



HIPAA Compliance Use Case

Use Case | November, 2013

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

Settings

Audit Log

Audit Log

Search...

Views Filters

Timestamp	User Name	Event Type	Message
2013-10-24 13:40:12	admin	User Login/Logout	admin successfully logged in to Network Automation.
2013-10-24 13:38:15	admin	User Login/Logout	admin successfully logged in to Network Automation.
2013-10-24 13:36:32	admin	User Login/Logout	admin successfully logged in to Network Automation.
2013-10-24 09:49:51	admin	User Login/Logout	admin successfully logged in to Network Automation.
2013-10-23 16:33:10	admin	User Login/Logout	admin successfully logged in to Network Automation.
2013-10-23 16:33:06	admin	User Login/Logout	admin has logged out
2013-10-23 10:13:12	admin	User Login/Logout	admin successfully logged in to Network Automation.
2013-10-22 16:42:01	admin	User Login/Logout	admin successfully logged in to Network Automation.
2013-10-22 16:41:57	admin	User Login/Logout	admin has logged out
2013-10-22 15:08:38	admin	User Login/Logout	admin has been logged out of the Network Automation admin shell because of inactivity
2013-10-22 14:08:26	admin	User Login/Logout	admin successfully logged in to Network Automation admin shell
2013-10-22 14:02:51	admin	User Login/Logout	admin successfully logged in to Network Automation.
2013-10-22 14:02:48	admin	User Login/Logout	admin has logged out
2013-10-22 11:56:47	admin	User Login/Logout	admin successfully logged in to Network Automation.
2013-10-22 11:56:44	admin	User Login/Logout	admin has logged out
2013-10-22 10:40:07	admin	User Login/Logout	admin successfully logged in to Network Automation.
2013-10-22 10:40:03	admin	User Login/Logout	admin has logged out

Page 1 of 8 | Displaying 1 - 18 of 129

Updated at 2013-10-24 15:15:01

© 2013 Infoblox, Inc. All rights reserved.

User Admin

- Users
- Roles
- Audit Log**

Setup +

Issue Analysis +

Notifications +

General Settings +

Database Settings +

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.

MyNetwork

Infoblox

Dashboard Network Analysis Network Insight Security Control Config Management Reports

Config Archive Config Search Job Management Policy Design Center

Scripts Library Config Templates Lists Scheduled Jobs Triggered Jobs Job History Custom Issues

Search...

Views Filters

Actions	Name	Language	Run Level	Created By	Updated By	Updated On	Last Run
⚙	2009 Extended DST Compliance	CCS	High	admin	admin	2011-01-05 22:14:30	
⚙	Ad Hoc Command Batch	CCS	High	admin	admin	2011-01-05 22:14:30	
⚙	Assign Port to VLAN	Perl	High	admin	admin	2012-11-07 13:13:27	
⚙	Catalyst 3750 Bad Stack Switch	CCS	High	admin	admin	2011-01-05 22:14:30	
⚙	Catalyst Port ErrDisabled	CCS	High	admin	admin	2011-01-05 22:14:30	
⚙	Example 1 - Cisco Set User Password	CCS	High	admin	admin	2011-01-05 22:14:30	
⚙	Example 1 - Cisco Set User Password (Perl)	Perl	High	admin	admin	2012-11-06 17:56:06	
⚙	Example 2 - Multi-Vendor Set User Password	CCS	High	admin	admin	2011-01-05 22:14:31	
⚙	Example 2 - Multi-Vendor Set User Password (Perl)	Perl	High	admin	admin	2012-11-06 17:56:06	
⚙	Example 3 - Cisco Set Existing User Password	CCS	High	admin	admin	2011-01-05 22:14:31	
⚙	Example 3 - Cisco Set Existing User Password (Perl)	Perl	High	admin	admin	2012-11-06 17:56:06	
⚙	Example 4 - Cisco Set Duplex	CCS	High	admin	admin	2011-01-05 22:14:31	
⚙	Example 4 - Cisco Set Duplex (Perl)	Perl	High	admin	admin	2012-11-06 17:56:07	
⚙	Example 5 - Cisco Set Duplex Redux	CCS	High	admin	admin	2011-01-05 22:14:31	
⚙	Example 5 - Cisco Set Duplex Redux (Perl)	Perl	High	admin	admin	2012-11-06 17:56:07	
⚙	Example 6 - Cisco Set Port Fast	CCS	High	admin	admin	2011-01-05 22:14:31	
⚙	Example 6 - Cisco Set Port Fast (Perl)	Perl	High	admin	admin	2012-11-06 17:56:08	

Page 1 of 4 | Displaying 1 - 17 of 64

Updated at 2013-10-24 15:28:23

© 2013 Infoblox, Inc. All rights reserved.

2013-10-24 15:33

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.

Actions	Name	Language	Run Level	Created By	Updated By	Updated On	Last Run
	2009 Extended DST Compliance	CCS	High	admin	admin	2011-01-05 22:14:30	
	Ad Hoc Command Batch	CCS	High	admin	admin	2011-01-05 22:14:30	
	Assign Port to VLAN	Perl	High	admin	admin	2012-11-07 13:13:27	
	Catalyst 3750 Bad Stack Switch	CCS	High	admin	admin	2011-01-05 22:14:30	
	Catalyst Port ErrDisabled	CCS	High	admin	admin	2011-01-05 22:14:30	
	Example 1 - Cisco Set User Password	CCS	High	admin	admin	2011-01-05 22:14:30	2013-10-24 15:32:38
	Example 1 - Cisco Set User Password (Perl)	Perl	High	admin	admin	2012-11-06 17:56:06	
	Example 2 - Multi-Vendor Set User Password	CCS	High	admin	admin	2011-01-05 22:14:31	
	Example 2 - Multi-Vendor Set User Password (Perl)	Perl	High	admin	admin	2012-11-06 17:56:06	
	Example 3 - Cisco Set Existing User Password	CCS	High	admin	admin	2011-01-05 22:14:31	
	Example 3 - Cisco Set Existing User Password (Perl)	Perl	High	admin	admin	2012-11-06 17:56:06	
	Example 4 - Cisco Set Duplex	CCS	High	admin	admin	2011-01-05 22:14:31	
	Example 4 - Cisco Set Duplex (Perl)	Perl	High	admin	admin	2012-11-06 17:56:07	
	Example 5 - Cisco Set Duplex Redux	CCS	High	admin	admin	2011-01-05 22:14:31	
	Example 5 - Cisco Set Duplex Redux (Perl)	Perl	High	admin	admin	2012-11-06 17:56:07	
	Example 6 - Cisco Set Port Fast	CCS	High	admin	admin	2011-01-05 22:14:31	
	Example 6 - Cisco Set Port Fast (Perl)	Perl	High	admin	admin	2012-11-06 17:56:08	
	Example 7 - Cisco Set Port Fast Redux	CCS	High	admin	admin	2011-01-05 22:14:31	

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:

Script Run Now

Fill out Job Details

Scripts | **Templates**

Search...

Script Name

- 2009 Extended DST Compliance
- Ad Hoc Command Batch
- Assign Port to VLAN
- Catalyst 3750 Bad Stack Switch
- Catalyst Port ErrDisabled
- Example 1 - Cisco Set User Password
- Example 1 - Cisco Set User Password (Perl)
- Example 2 - Multi-Vendor Set User Password
- Example 2 - Multi-Vendor Set User Password (...)
- Example 3 - Cisco Set Existing User Password

Example 1 - Cisco Set User Password

This script sets the password for a given username on all Cisco devices. The user will be prompted for a valid username and password when the script is executed. If an account does not exist, the script will create it.

Username:

Password:

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



HIPAA Compliance Use Case

Use Case|November, 2013

Script Run Now

Fill out Custom Information

Custom Fields
You do not have any Custom Fields defined to enter data.

Cancel < Previous Next >

3. Click on the Next button.

Script Run Now

Select Device Groups or Devices

Device Groups | **Devices**

Device Groups

- Entire Network (316)
 - App Servers (6)
 - NAME ONLY (76)
 - Network Management (8)
 - Network w/o SNMP (43)
 - NIOS (19)
 - Routing (16)
 - Security (5)
 - Security Control (15)
 - Switching (13)
 - thomas' switch (1)
 - UNKNOWN (142)

Selected Device Groups

thomas' switch (1)

Clear

Cancel < Previous Next >

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.



HIPAA Compliance Use Case

Use Case|November, 2013

Script Run Now

Review and run

Script:

Example 1 - Cisco Set User Password

Inputs:

Username: thomasl

Password: *****

Credentials:

User account CLI credentials are not required

Device Groups:

thomas' switch (1)

Devices:

None selected

Run Now

Cancel

< Previous

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

Run Now

?

Run this job right now?

Yes

No

7. Click on the Yes button.

MyNetwork

INFOBLOX

FindIT

User: admin Logout

Infoblox

Dashboard

Network Analysis

Network Insight

Security Control

Config Management

Reports

Config Archive

Config Search

Job Management

Policy Design Center

2013-11-15 / Daily

Scripts

Library

Config Templates

Lists

Scheduled Jobs

Triggered Jobs

Job History

Custom Issues

Search...

Views Filters

Status	Job ID	Name	Script	Initiated By	Approved By	Start Time	End Time	Summary Count
OK	2	Ad Hoc Job 11/15 16:45	Example 1 - Cisco Set User Password	admin	admin	2013-11-15 16:45:54	2013-11-1...	Total: 1, Pending: 0, OK: 1, Error: 0, Other: 0

Page 1 of 1

Displaying 1 - 1 of 1

Updated at 2013-11-15 16:45

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



HIPAA Compliance Use Case

Use Case|November, 2013

Job Viewer

Job ID: 2 **Start Time:** 2013-11-15 16:45:54
Script: Example 1 - Cisco Set User Password **End Time:** 2013-11-15 16:46:19
Job Count: 1 **Status:** ✔ OK

[Details](#) [Issues](#) [Files](#)

Job Details

2013/11/15

Ad Hoc Job 11/15 16:45 - Example 1 - Cisco Set User Password

Views ▾ Filters ▾ ↺

Status	Start Time	End Time	IP Address	Device Name	Actions
✔ OK	2013-11-15 16:46:03	2013-11-15 16:46:19	10.60.16.5	sw2	

⏪ ⏩ Page 1 of 1 ⏪ ⏩ Displaying 1 - 1 of 1

[Cancel All](#) [Rerun Errors](#) [Reschedule Errors](#)

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

Job Details Viewer

Connections: sw2 (10.60.16.5) [Primary] ▾

Job Detail ID: 2
Job ID: 2 **Start Time:** 2013-11-15 16:46:03
Script: Example 1 - Cisco Set User Password **End Time:** 2013-11-15 16:46:19
Device: sw2 (10.60.16.5) **Status:** ✔ OK

[Script](#) [Status Log](#) [Process Log](#) [Custom Log](#) [Session Log](#) [Files](#)

Script: Example 1 - Cisco Set User Password

```

16:46:04 Script-Variables
16:46:04 ⓘ $username = 'thomasl'
16:46:04 ⓘ $password = '*****'
16:46:04 Script-Filter
16:46:04 ✔ Filter matches
16:46:04 $Vendor eq "Cisco" and $sysDescr like /IOS/
        
```

1. Action: 'Set IOS User Password'

```

16:46:06 Action-Commands
16:46:07 ✔ config terminal
16:46:07 ✔ username thomasl password 0 infoblox
16:46:08 ✔ exit
16:46:08 ✔ write memory
        
```

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;

The screenshot displays the 'Settings' page in the Infoblox management interface. The page is divided into several sections:

- Settings Summary:** A green header bar with a question mark icon.
- Network Automation Configuration:**
 - Network Automation Version : 6.7.2.15
 - API Version : 2.8
 - Model : IB1102A
 - Serial Number : 1200201012000015
 - Device Limit : 200
 - Security Automation Limit : 25
 - NIOS Host : None registered
- Network Configuration:**
 - Network Name : MyNetwork
 - Server Name : NetMRI-1200201012000015
 - Domain Name 1 : tme.infoblox.com
 - Domain Name 2 :
 - Name Priority : DNS
 - Time Zone : US/Pacific
- MGMT Interface Configuration:**
 - IP Address : 10.60.16.4
 - Subnet Mask : 255.255.255.0
 - Default Gateway : 10.60.16.1
 - MAC Address : 00:25:90:14:EF:2A
 - Speed : 1000Mb/s
- Collector Settings:**
 - SNMP Data Collector : Enabled
 - Route Collection Priority : SNMP
 - ARP Collection Priority : SNMP
 - Port Control Preference : CLI
 - Telnet Config Collector : Enabled
 - SSH Config Collector : Enabled
 - HTTP Config Collector : Disabled
 - Discovery Engine : Enabled
 - Vendor Default Credential Collector : Disabled
 - Port Scanning : Disabled
 - Smart Subnet Ping Sweep : Disabled
 - Automatic ARP Refresh Before Switch-Port Polling : Enabled
 - Fingerprinting : Disabled
 - NetBIOS Collector : Disabled
 - Switch Port Management : Enabled
- Module Settings:**
 - NetMRI without SPM : Enabled
 - Switch Port Management : Enabled
 - Automation Engine : Enabled
 - Switch Port Manager : Enabled
 - Automation Change Manager : Enabled
 - NetMRI : Enabled
- Right Sidebar:** A list of settings categories with expand/collapse icons:
 - User Admin
 - Setup
 - Issue Analysis
 - Notifications
 - General Settings
 - Database Settings (expanded):
 - Database Statistics
 - Archive Database
 - Restore Database
 - Scheduled Archive
 - Remote Config Archive
 - Maintenance
 - Send Support Bundle
 - Data Retention
 - Storage Management

© 2013 Infoblox, Inc. All rights reserved.

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;



HIPAA Compliance Use Case

Use Case|November, 2013

Script Run Now

Fill out Job Details

Scripts

Templates

Search...

Script Name
2009 Extended DST Compliance
Ad Hoc Command Batch
Assign Port to VLAN
Catalyst 3750 Bad Stack Switch
Catalyst Port ErrDisabled
Example 1 - Cisco Set User Password
Example 1 - Cisco Set User Password (Perl)
Example 2 - Multi-Vendor Set User Password
Example 2 - Multi-Vendor Set User Password (...)
Example 3 - Cisco Set Existing User Password

Ad Hoc Command Batch

This script executes an arbitrary batch of commands on all selected devices. The user will be prompted to enter the batch of commands when the script is executed.

Commands To Be Executed:

Reset to Defaults

Cancel

< Previous

Next >

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.

The screenshot shows the Infoblox MyNetwork interface. The top navigation bar includes tabs for Dashboard, Network Analysis, Network Insight, Security Control, Config Management, and Reports. The 'Config Management' tab is active, showing sub-tabs for Config Archive, Config Search, Job Management, and Policy Design Center. The 'Job Management' sub-tab is selected, displaying a table of scripts. The table has columns for Actions, Name, Language, Run Level, Created By, Updated By, Updated On, and Last Run. The 'Ad Hoc Command Batch' script is highlighted. Below the table, there are pagination controls showing 'Page 1 of 4' and 'Displaying 1 - 18 of 64'. The footer indicates '© 2013 Infoblox, Inc. All rights reserved.' and 'Updated at 2013-11-25 12:48:41'.

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

The screenshot shows the 'Script Run Now' dialog box. The 'Ad Hoc Command Batch' script is selected. The dialog has a 'Scripts' tab and a 'Templates' tab. The 'Scripts' tab is active, showing a list of scripts. The 'Ad Hoc Command Batch' script is selected. The dialog shows a description of the script: 'This script executes an arbitrary batch of commands on all selected devices. The user will be prompted to enter the batch of commands when the script is executed.' Below the description, there is a text area for 'Commands To Be Executed:'. The commands entered are 'config t', 'line vty 0 15', and 'session-timeout 15'. There is a 'Reset to Defaults' button. At the bottom, there are 'Cancel', '< Previous', and 'Next >' buttons.

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



HIPAA Compliance Use Case

Use Case|November, 2013

Script Run Now

Fill out Custom Information

Custom Fields

You do not have any Custom Fields defined to enter data.

Cancel < Previous Next >

3. Click on the Next button.

Script Run Now

Select Device Groups or Devices

Device Groups | **Devices**

Device Groups

- Entire Network (301)
 - App Servers (6)
 - NAME ONLY (76)
 - Network Management (8)
 - Network w/o SNMP (50)
 - NIOS (18)**
 - Routing (18)
 - Security (5)
 - Security Control (17)
 - Switching (15)
 - thomas' switch (1)
 - UNKNOWN (118)

Selected Device Groups

thomas' switch (1)

Clear

Cancel < Previous Next >

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

Script Run Now

Review and run

Script: Ad Hoc Command Batch

Inputs: Commands To Be Executed: config t line vty 0 15 session-timeout 15

Credentials: User account CLI credentials are not required

Device Groups: thomas' switch (1)

Devices: None selected

Run Now Cancel < Previous

- 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.

MyNetwork

Infoblox

Dashboard Network Analysis Network Insight Security Control Config Management Reports

Config Archive Config Search Job Management Policy Design Center

2013-12-04 / Daily

Scripts Library Config Templates Lists Scheduled Jobs Triggered Jobs **Job History** Custom Issues

Search...

Status	Job ID	Name	Script	Initiated By	Approved By	Start Time	End Time	Summary Count
Running	4	Ad Hoc Job 12/04 10:44	Ad Hoc Command Batch	admin	admin	2013-12-04 10:44:46		Total: 1, Pending: 1, OK: 0, Error: 0, Other: 0

Page: 1 of 1 | Displaying 1 - 1 of 1

Updated at 2013-12-04 10:44:49

© 2013 Infoblox, Inc. All rights reserved.

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



HIPAA Compliance Use Case

Use Case|November, 2013

Job Viewer

Job ID: 4

Start Time: 2013-12-04 10:44:46

Script: Ad Hoc Command Batch

End Time: 2013-12-04 10:45:01

Job Count: 1

Status: ✓ OK

Details

Issues

Files

Job Details

2013/12/04

Refresh
Off

Ad Hoc Job 12/04 10:44 - Ad Hoc Command Batch

Views Filters

Status	Start Time	End Time	IP Address	Device Name	Actions
✓ OK	2013-12-04 10:44:49	2013-12-04 10:45:01	10.60.16.5	sw2	

Page 1 of 1

Displaying 1 - 1 of 1

Cancel All

Rerun Errors

Reschedule Errors

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



HIPAA Compliance Use Case

Use Case|November, 2013

Job Details Viewer
Connections: sw2 (10.60.16.5) [Primary]

Job Detail ID: 4
Job ID: 4
Script: Ad Hoc Command Batch
Device: sw2 (10.60.16.5)

Start Time: 2013-12-04 10:44:49
End Time: 2013-12-04 10:45:01
Status: OK

Script
Status Log
Process Log
Custom Log
Session Log
Files

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

The screenshot shows the Infoblox MyNetwork interface with the 'Reports' tab selected. The interface includes a navigation bar with 'Dashboard', 'Network Analysis', 'Network Insight', 'Security Control', 'Config Management', and 'Reports'. Below the navigation bar, there are tabs for 'Report Gallery', 'Scheduled Reports', and 'Report Manager'. The main content area displays a grid of reports under two sections: 'Compliance' and 'Health'.

Compliance Section:

- Default Credentials Report:** This report lists network devices found to be accessible using vendor default credentials during a specific time period.
- ISO 27002:** This report documents compliance with certain network aspects of the ISO 27002:2005 standard, commonly used as best practices guidelines for Sarbanes-Oxley, HIPAA and GLBA compliance.
- PCI:** This report documents compliance with certain network aspects of the Payment Card Industry Data Security Standard Versions 1.2 and 2.0.
- Policy Compliance Summary:** This report provides an overview of the policy compliance status for all policies and the network devices against which they are deployed.
- Policy Compliance Details:** This report provides a detailed list of all policies and policy rules, along with the devices passing and failing, and the specific reasons for policy violations.

Health Section:

- Example: Issues for today:** A report of only today's issues.
- Issue Details:** This report provides a listing of the issues reported by a group of network devices over a specific time period.
- Network Health:** This report provides a summary of key health metrics for a group of network devices over a specific time period.
- Network History:** This report provides a summary of key attributes for the entire network over a specific time period.

© 2013 Infoblox, Inc. All rights reserved. 2013-11-06 11:14

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.