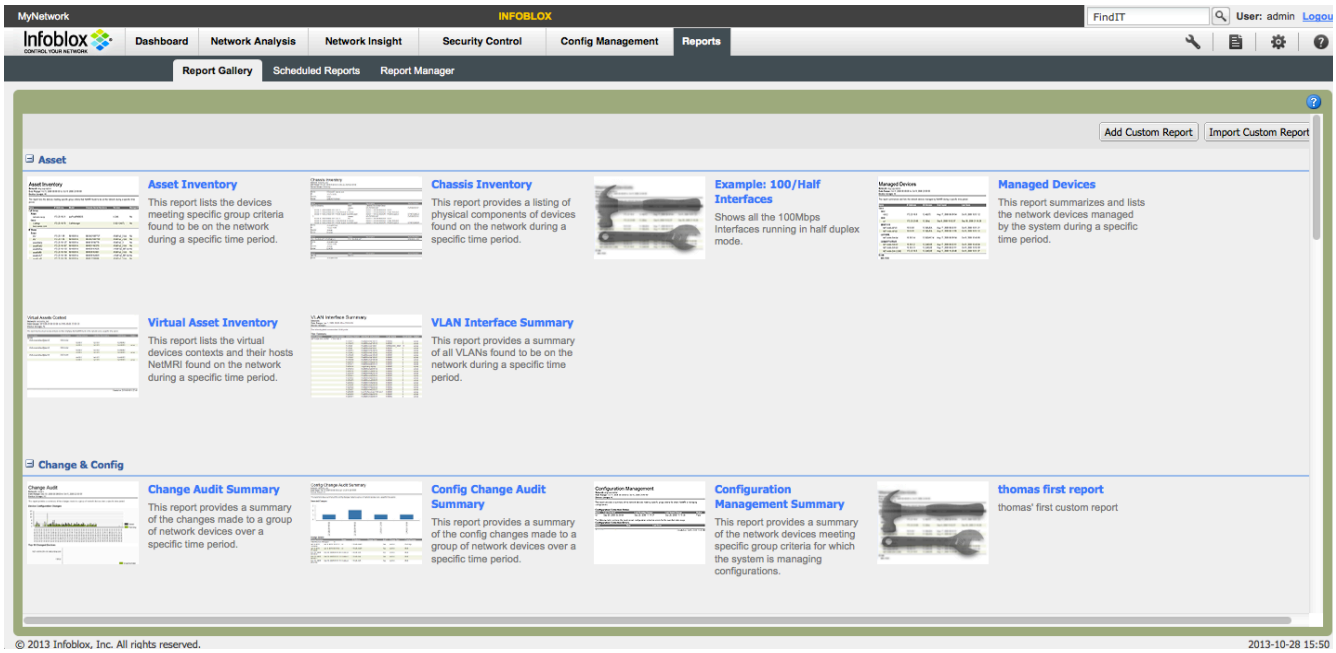
Discovery-Inventory listing of discovered devices and the status of their discoveries. For more information, consult the Network Automation Administrator Guide.



The Switch Port Management screen shows the following:

- Capacity Summary-Access Ports
  - Total Ports-The number of switched Ethernet ports, in the selected Device Group, that are being managed by Switch Port Manager (if Entire Network is chosen, this counter represents all managed switching ports).
  - Free Ports-The count of ports most recently polled that show a link state of Down, having lost connectivity.
  - Free Ports %-The percentage of all managed switch ports in the chosen Device Group showing Down link state.
  - Available Ports-The count of ports that remained in a link state of Down for more than the prescribed time period; when a port is considered Available, it is deemed available for other network resources.
  - Available Ports %-The percentage of all managed switch ports appearing as Available.
  - PoE Ports-The count of Cisco switched Ethernet ports running the Power over Ethernet switching protocol for IP telephony applications.
- Devices
  - Devices present-provides the complete list of switches and switch routers that are being managed by Network Automation.
  - Device Vendor/Model-displays a different subset of Switch Port Manager data, focusing on equipment vendor, product model, device serial number and other information.
  - New devices-lists the subset of switching network devices that have been discovered by Network Automation during the displayed measurement period.
  - Changed devices-lists any network devices that have changed in some fashion within the most recent polling time period.
  - Devices not present-lists the subset of active switch and switch-router devices, excluding end hosts, with which Switch Port Manager has lost communication over the last measurement time period.
- Interfaces
  - Access Ports Present-provides the list of switched access interfaces for the entire network, the aggregate interface list for any chosen device group and the list of interfaces for any chosen LAN switch or distribution switch.
  - Link Changes-provides a list of interfaces that have most recently changed state.
  - Hub Locator- lists all switched interfaces in the network that operate as Smart Hubs, with more than one end host connected to the switch port.

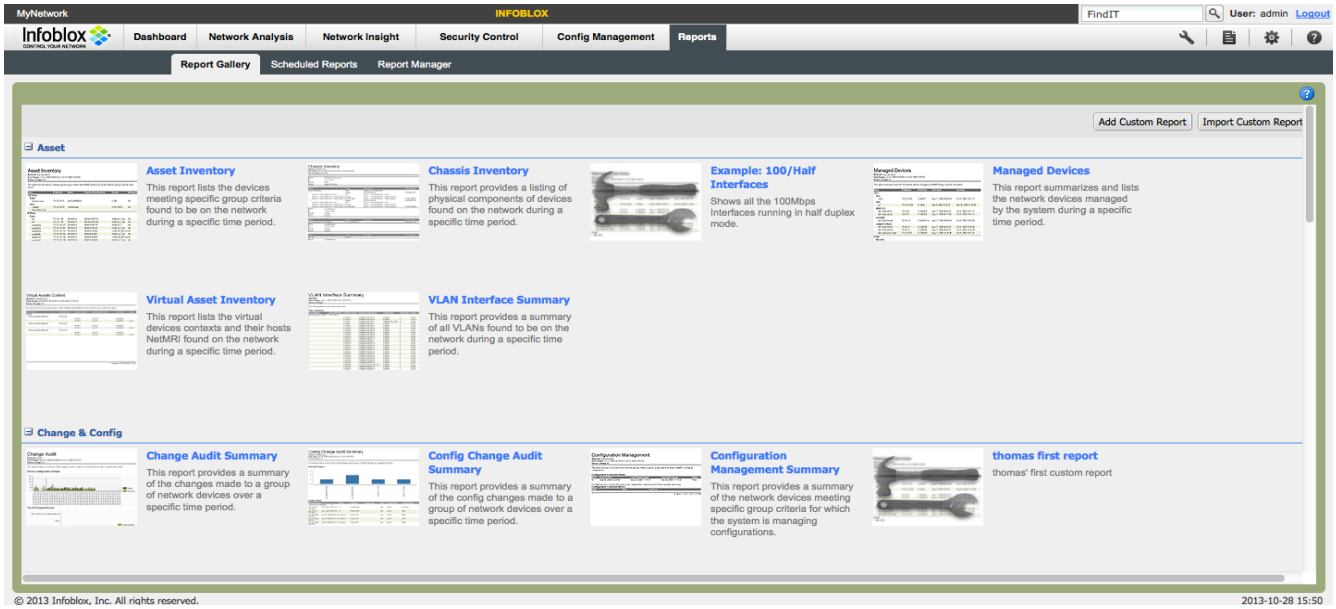
- End Hosts
  - End Host present-provides a complete list of all end host devices detected and successfully probed by the Network Automation appliance.
  - New End Hosts- filters the list of Devices Present to show the devices and hosts that were found by Network Automation since the last polling took place.
  - End Host not Present-lists the end devices or hosts that are discovered to be disconnected or otherwise become unreachable on the network when the last polling took place.
  - VLAN changes-lists all devices that switched from one VLAN to a different VLAN during the user-configured time period.



The report tab has 35 default reports to choose. In addition, you can create your own reports using one of 84 data types.

CIP-002-4 R2, R3- Network Automation covers this standard with the following features:

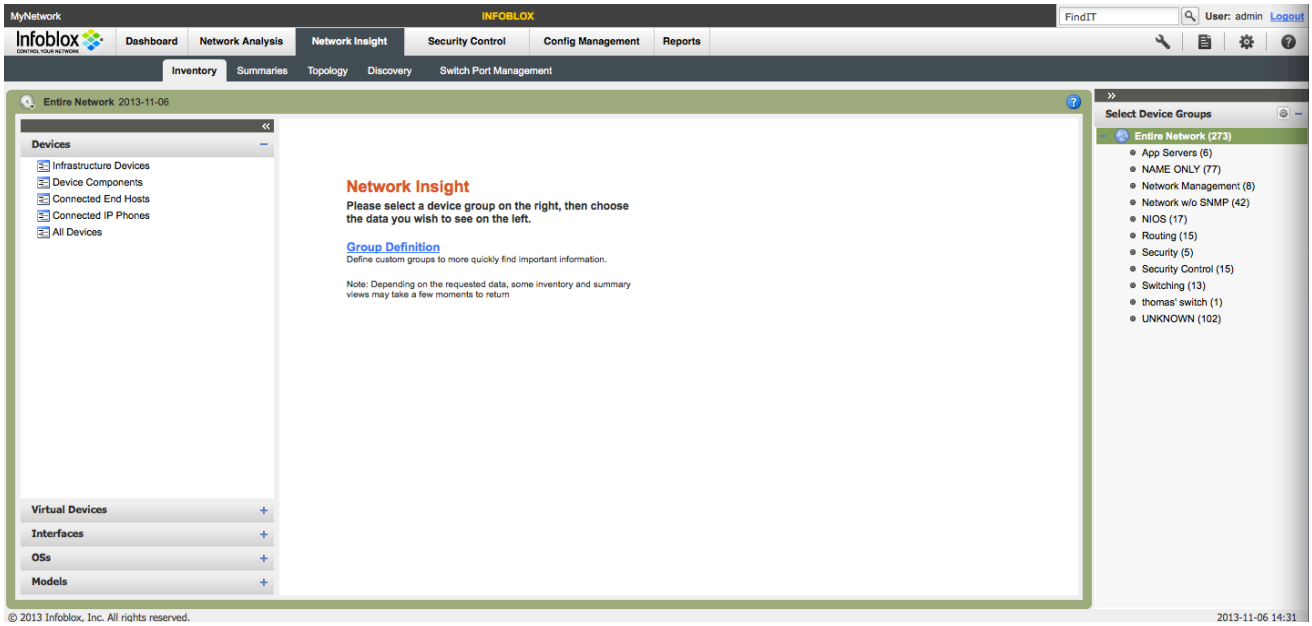
- **Reports**



The report tab has 35 default reports to choose. In addition, you can create your own reports using one of 84 data types.

CIP-003-3 R1, R4, R5, R6- Network Automation covers this standard with the following features:

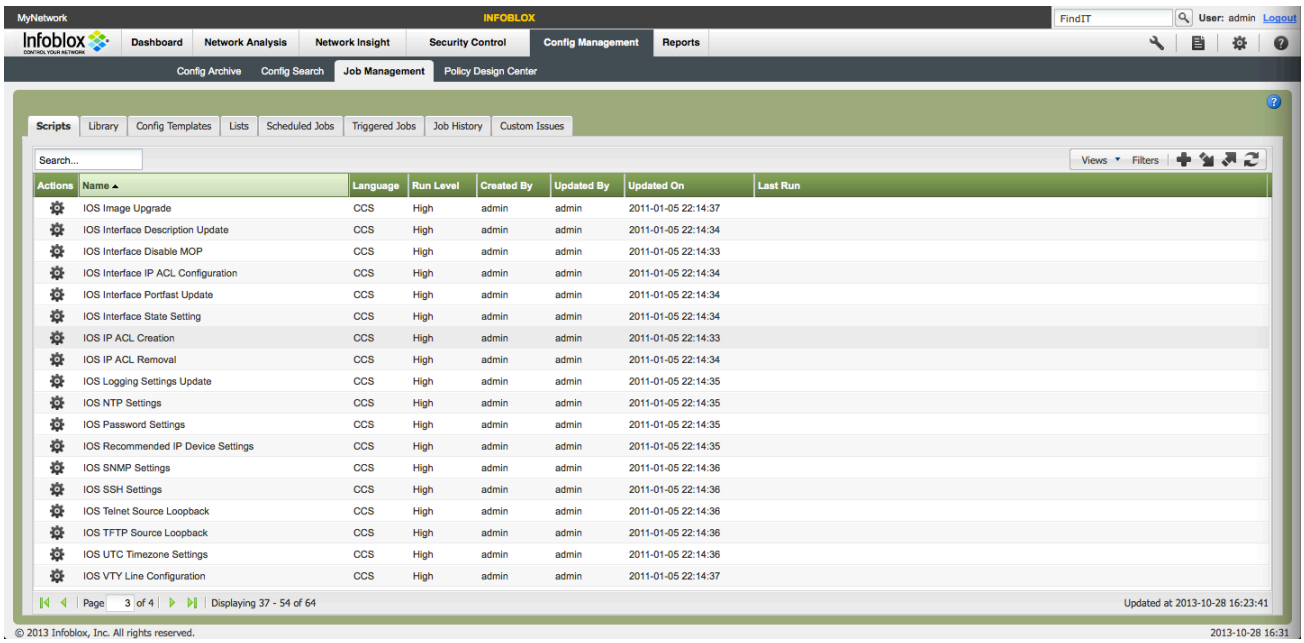
- Topology



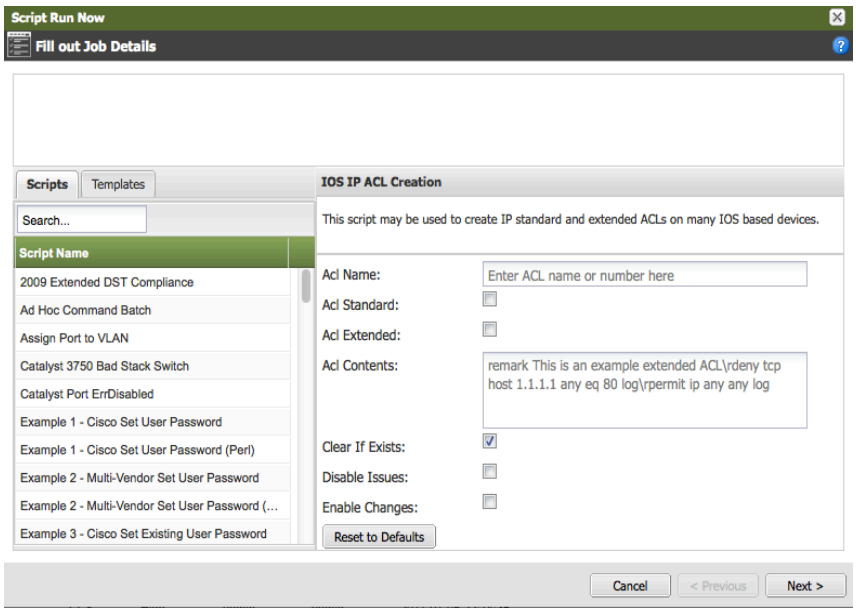
The Topology shows the following views:

- Topology
  - Network
    - Aggregate View-combines the Link Discovery Protocols, Serial Links and Switch Forwarding views.
    - Link Discovery Protocol view-shows L2/L3 devices using Link Layer Discovery Protocol (LLDP) or Cisco Discovery Protocol (CDP), and their interconnections.
    - Serial Links view-shows L2/L3 devices connected by serial links.
    - Switch Forwarding view- shows L2/L3 devices using switch forwarding.
  - L2 n Hop- shows devices that can be reached from a selected starting device through a chosen number of Layer 2 (actually a hybrid of L1 and L2) connections.
  - L3 n Hop - shows all active devices that can be reached from a selected starting device in the network through a chosen number of routed Layer 3 connections.
  - L2/L3 Most Likely Path - shows the most likely path traffic would take between two devices, including both Layer 2 and Layer 3 connectivity.
  - L3 Most Likely Path - shows the most likely path that routable Layer 3 traffic would take between a source device and a destination device, ignoring Layer 2 connectivity between Layer 3 devices
  - VLAN - shows the spanning tree that a given VLAN uses on the network.
  - Path Analysis - allows tracing a Layer 3 path across a network of any scale, subject only to the restriction that Network Automation must discover and manage both the source and destination devices.

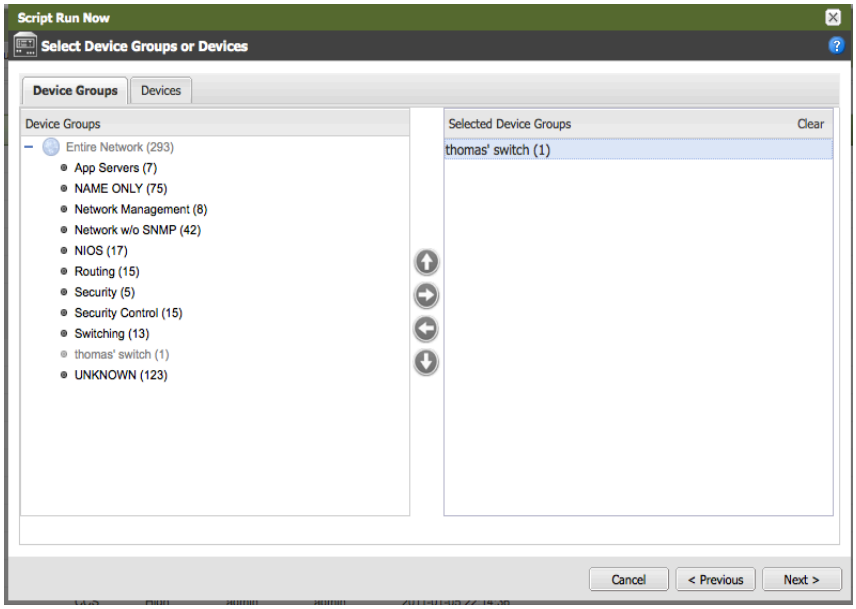
- Access control configuration



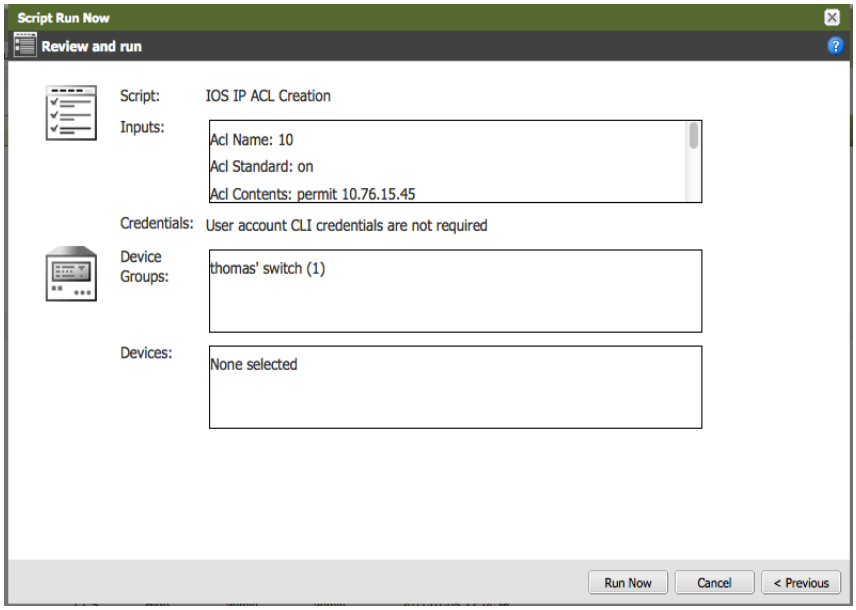
Using the IOS IP ACL Creation script, you can create access lists to control access to the network device. Click on the Actions wheel to run the script.



Fill in the fields on the right side of the screen for the ACL. Click Next to continue.

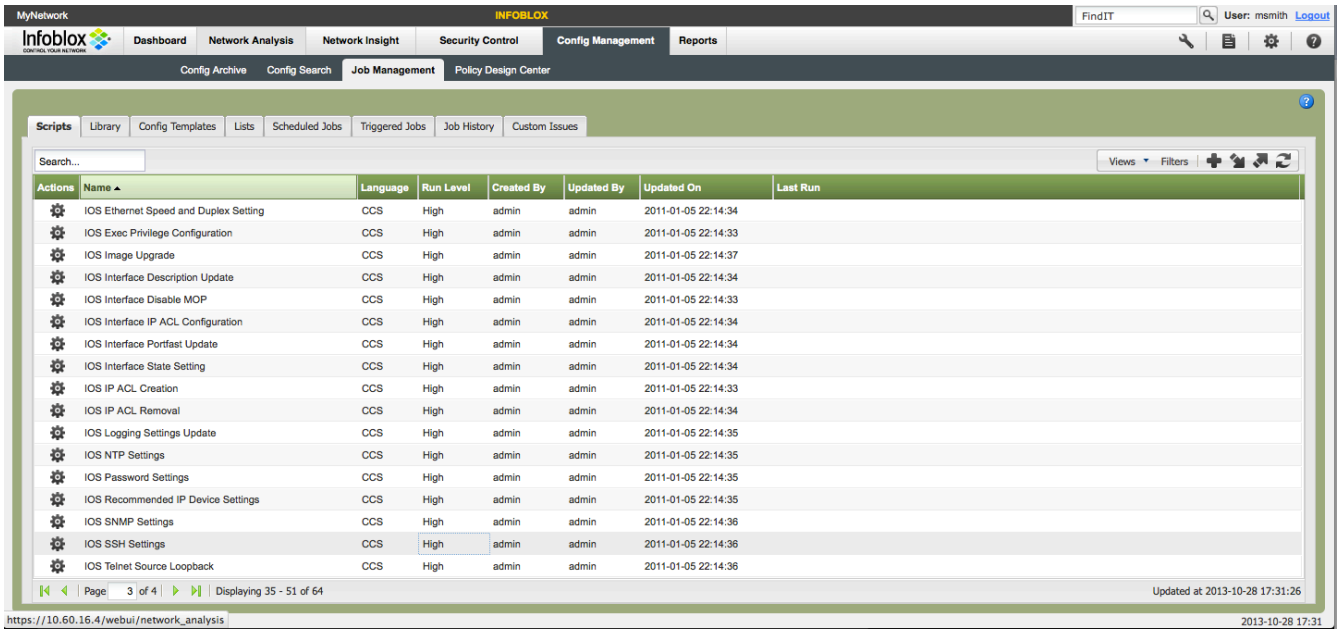


Select a device group to apply the script to.

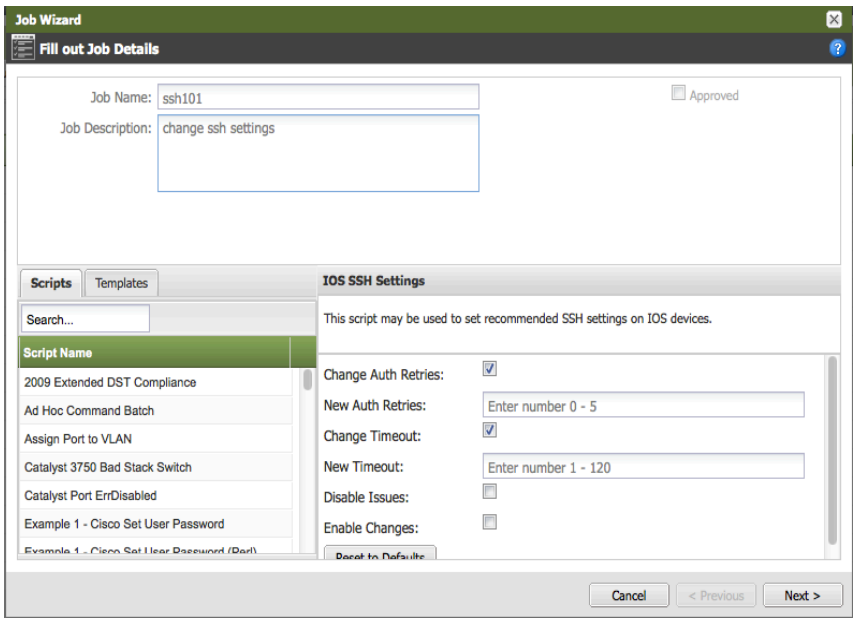


Click on the Run Now button.

- Work Flow

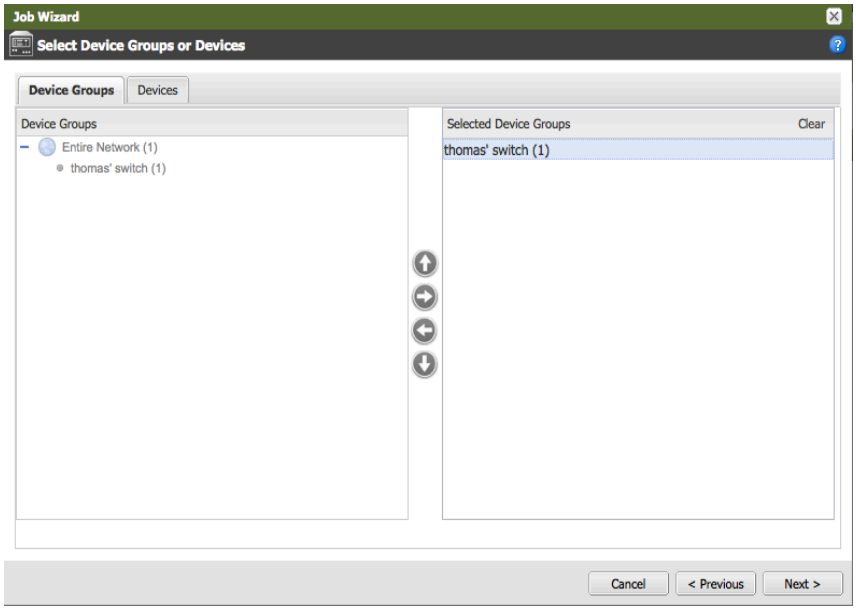


Click on one of the scripts to schedule.

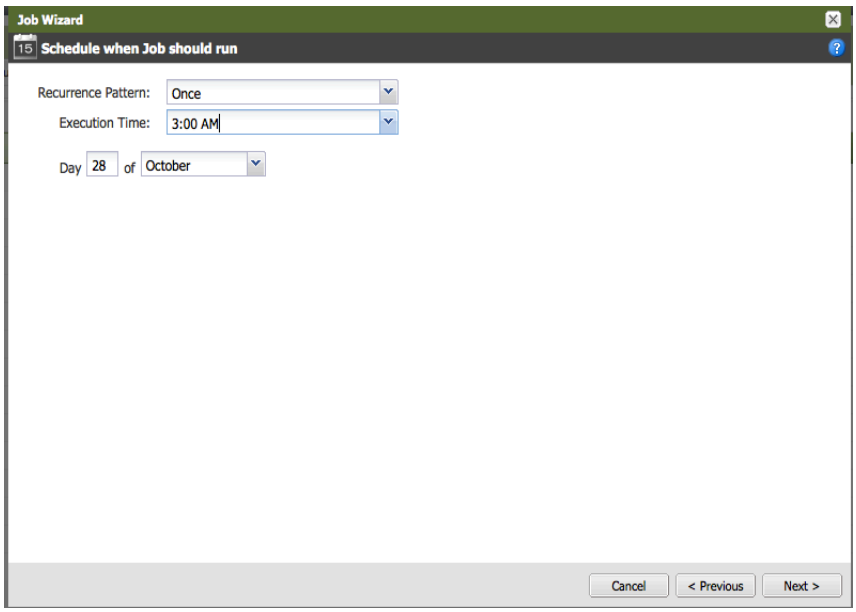


For example, we chose the IOS SSH settings script to schedule. The user does not have rights to run this script without approval from a higher user authority. Notice the Approved button is grayed out.

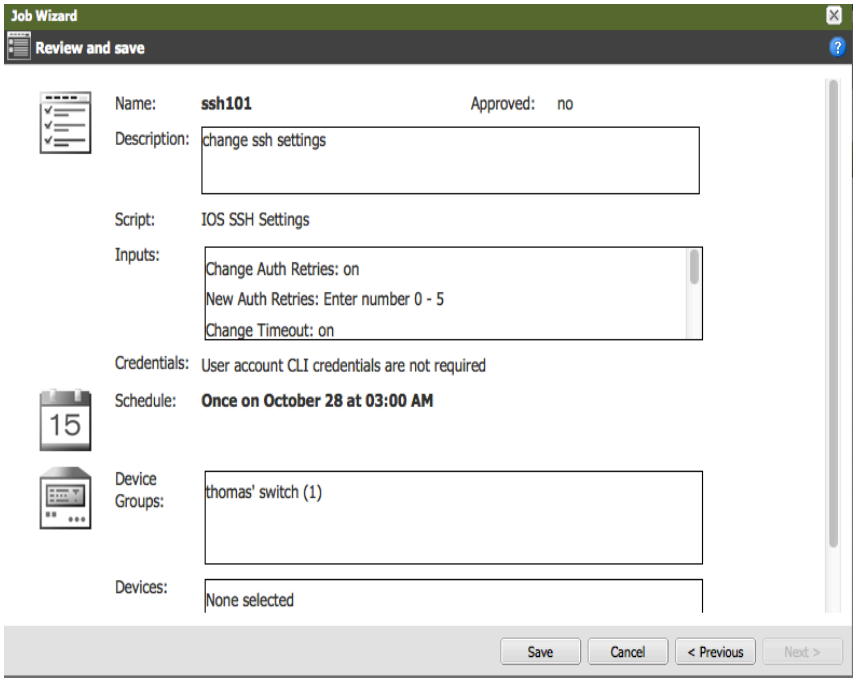
1. Input the requested values in the fields to the right.
2. Click on the Next button.



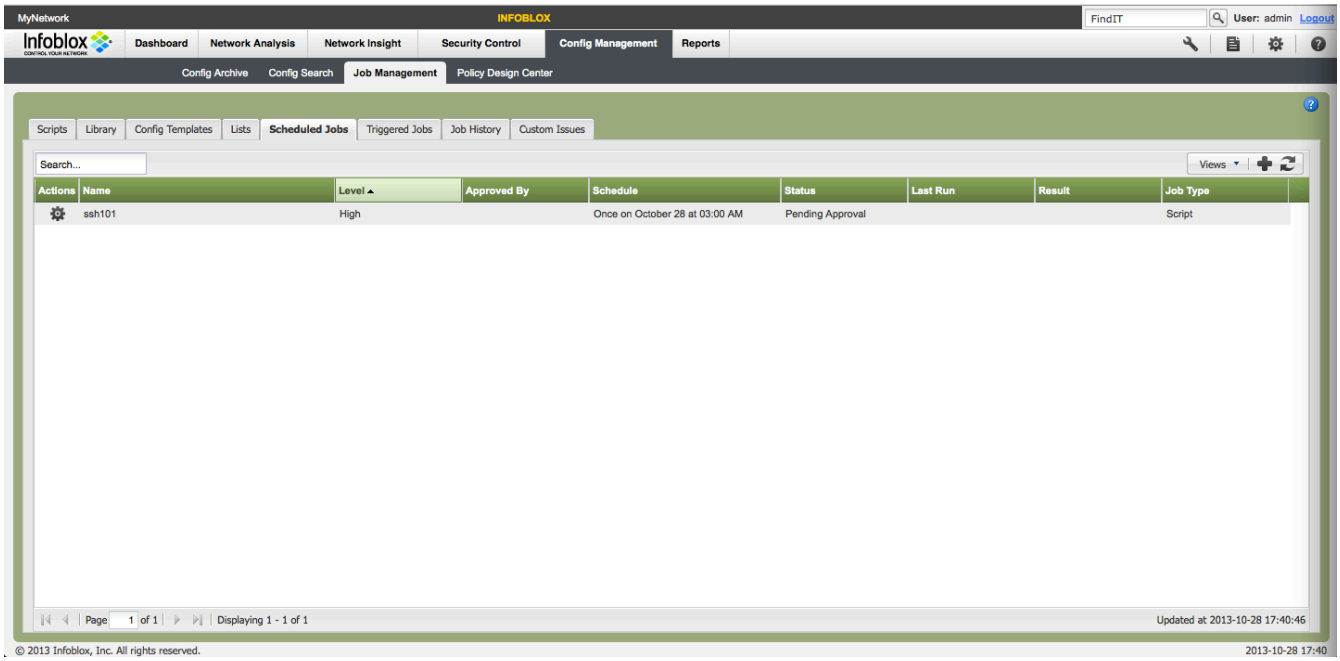
1. Select the device group to run the script on.
2. Click on the Next button.



1. Select the Recurrence Pattern, Execution time, and date.
2. Click Next.

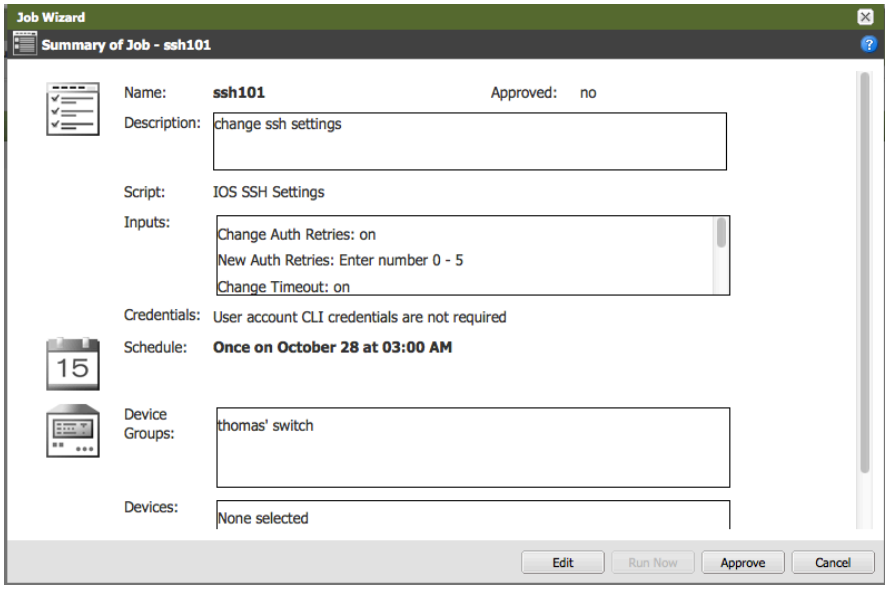


1. Click on the Save button.



The user with a higher authority logs in to look for jobs that are scheduled.

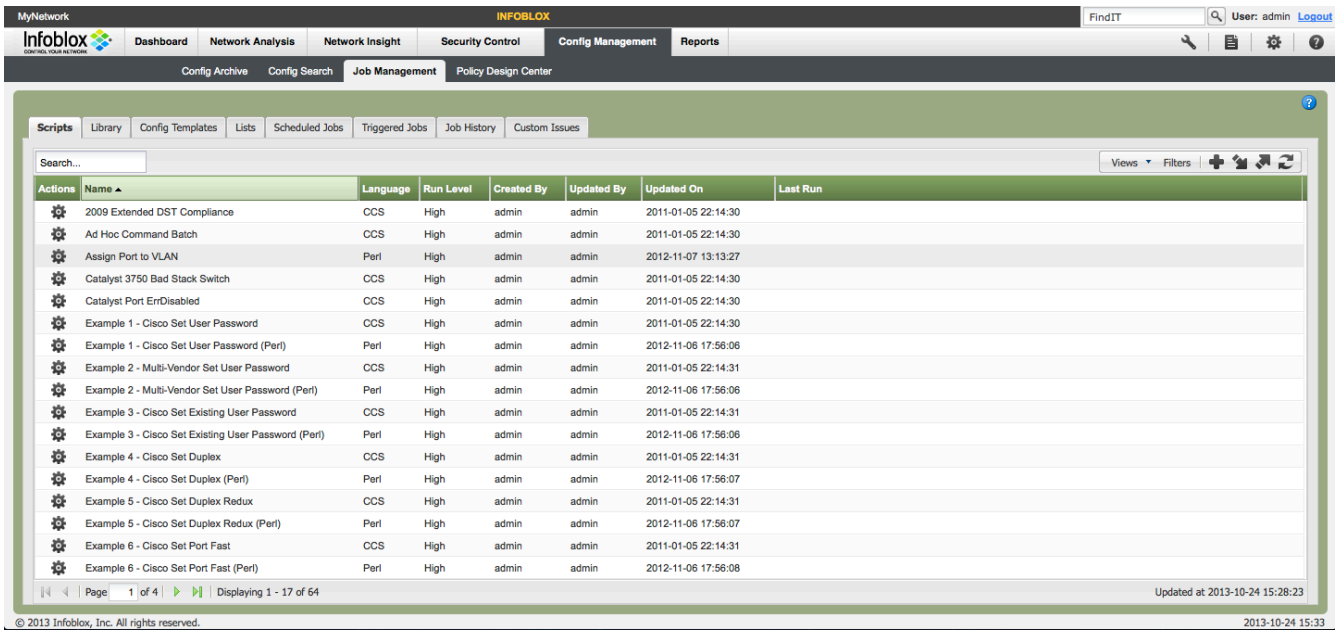
1. Click on the Actions wheel to view/edit the job.



1. Click on the Approve button to approve the job. The job will now run at the selected time.

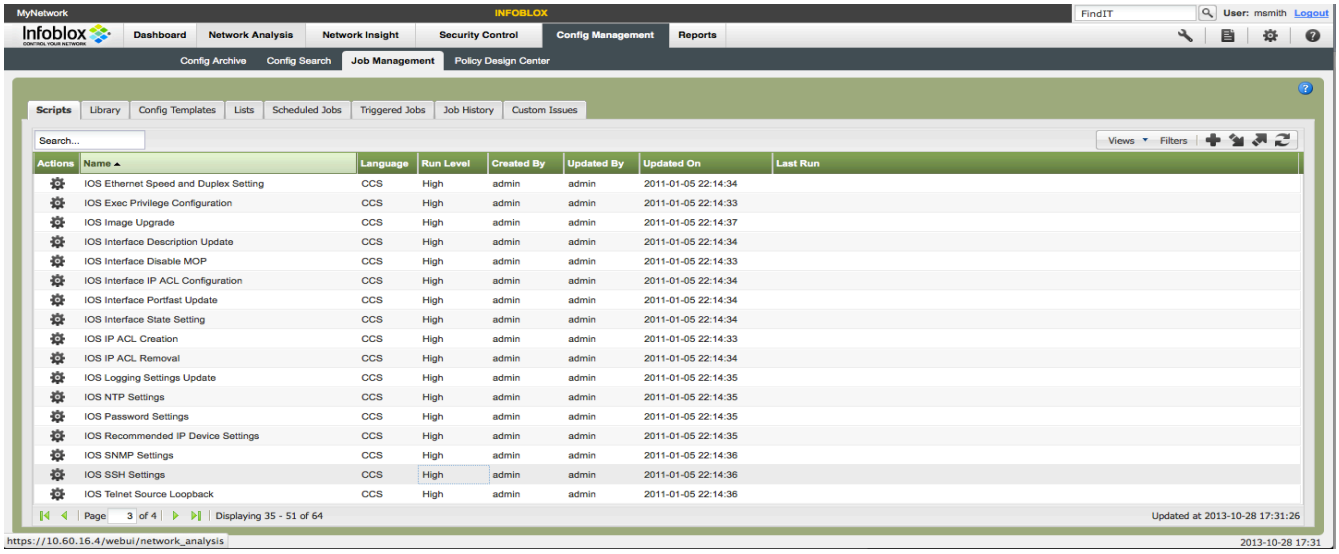
CIP-003-4 R4, R5, R6- Network Automation covers this standard with the following features:

- **Audit logs**

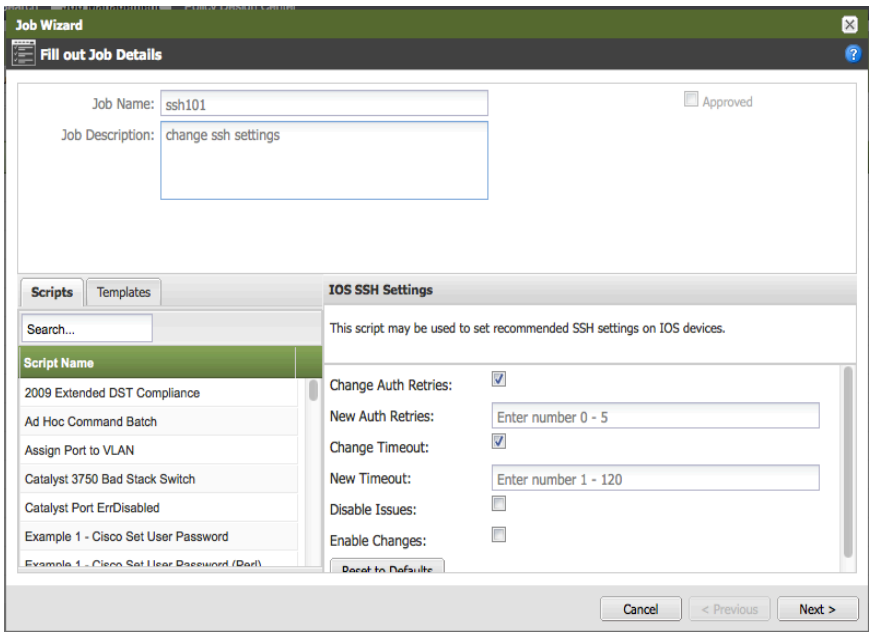


You can manage passwords of network devices with the use of the password change script. Navigate to Config Management -> Job Management -> Scripts. By default, there are seven different scripts that can be used to add usernames and/or modify passwords. These scripts can be copied and modified by the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

- **Workflow**

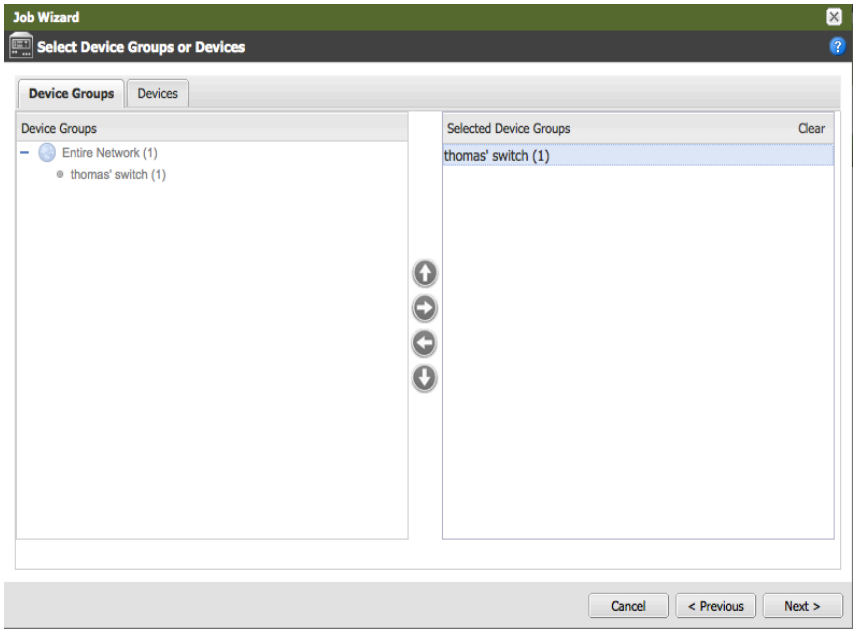


1. Click on one of the scripts to schedule.

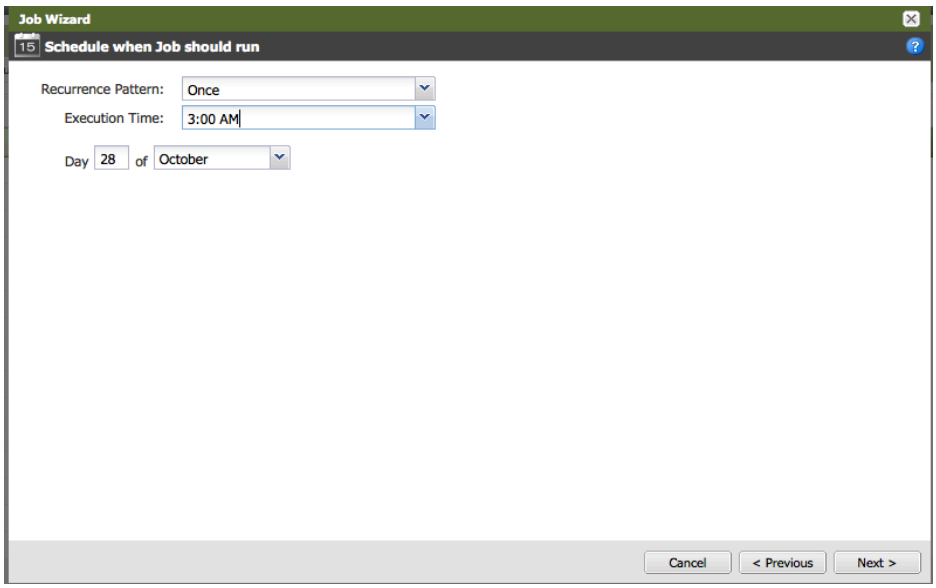


For example, we chose the IOS SSH settings script to schedule. The user does not have rights to run this script without approval from a higher user authority. Notice the approved button is grayed out.
Input the requested values in the fields to the right.

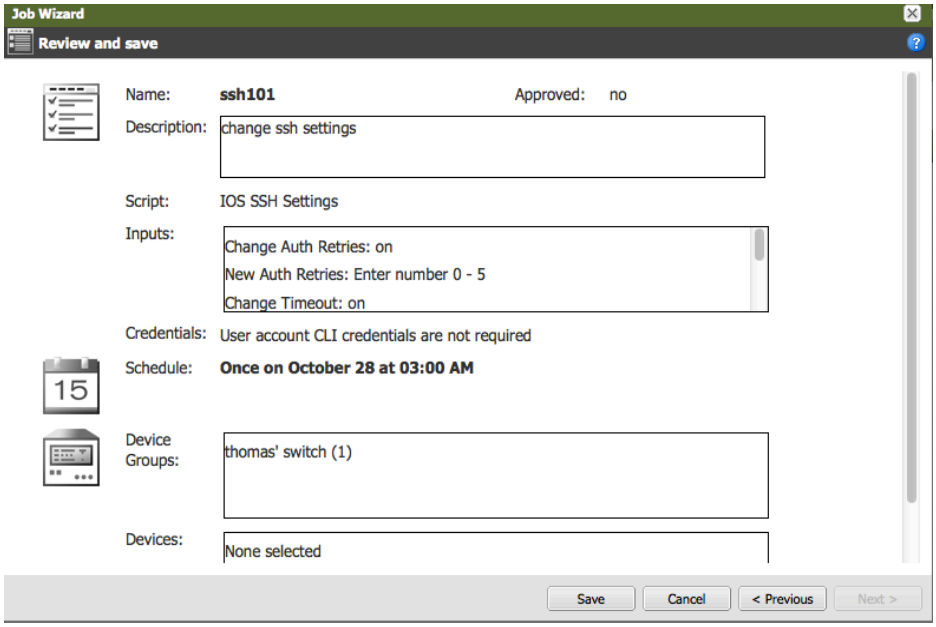
1. Click on the Next button.



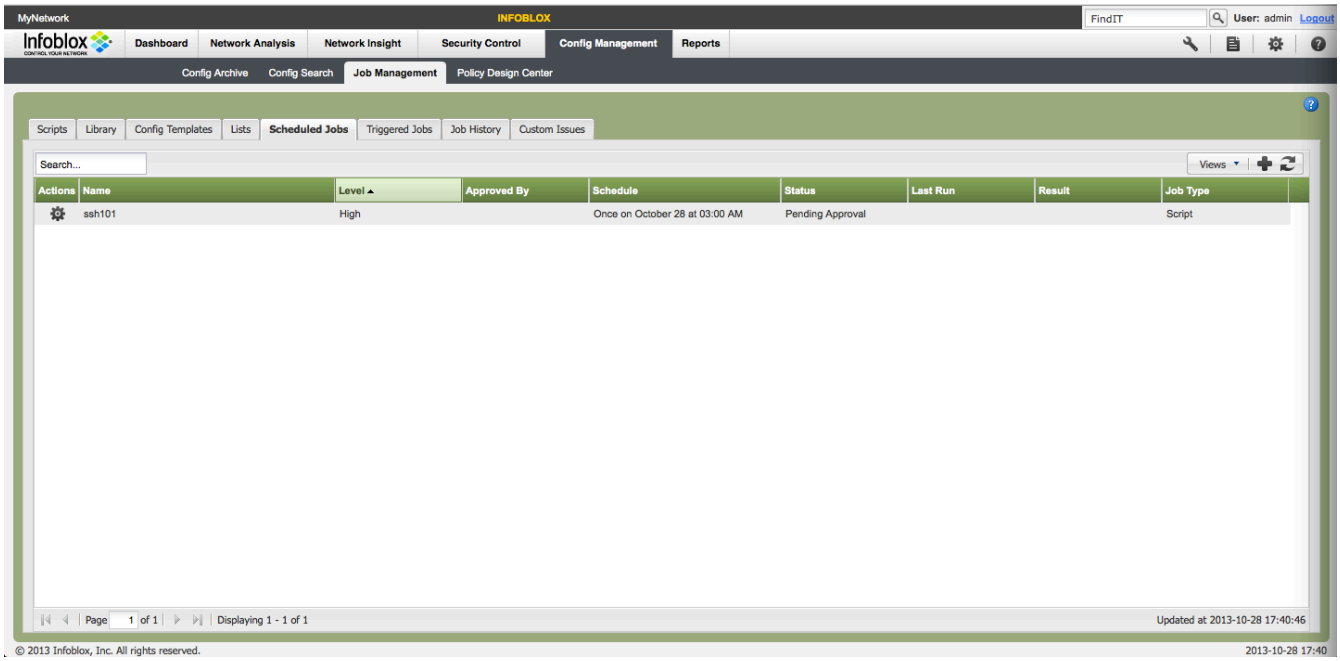
1. Select the device group to run the script on.
2. Click on the Next button.



1. Select the Recurrence Pattern, Execution time, and date.
2. Click Next.

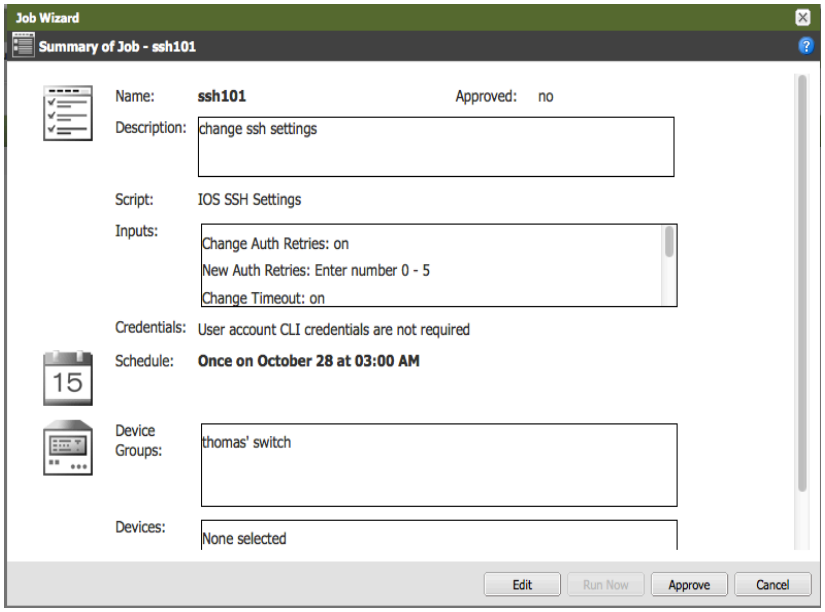


1. Click on the Save button.



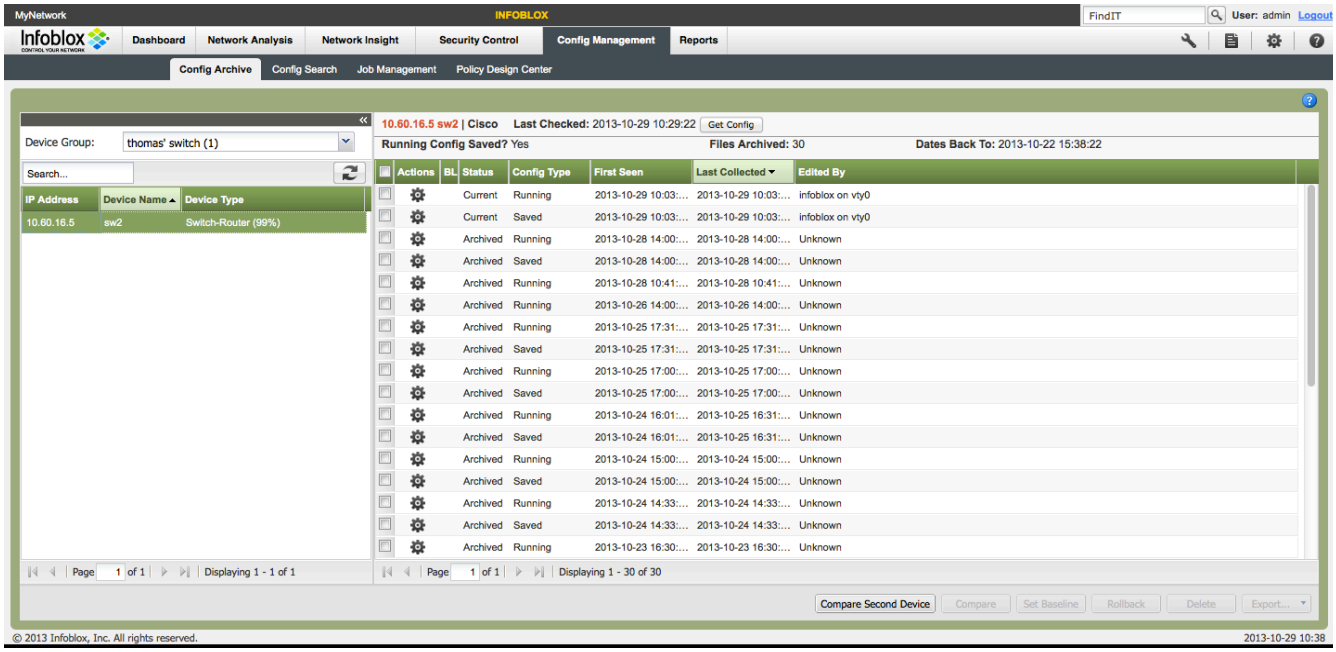
The user with a higher authority logs in to look for jobs that are scheduled. In this case it is the admin user.

1. Click on the Actions wheel to view/edit the job.

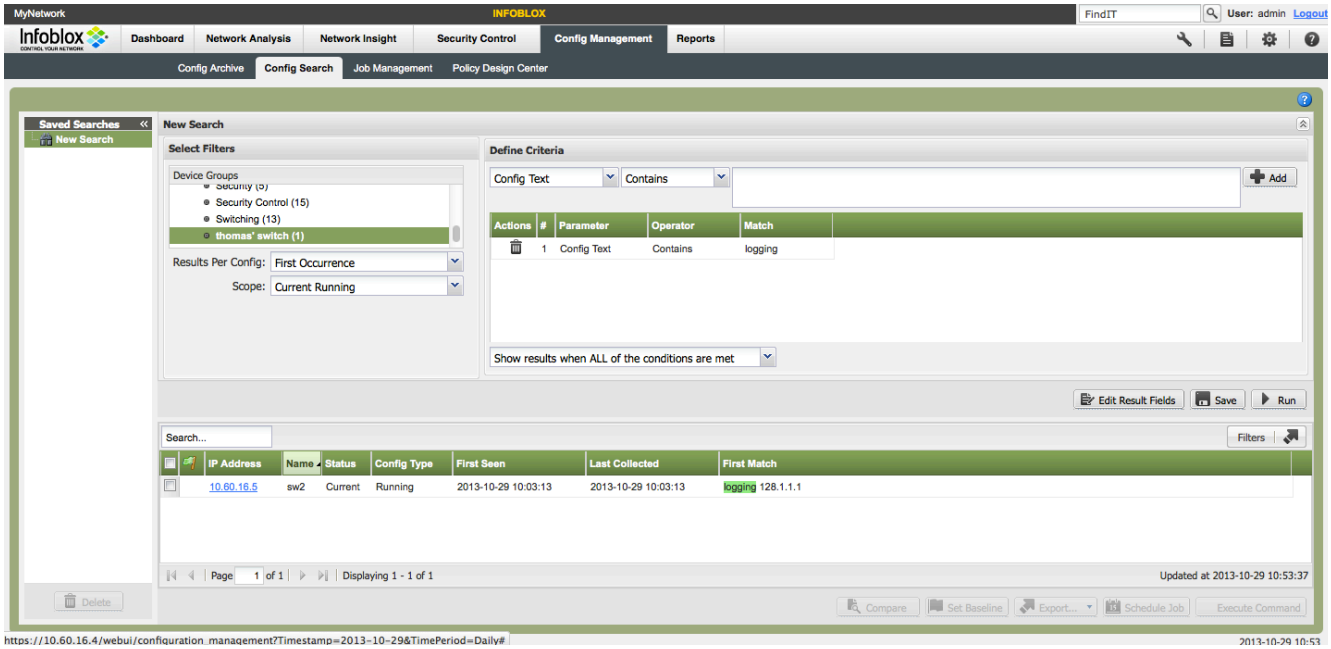


1. Click on the Approve button to approve the job.
2. The job will now run at the selected time.

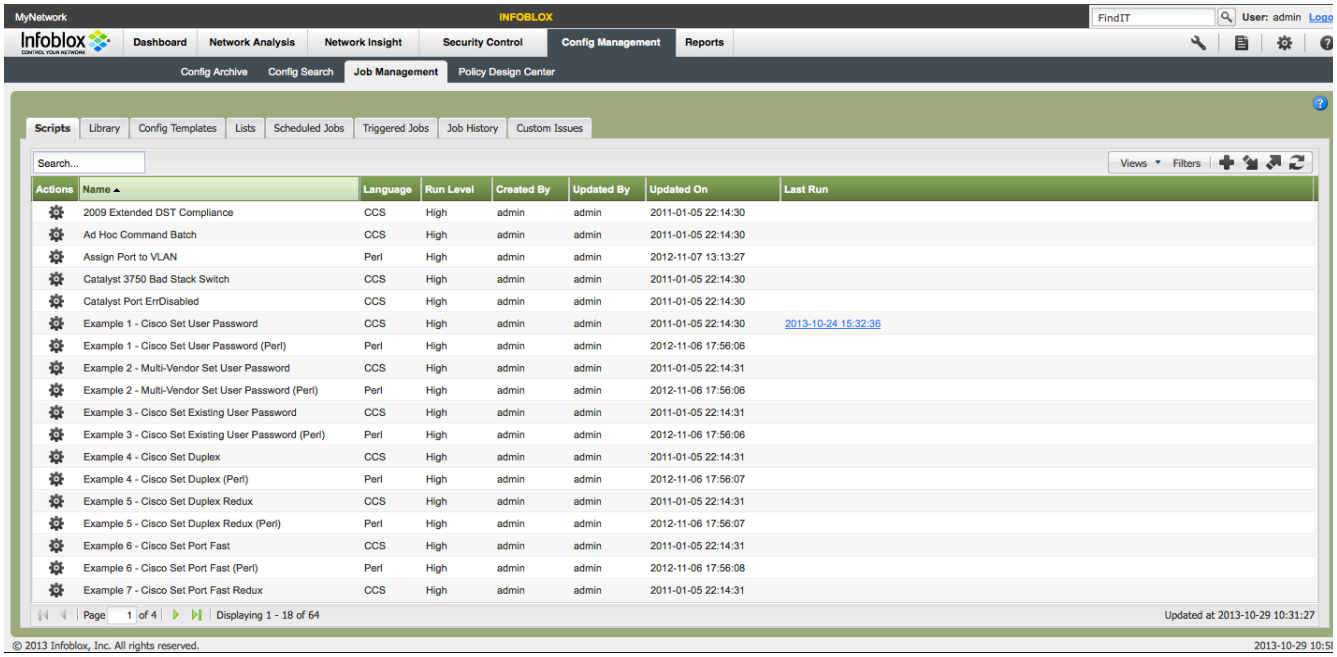
- **The Config Management Tab contains the following tabs:**



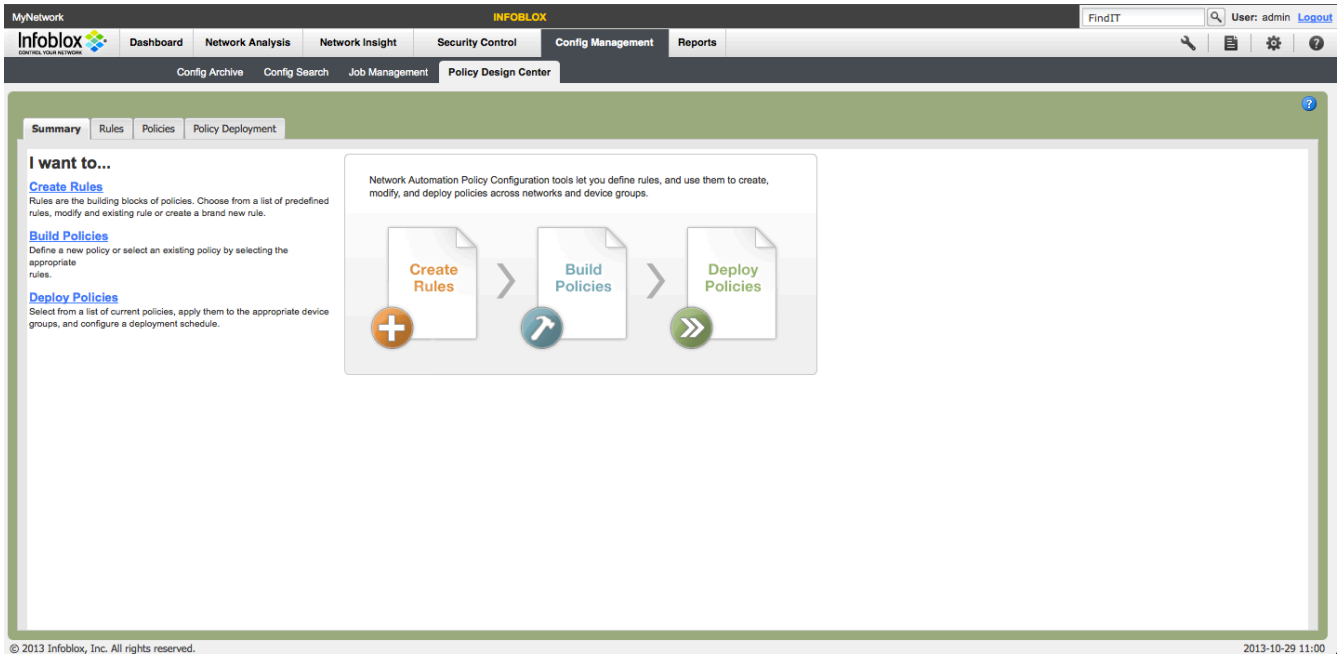
- Config Archive-The Config Archive is the screen that lists all of the configuration file changes that have occurred for a selected device. Two configuration files can be compared for any differences. A baseline configuration can be chosen. You can also use a configuration to rollback a device to a known working state. One or more configuration files can be exported to your local workstation.



- Config Search-The Config Search tab lets you search devices in the network for a particular configuration string, an IP address or other specific device specification such as a MAC address, device model, or other parameters, using many different types of search criteria and even regular expressions.



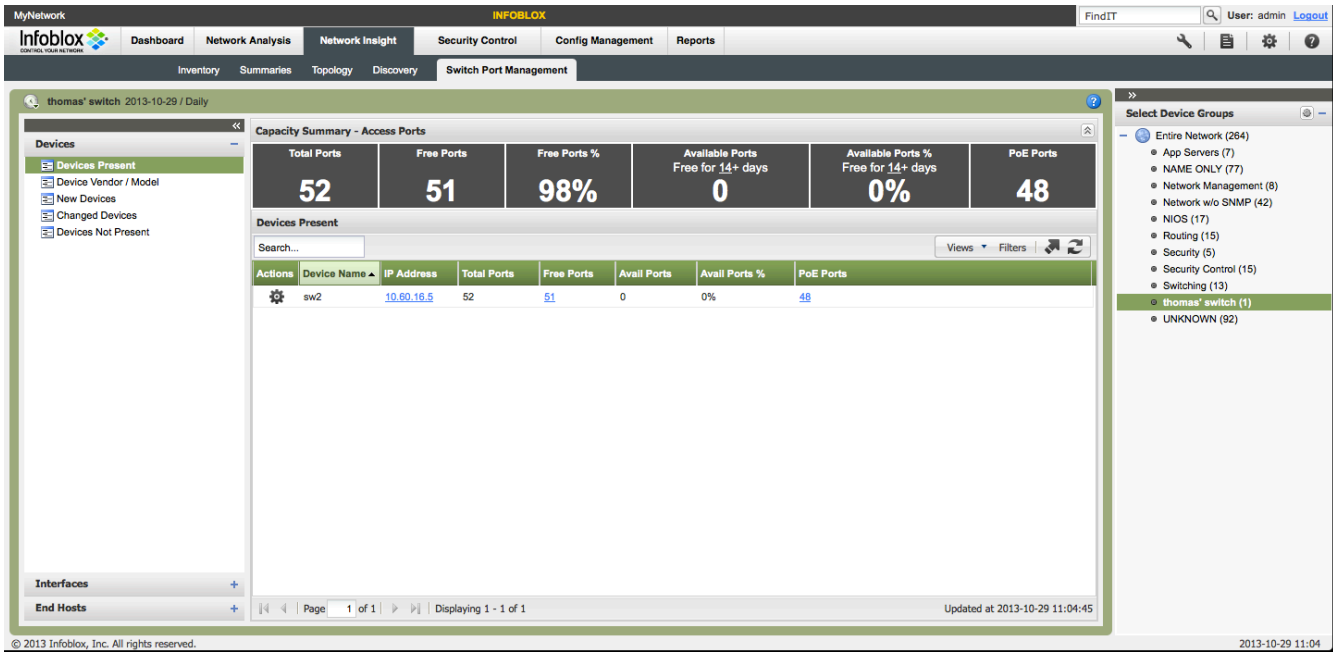
- Job Management-The Job Management tab enables creation, scheduling, approval and execution of Job Management scripts in the Perl and CCS languages, and the definition of custom issues to extend the library of issue types that Network Automation uses for reporting and monitoring of adverse events in the network.



- Policy Design Center-The Policy Design Center, to create rules and policies, and deploy policies on the network. Policies are a tool for ensuring all devices in the network meet a minimum standard of readiness and security.

CIP-005-3a R3.1, R3.2- Network Automation covers this standard with the following features:

- **Switch Port Manager**



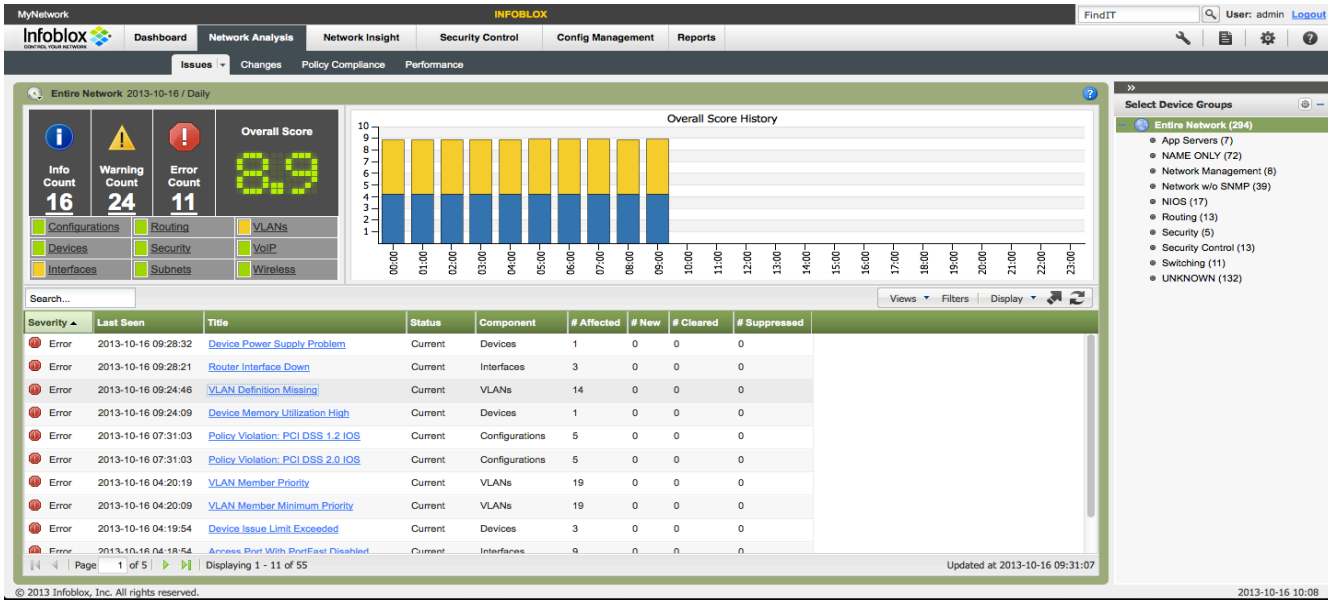
The Switch Port Management screen shows the following:

- Capacity Summary-Access Ports
  - Total Ports: The number of switched Ethernet ports, in the selected Device Group, that are being managed by Switch Port Manager (if Entire Network is chosen, this counter represents all managed switching ports).
  - Free Ports: The count of ports most recently polled that show a link state of Down, having lost connectivity.
  - Free Ports %: The percentage of all managed switch ports in the chosen Device Group showing Down link state.
  - Available Ports: The count of ports that remained in a link state of Down for more than the prescribed time period; when a port is considered Available, it is deemed available for other network resources.
  - Available Ports %: The percentage of all managed switch ports appearing as Available.
  - PoE Ports: The count of Cisco switched Ethernet ports running the Power over Ethernet switching protocol for IP telephony applications.
- Devices
  - Devices present-provides the complete list of switches and switch routers that are being managed by Network Automation.
  - Device Vendor/Model-displays a different subset of Switch Port Manager data, focusing on equipment vendor, product model, device serial number and other information.
  - New devices-lists the subset of switching network devices that have been discovered by Network Automation during the displayed measurement period.
  - Changed devices-lists any network devices that have changed in some fashion within the most recent polling time period.
  - Devices not present-lists the subset of active switch and switch-router devices, excluding end hosts, with which Switch Port Manager has lost communication over the last measurement time period.
- Interfaces
  - Access Ports Present-provides the list of switched access interfaces for the entire network, the aggregate interface list for any chosen device group and the list of interfaces for any chosen LAN switch or distribution switch.

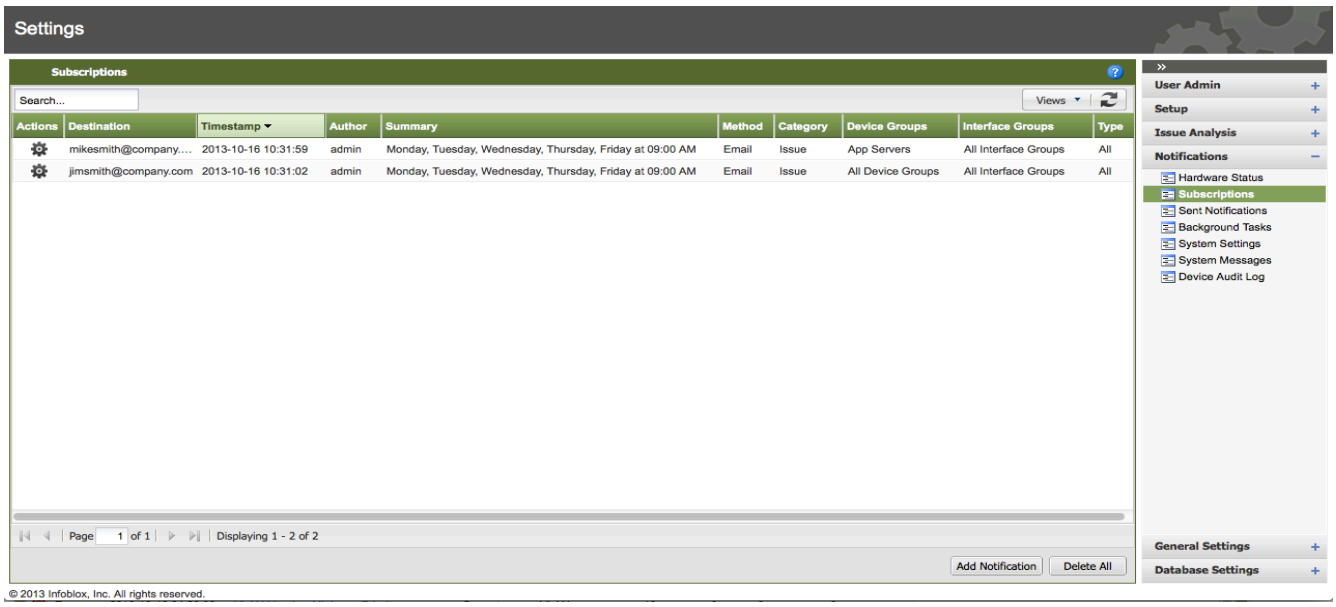
- Link Changes-provides a list of interfaces that have most recently changed state.
- Hub Locator- lists all switched interfaces in the network that operate as Smart Hubs, with more than one end host connected to the switch port.

- End Hosts
  - End Host present-provides a complete list of all end host devices detected and successfully probed by the Network Automation appliance.
  - New End Hosts- filters the list of Devices Present to show the devices and hosts that were found by Network Automation since the last polling took place.
  - End Host not Present-lists the end devices or hosts that are discovered to be disconnected or otherwise become unreachable on the network when the last polling took place.
  - VLAN changes-lists all devices that switched from one VLAN to a different VLAN during the user-configured time period.

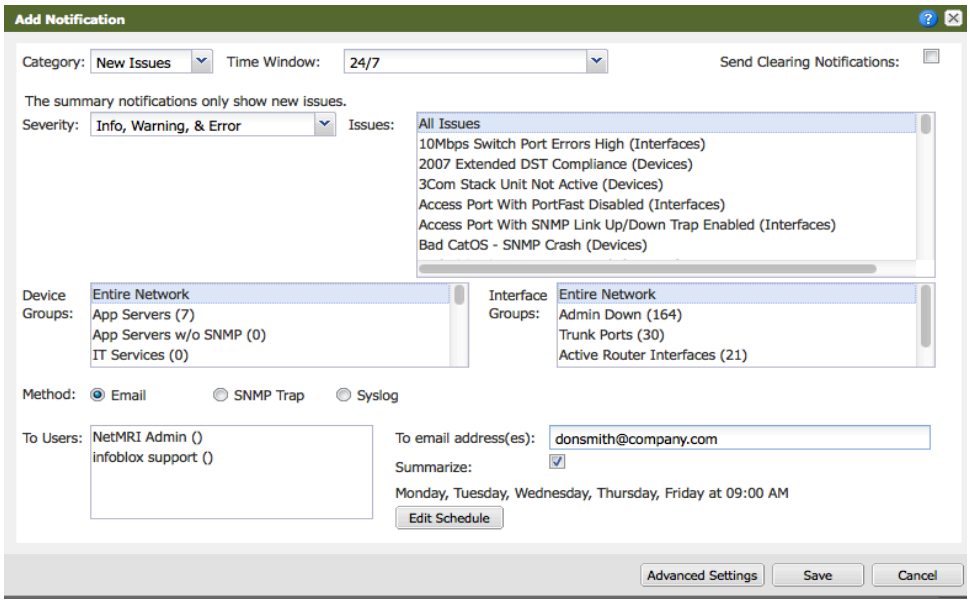
- **Issues Notification**-A good way to use issues for troubleshooting is to assign them to network support staff by the category of issues. In a large organization, everybody does not need to see every issue with every device. Most likely, the network support staff is grouped by function, devices, or region. This allows the appropriate staff to focus areas within their work responsibilities. Here are the steps:



1. Log into Network Automation.
2. In the upper right corner of the screen, click on the settings button which is highlighted in the circle.



1. Click on Notifications -> Subscriptions.
2. Click on the Add Notification button to assign network support staff to specific or groups of issues.

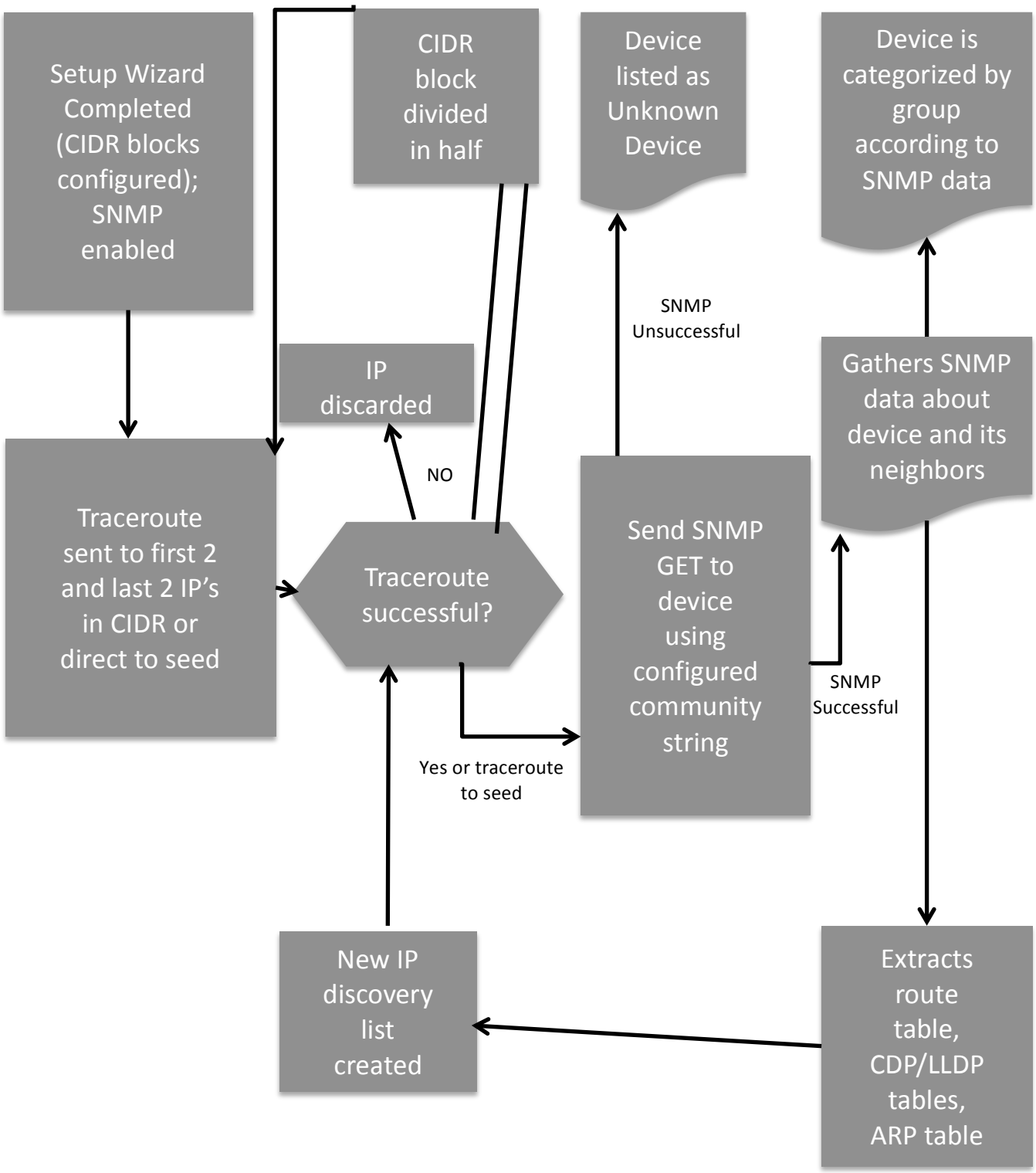


1. Select the time window. This setting determines when an issue notification is sent. The choices are:
   - 24/7
   - Work Hours (M-F 8am-6pm)
   - Off Hours (M-F 6pm-8am, Sat, Sun)
   - First Shift (M-F 12am-8am)
   - Second Shift (M-F 8am-4pm)
   - Third Shift (M-F 4pm-12am)
   - Weekends (Sat/Sun)

2. Select the Severity. This setting determines the level of severity of the issues sent to the user. The choices are:
   - Info, Warning, & Error
   - Warning and Error
   - Error
3. Select the Issue(s) to be sent to the user. You can select one or more issues to be sent.
4. Select the device groups and interface groups.
5. Enter the email address.
6. Optionally, edit the schedule to control the days that the issue notifications are sent.
7. Click save to save the subscription.

CIP-005-3a R3.1, R3.2 R4.3, R4.4- Network Automation covers this standard with the following features:

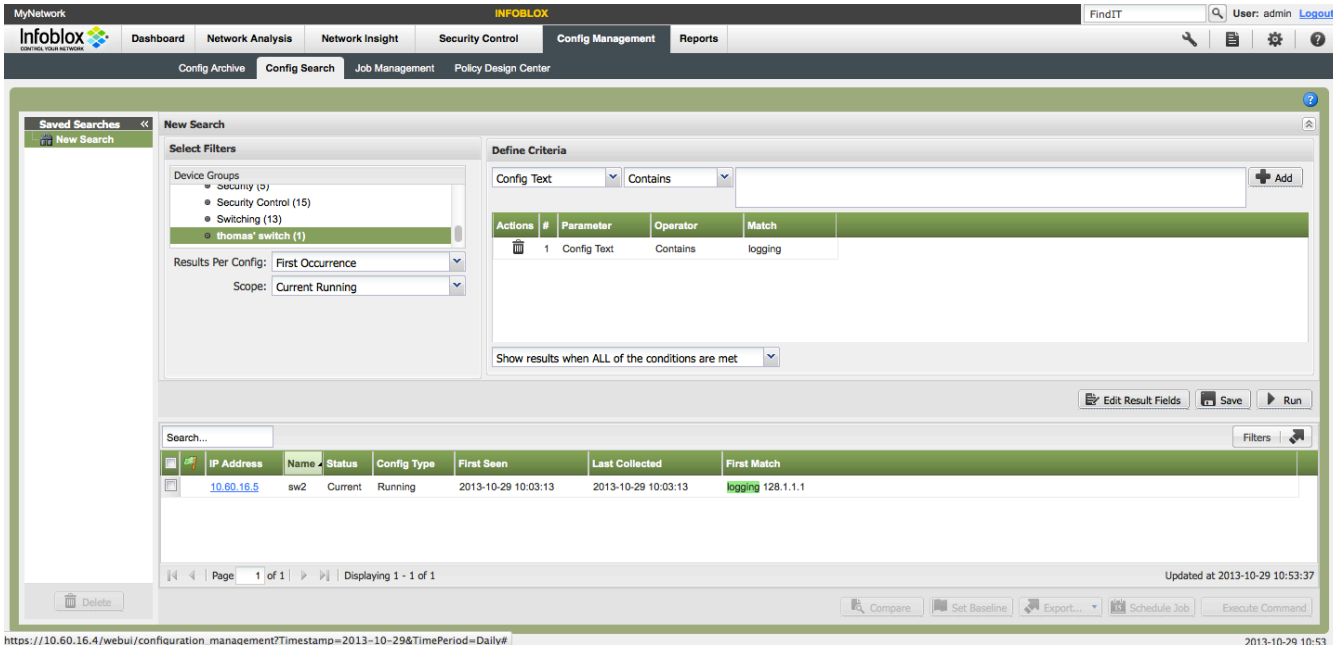
- **Discovery**



The diagram above describes how devices are discovered. Discovery is done on a periodic basis to ensure the discovery process updates the inventory without being consuming a large amount of bandwidth. You enter the subnets, SNMP community strings, and CLI credentials to start the process of device discovery. Network Automation also uses default SNMP community strings and CLI credentials if your SNMP community strings and

CLI credentials do not work. This will help in discovering devices that you did not know about. Refer to the Network Automation Administrator Guide for more information on the setup wizard.

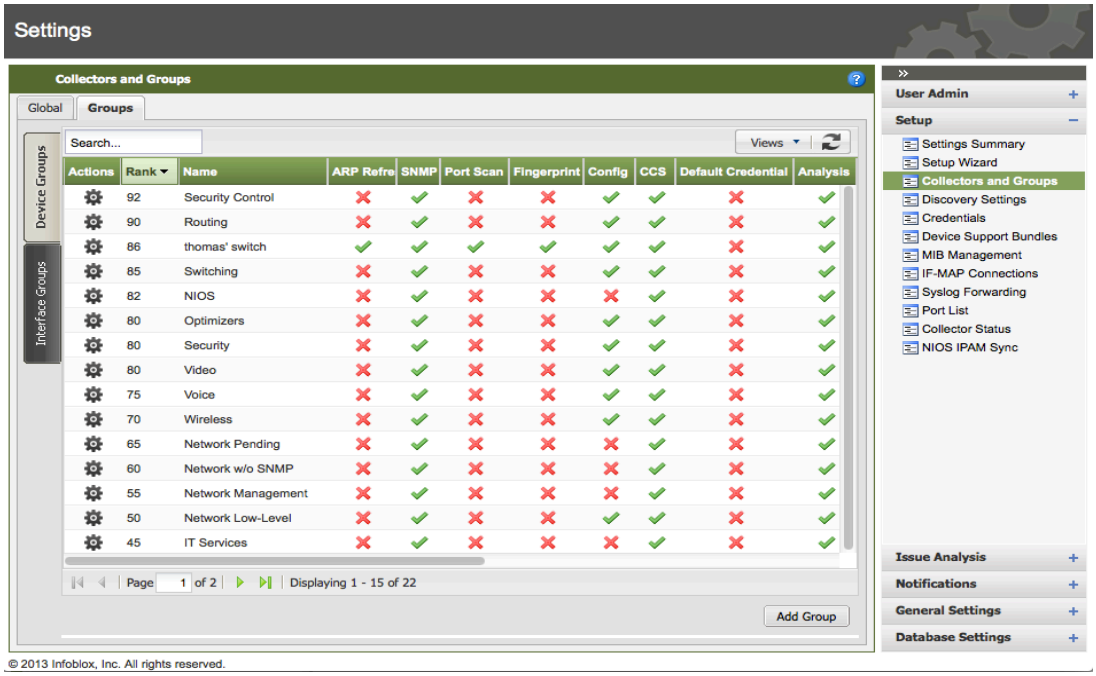
- **Configuration Search**



The Config Search tab lets you search device configuration files for a particular configuration string, an IP address or other specific device specification such as a MAC address, device model or other parameters, using many different types of search criteria and even regular expressions.

CIP-005-4a R1, R2- Network Automation covers this standard with the following features:

- **Device groups**

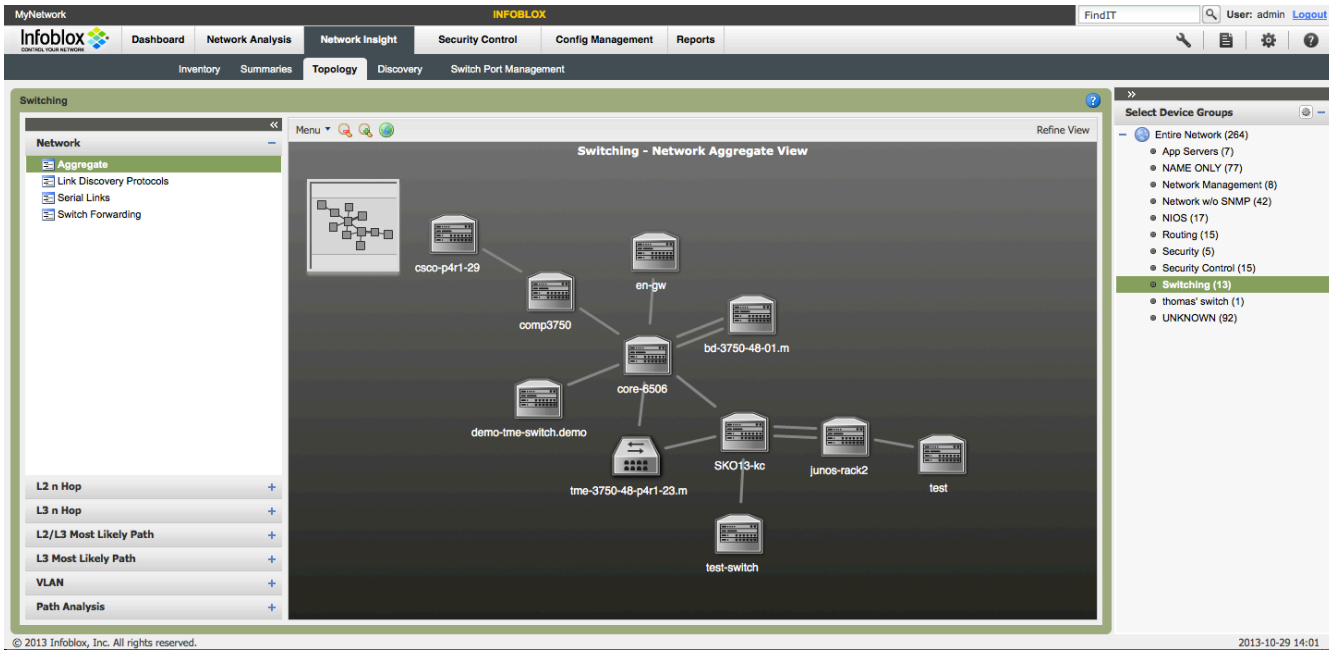


Device Groups are used to group devices that match a criteria like:

- IP address of the device (e.g., 192.168.1.33)
- name of the device (e.g., rtr1.netcordia.com)
- type of the device (e.g., Router, Switch, etc.)
- assurance level for the device type
- vendor of the device (e.g., Cisco)
- model of the device $Version software version of the device
- SNMP community of the device
- SNMP system name (CPD only)
- SNMP system description (CPD only)
- SNMP system location
- SNMP system name
- SNMP system description
- SNMP system contact

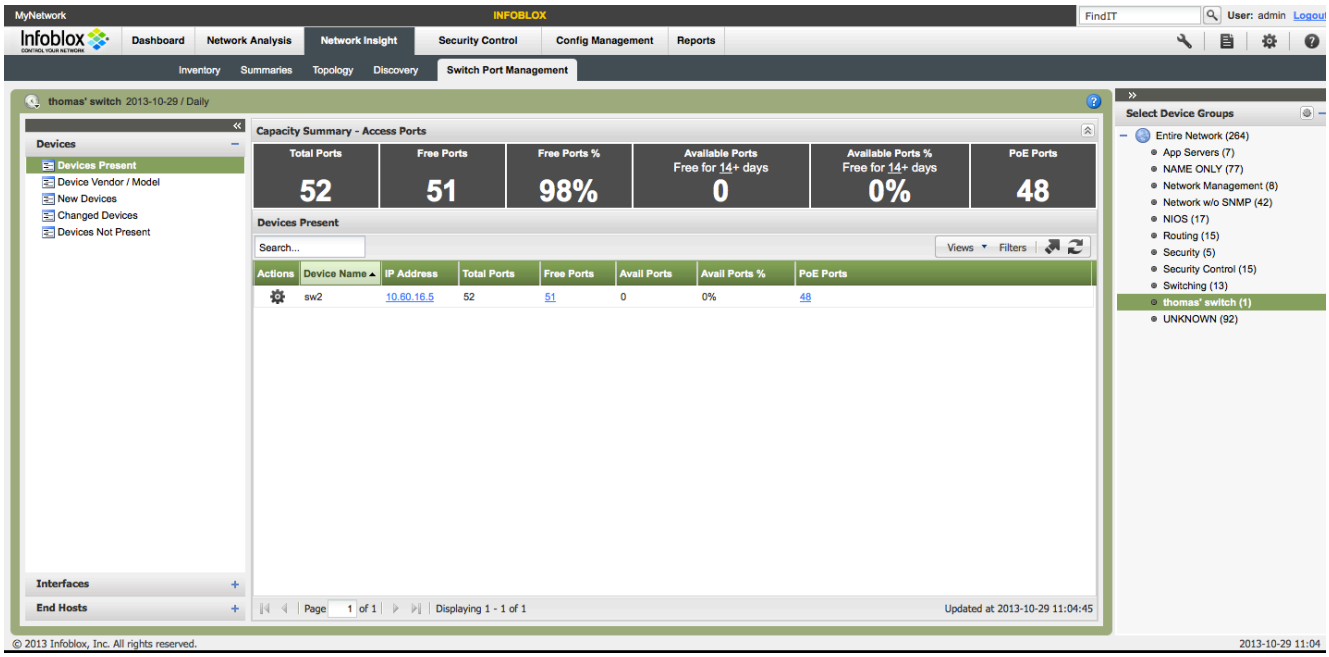
Beyond the default device groups, you can create additional device groups to group devices based upon your own criteria like location, subnet, department, etc.

- **Topology**



- Topology
  - Network
    - Aggregate View-combines the Link Discovery Protocols, Serial Links and Switch Forwarding views.
    - Link Discovery Protocol view-shows L2/L3 devices using Link Layer Discovery Protocol (LLDP) or Cisco Discovery Protocol (CDP), and their interconnections.
    - Serial Links view-shows L2/L3 devices connected by serial links.
    - Switch Forwarding view- shows L2/L3 devices using switch forwarding.
  - L2 n Hop- shows devices that can be reached from a selected starting device through a chosen number of Layer 2 (actually a hybrid of L1 and L2) connections.
  - L3 n Hop - shows all active devices that can be reached from a selected starting device in the network through a chosen number of routed Layer 3 connections.
  - L2/L3 Most Likely Path - shows the most likely path traffic would take between two devices, including both Layer 2 and Layer 3 connectivity.
  - L3 Most Likely Path - shows the most likely path that routable Layer 3 traffic would take between a source device and a destination device, ignoring Layer 2 connectivity between Layer 3 devices
  - VLAN - shows the spanning tree that a given VLAN uses on the network.
  - Path Analysis - allows tracing a Layer 3 path across a network of any scale, subject only to the restriction that Network Automation must discover and manage both the source and destination devices.

- **Switch Port Manager (SPM)**



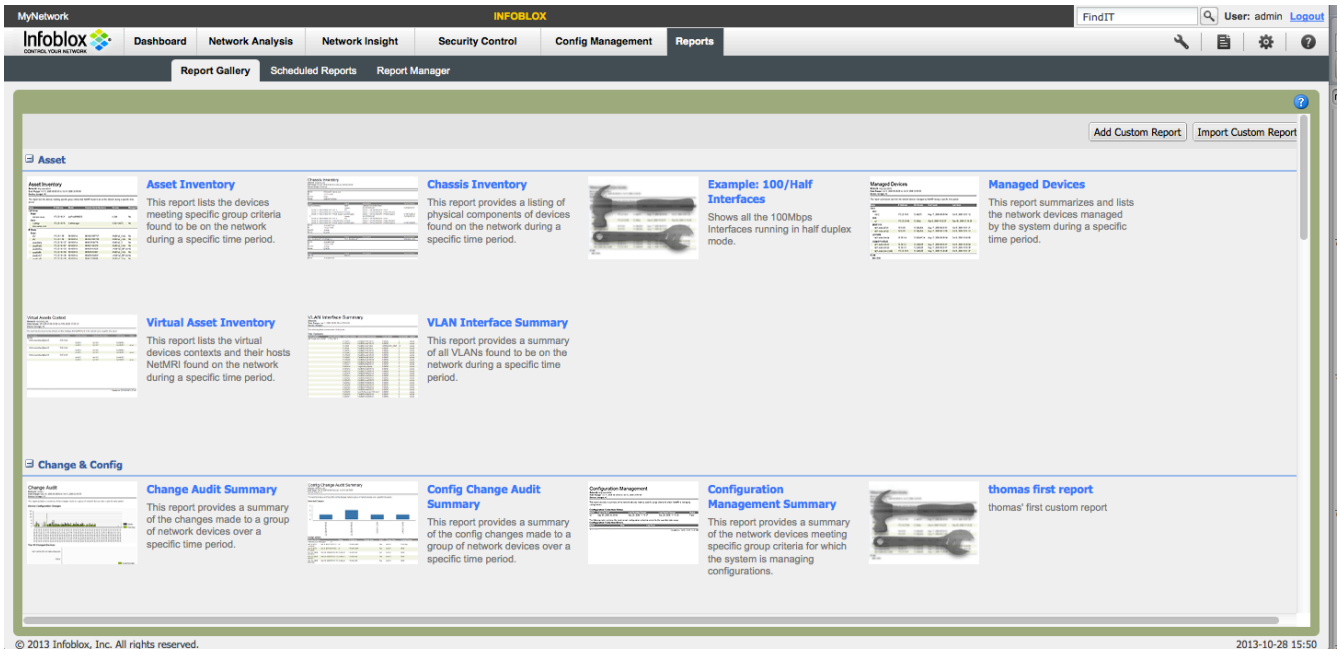
The Switch Port Management screen shows the following:

- Capacity Summary-Access Ports
  - Total Ports: The number of switched Ethernet ports, in the selected Device Group, that are being managed by Switch Port Manager (if Entire Network is chosen, this counter represents all managed switching ports).
  - Free Ports: The count of ports most recently polled that show a link state of Down, having lost connectivity.
  - Free Ports %: The percentage of all managed switch ports in the chosen Device Group showing Down link state.
  - Available Ports: The count of ports that remained in a link state of Down for more than the prescribed time period; when a port is considered Available, it is deemed available for other network resources.
  - Available Ports %: The percentage of all managed switch ports appearing as Available.
  - PoE Ports: The count of Cisco switched Ethernet ports running the Power over Ethernet switching protocol for IP telephony applications.
- Devices
  - Devices present-provides the complete list of switches and switch routers that are being managed by Network Automation.
  - Device Vendor/Model-displays a different subset of Switch Port Manager data, focusing on equipment vendor, product model, device serial number and other information.
  - New devices-lists the subset of switching network devices that have been discovered by Network Automation during the displayed measurement period.
  - Changed devices-lists any network devices that have changed in some fashion within the most recent polling time period.
  - Devices not present-lists the subset of active switch and switch-router devices, excluding end hosts, with which Switch Port Manager has lost communication over the last measurement time period.
- Interfaces
  - Access Ports Present-provides the list of switched access interfaces for the entire network, the aggregate interface list for any chosen device group and the list of interfaces for any chosen LAN switch or distribution switch.
  - Link Changes-provides a list of interfaces that have most recently changed state.

- Hub Locator- lists all switched interfaces in the network that operate as Smart Hubs, with more than one end host connected to the switch port.

- End Hosts
  - End Host present-provides a complete list of all end host devices detected and successfully probed by the Network Automation appliance.
  - New End Hosts- filters the list of Devices Present to show the devices and hosts that were found by Network Automation since the last polling took place.
  - End Host not Present-lists the end devices or hosts that are discovered to be disconnected or otherwise become unreachable on the network when the last polling took place.
  - VLAN changes-lists all devices that switched from one VLAN to a different VLAN during the user-configured time period.

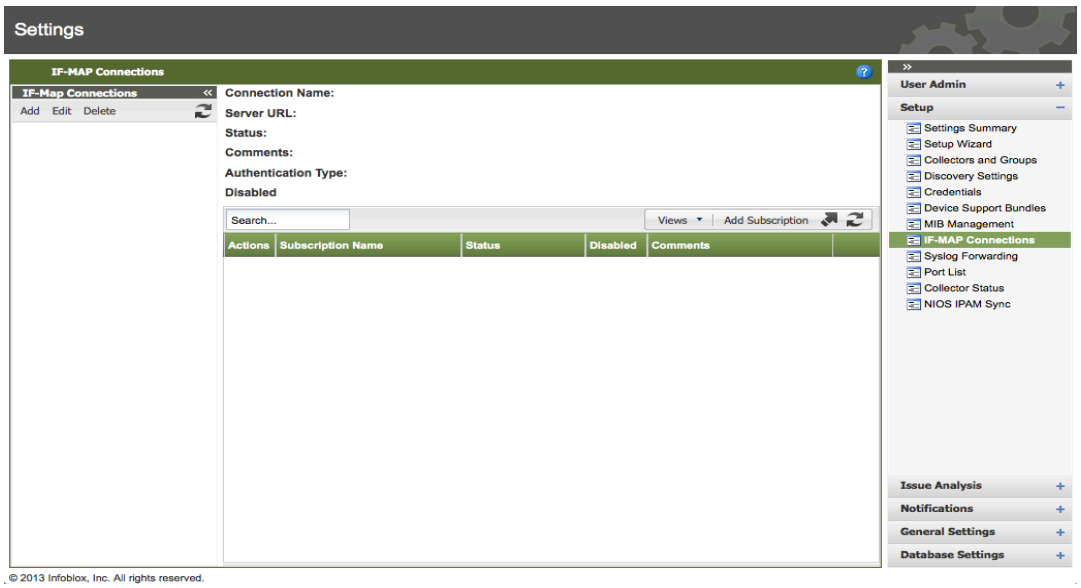
- **Reports**



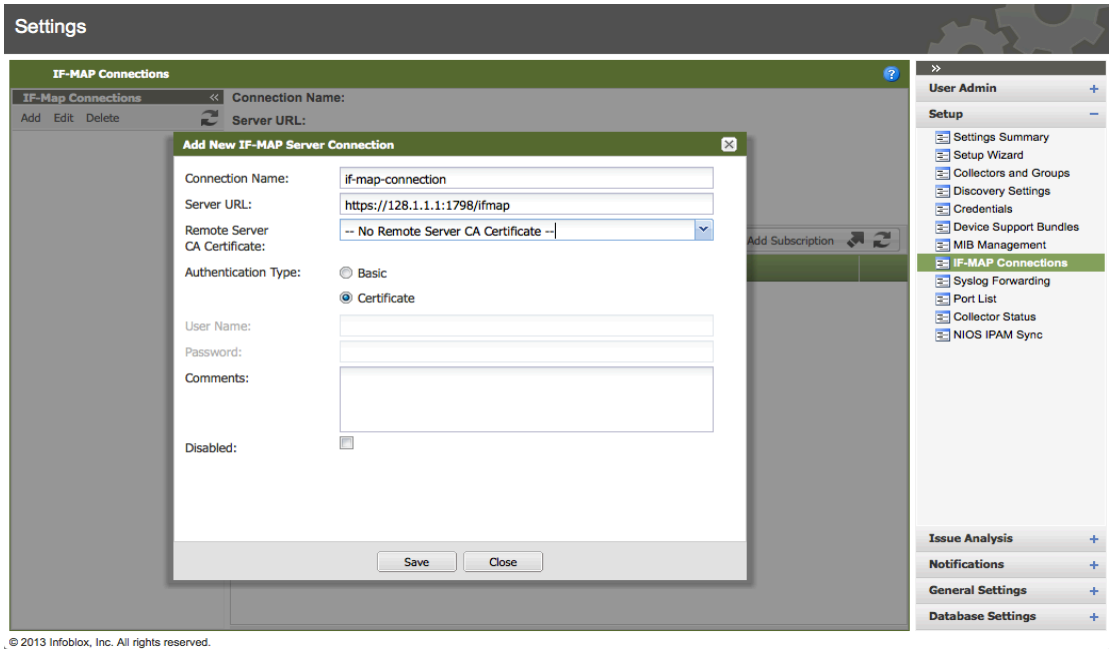
The report tab has 35 default reports to choose. In addition, you can create your own reports using one of 84 data types.

CIP-006-3c- Network Automation covers this standard with the following features:

- **IF-MAP integration**- IF-MAP (Interface to Metadata Access Points) is a client-server based protocol that allows network resources to share real-time network information.



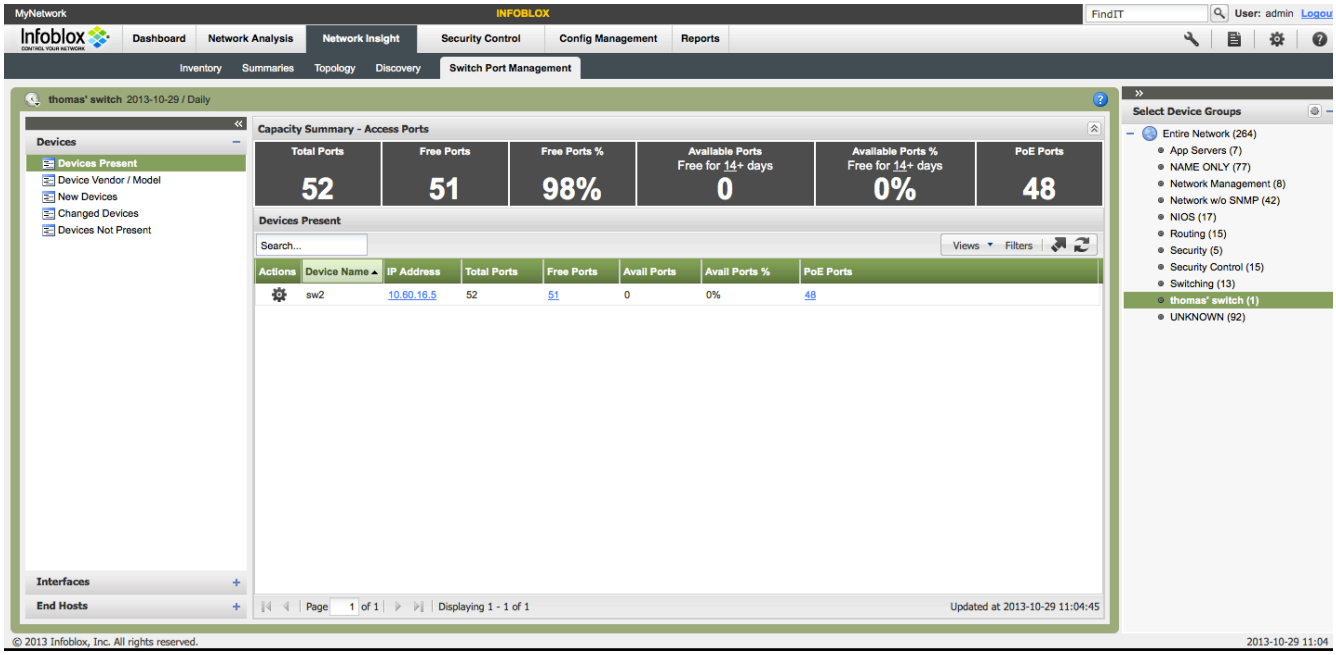
1. Click on the Settings wheel from the main screen and then click on IF-MAP Connections.
2. Click on the Add button to add an IF-MAP connection.



1. Enter a Connection Name.
2. Enter a Server URL.
3. Select the Authentication Type
4. Click on the Save button.

CIP-007-3 R2, R5- Network Automation covers this standard with the following features:

- **Switch Port Manager**



The Switch Port Management screen shows the following:

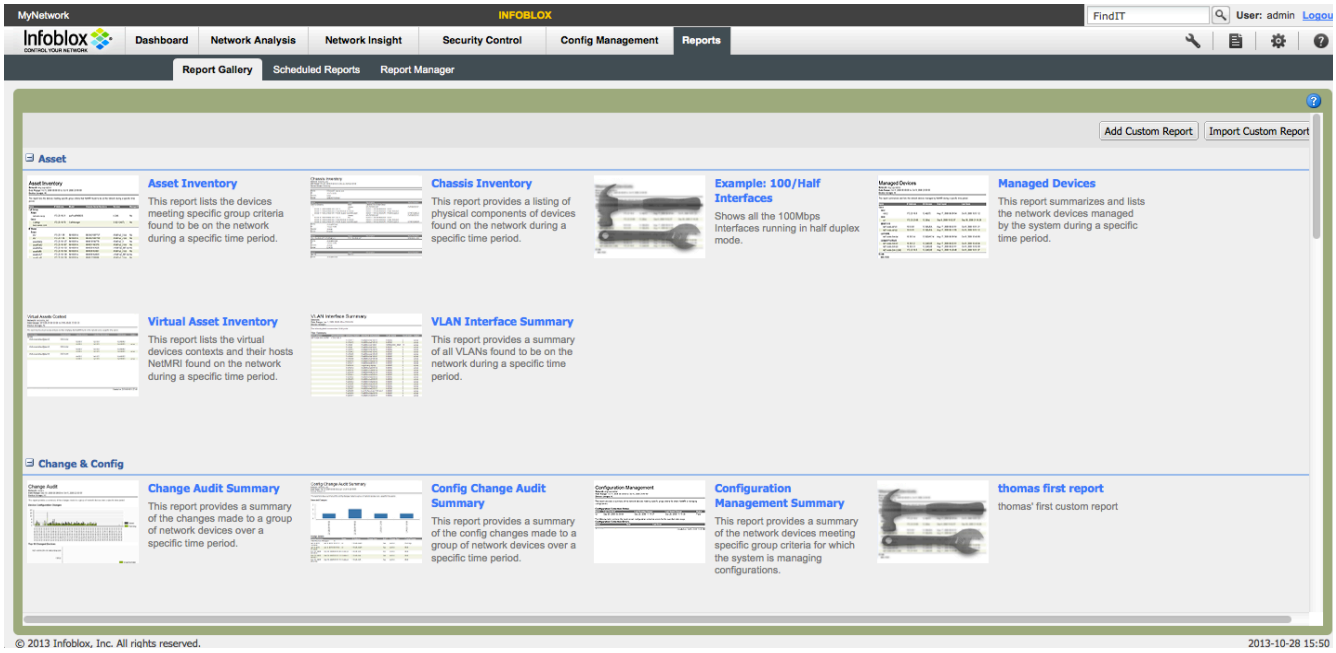
- Capacity Summary-Access Ports
  - Total Ports: The number of switched Ethernet ports, in the selected Device Group, that are being managed by Switch Port Manager (if Entire Network is chosen, this counter represents all managed switching ports).
  - Free Ports: The count of ports most recently polled that show a link state of Down, having lost connectivity.
  - Free Ports %: The percentage of all managed switch ports in the chosen Device Group showing Down link state.
  - Available Ports: The count of ports that remained in a link state of Down for more than the prescribed time period; when a port is considered Available, it is deemed available for other network resources.
  - Available Ports %: The percentage of all managed switch ports appearing as Available.
  - PoE Ports: The count of Cisco switched Ethernet ports running the Power over Ethernet switching protocol for IP telephony applications.
- Devices
  - Devices present-provides the complete list of switches and switch routers that are being managed by Network Automation.
  - Device Vendor/Model-displays a different subset of Switch Port Manager data, focusing on equipment vendor, product model, device serial number and other information.
  - New devices-lists the subset of switching network devices that have been discovered by Network Automation during the displayed measurement period.
  - Changed devices-lists any network devices that have changed in some fashion within the most recent polling time period.
  - Devices not present-lists the subset of active switch and switch-router devices, excluding end hosts, with which Switch Port Manager has lost communication over the last measurement time period.
- Interfaces

- Access Ports Present-provides the list of switched access interfaces for the entire network, the aggregate interface list for any chosen device group and the list of interfaces for any chosen LAN switch or distribution switch.
- Link Changes-provides a list of interfaces that have most recently changed state.
- Hub Locator- lists all switched interfaces in the network that operate as Smart Hubs, with more than one end host connected to the switch port.

- End Hosts
  - End Host present-provides a complete list of all end host devices detected and successfully probed by the Network Automation appliance.
  - New End Hosts- filters the list of Devices Present to show the devices and hosts that were found by Network Automation since the last polling took place.
  - End Host not Present-lists the end devices or hosts that are discovered to be disconnected or otherwise become unreachable on the network when the last polling took place.
  - VLAN changes-lists all devices that switched from one VLAN to a different VLAN during the user-configured time period.

CIP-008-3- Network Automation covers this standard with the following features:

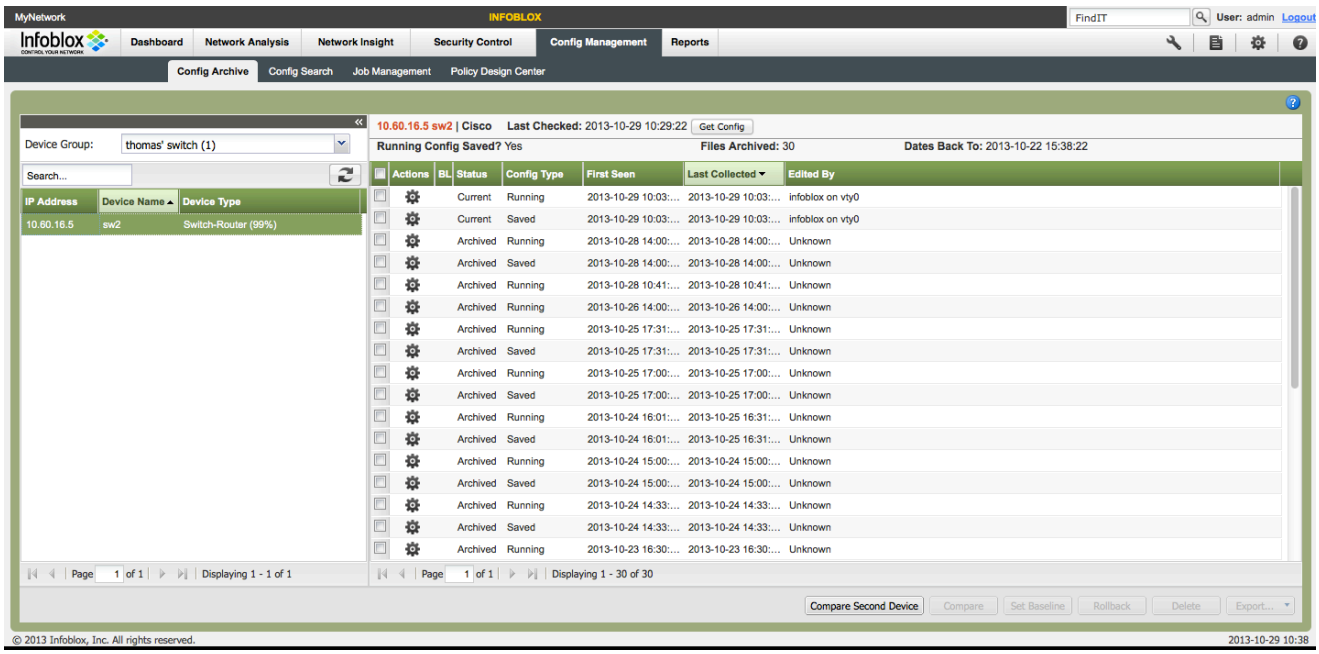
- **Reports**



The report tab has 35 default reports to choose. In addition, you can create your own reports using one of 84 data types.

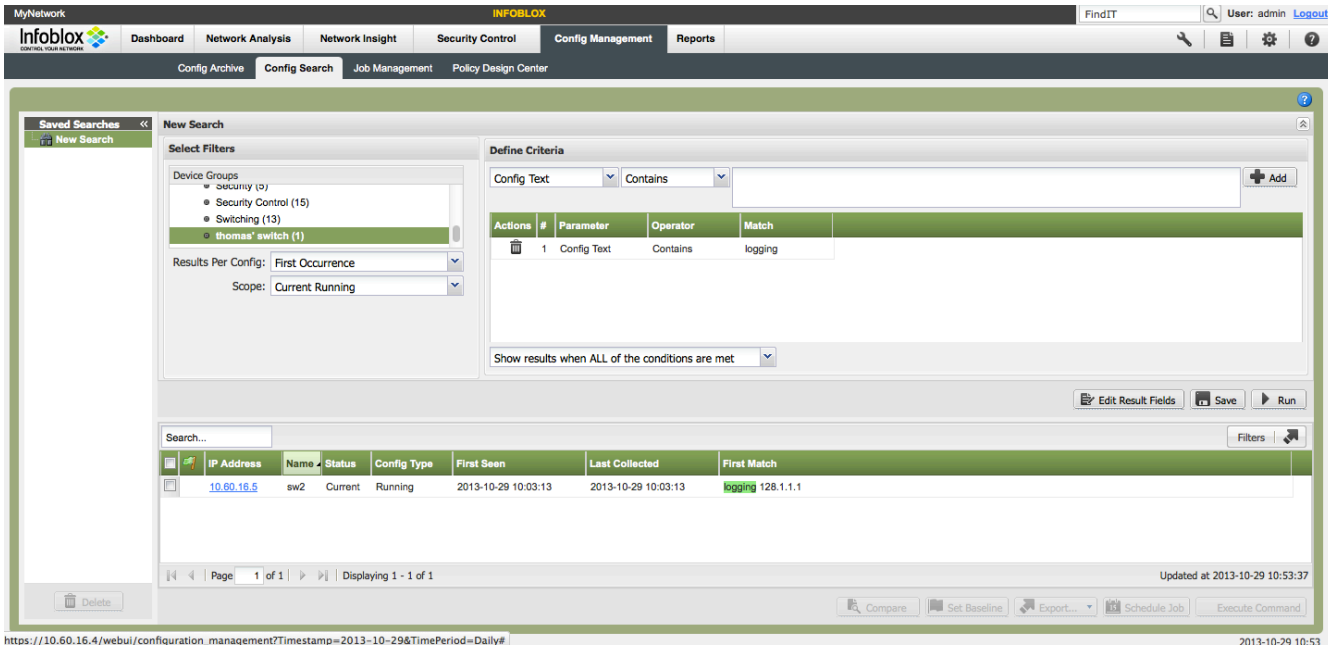
CIP-009-3- Network Automation covers this standard with the following features:

- **Configuration management**

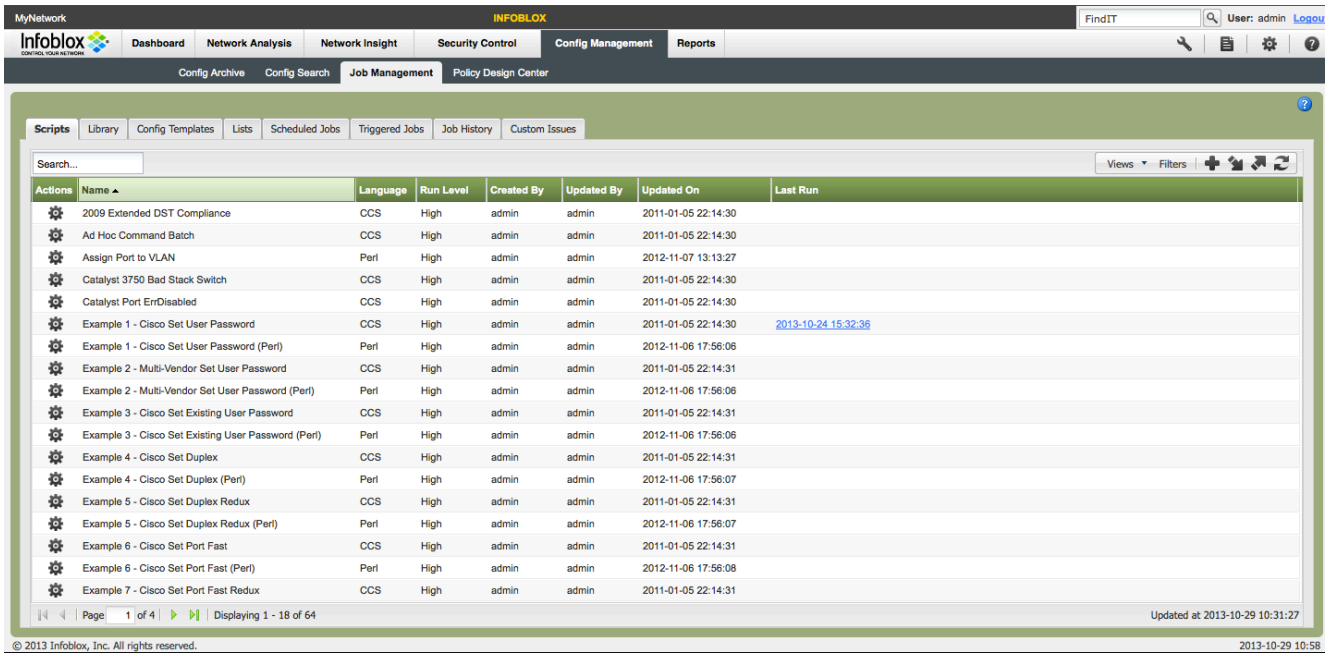


The Config Management Tab contains the following sub tabs:

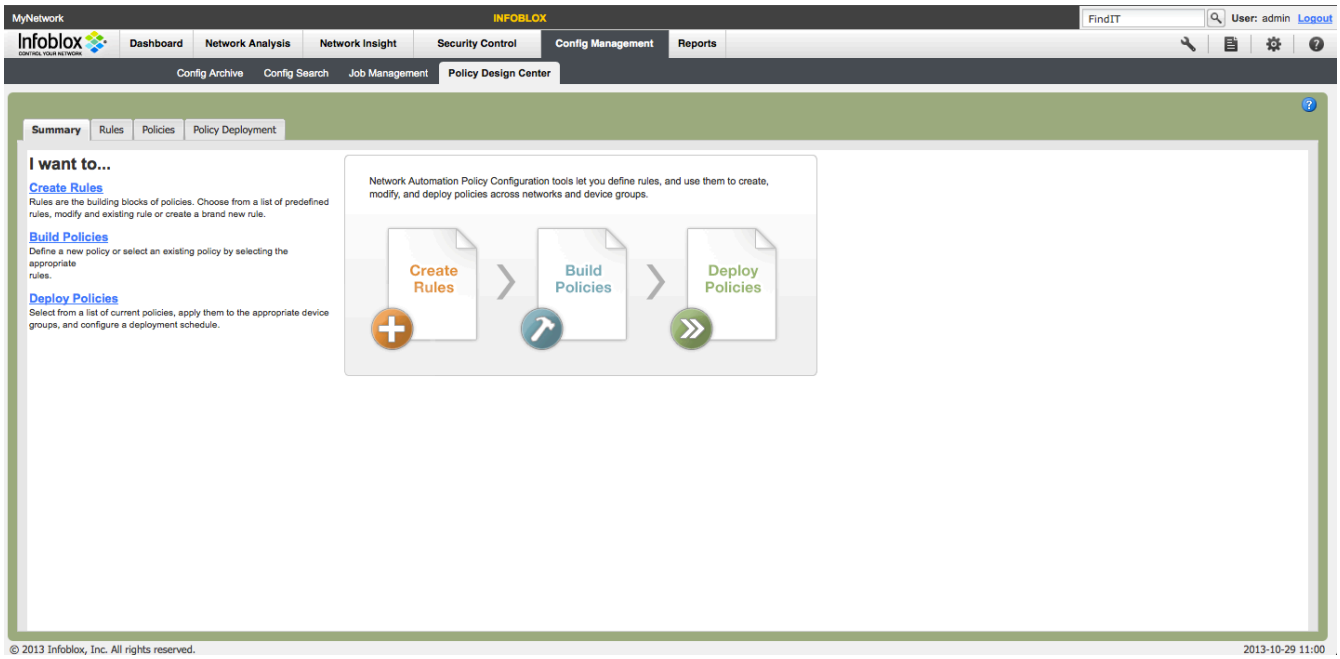
- Config Archive-The Config Archive is the screen that lists all of the configuration file changes that have occurred for a selected device. Two configuration files can be compared for any differences. A baseline configuration can be chosen. You can also use a configuration to rollback a device to a known working state. One or more configuration files can be exported to your local workstation.



- Config Search-The Config Search tab lets you search devices in the network for a particular configuration string, an IP address or other specific device specification such as a MAC address, device model or other parameters, using many different types of search criteria and even regular expressions.

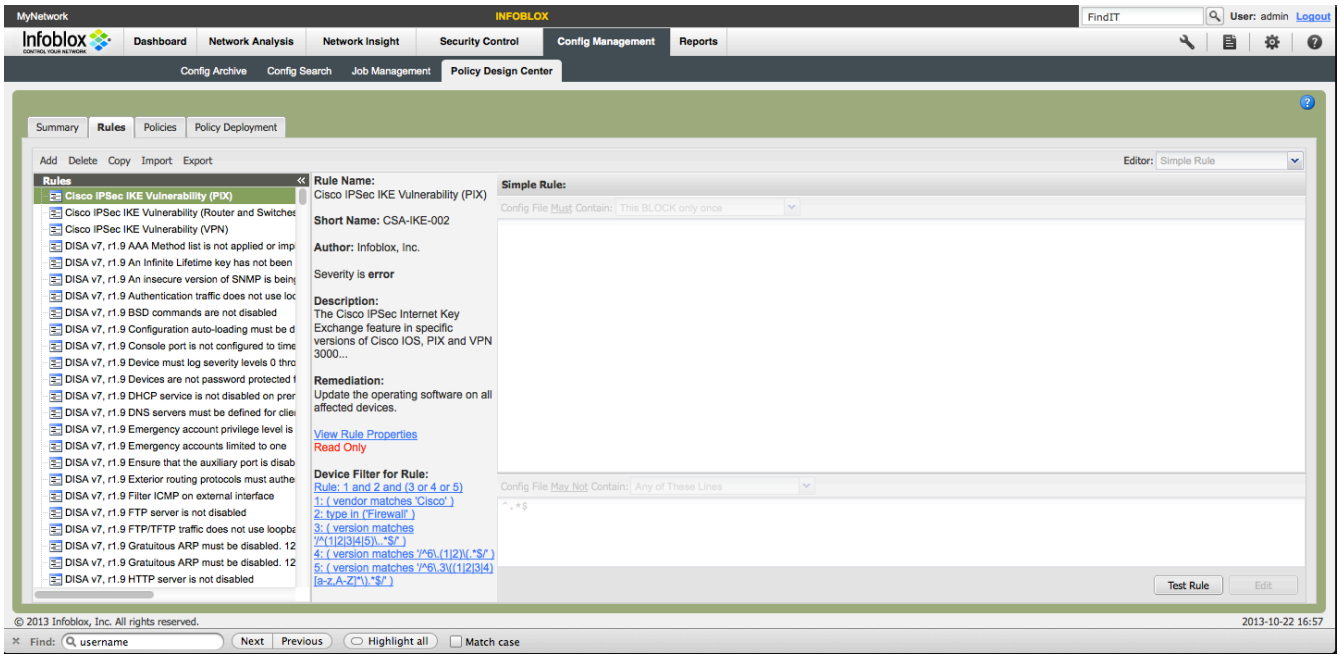


- Job Management-The Job Management tab enables creation, scheduling, approval and execution of Job Management scripts in the Perl and CCS languages, and the definition of custom issues to extend the library of issue types that Network Automation uses for reporting and monitoring of adverse events in the network.

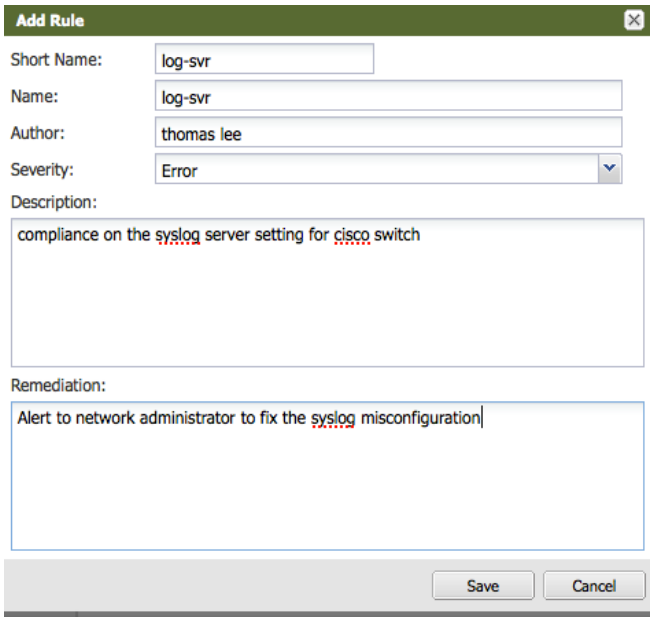


- Policy Design Center-The Policy Design Center, to create rules and policies, and deploy policies on the network. Policies are a tool for ensuring all devices in the network meet a minimum standard of readiness and security.

- Compliance. Rules and policies can be created to ensure the configuration files adhere to NERC standards. The following is an example of create a rule to ensure the SYSLOG server setting stays within compliance.



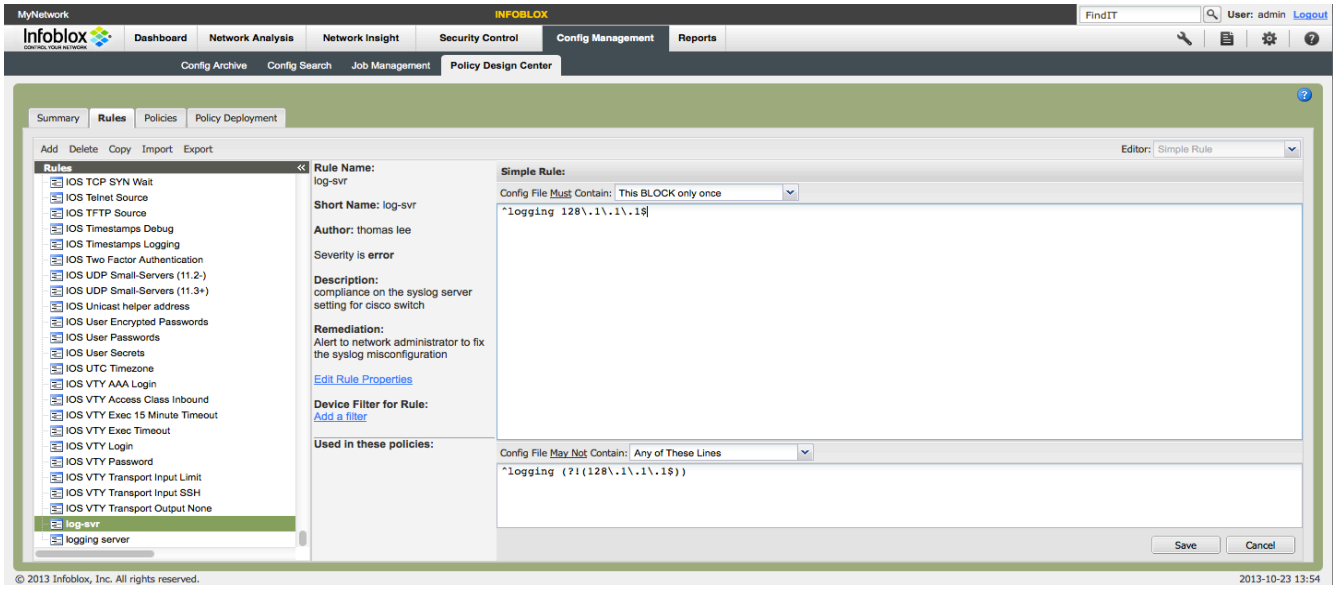
1. Go to Config Management -> Policy Design Center -> Rules.
2. Click on the Add button to add a rule.



3. Enter a Short Name. The name is limited to 12 characters.
4. Enter author name.
5. Enter the severity. The choices are: Error, Info, or Warning

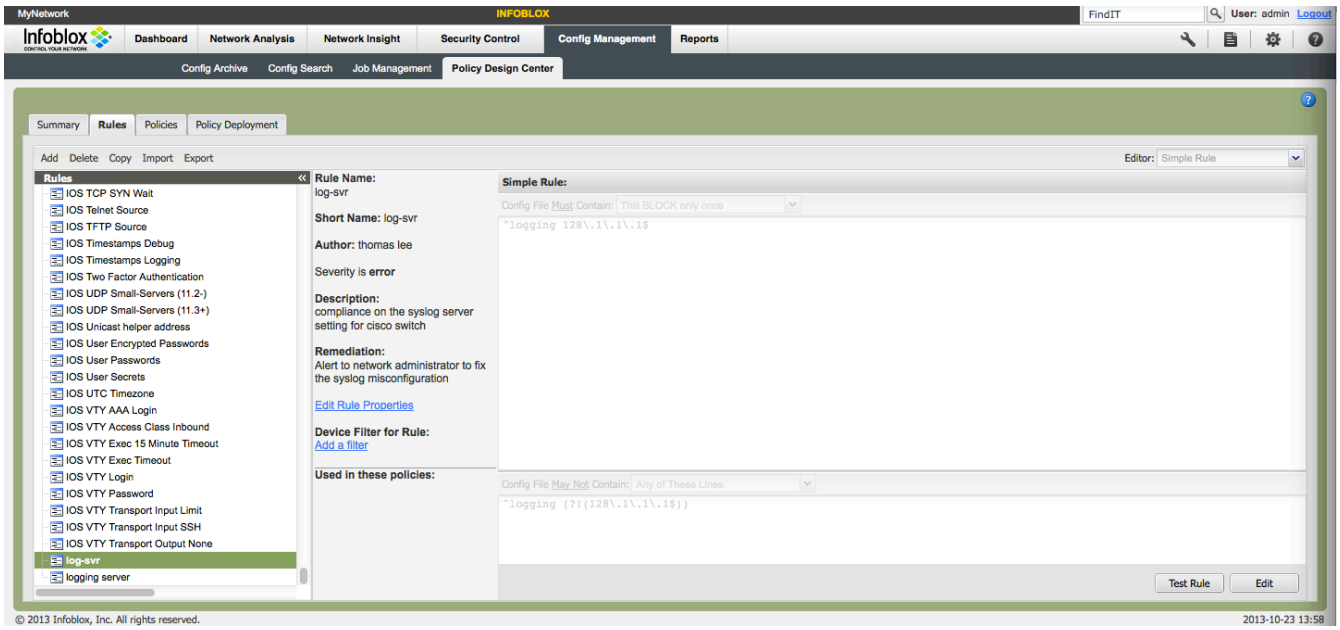
A configuration Policy consists of one or more rules. Rules use different forms of regular expression pattern matching against configuration files—and tests of other data Network Automation has collected—to verify that the configuration of the device meets the rule(s). Each rule has a **severity** level, and may optionally define a device filter to limit the types of devices to which it applies. Rules may be freely re-used between policies.

6. Enter a description of the rule.
7. Enter a remediation description. This description describes what needs to be done when this rule reports an error.
8. Click Save to save the rule.

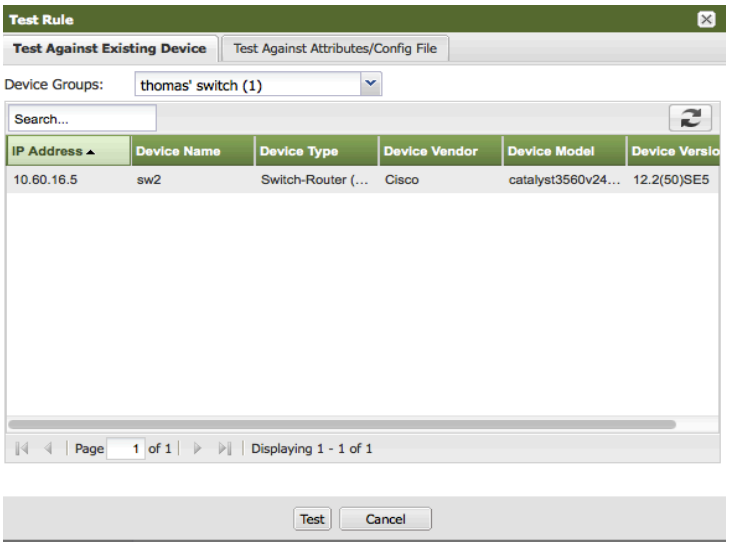


9. With the newly created rule highlighted on the left, select an editor on the upper right side. The choices are: simple editor, CPD, Rule Logic Builder, Raw XML. Refer to the Network Automation Administrator Guide for more information. For this example, simple editor is selected.
10. Enter the configuration line or block in the 'Config file must contain' section. In this case, it is ^logging 128\.1\.1\.1$. In the configuration file of the device, the command is 'logging 128.1.1.1'. Network Automation uses Ruby-style regular expressions. The reason for using the '^', '$', and the '\' characters is to ensure rules engine searches for this exact statement. The '^' character denotes the beginning of a line. The '$' denotes the end of a line. The '\' character denotes treating the subsequent character as a literal character instead of a regular expression.

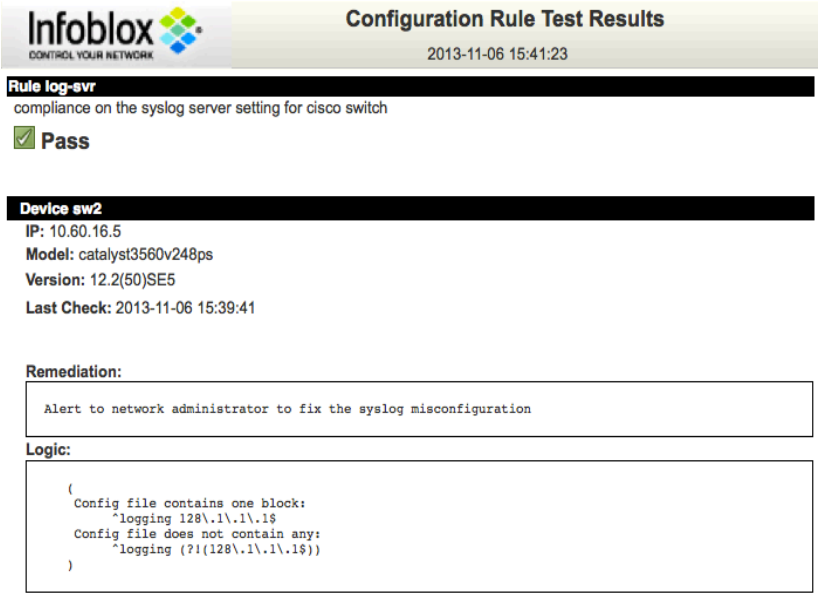
    In the 'Config file may not contain' section, input ^logging (?!(128\.1\.1\.1$)) . The '?!' means do not match 128.1.1.1. However, this section states must not contain the following statement. The overall effect is that if the logging statement IP address differs from 128.1.1.1, an error will be flagged. Refer to the following link on Ruby regex characters: http://www.ruby-doc.org/core-2.0.0/Regexp.html to get more information on regex characters.
11. Click Save.



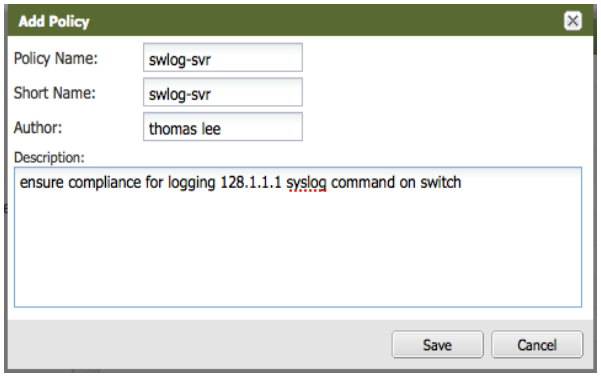
1. Click on the Test Rule button to test the rule.



2. Click ‘Test Against Existing Device’ tab.
3. Select and highlight the device from the device groups.
4. Click on the Test button.

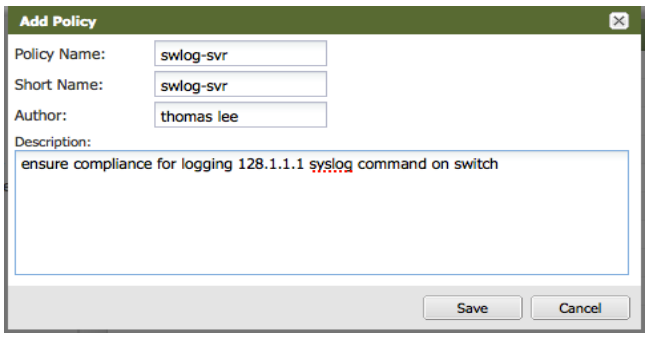


5. It should come back as Pass if the configuration setting is correct.



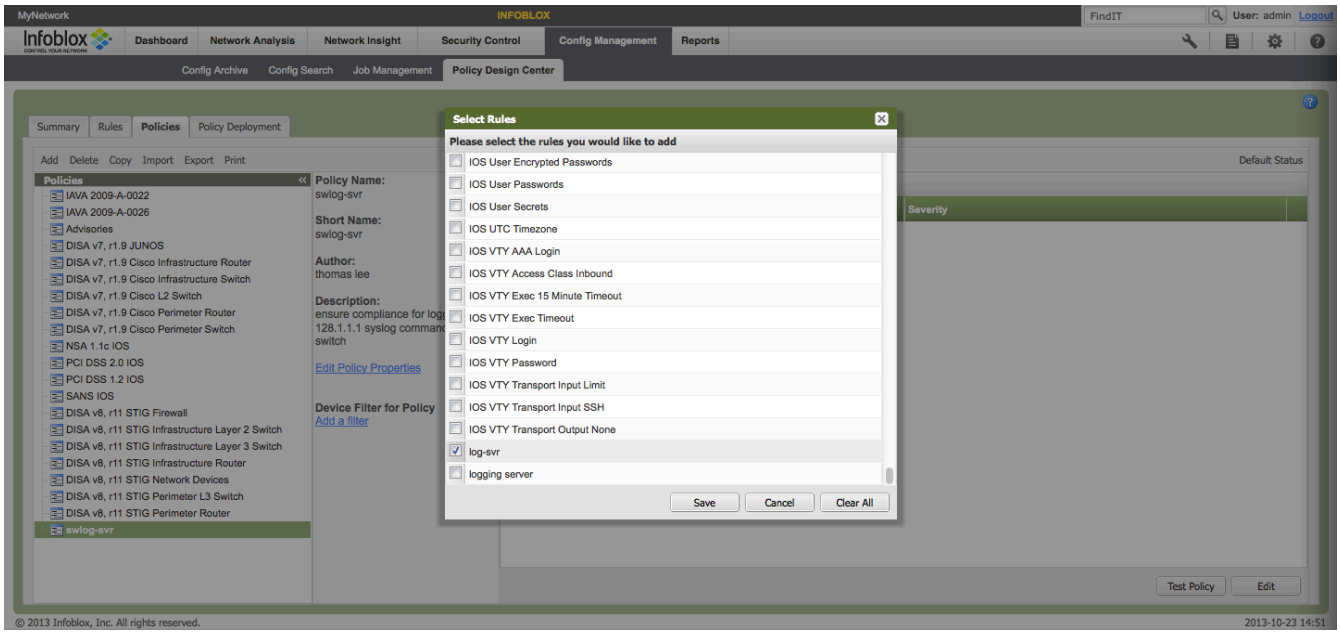
Now that you have created your rule and tested it successfully, you can automate the process of checking compliance when a configuration change is detected. Click on the Polices Tab from the previous screen.

1. Click on the Polices Tab from the previous screen.
2. Click on the Add button to a policy.

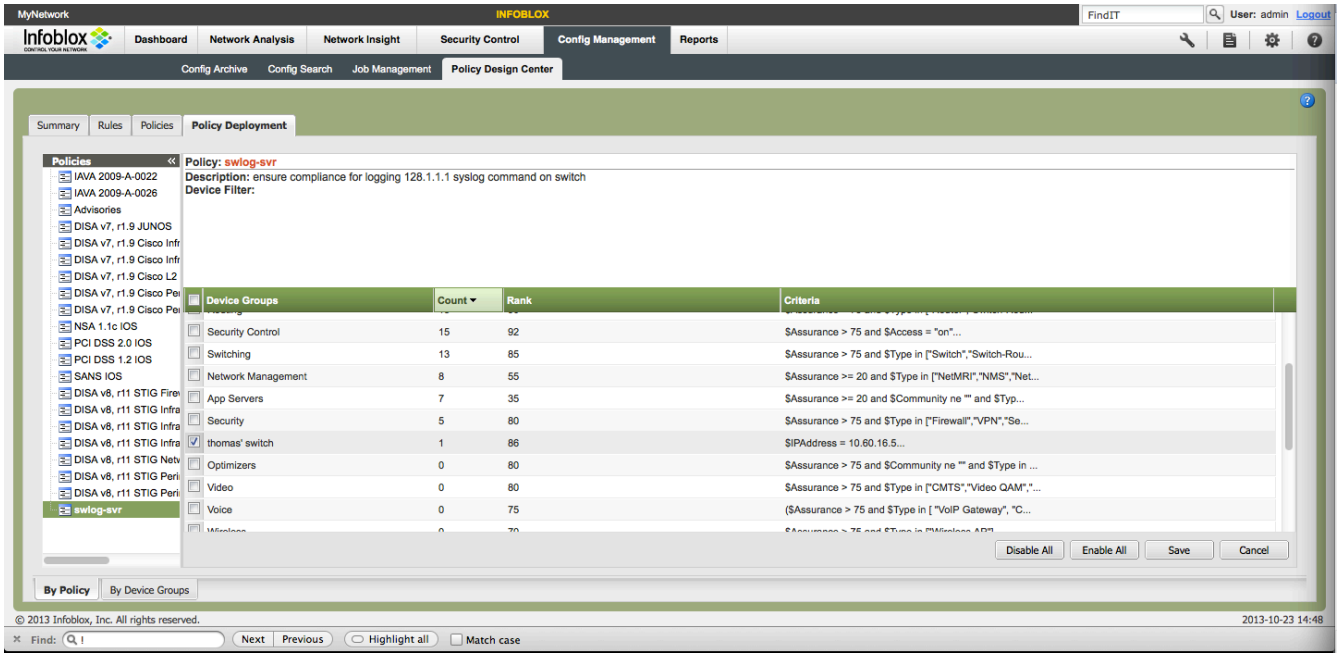


3. Enter Policy Name, Short Name, Author, and Description.

4. Click on the Save button.



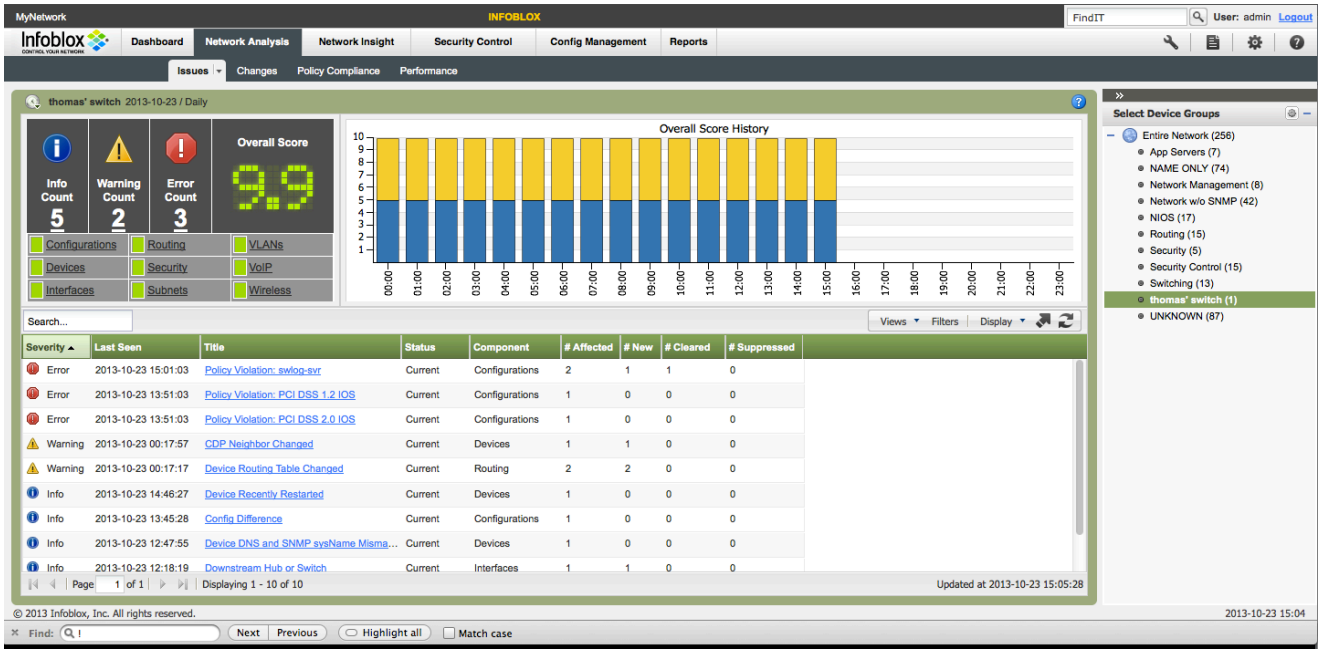
5. Highlight the policy was you just created and saved.
6. Click on the Edit button to add the rule that was created previously. In this example, it's the swlog-svr policy.
7. Click on the rule or rules to be placed into this policy. In this case, we click on the rule called log-svr.
8. Click the Save button.



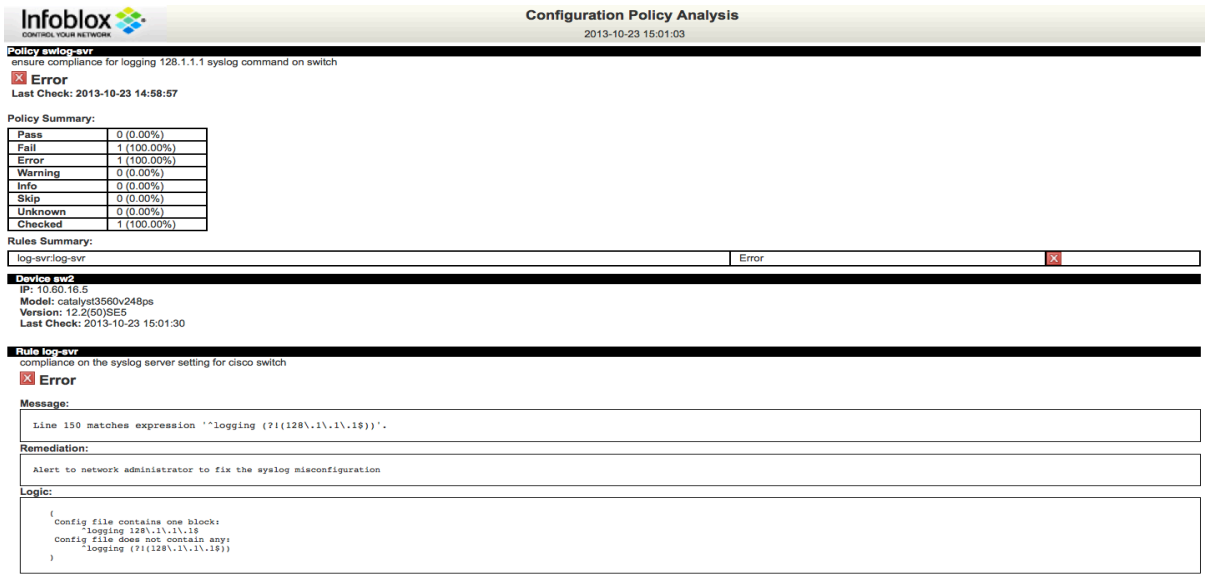
The last step is to deploy the policy. This means you are assigning the policy to the device or device group.

1. Click on the Policy Deployment Tab. Select the device group that you want the policy to enforce.
2. Click on the Save button.

3. Now the policy will examine the latest configuration file for this device or device group to ensure the logging statement is correct.



To test the policy, connect to the device and modify the configuration by adding another logging statement or modify the existing logging statement. Within 15 minutes, you should see an entry appear on the Network Analysis -> Issues screen like the first entry in the list above.



You can then drill down and see the details of the error.