

User Guide

indeni 5.5



Table of Contents

[Chapter 1: Overview](#)

[Requirements](#)

[Hardware Requirements](#)

[Software Requirements](#)

[Analyzed Device Requirements](#)

[Chapter 2: Installation](#)

[Installations on Virtual and Physical Servers](#)

[Configuring and installing indeni](#)

[Logging in to the System - Console](#)

[Logging in to the System - Web Interface](#)

[Compliant vs. Non-Compliant Mode](#)

[Chapter 3: Overview](#)

[Operate and Help Menus](#)

[Operations Management](#)

[Compliance Management](#)

[Tools](#)

[Reporting](#)

[Settings](#)

[Chapter 4: Getting Started](#)

[Managing Users](#)

[Adding a User](#)

[Adding Devices to the System](#)

[Check Point](#)

[SecurePlatform](#)

[IPSO](#)

[GAiA](#)

[61000 Security System](#)

[Provider-1/MDM on SPLAT, IPSO, GAiA](#)

[Crossbeam \(Blue Coat\) running Check Point](#)

[Cisco](#)

[ASAs, Routers, Switches](#)

[F5 BIG-IPs](#)

[Fortinet Fortigates](#)

[Juniper](#)

[ScreenOS](#)

[Junos](#)

[Palo Alto](#)

[Adding a Device in the UI](#)

[Adding Known Devices](#)

[Upload List of Devices](#)

[Choosing Credentials](#)

[SSH \(Advanced Monitoring\):](#)

[SNMP \(Standard Analysis\)](#)

[Vendor Specific](#)

[Editing Devices](#)

[Live Configuration](#)

[Chapter 5: Operations Management](#)

[The Alerts Sub-Tab](#)

[Monitored Devices](#)

[Current Alerts](#)

[Searching Alerts](#)

[Filtering Alerts](#)

[Columns and Functionality](#)

[Expanding an Alert](#)

[Resolving Alerts](#)

[Using the Resolve Button](#)

[Resolving Multiple Alerts](#)

[Annotating Alerts](#)

[Temporarily Disabling Analysis](#)

[The Analysis Tab](#)

[The Network Health Tab](#)

[Using Signatures in Alerts](#)

[Managing the Signatures](#)

[Configure](#)

[Alert Archive](#)

[Chapter 6: Compliance Management](#)

[Configuration Checks](#)

[Adding a Profile](#)

[Using Item Types](#)

[Hotfix\(es\) Installed](#)

[NTP Servers In Use](#)

[Users Defined](#)

[Syslog Servers In Use](#)

[RADIUS Servers In Use](#)

[Ensure a Minimal Number of Connections or Sessions are Open](#)

[DNS Servers In Use](#)

[Core dumping Enabled/Disabled](#)

[Deleting an Item from the Profile](#)

[Deleting a Profile](#)

[Backup Schedules](#)

[Scheduling Backups](#)

[Adding Additional Backup Schedules](#)

[Configuration Journal \(change tracking\)](#)

[Configuration Check Reports](#)

[Chapter 7: Tools](#)

[Search](#)

[Live Configuration](#)

[Troubleshooting](#)

[Chapter 8: Reporting](#)

[Device Configuration Report](#)

[Alert Summary Report](#)

[Procurement Report](#)

[Inventory Report](#)

[Chapter 9: Settings Tab](#)

[Monitored Devices](#)

[Connectivity](#)

[Paths](#)

[Troubleshooting parameters](#)

[Scheduled Maintenance Window](#)

[Groups](#)

[Scheduled Maintenance Windows](#)

[Integration](#)

[Adding an SNMP Master](#)

[Configuring indeni as an SNMP Device in the SNMP Master](#)

[Adding an SMTP Server](#)

[Adding a Syslog Server](#)

[Users](#)

[Licenses](#)

[indeni Backup](#)

[indeni Insight](#)

[Audit Log](#)

[Chapter 10: Upgrades and Support](#)

[Upgrades](#)

[Support](#)

[Appendix A: Terminology](#)

[Appendix B: System Security and Safeguards](#)

[Appendix C: Basic Troubleshooting](#)

[Accessing the Web UI](#)

[Adding Devices to indeni](#)

[Appendix D: Setting Up indeni on VMware ESX](#)

[Creating a New Virtual Machine](#)

CHAPTER 1: OVERVIEW

indeni offers the first proactive root cause analysis solution for network devices, designed to cut setup and administration time, lower costs, and ensure a stable, secure network. It is the first truly proactive system that:

- Automatically identifies known devices.
- Correctly identifies proper settings for known devices, cutting deployment time to five minutes or less.
- Understands and analyzes thousands of parameters and compares settings in relation to each other.
- Measures traffic throughput and flags approaching maximums.
- Determines whether devices are partly or wholly functional or dead and, if non-functioning, identifies the cause and suggests remedial actions.
- Flags the administrator when an error is seen, via alerts which can be forwarded by SNMP, email or pager.
- Allows priority analysis of chosen critical parameters so that potentially severe problems can be flagged and dealt with first.

This user guide provides detailed instructions for installing and using indeni. Additional support is available at www.indeni.com/support.

Requirements

This guide is for technical users with a strong working knowledge of networking and network security administration. Users should be able to set up network devices on their own (Cisco routers, Check Point firewalls, etc., as the case may be) (see [Appendix A: Terminology](#)) and be familiar with how to use the command line interface (CLI) for the chosen software.

Hardware Requirements

indeni supports both physical and virtual servers. The following hardware requirement rely on a parameter **N** which represents the number of network devices you plan to analyze with indeni.

- CPU: 64-bit capable CPU (quad-core CPU recommended: One core per every 20 devices in **N**)
- Hard drive: 40GB + (2GB * **N**). For example, for 10 devices, a total of 60GB is required.
- RAM: The formula is 50MB times **N** + 2GB, with the minimum being 2GB. For example, for 30 devices a total of 3.5GB is required. For a production setup, indeni requires the use of at least 4GB.

The installation disc includes CentOS 6.x with the required packages, so there is no need to pre-install anything on the designated physical or virtual server.

NOTE: The server must be connected to the network during the ISO installation. This should not be a problem on VMs but hardware servers are more prone to being disconnected from the network. If it's not possible to connect to the network then please contact support@indeni.com

Software Requirements

- The indeni application
- Internet browser: Microsoft Internet Explorer 8 or later, Mozilla Firefox 3 or later, Google Chrome

indeni can analyze both local and remote network devices over VPN or directly, providing you with a complete and comprehensive view of your network deployment at a global level.

Analyzed Device Requirements

If communications between the user workstations and indeni and/or the communications between indeni and the analyzed devices pass through a firewall, please allow the following:

Traffic from the user workstations to indeni on the following ports:

- SSH (TCP 22) - Allows SSH access to the indeni device's operating system.
- TCP 8181 - Used for accessing the indeni application from users' workstations.

Traffic from indeni to the analyzed devices:

- All Supported Devices (Advanced Analysis):
 - SSH (TCP 22) - Used for collecting information from the analyzed devices.
 - Ping (ICMP Echo) - Devices are pinged regularly by indeni to ensure they are responding.
Note: the ping test can be deactivated in the individual device's configuration at the **Monitored Devices** sub-tab under **Settings**.
- Devices interrogated with API (Palo-Alto, F5)
 - HTTPS (TCP 443)

CHAPTER 2: INSTALLATION

As stated in the previous chapter, users can set up indeni on either a virtual server or on a physical server. In either case, users will need to download the latest version of indeni from www.indeni.com.

Installations on Virtual and Physical Servers

The indeni ISO is used for deploying the system in virtualization environments or on a physical server.

1. Access the download page at try.indeni.com to download the indeni ISO.
2. Copy the downloaded ISO to a CD and boot the system from the CD. Installation will begin immediately (more on the installation screens below). Upon completion, the server will shut down.

NOTE: Before using VMware for a virtual machine installation, please see [“Setting Up indeni on VMware ESX”](#).

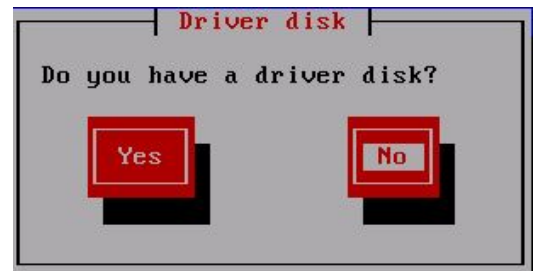
3. Remove the CD from the drive before restarting the server to avoid re-installing the software.

In either physical or virtual installations, the system is now ready to be configured, using the same procedures in either installation.

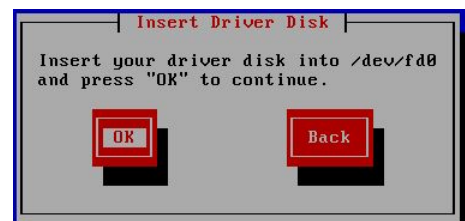
Configuring and installing indeni

Use the tab, arrow, and Enter keys to navigate within the installation screens.

1. If you select **No** from the Driver Disk screen, go immediately to Step 4 to continue configuration of the network interface.



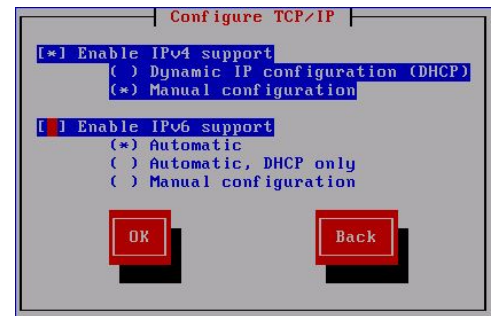
2. If you select **Yes** from the Driver Disk screen, Figure 2 appears. Click **OK**.



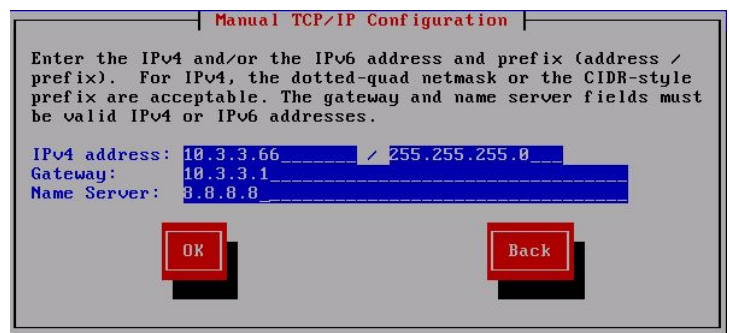
3. In the Driver Disk Source screen, select the device you want to use as the source for the driver disk. Click **OK**.



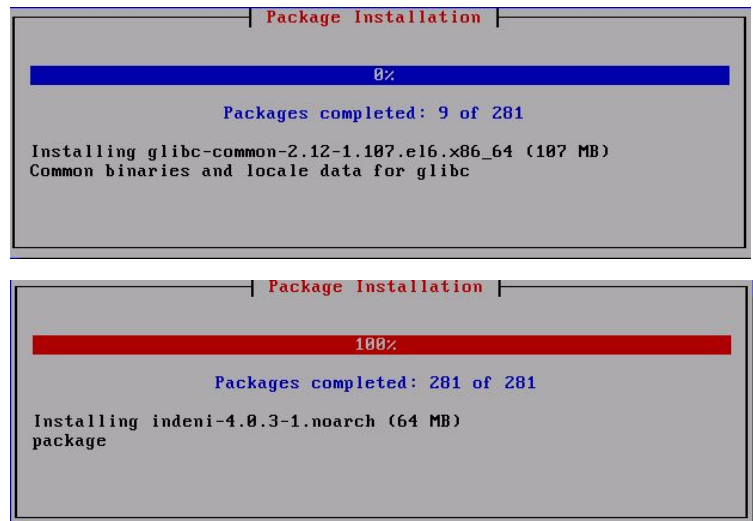
4. Select **Enable IPv4 support** as shown in the figure to the right.
Select **Manual configuration** and click **OK**.



5. Enter the IP address, Netmask Prefix, Gateway and DNS server IP. Click **OK**.



6. The **Package Installation** will run as shown to the right.



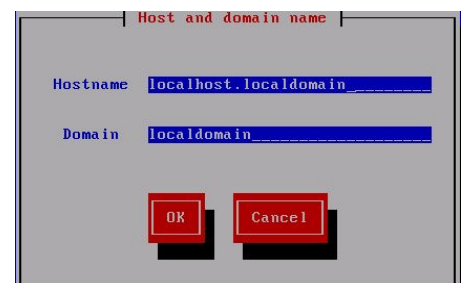
7. When the setup is complete, the system will notify you and ask for a reboot. Click on the **Reboot** button.



Figure SEQ Figure * ARABIC 6

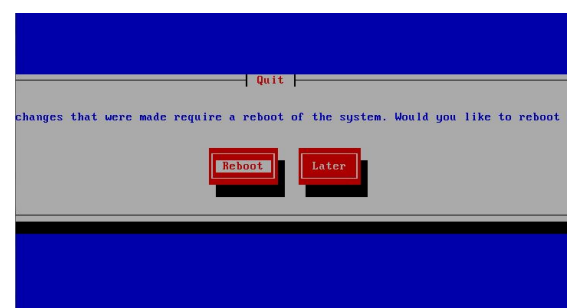
Once the system reboots, the next two screens shown below automatically appear.

8. Specify the host and domain name. Click **OK**.



9. After completing the configuration, click the **Reboot** button to reboot the system for the second time.

NOTE: You can always return to the set up screens by running *sudo isetup* via the console or an SSH connection.



Logging in to the System - Console

You can log in to the system only after you have rebooted twice, as shown in the previous section:

Username: **indeni**

Password: **indeni4it**

In production environments, it is highly recommended that users change the default password, using the **passwd** command.

Logging in to the System - Web Interface

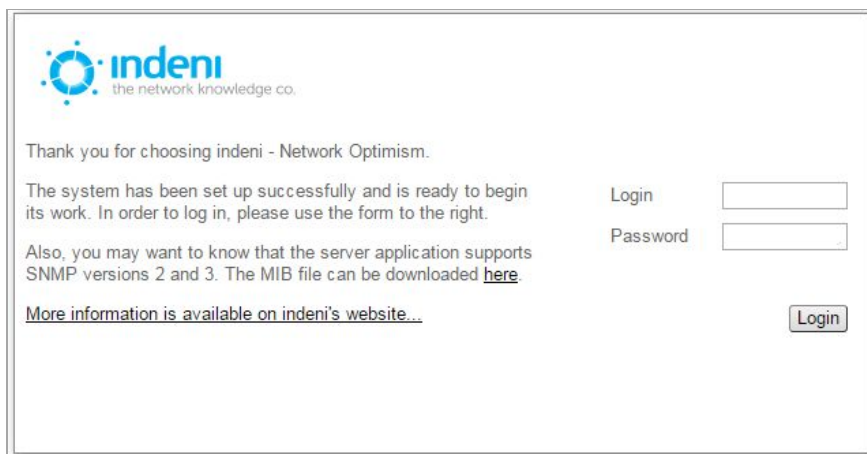
1. Open a browser window
2. Access indeni's web dashboard at:
https://<indeni_ip>:8181/
3. Substitute your server's IP address for <indeni_ip> (example: <https://10.3.1.87:8181/>).

Note that the web browser may display a warning when connecting to the indeni server for the first time. Accept the connection: it is secure.

4. Log in to the indeni web dashboard:

Username: **admin**

Password: **admin123!**



indeni
the network knowledge co.

Thank you for choosing indeni - Network Optimism.

The system has been set up successfully and is ready to begin its work. In order to log in, please use the form to the right.

Also, you may want to know that the server application supports SNMP versions 2 and 3. The MIB file can be downloaded [here](#).

[More information is available on indeni's website...](#)

Login

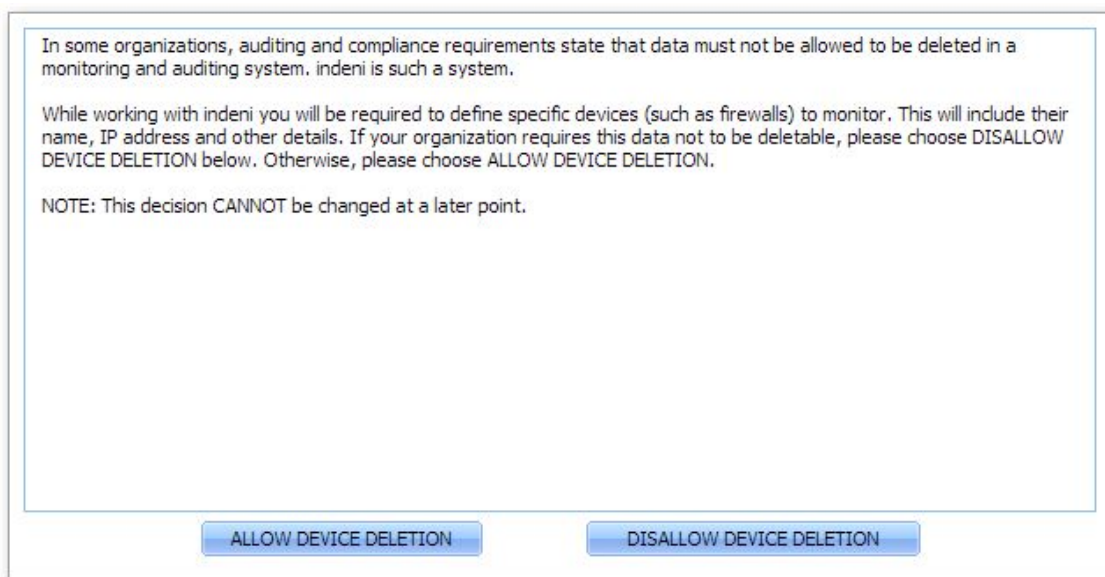
Password

Login

Compliant vs. Non-Compliant Mode

indeni users have full control over which devices to add to the system and analyze. This process is described in [Chapter 4: Getting Started](#).

The system offers two modes: **compliant** and **non-compliant**. Upon installation, indeni will ask whether the user wishes to operate in compliant or non-compliant mode. If “non-compliant” is chosen, devices can be deleted at will. Any or all devices may be removed from analysis if the user so desires, and thus will not show up on the overview screen that is shown in the next chapter.



See [Chapter 5: Analysis and Alert Management](#), for full instructions on analyzing devices.

CHAPTER 3: OVERVIEW

All major functions within indeni are accessed from the tabs at the top of the dashboard. They include:

- **Operations Management**
- **Compliance Management**
- **Tools**
- **Reporting**
- **Settings**

These tabs are available from all main screens within indeni. The functionality of each one is described in this chapter.

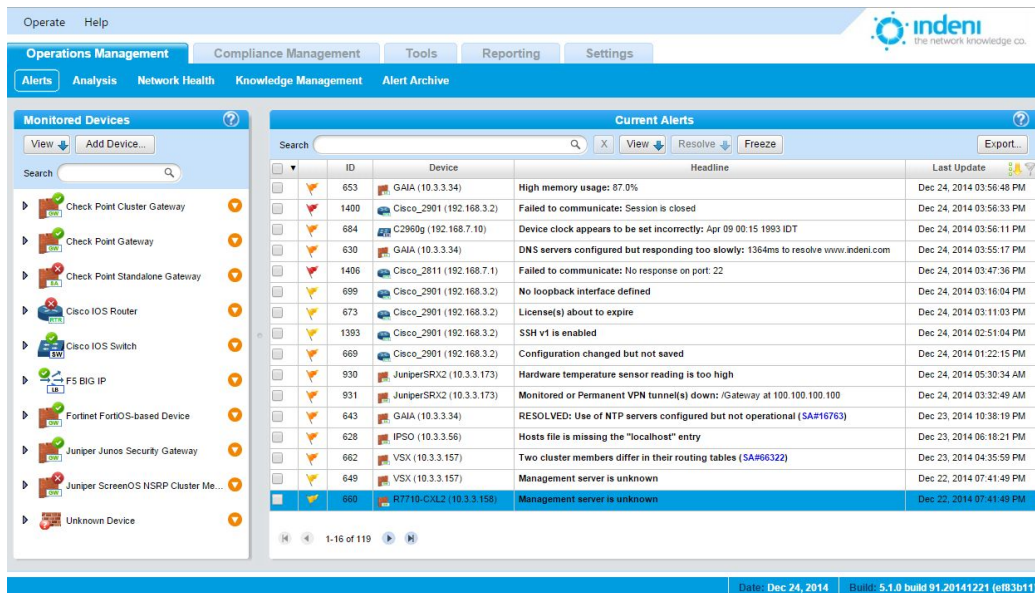
Operate and Help Menus

These two menus are shown at the top left of the web dashboard:

- Use the **Operate** menu to log out of indeni. This menu also allows you to update the system.
- Use the **Help** menu to link directly to this user guide online. The **Help** menu also provides indeni support tools that allow you to create a debug report or to run a live debug of the indeni application.

Operations Management

The **Operations Management** tab allows users to quickly add and configure new devices as well as view all current and archived alerts. Once devices have been added to the system, the screen for this tab provides at-a-glance information regarding alerts relating to each device, with rollover access to detailed information for each alert. Use the sub-tabs within this window (**Alerts**, **Analysis**, **Network Health**, **Knowledge Management** , and **Alert Archive**) to access further functionality as described on the next page.



The **Add Device** button shown in the **Monitored Devices** panel on the left side of the screen is accessible only from this window.

Use the black arrow beside each device group in the **Monitored Devices** panel to expand or collapse the display for more alert information related to individual devices.



The sub-tabs in the **Operations Management** tab provide full access to all information and configuration settings related to alerts generated by indeni:

Alerts

This tab displays all current alerts as well as the complete list of all analyzed devices and their associated alerts. Users can add devices, filter and search for alerts, and export alert data in several formats (pdf, csv, and xml).

Network Health

The Network Health tab presents a dashboard that provides an at-a-glance view of network health in real time.

Analysis

The Analysis tab provides the ability to visually track critical metrics over time. These metrics are correlated with the alerts that were issued at the relevant time.

Knowledge Management

Users have full control over how indeni handles alerts for each device.

This screen provides a full list of alert categories and access to configuration settings by alert and by device.

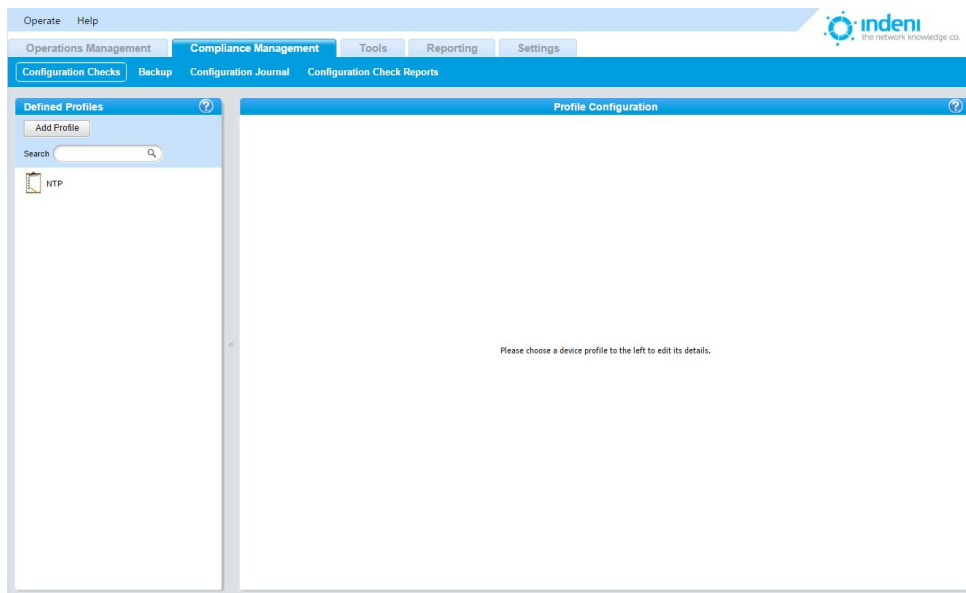
Alert Archive

Acknowledging alerts moves them from the Alerts list to the Alert Archive list. This screen allows quick access and filtering tools to search for specific archived alerts by date, device, or alert type.

Complete functionality for the **Operations Management** tab is described in [Chapter 5: Operations Management](#).

Compliance Management

The **Compliance Management** tab allows users to schedule daily backups for specified devices and directories, set up and edit configuration checks, conduct searches of analyzed devices and track changes made to devices (configuration journal).



Configuration Checks Use this feature to define a profile that states what the baseline settings/configurations should be for a device or a group of devices, and then which devices should have that profile applied. For instance, users can set up a company-wide base profile designating the severity level for generating alerts, or create a profile for a specific type of device (e.g., Cisco Routers).

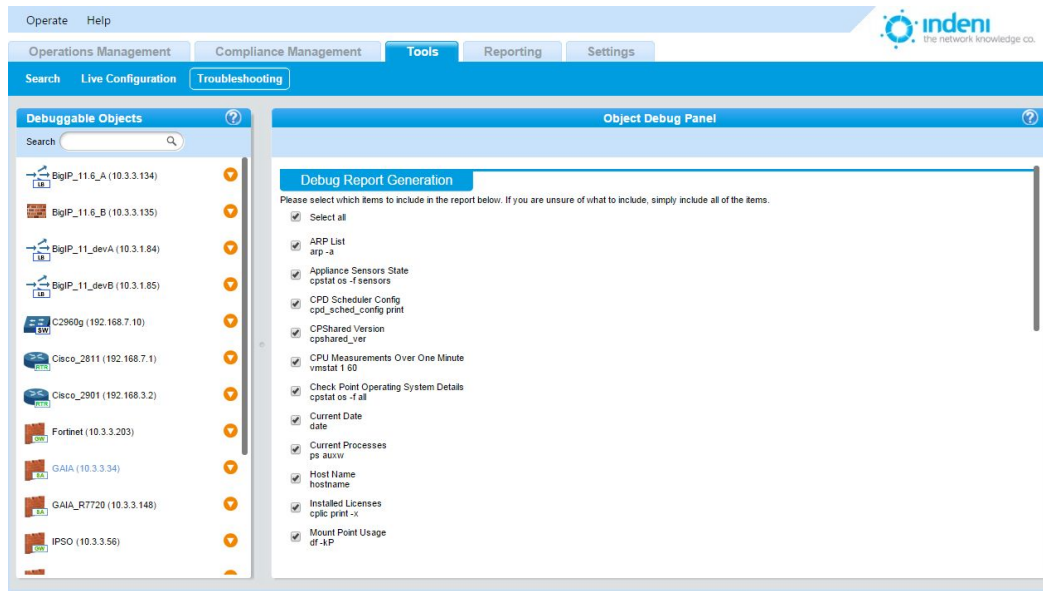
Backup indeni automatically collects backups for the chosen devices and backs up the device's configuration in a separate file with a time stamp. The backup includes the files and data recommended by the vendor and system users for backing up a specific device.

Configuration Journal This feature aggregates and tracks all changes made by any user to any device and time stamps them by the most recent change, for a convenient at-a-glance listing.

Configuration Check Reports This sub-tab allows for the scheduling of a report that displays a summary of all the devices/groups that have not maintained compliance with the configuration checks that were set for those devices in the system

Tools

The **Tools** tab allows users to Search for information in indeni's internal database, explore the device's Live Configuration and export data from devices for further Troubleshooting.



Search

This sub-tab allows users to search using free text through their network estate (all the analyzed devices). The search includes things like NIC configurations, SW versions, licenses, general settings, and configurations. Once the search is completed, the user also has the ability to compare findings between the devices and to print the outcome.

Live Configuration

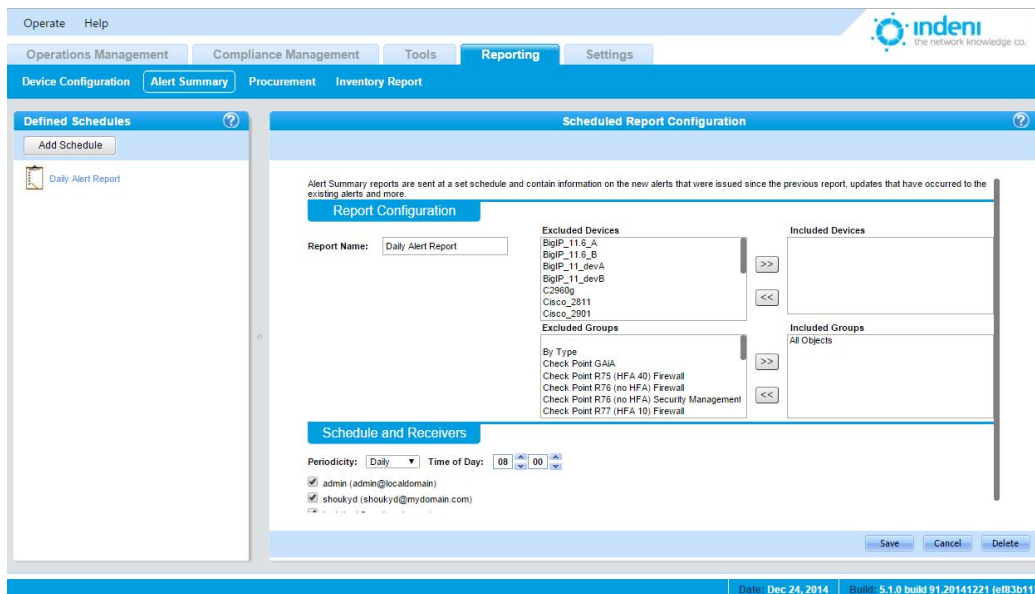
Users may instantly view the actual configurations on the analyzed devices using the **Live Configuration** sub-tab. The information presented by indeni contains both software and hardware data and is clearly presented in a table format

Troubleshooting

The **Troubleshooting** sub-tab displays the list of analyzed devices. Choosing a device displays a list of commands and variables commonly used or required by the vendor when creating a debug report. This tool automatically generates a report that may be used with the devices' vendor for debugging or bug reporting.

Reporting

You can quickly add, delete, or edit indeni reports using the Reporting tab and its sub-tabs.



Device Configuration

Device Configuration reports are sent at a set schedule and contain a set of archives using this sub-tab. Each archive represents the current configuration of a analyzed device.

Alert Summary

Alert Summary reports are sent at a set schedule and contain information on the new alerts that were issued since the previous report, updates that have occurred to the existing alerts, and more.

Procurement

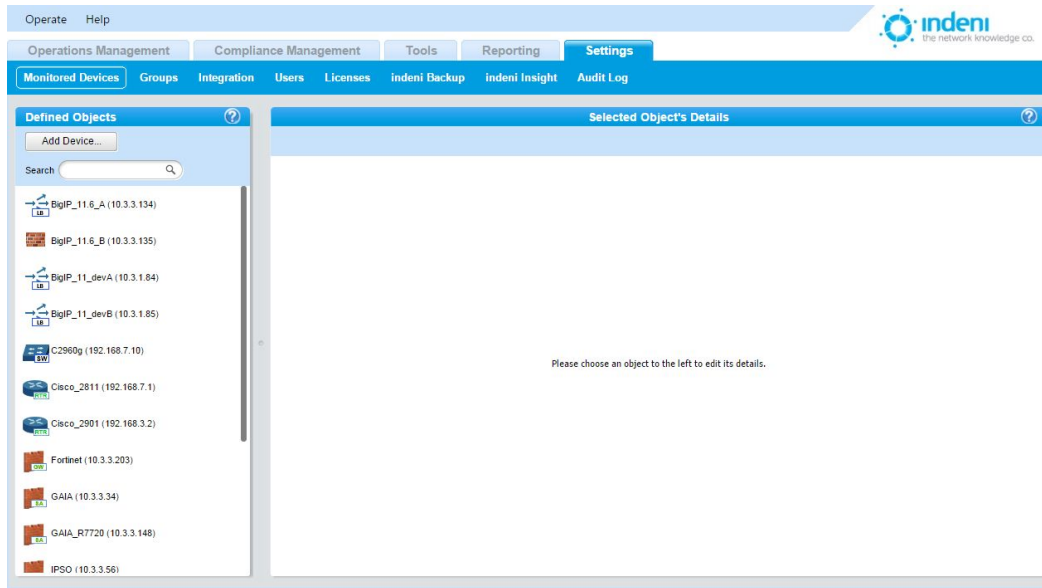
The Procurement sub-tab reports list all the analyzed devices that may require changes or upgrades. They also display information such as expired licenses and EOL devices.

Inventory Report

This exportable Excel spreadsheet report provides both an overview of your entire network inventory and insight at a granular level, including model names and numbers, interface vendors, firmware versions, licenses, disk manufacturers, routes, VPNs, and much more.

Settings

The **Settings** tab includes a wide range of functions using the sub-tabs.



- | | |
|--------------------------|---|
| Monitored Devices | Add and configure devices from this sub-tab, which functions identically to the Add Device button under Operations Management . Clicking on any device listed provides full access to its settings. |
| Groups | Setting up device groups as shown above is a quick way to keep track of many different types of devices on the network. This sub-tab allows users to quickly add or delete devices from existing groups and set up new groups which can include individual devices and other device groups. |
| Integration | From this sub-tab, users can add SNMP masters for sending indeni alerts directly to existing systems (such as NMSs) as well as add Syslog and SMTP servers. |
| Users | Add or delete users, set passwords, designate permissions, and allocate specific groups of devices to specific users from this sub-tab. |
| Licenses | On this sub-tab, indeni displays the current state of user licenses, whether valid or expired. Users can also use this sub-tab to upload new licenses or download license details. |
| indeni Backup | This functionality backs up the indeni system. |
| Audit Log | The Audit Log sub-tab provides a list of changes and activities that have occurred on the indeni application. |

CHAPTER 4: GETTING STARTED

To begin using indeni, users must first add at least one device for the system to analyze. By default at installation, the system has one user with a default login and password.

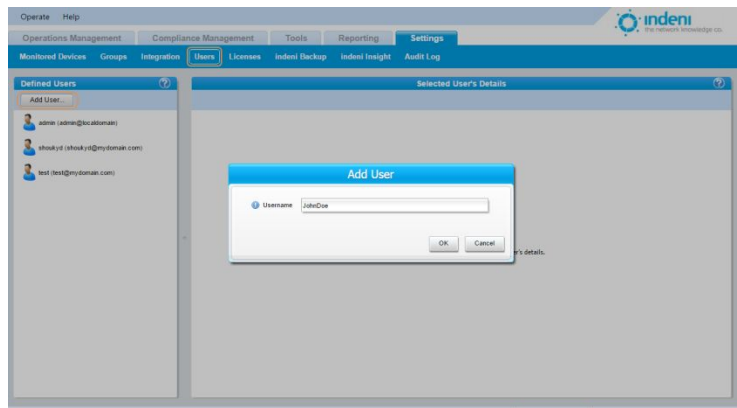
Managing Users

indeni assigns administrator privileges by default to all users logged into the system. To add new users, set passwords, assign email contact information, and modify permissions for each person to be allowed access to the system, select the **Settings** tab, and then the sub-tab **Users**.

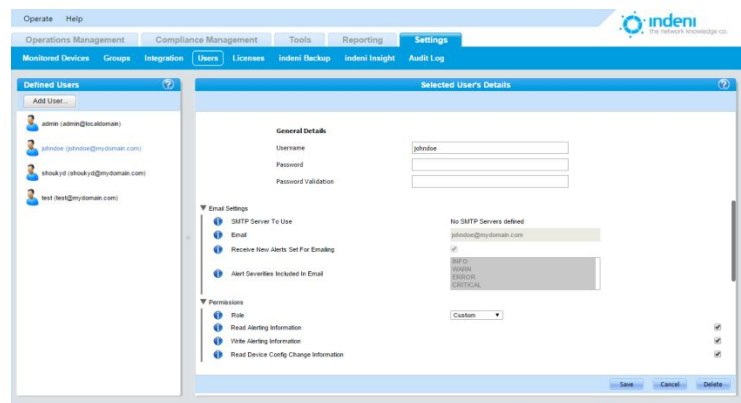
Adding a User

1. Click the **Add User** button under **Defined Users** on the left side of the screen.
2. In the dialog box, type a user name and select **OK**.

indeni displays the **Selected User's Details** screen with additional fields as shown. *indeni does not allow renaming the individual user.* If a mistake was made when entering the username, the administrator must use the **Delete User** button at the top of the screen to delete the user. Re-add the user with the correct name. *Usernames are case sensitive.*



3. Set the user's password. indeni requires the use of strong passwords. Passwords must be at least eight characters long and use both alphabetic and numeric characters. Passwords are case sensitive.



4. Enter the individual's email settings and the SMTP server.
5. Assign permissions appropriate to this user.
6. Choose the Groups this user will be allowed to view/manage.
7. Scroll down to the bottom of the screen and select **Save**. The **Defined Users** list on the left now displays the new users added to the system.

Adding Devices to the System

To begin using indeni to manage and analyze network devices, recognized users must add devices to the system. This is a fast and easy process.

Check Point

SecurePlatform

1. Log in to the device to be added using SSH or the console.
2. Add a new user to be designated for indeni's use:
 - Use the **bash** shell instead of the default **cpshell** shell (also known as “expert mode”).
 - First, run **adduser <username>**.
 - Provide a strong password for the new user.
 - Run **chsh -s /bin/bash <username>**.

IPSO

1. Log in to the device to be added, using Voyager.
2. Add a new user to be designated for indeni's use.
 - The user should have the same permissions as the default admin user, and specifically, **uid** should be set to 0 (zero).
 - The user should be in **cs** shell.
 - The user should be part of the “wheel” operating-system-level group.

GAiA

Adding a User to GAiA via the Portal

1. Log in to the GAiA Portal.
2. Add a new user to be designated for indeni's use:
 - Use the **bash** shell.
 - Have **adminRole** in Assigned Roles.

Add User

Login Name:

Password: Good

Confirm Password:

Real Name:

Home Directory:

Shell:

Available Roles

- monitorRole

Assigned Roles

- adminRole

Access Mechanisms

☒ Web

☒ Command Line

Adding a User to GAIa Through CLI

To add a new user to indeni via CLI, use the following commands:

```
clish
add user indeni uid 0 homedir /home/indeni
set user indeni gid 100 shell /bin/bash
add rba user indeni roles adminRole
set user indeni password
save config
exit
```

61000 Security System

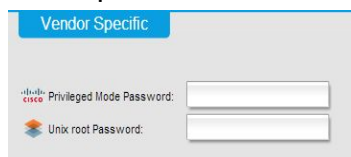
Please follow the “Adding a User to GAIa Through CLI” instructions above.

Provider-1/MDM on SPLAT, IPSO, GAIa

1. Add the user as described above for the relevant OS.
2. In the indeni UI, add the MDS first.
3. After the MDS is successfully added, add the CMAs/domains you would like to analyze. Ideally, these would be the CMAs/domains that manage the firewalls you have set indeni to analyze.

Crossbeam (Blue Coat) running Check Point

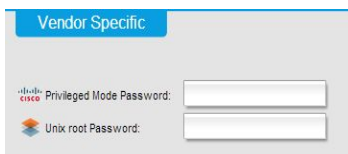
1. Add a user with the Unix su privileges.
2. Please provide the Unix root password in the Add Device dialog:



Cisco

ASAs, Routers, Switches

Add a user who can enter Privileged Mode (level 15). If the user is not set to level 15, you will be required to enter the Privileged Mode Password in the Add Devices dialog:



F5 BIG-IPs

Add a user with the Administrator role or equivalent permissions. Make sure all partitions are accessible.

Fortinet Fortigates

Add a user with the super_admin profile or equivalent permissions.

Juniper

ScreenOS

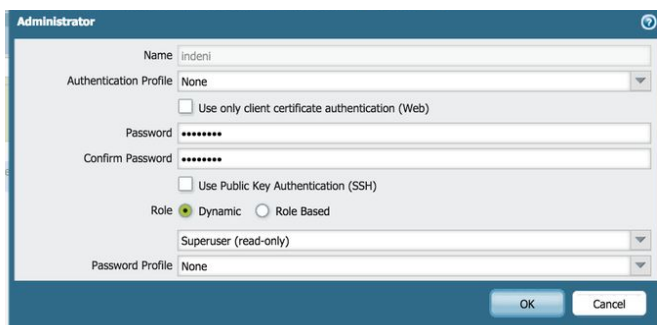
1. Log in to the device to be added using SSH.
2. Add a new user to be designated for indeni's use.

Junos

1. Follow Juniper Networks' relevant user guides for adding a user.
2. Make sure the user's login class is "super-user."

Palo Alto

Add a user with Role "Superuser" (can be "read-only")



The screenshot shows the 'Administrator' dialog box for creating a new user. The fields are as follows:

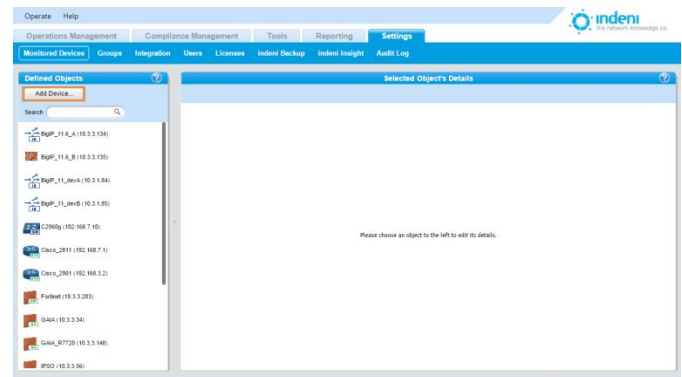
- Name:** indeni
- Authentication Profile:** None
- ☐ Use only client certificate authentication (Web)
- Password:** [masked with asterisks]
- Confirm Password:** [masked with asterisks]
- ☐ Use Public Key Authentication (SSH)
- Role:** Dynamic (selected), Role Based
- Role Selection:** Superuser (read-only) (selected from a dropdown)
- Password Profile:** None

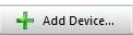

At the bottom right, there are 'OK' and 'Cancel' buttons.

Adding a Device in the UI

Once a user has been designated, click on **Add Device** at one of these locations:

- **Operations Management** tab
- **Monitored Devices** sub-tab in the **Settings** tab.



indeni supports adding multiple devices at once. If two or more devices are to be added at once, add additional device lines as needed by clicking the  button in the dialog box. Delete unneeded blank boxes by clicking on the  symbol.

Supply the device name and IP address for each device to be added. For example:

Device Name: Cluster_Member1

IP: 10.3.1.88

You can choose from three options: **Add New Device**, **Add Known Device**, and **Upload List of Devices**. Users should add all devices that are not known first, and then known devices (see next section), to build a complete list before setting credentials.



When indeni is first installed it will ask whether the user wishes to operate in compliant or non-compliant mode. If “non-compliant” is chosen, devices can be deleted at will. Any or all devices may be removed from analysis if the user so desires, and thus will not show up on the overview screen. See [Disable Monitoring](#).

Adding Known Devices

When adding devices, indeni allows users to choose from a list of devices known to indeni, based on indeni’s analysis of management servers’ databases (where applicable). Known devices are those which meet the following conditions:

- They appear in the database of at least one of the management servers currently being analyzed by indeni.
- The associated management server considers the device to be one it manages (as opposed to an externally managed device).

- The device has not previously been added to the list of analyzed devices in indeni.

Use the **Add Known Device** button to access the **Select Known Device** field. Choose the appropriate device IP address from the dropdown lists as shown above.

Upload List of Devices

Using the third option, **Upload List of Devices**, allows users to quickly upload a CSV file listing all known user devices to be added. indeni will analyze the file and allow the user to review the results and decide whether to proceed or not. The format of the CSV file is simple, it should only contain lines of the following format:

DEVICENAME,DEVICEIP

Choosing Credentials

Once all devices have been added, use the appropriate radio button to supply the proper credentials for these devices. indeni supports two methods of doing so under **Credentials to Use**: **SSH (Advanced Monitoring)** and **SNMP (Standard Monitoring)**.

SSH (Advanced Monitoring):

1. Supply the SSH login details for the user added previously. For example:

SSH Username: indeni

SSH Password: indeni11

You may use an **SSH Key**, which replaces the need for a password. Clicking on this activates a text box that you can paste the SSH key into. If the key file is encrypted, an **SSH Passphrase** is also required. The password requirement depends upon the type of key file used.

NOTE: When using SSH RSA keys for authentication, you must make sure that on the device indeni is connecting to the `authorized_keys` file is only writeable by the user (mode 755 for `~/.ssh` and mode 600 for `~/.ssh/authorized_keys`).

2. Click **Add**, which simultaneously adds the defined devices and stores the chosen analysis method and credentials. The system will attempt to connect to the new devices using the credentials provided. indeni will gather as much information as it can to determine what the new devices are and what analysis should be conducted.

This includes:

- Operating System (IOS, BIG-IP, SecurePlatform, IPSO, etc.)
- Products (Routing, Switching, Load Balancing, Firewall, VPN, IPS, Management, etc.)
- Version
- Relationships between devices (such as relationships between cluster or device group members)

indeni re-validates its conclusion every few minutes. If there is a change in the device (for example, products added/removed, change of version) the system will automatically adapt.

SNMP (Standard Analysis)

Standard analysis allows for the SNMP-based analysis of any device not listed in the advanced analysis devices. Via SNMP, indeni will pull information regarding CPU and memory usage, NIC statistics, storage information, and the defined routing table. The information is retrieved based on RFC1213 (<http://www.ietf.org/rfc/rfc1213.txt>), so the analyzed device is required to implement that RFC. To add a device under Standard Analysis:

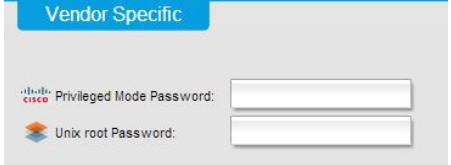
1. Go to the **Settings** tab and select the **Monitored Devices** sub-tab.
2. Click the **Add Device** button.
3. In the **Add Device** dialog box, choose the **Standard Monitoring** radio button.
4. Fill in the **Read Community** string for accessing the device(s) via SNMP.
5. Click **Add** to add the new device(s) to indeni.

Devices that have been added appear in the list of analyzed devices on the left panel of the **Operations Management** tab. Users should review the alerts for any devices which were not added successfully to understand why and take corrective action.

NOTE: Devices for which advanced monitoring and analysis is supported **MUST NOT** be added through SNMP monitoring and analysis. This mode of operation is not supported.

Vendor Specific

Some vendors that indeni supports require additional credentials or specific settings in order to allow indeni to access certain information. This is provided using the **Vendor Specific** section of the **Add Device** box.



These include **Privileged Mode Password** (for Cisco devices) and/or **Unix root Password** (for Crossbeam devices).

Editing Devices

Administrators can also adjust settings for devices which have been added to the system using the **Settings** tab at the top of the screen and then the **Monitored Devices** sub-tab. Configuration settings for all other objects which are not the analyzed devices (such as SNMP, SMTP, and Syslog servers) can be accessed from the **Integration** sub-tab under **Settings**.

Live Configuration

The **Live Configuration** option under the **Tools** tab displays the entire actual configuration of the device, including resource utilization, device model, routing, etc.

CHAPTER 5: OPERATIONS MANAGEMENT

The Alerts Sub-Tab

indeni was designed to simplify management of networks and to free an administrators' time for business initiatives rather than endlessly chasing network issues. Using the power of indeni to analyze devices and resolve alerts lies at the heart of the system's usefulness.

The **Alerts** tab displays all alerts noted by the system under the **Current Alerts** pane.


Even when the issue has been successfully resolved, the alert will remain on the display until the user acknowledges and archives the resolved alert, or chooses to show only unresolved alerts. Resolved alerts are marked as “RESOLVED:”.

Monitored Devices

indeni displays all devices by name under **Monitored Devices**. The **View** button in the left panel allows users to display objects by group, device type, cluster, or management hierarchy.

The screenshot shows the indeni Alerts sub-tab interface. The left panel, titled 'Monitored Devices', has a 'View' button that has been clicked, opening a dropdown menu with the following options: 'By Group', 'By Cluster', 'By Type', and 'By Management Hierarchy'. The main panel, titled 'Current Alerts', displays a table of alerts. The table has four columns: 'ID', 'Device', 'Headline', and 'Last Update'. The alerts are listed in descending order of their last update time. The first few alerts are marked as 'RESOLVED' and describe issues with DNS servers responding too slowly. Other alerts include 'Contract(s) have expired', 'License(s) have expired', 'Device clock appears to be set incorrectly', 'High memory usage', 'Service database not updated', 'Proxy ARP is enabled', 'SSH v1 is enabled', and 'AAA is disabled'.

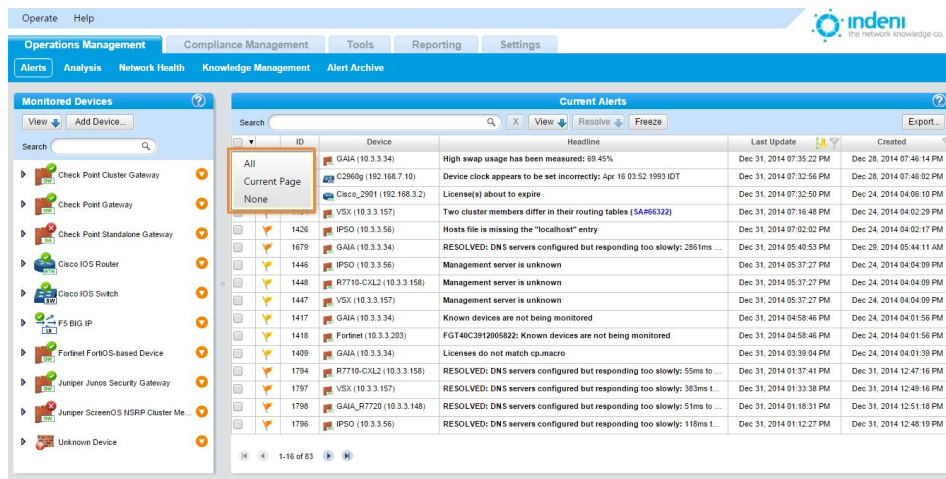
ID	Device	Headline	Last Update
1525	GAIA_R7720 (10.3.3.148)	RESOLVED: DNS servers configured but responding too slowly: 61ms to resolve www.in...	Dec 25, 2014 01:51:28 PM
1524	R7710-CXL2 (10.3.3.158)	RESOLVED: DNS servers configured but responding too slowly: 102ms to resolve www.i...	Dec 25, 2014 01:55:30 PM
1523	V5X (10.3.3.157)	RESOLVED: DNS servers configured but responding too slowly: 60ms to resolve www.in...	Dec 25, 2014 01:55:30 PM
1522	IPSO (10.3.3.56)	RESOLVED: DNS servers configured but responding too slowly: 77ms to resolve www.in...	Dec 25, 2014 01:51:28 PM
1521	BigIP_11_devA (10.3.1.84)	RESOLVED: Two cluster members differ in their routing tables (SA#66322)	Dec 25, 2014 01:26:27 PM
1484	GAIA (10.3.3.34)	Use of NTP servers configured but not operational (SA#16763): urlhover.com	Dec 24, 2014 10:51:59 PM
1485	GAIA (10.3.3.34)	RESOLVED: DNS servers configured but responding too slowly: 829ms to resolve www.i...	Dec 25, 2014 01:54:30 PM
1479	GAIA (10.3.3.34)	Contract(s) have expired	Dec 24, 2014 04:06:14 PM
1478	GAIA (10.3.3.34)	License(s) have expired	Dec 24, 2014 04:06:14 PM
1477	C2960g (192.168.7.10)	Device clock appears to be set incorrectly: Apr 10 02:10 1993 IDT	Dec 25, 2014 05:51:42 PM
1476	GAIA (10.3.3.34)	RESOLVED: High memory usage: 87.0%	Dec 25, 2014 05:52:50 PM
1475	Fortinet (10.3.3.203)	FGT40C3912005822: Service database not updated	Dec 24, 2014 04:06:11 PM
1474	C2960g (192.168.7.10)	Proxy ARP is enabled	Dec 24, 2014 04:06:11 PM
1473	Cisco_2901 (192.168.3.2)	Proxy ARP is enabled	Dec 24, 2014 04:06:11 PM
1472	Cisco_2901 (192.168.3.2)	SSH v1 is enabled	Dec 24, 2014 04:06:11 PM
1471	C2960g (192.168.7.10)	SSH v1 is enabled	Dec 24, 2014 04:06:11 PM
1470	C2960g (192.168.7.10)	AAA is disabled	Dec 24, 2014 04:06:11 PM

As noted in Chapter 4, the left panel of the **Monitoring** tab displays all devices currently being analyzed by indeni. Use the **View** button on the left to toggle between displaying devices by cluster, type, or management hierarchy. Use the orange arrow  to edit or filter alerts for individual devices or groups of devices. The **Search** field allows users to search for devices by any portion of a device name.

Current Alerts

The checkboxes in the left column of this portion of the screen allow users to manage multiple alerts.

- Use the topmost checkbox (in the header row) to check or uncheck all boxes at once or to select those for the current page only.
- Use the small, black down arrow beside the box to adjust selections as shown below.
- Click “None” or click the box again to uncheck all selections.



The **View** button and the **Search** box above the list of alerts can be used to filter the alert list or to search for a particular alert ID. The **Freeze** toggle button halts the automatic update of the list of alerts.

Searching Alerts

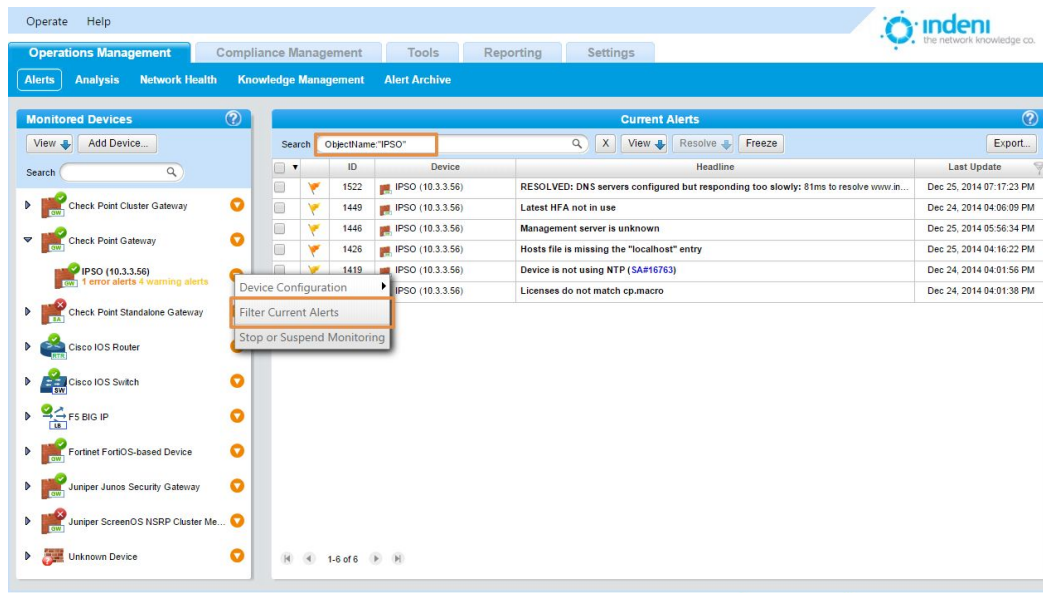
The **Search** box in the **Current Alerts** pane supports searching for alerts associated with certain devices using the device name or IP address, searching for an alert ID, or searching for text within alert headlines and descriptions. (Complete search parameters are listed in [Appendix C.](#))

- To display alerts for a particular device, type the device name in the **Search** field. (You can also click on the orange circle to the right of the device name in the **Monitored Devices** section to display alerts for that device only.)
- To display a particular kind of alert, type the desired parameter in the **Search** field.
- To search for text, type a text string. For example, typing “R60SMC” in the **Search** field will display alerts for all R60SMC members. Clearing the field restores the entire list.

Filtering Alerts

To filter alerts, use the orange arrow next to its name in the **Monitored Devices** display and choose **Filter Current Alerts** from the pop-up menu.

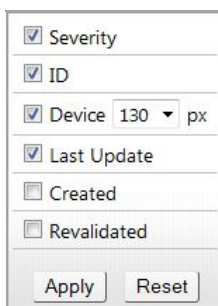
Note that the screen view on the next page displays alerts only for IPSO, IP address 10.3.3.56.



Use the checkbox to the left of the ID field to check or uncheck all filtered alerts at once.

Columns and Functionality

To adjust the width of individual columns on the screen, select the **Columns...** option on the **View** flyout:









Use the checkboxes to select which columns to display. Alternatively, right-click on any column header to access this menu.

Severity

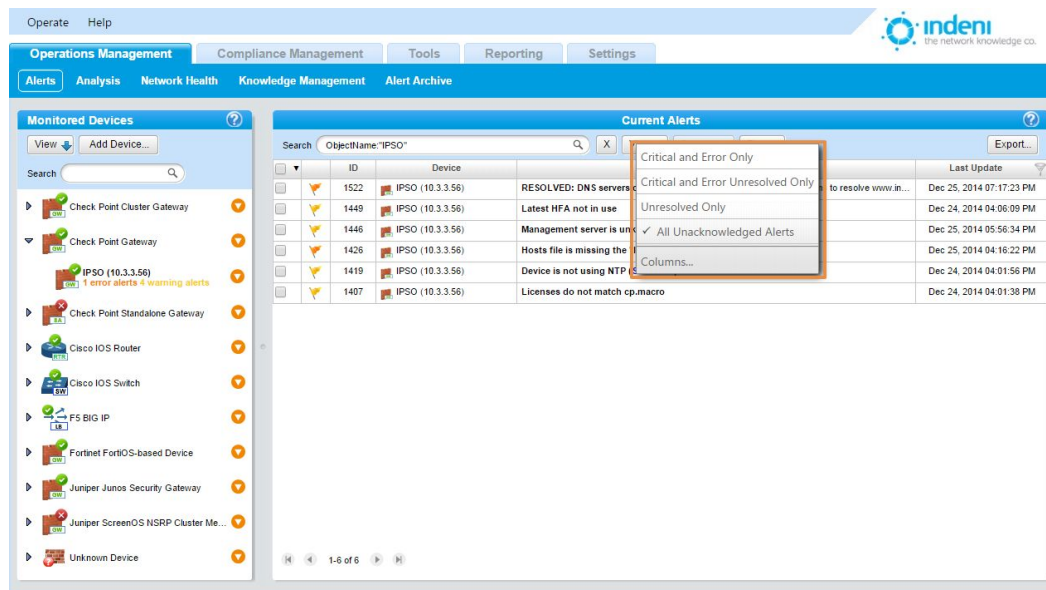
This column displays a colored flag for each alert. Colors range from red to blue to distinguish critical warnings from less severe alerts. This allows users to find and resolve alerts most likely to cause imminent downtime and to visually assess the type of alert and remedial action required.



The **Monitored Devices** list also displays the current state of the device itself using the icons shown here. If a device has other alerts, it will indicate the number and type using text colors corresponding to the flags (blue for Info, etc.).

Device State		Severity
	Critical	
	Error	
	Warn	
	Info	
	Okay	

By default, indeni displays alerts as they occur.

1. To quickly sort by severity, click the **View** button above the **Device** column.
2. Click on or off any of the alert categories in the flyout box shown on the next page (only one option can be selected at a time) and indeni will display only that information. For example, if you do not wish to see resolved alerts, click **Unresolved Only**. indeni will only display alerts the system has not yet resolved or could not automatically resolve.



indeni also provides a fast and convenient listing of each device's individual alerts under its name in the list of **Monitored Devices** on the left. This provides at-a-glance status for each device. Critical status  only appears if the device is truly unresponsive or indeni is having trouble analyzing it; otherwise the Okay symbol  will be shown even if there are alerts for this device. The user can see that the device, while still functional, has errors and can investigate and correct them as required.

ID

indeni assigns a unique number to each alert as it occurs. By default, alerts display in descending order of severity and by date modified.

Device

This column displays the device name assigned to each device for which an alert has been flagged.

Headline

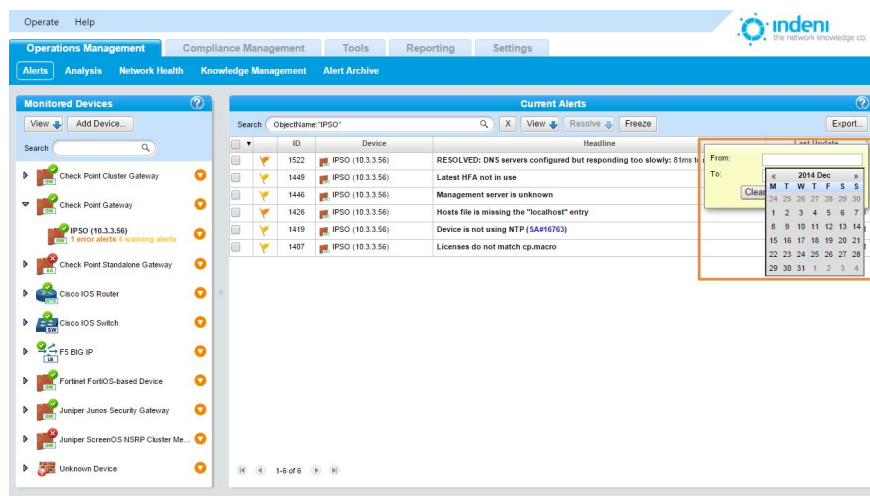
This column displays the actual alert information: a brief description of the condition indeni has observed as well as its status.

In this column by default, each alert in the list displays in the “collapsed” or at-a-glance mode, showing just the summary headline for the alert.

Last Update

This column allows users to further refine the displayed list of alerts by date range.

1. Click the **Filter** icon in the column header.
2. Click inside each blank field box to display a calendar.



3. Choose the date range for the alerts you want to display and then click **Apply**.

The close-up shows the date range selection form. It has two input fields labeled 'From:' and 'To:'. Below the 'To:' field is a 'Clear' button. At the bottom of the form is an 'Apply' button.

4. To filter within a particular day, change the hour settings after the date in both the **From** and **To** fields to display alerts within a specified time range.
5. Click **Clear** to clear the previous criteria. This will restore the entire list of alerts.
6. To quickly sort alerts in ascending or descending order by date, click on the column name. A yellow arrow will appear. Click on it to sort the alerts.

Expanding an Alert

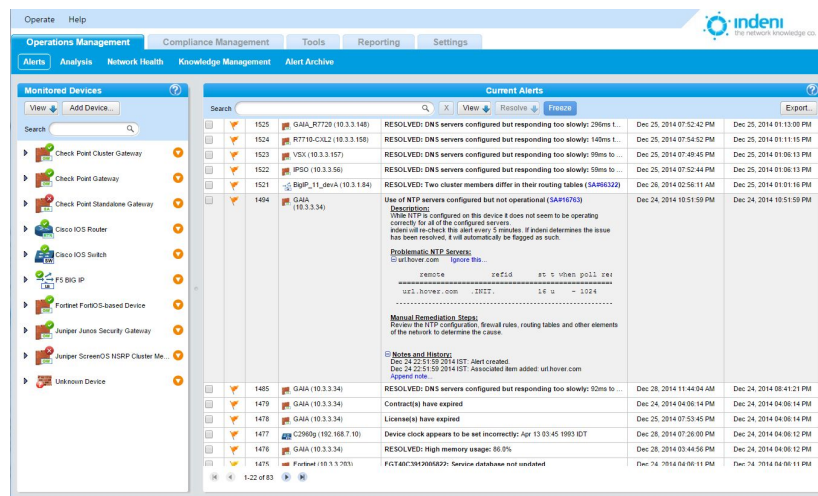
To expand an alert to show its details, click on any headline. In the expanded detail, information is categorized in several ways:

Description: A general overview and explanation of the problem.

Custom Notes: Gives users the option to add their own notes to a specific signature or to a specific group.

Manual Remediation Steps: indeni's recommendation for how to manually correct the problem.

Notes and History: A summary of when the alert has been created, resolved, or remains unresolved, along with any notes which were added to the alert by using the blue “Append note” link.



indeni constantly updates unresolved alerts. You can freeze the display to stop the system from updating content for the current alerts by toggling the **Freeze** button. (Click the button again to resume updates.)

Resolving Alerts

indeni can flag certain errors and offer suggestions on how to resolve issues manually.

Each **Headline** message, when expanded, tells the user if an error can be resolved or not, and what the recommended manual action should be.

Click on the alert to expand it and read the details provided by indeni for resolution. If hyperlinks are included, clicking on those will provide more information on the alert and the process for remediating the issue.

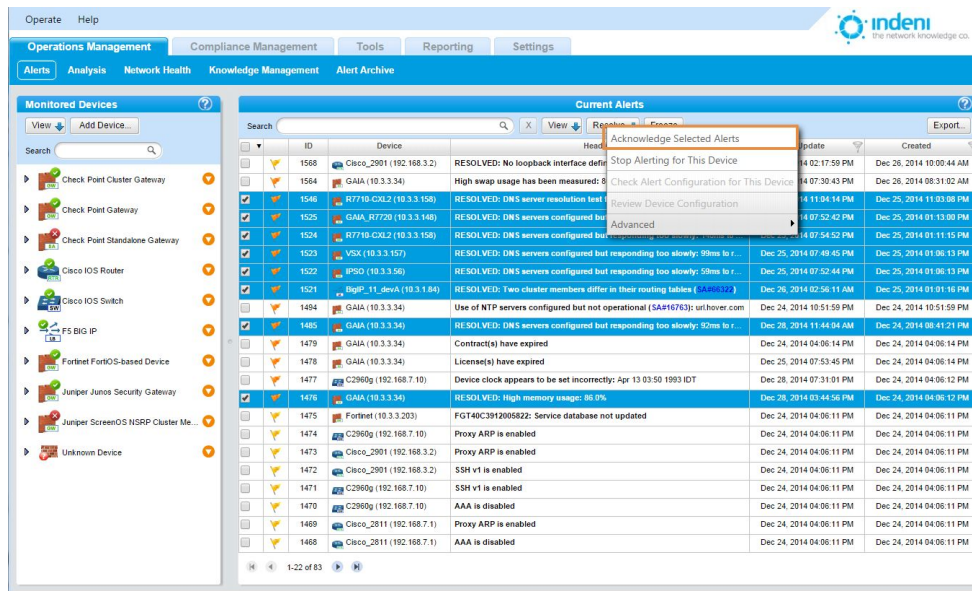
The screenshot displays the indeni Operations Management interface. On the left, a sidebar lists 'Monitored Devices' including Check Point Cluster Gateway, Check Point Gateway, Check Point Standalone Gateway, Cisco IOS Router, Cisco IOS Switch, F5 BIG-IP, Fortinet FortiOS-based Device, Juniper Junos Security Gateway, Juniper ScreenOS NSRP Cluster Member, and Unknown Device. The main area shows 'Current Alerts' with a table of alerts. One alert is selected and expanded, showing details for a GAIA device (10.3.3.34) with the message 'Use of NTP servers configured but not operational (4490762)'. The expanded view includes a description, a table of problematic NTP servers, and manual remediation steps.

Alert ID	Device	Message	Created	Last Updated
1525	GAIA_R7720 (10.3.3.148)	RESOLVED: DNS servers configured but responding too slowly: 296ms to ...	Dec 25, 2014 07:52:42 PM	Dec 25, 2014 01:13:00 PM
1524	R7710-CXL2 (10.3.3.158)	RESOLVED: DNS servers configured but responding too slowly: 140ms to ...	Dec 25, 2014 07:54:52 PM	Dec 25, 2014 01:11:15 PM
1523	V5X (10.3.3.157)	RESOLVED: DNS servers configured but responding too slowly: 99ms to ...	Dec 25, 2014 07:49:45 PM	Dec 25, 2014 01:06:13 PM
1522	IPSO (10.3.3.56)	RESOLVED: DNS servers configured but responding too slowly: 59ms to ...	Dec 25, 2014 07:52:44 PM	Dec 25, 2014 01:06:13 PM
1521	BigIP_11_devA (10.3.1.84)	RESOLVED: Two cluster members differ in their routing tables (5A96332)	Dec 26, 2014 02:56:11 AM	Dec 25, 2014 01:01:16 PM
1494	GAIA (10.3.3.34)	Use of NTP servers configured but not operational (4490762) Description: While NTP is configured on this device it does not seem to be operating correctly for all of the configured servers. indeni will re-check this alert every 5 minutes. If indeni determines the issue has been resolved, it will automatically be flagged as such. Problematic NTP Servers: remote refid st t when poll ser ----- ----- --- --- ----- ----- --- ucl.burser.com .INIT 16 u - 1024 Manual Remediation Steps: Review the NTP configuration, firewall rules, routing tables and other elements of the network to determine the cause. Notes and History: Dec 24 22:51:59 2014 IDT - Alert created. Dec 24 22:51:59 2014 IDT - Associated item added: ucl.burser.com ----- ----- --- --- ----- ----- ---	Dec 24, 2014 10:51:59 PM	Dec 24, 2014 10:51:59 PM
1485	GAIA (10.3.3.34)	RESOLVED: DNS servers configured but responding too slowly: 52ms to ...	Dec 26, 2014 11:44:04 AM	Dec 24, 2014 08:41:21 PM
1479	GAIA (10.3.3.34)	Contract(s) have expired	Dec 24, 2014 04:06:14 PM	Dec 24, 2014 04:06:14 PM
1478	GAIA (10.3.3.34)	License(s) have expired	Dec 25, 2014 07:53:45 PM	Dec 24, 2014 04:06:14 PM
1477	C2960g (192.168.7.10)	Device clock appears to be set incorrectly: Apr 13 03:45 1993 IDT	Dec 26, 2014 07:26:00 PM	Dec 24, 2014 04:06:12 PM
1476	GAIA (10.3.3.34)	RESOLVED: High memory usage: 86.0%	Dec 26, 2014 03:44:56 PM	Dec 24, 2014 04:06:12 PM
1475	Fortinet (10.3.3.703)	FGY40C3812005822: Service database not updated	Dec 24, 2014 04:06:11 PM	Dec 24, 2014 04:06:11 PM

Using the Resolve Button

indeni provides a **Resolve** button above the **Headline** column to assist users in resolving alerts. It is enabled when at least one visible alert is checked. Clicking on the **Resolve** button gives the user several options, from acknowledging and archiving an alert to manually changing configuration settings for the device in question. Note that the **Resolve** button will not activate unless an alert is checked, not just highlighted.

Clicking on the **Resolve** button produces a flyout menu with the options shown on the next page:



NOTE: Functions on the **Resolve** menu vary by the type of alert, as well as whether or not multiple alerts were selected or not. For instance, “Stop Alerting for this Device” may not be an option for all alerts.

Acknowledge Selected Alerts

Selecting this option archives the alert in the Alert Archive and removes it from the list. Resolved alerts which have been reviewed by an administrator should be acknowledged in order to move them to the history. To do so, click on the **Resolve** button and then select **Acknowledge Selected Alerts**.

Stop Alerting for this Device

Selecting this option will prevent indeni from flagging this particular error on this device. It does not block flagging of other errors for this device.

Check Alert Configuration for this Device

This option allows users to quickly review and edit alert settings for a particular device.

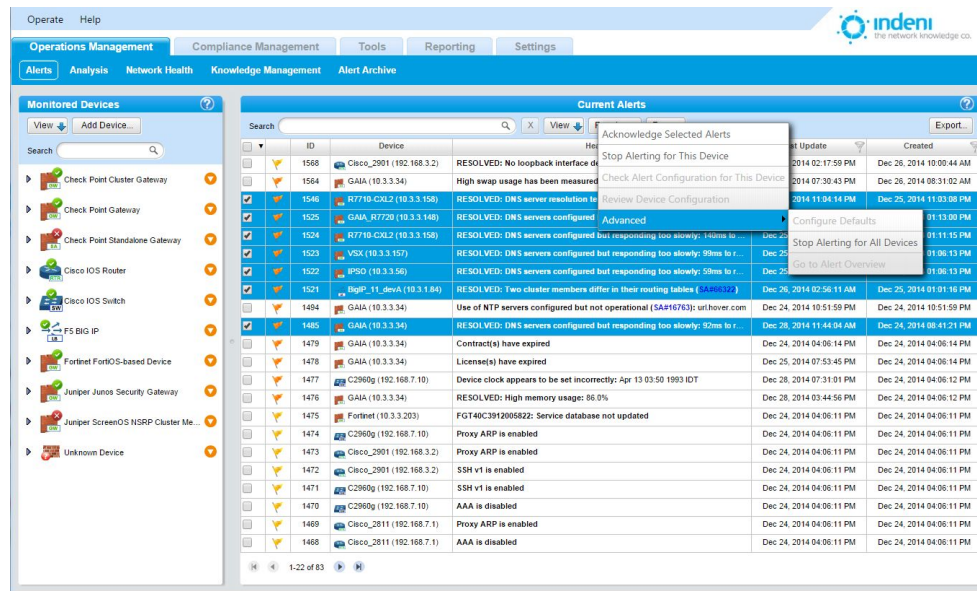
Review Device Configuration

This option quickly takes the user to the configuration screen for this device to check and/or change settings that might be causing the error.

Advanced

This option provides several choices, from configuring default parameters to halting alerts on selected devices.

It allows the user to either stop alerting for a particular error on one device only, or to prevent indeni from flagging this error on all analyzed objects.



Resolving Multiple Alerts

Use the checkboxes in the far left column of the **Monitoring** tab to archive multiple **Resolved** alerts at once.

1. Check the box for each alert you want to archive.
2. Click the **Resolve** button and select **Acknowledge Selected Alerts** to archive these alerts.

Annotating Alerts

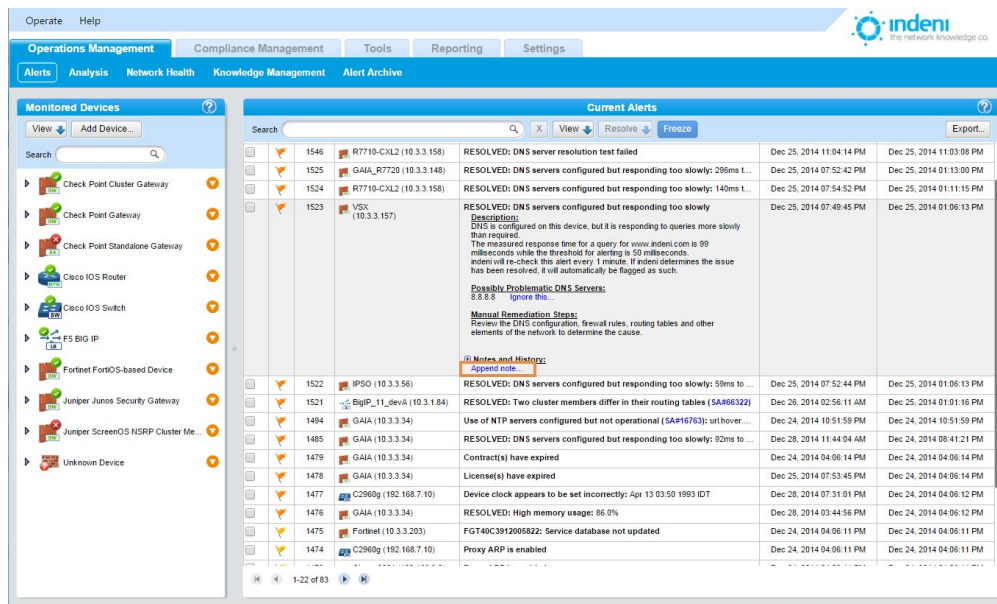
Each individual alert issued by indeni can be manually annotated by users, allowing them to communicate among themselves regarding specific alerts, as well as noting down observations and actions to be taken. indeni automatically populates the notes with major status changes of the alert such as when it was created, when it was deemed resolved, and when it was acknowledged.

Appended notes pertain solely to the alert they were added to, and not to future or other instances of the same issue in other devices. If you would like to add notes to all future alerts issued for a certain issue, add Custom Notes to the configuration of the alert.

To append a note to an alert:


1. Click on the alert to expand it.
2. Scroll to the bottom of the expanded details to **Notes and History**.
3. Click **Append note**. indeni will display a dialog box.
4. Type your note text in the box and click **Append** to save it permanently to the alert's details.

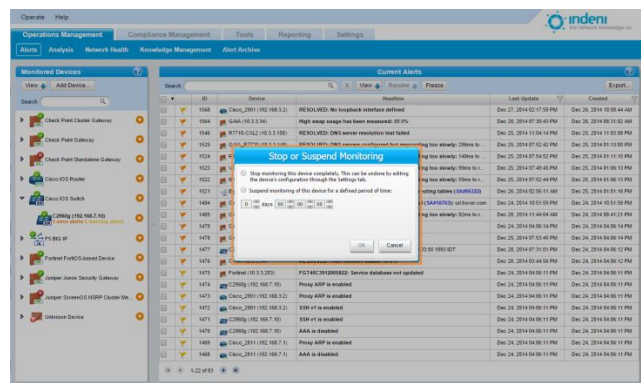
Notes pertain to the alert for an individual device; they do not appear in an identical alert for a different device.




Temporarily Disabling Analysis

If alerting is to be suspended for a period of time on a particular device, its configuration can be set so that indeni will not analyze it.

1. At the **Monitoring** tab, choose the device from the list of **Monitored Devices** on the left.
2. Click the  symbol to access the **Edit Device Configuration** menu.
3. Choose **Stop** or **Suspend Monitoring Device** from the flyout menu. The dialog box will appear as shown.



When analysis is suspended for a particular device, its status icon will change to .

Users can choose to stop analysis permanently, or suspend it for a specified period of time.

To resume analysis that has been disabled, use the **Settings** tab to adjust the device configuration in the **Monitoring Method** field. You may also use this field to set the device to **Do Not Analyze**. Save your changes. indeni will no longer analyze this device or display alerts for it.

The Analysis Tab

The Analysis tab allows users to graph certain metrics over time, view historical values and correlate the data with alerts issued by indeni.



The analysis tab allows for easy control of the data that is presented:

- At the top left, you can select the timeframe the data should be presented for.
- At the bottom left, under **Choose Parameters**, you can choose one or more parameters to display on the graph.
- At the bottom right, you may choose whether or not to show alert flags on the graph. These appear as “lollypops” at the bottom of the graph.

To export the data, use the buttons at the top right of the view.




The Network Health Tab

The Network Health tab presents a dashboard that provides an at-a-glance view of network health in real time. All data is updated continuously.

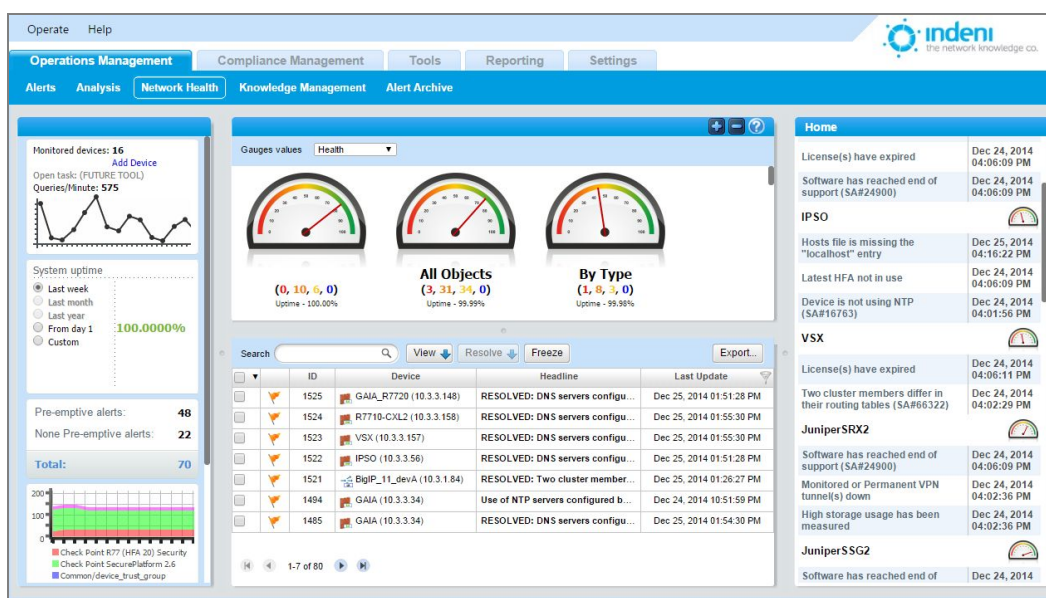
The left-hand panel of the screen for the **Network Health** tab displays information related to the entire system being analyzed: number of devices, number and type of alerts, system uptime, etc. Users can add new devices to analyze directly from this panel using the blue **Add Device** link shown. (See [Chapter 4](#) for detailed information on adding devices.)

The top central section of this screen displays a series of gauges which show the general health of an individual device or a group of devices. Using the **Gauges values** dropdown box, users can choose whether to display the Health status, CPU type, or Memory status of the individual devices or groups.

The user may also choose to customize the groups and devices shown by default on the central section.

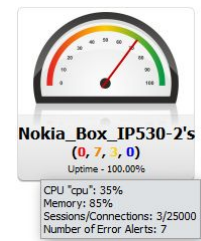
This is done by clicking on the  to add an additional group or device, or by clicking on the  and then the  symbol beside each gauge to remove it from the list.

- The “Others” group is a system group (automatically created) which appears only when indeni finds analyzed devices which are not included in other groups on the dashboard. This group disappears if the user displays devices by **All Objects** or **By Type** or if all groups and devices are accessible from other groups in the dashboard.



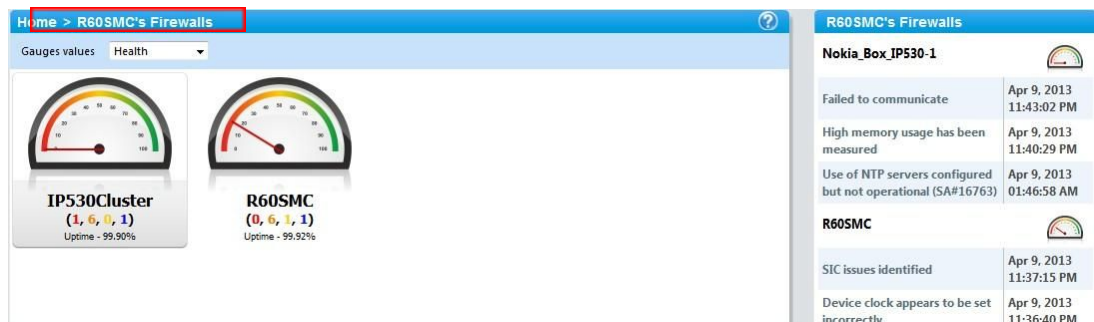
By Type groups all devices of a particular type (Check Point firewalls or Cisco Routers, for instance). Individual devices or device groups created by the user are labeled by name.

When hovering over a device or a group with a single device in it, the system displays device parameters such as: its name, CPU, memory, the number of connections, and active alerts. Below each gauge is a summary of alerts and the uptime of the device.



Clicking on any gauge changes the displayed data in the right-hand panel of the **Network Health** tab. The panel shows the top alerts associated with the selected gauge. Double-click the gauge or the status line below it to drill down into the groups/devices which are included in that group.

For example, the following screen shows the individual devices within the R60SMC's firewall group.



- Clicking on a specific device, “R60SMC,” displays its detailed status information on the right.
- Clicking “Home” returns the user to the main screen. The gauges for all selected device groups will reappear.

Note that there is a "bread crumbs" type navigation bar (highlighted) which is found above the gauges to facilitate navigation between the group levels.

Below the gauges is a real-time list of alerts flagged by indeni. By default, the system displays the most critical (red) first. There are two layers for sorting: the first alerts are sorted by severity, and then within the severity groups, they are sorted by date.

Home > All Objects

Gauges values Health

Fortigate-40C
(1, 0, 0, 0)
Uptime - 99.57%

Fortigate-40C-2
(1, 0, 0, 0)
Uptime - 99.57%

G_UNDER_CMA1
(1, 3, 0, 1)
Uptime - 99.15%

IP-390
(1, 0, 0, 0)
Uptime - 99.40%

Search: G_UNDER_CMA1 View Resolve Freeze Export...

ID	Device	Headline	Last Update
100141	G_UNDER_CMA1 (10)	Firewall is in a critical state: No firewall policy loaded, due to "...	Apr 8, 2013 02:59:09 AM
100135	G_UNDER_CMA1 (10)	Device clock appears to be set incorrectly: Oct 24 19:58 2011 +...	Apr 15, 2013 11:11:17 PM
100136	G_UNDER_CMA1 (10)	License(s) have expired	Apr 8, 2013 02:58:59 AM
100132	G_UNDER_CMA1 (10)	SecurePlatform Pro in use without a license	Apr 8, 2013 02:58:51 AM
100171	G_UNDER_CMA1 (10)	Firewall vulnerable to Sockstress TCP Denial of Service (CVE-2...	Apr 8, 2013 03:20:37 AM
100150	G_UNDER_CMA1 (10)	Device is not using DNS	Apr 8, 2013 03:19:51 AM
100137	G_UNDER_CMA1 (10)	Device is not using NTP (SA#16763)	Apr 8, 2013 02:58:58 AM

1-7 of 11

G_UNDER_CMA1

G_UNDER_CMA1

Firewall is in a critical state Apr 8, 2013 02:59:09 AM

High memory usage has been measured Apr 8, 2013 02:59:26 AM

SecurePlatform Pro in use without a license Apr 8, 2013 02:58:51 AM

This list of alerts is also found in the **Operations Management** tab.

Using Signatures in Alerts

To set how a particular alert should be managed, use the **Knowledge Management** sub-tab under **Operations Management**. The screen below lists every type of alert indeni can identify within the **Alert Categories** listed on the left side of the screen. This list is updated and expanded regularly.

The **Alert Categories** section groups alerts to make it easier for users to go straight to the type of alert they want to manage (VPN, firewall, cluster, etc.). By default, the list is expanded to show all sub-categories as well, but users can expand or collapse it as they choose.

The screenshot displays the Indeni Knowledge Management interface. The top navigation bar includes 'Operate', 'Help', and tabs for 'Operations Management', 'Compliance Management', 'Tools', 'Reporting', and 'Settings'. Below this, a sub-navigation bar shows 'Alerts', 'Analysis', 'Network Health', 'Knowledge Management' (selected), and 'Alert Archive'.

The main content area is divided into two sections:

- Alert Categories:** A tree view on the left showing various categories such as 'Device Monitoring', 'Load Balancer Monitoring', 'FS BIG-IP Monitoring', 'FS Log Lines Monitoring', 'Network Device Monitoring', 'Cisco ASA Devices Monitoring', 'Cisco IOS Devices Monitoring', 'Security Device Monitoring', 'Check Point Devices Monitoring', 'Check Point Advanced Routing', 'Check Point Cluster Monitoring', 'Check Point Firewall Monitoring', 'Check Point VSX Monitoring', 'Check Point IPS Blade or Smart...', 'Check Point Operating System M...', 'Check Point GUA-specific M...', 'Check Point IPSO-specific M...', 'Check Point Linux On Crossb...', 'Check Point SecurePlatform...', 'Check Point Performance Monito...', 'Check Point VoIP Support Monito...', 'Check Point VPN Monitoring', and 'Cluster Monitoring'.
- Alerts Within Category:** A table on the right listing specific alerts. The table has columns for 'Name', 'Default Settings for Alert', and 'Configure'. The alerts listed include:
 - A Complex Programmable Logic Device register read may intermittently fail (Sol14545)
 - A VLAN false action may not trigger for individual VLANs in a VLAN group (Sol15210)
 - A configuration may fail to load when the default network route name is an IP address (Sol14795)
 - A virtual server IP address may fail to bind to TMM (Sol14747)
 - A virtual server associated with a web acceleration profile or request logging profile may cause TMM to leak memory (Sol14591)
 - A virtual server using a web acceleration profile may cause TMM to leak memory (Sol14239)
 - A virtual server with a multi-pool Rule may be erroneously marked offline (Sol15410)
 - AAA (Authentication, Authorization, Accounting) should be Enabled
 - ARP Issues Identification
 - ARP Neighbor Overflow Identification (SAC25890)
 - Active connections may experience a long delay following failover (Sol14203)
 - Adaptive connection reaping monitoring
 - Adding a self IP address to a VLAN that is a member of a non-default route domain may fail (Sol14331)
 - An Rule may erroneously pass syntax validation (Sol15363)
 - An imported external monitor may erroneously mark resources down (Sol14271)
 - An invalid stream profile target may cause the TMM processes to restart (Sol14896)
 - Attempting to create a duplicate user account may cause the mcpd process to crash (Sol12908)
 - Auto-sync may fail in the case where there are many synchronizations in rapid succession (Sol15536)
 - BIG-IP 2000/2200 and 4000/4200 may experience slow hardware compression (Sol14831)
 - BIG-IP 6000 platforms HSB firmware may generate 'Super I/O watchdog timeout' error (Sol14081)
 - BIG-IP 8000/8500/8505 platforms HSB firmware may generate 'Super I/O watchdog timeout' error messages (Sol14082)
 - BIG-IP Analytics may cause the TMM process to crash when receiving HTTP responses with large payloads (Sol14070)
 - BIG-IP GTM sync group members running big3d 11.3.0 may experience iQuery communication issues with systems running previous versions of big3...
 - BIG-IP VIPRION blades may be marked down when using Packet Filters (Sol14215)

At the bottom of the table, there is a pagination bar showing '1-24 of 436' and a 'Save' button.

Managing the Signatures

The **Alerts Within Category** section of the **Knowledge Management** sub-tab allows users to quickly adjust settings for each type of alert.

Name: Individual alert descriptions are provided in the first column, identifying what indeni can observe. This column is informational only.

Default Settings for Alert: This allows users to choose how alerts will be flagged. Some alerts you may want to simply log; others are important enough to forward immediately to a user's attention. By default, alerts with a severity of Critical or Error are set to **SNMP+Log**; the rest are set to **Alert Only**.

The screenshot shows the Indeni Knowledge Management interface. On the left, there's a sidebar with 'Alert Categories' including Device Monitoring, Network Device Monitoring, Security Device Monitoring, and Cluster Monitoring. The main area is titled 'Alerts Within Category' and contains a table of alerts. The table has three columns: 'Name', 'Default Settings for Alert', and 'Configure'. A dropdown menu is open for the 'Default Settings for Alert' column, showing options: 'No Alert', 'Alert Only', 'Email Only', 'Alert and SNMP Trap Only', 'Alert and Email Only', 'SNMP Trap and Email Only', and 'SNMP + Email + Log'. The 'Alert Only' option is selected.

indeni will log or flag specific alerts in accordance with user preferences.

Configure

Clicking this button on the far right column opens a window where the user can individually configure alert settings for every currently analyzed device on the network. This includes setting a default configuration for this particular alert that will apply to every new object added to the network.

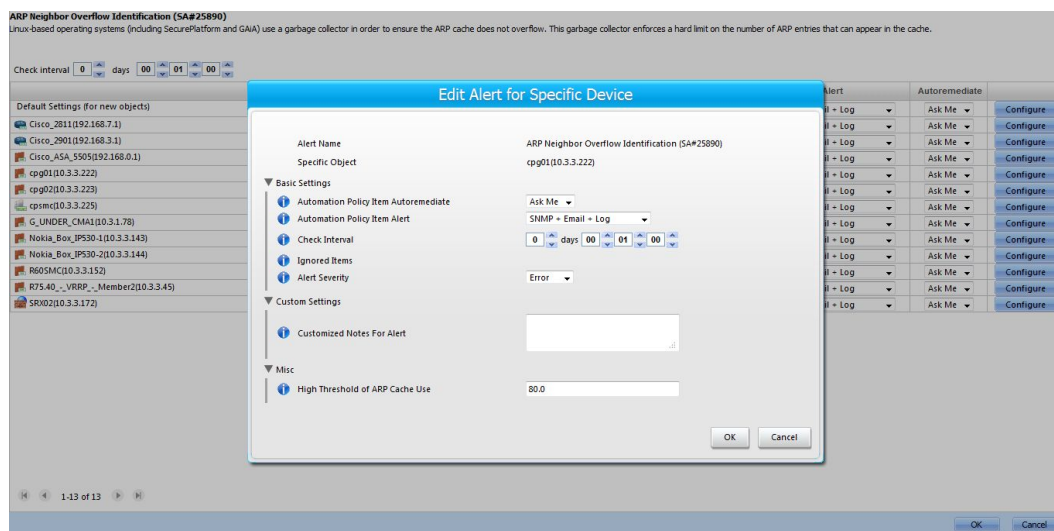
The screenshot shows the 'ARP Issues Identification' configuration window. At the top, there's a description: 'Some operating systems will report how many failures of ARP requests they are encountering. indeni will alert if a device whose ARP entry was known is now unknown - possibly indicating an issue with ARP traffic.' Below this, there's a 'Check interval' set to 0 days, 00 hours, 01 minute, and 00 seconds. The main table has columns for 'Name', 'Alert', and 'Autoremediate'. The 'Alert' column has a dropdown menu with options: 'Alert Only', 'Ask Me', and 'Configure'. The 'Autoremediate' column has a dropdown menu with options: 'Ask Me' and 'Configure'. The 'Alert Only' option is selected for the 'Alert' column.

Check Interval:

Each check that indeni runs has a different interval set by default. These may be adjusted in this screen for the entire group of devices.

Configure:

The **Default Settings** are shown for all new objects. However, you can also individually configure each device by clicking its **Configure** button to open the **Edit Alert for Specific Device** window.



All devices have the same configuration options per alert; however, the various alerts have different parameters to be configured for this window.

Note that indeni allows users to add customized notes here for all alerts. These can include additional information which system architects and administrators would like to present as part of indeni's alerting.

Select **OK** or **Apply** to save your changes, or **Cancel** to return to the **Configuration** screen.

Alert Archive

indeni stores all resolved alerts. These are placed under **Current Alerts** until they are acknowledged. To review alerts acknowledged in the **Alerts** sub tab, use the **Alert Archive** sub-tab under **Operations Management**.

Sort or filter alerts by using the arrow or filter icons in the **Last Update** column header.

1. Click the **Filter** icon in the column header.
2. Click inside each blank field box to display a calendar.
3. Choose the date range for the alerts you want to display and then click on **Apply**. To filter within a particular day, change the hour settings after the date in both the **From** and **Till** fields to display alerts within a specified time range. (See **Last Update** under [Columns and Functionality](#) in this chapter for more detail.)

Operate Help		indeni the network knowledge co.			
Operations Management		Compliance Management	Tools	Reporting	Settings
Alerts	Analysis	Network Health	Knowledge Management	Alert Archive	
ID	Device	Headline	Last Update		Created
1476	GAIA (10.3.3.34)	RESOLVED: High memory usage: 86.0%	Dec 28, 2014 07:43:21 PM		Dec 24, 2014 04:06:12 PM
1521	BqIP_11_devA (10.3.1.84)	RESOLVED: Two cluster members differ in their routing tables (SA#66322)	Dec 28, 2014 07:43:21 PM		Dec 25, 2014 01:01:16 PM
1469	Cisco_2811 (192.168.7.1)	Proxy ARP is enabled	Dec 28, 2014 07:43:21 PM		Dec 24, 2014 04:06:11 PM
1484	GAIA (10.3.3.34)	Use of NTP servers configured but not operational (SA#16763): url:over.com	Dec 28, 2014 07:43:21 PM		Dec 24, 2014 10:51:59 PM
1468	Cisco_2811 (192.168.7.1)	AAA is disabled	Dec 28, 2014 07:43:21 PM		Dec 24, 2014 04:06:11 PM
1474	C2960g (192.168.7.10)	Proxy ARP is enabled	Dec 28, 2014 07:43:21 PM		Dec 24, 2014 04:06:11 PM
1522	IPSO (10.3.3.56)	RESOLVED: DNS servers configured but responding too slowly: 59ms to resolve www.indeni.com	Dec 28, 2014 07:43:21 PM		Dec 25, 2014 01:06:13 PM
1477	C2960g (192.168.7.10)	Device clock appears to be set incorrectly: Apr 13 04:00 1993 EDT	Dec 28, 2014 07:43:21 PM		Dec 24, 2014 04:06:12 PM
1524	R7710-CXL2 (10.3.3.158)	RESOLVED: DNS servers configured but responding too slowly: 140ms to resolve www.indeni.com	Dec 28, 2014 07:43:21 PM		Dec 25, 2014 01:11:15 PM
1485	GAIA (10.3.3.34)	RESOLVED: DNS servers configured but responding too slowly: 52ms to resolve www.indeni.com	Dec 28, 2014 07:43:21 PM		Dec 24, 2014 08:41:21 PM
1546	R7710-CXL2 (10.3.3.158)	RESOLVED: DNS server resolution test failed	Dec 28, 2014 07:43:21 PM		Dec 25, 2014 11:03:08 PM
1525	GAIA_R7720 (10.3.3.148)	RESOLVED: DNS servers configured but responding too slowly: 206ms to resolve www.indeni.com	Dec 28, 2014 07:43:21 PM		Dec 25, 2014 01:13:00 PM
1473	Cisco_2901 (192.168.3.2)	Proxy ARP is enabled	Dec 28, 2014 07:43:21 PM		Dec 24, 2014 04:06:11 PM
1479	GAIA (10.3.3.34)	Contract(s) have expired	Dec 28, 2014 07:43:21 PM		Dec 24, 2014 04:06:14 PM
1472	Cisco_2901 (192.168.3.2)	SSH vt is enabled	Dec 28, 2014 07:43:21 PM		Dec 24, 2014 04:06:11 PM
1568	Cisco_2901 (192.168.3.2)	RESOLVED: No loopback interface defined	Dec 28, 2014 07:43:21 PM		Dec 26, 2014 10:00:44 AM
1523	V5X (10.3.3.157)	RESOLVED: DNS servers configured but responding too slowly: 89ms to resolve www.indeni.com	Dec 28, 2014 07:43:21 PM		Dec 25, 2014 01:06:13 PM
1478	GAIA (10.3.3.34)	License(s) have expired	Dec 28, 2014 07:43:21 PM		Dec 24, 2014 04:06:14 PM
1564	GAIA (10.3.3.34)	High swap usage has been measured: 80.89%	Dec 28, 2014 07:43:21 PM		Dec 26, 2014 08:31:02 AM
1470	C2960g (192.168.7.10)	AAA is disabled	Dec 28, 2014 07:43:21 PM		Dec 24, 2014 04:06:11 PM
1471	C2960g (192.168.7.10)	SSH vt is enabled	Dec 28, 2014 07:43:21 PM		Dec 24, 2014 04:06:11 PM
1475	Fortinet (10.3.3.203)	FGT40C3912005822: Service database not updated	Dec 28, 2014 07:43:21 PM		Dec 24, 2014 04:06:11 PM
1651	Cisco_2811 (192.168.7.1)	RESOLVED: Failed to communicate: No response on port: 22	Dec 28, 2014 06:20:42 PM		Dec 28, 2014 06:19:45 PM
1650	Cisco_2901 (192.168.3.2)	RESOLVED: Failed to communicate: Session is closed	Dec 28, 2014 06:11:37 PM		Dec 28, 2014 06:11:36 PM
1649	Cisco_2811 (192.168.7.1)	RESOLVED: Failed to communicate: No response on port: 22	Dec 28, 2014 06:06:35 PM		Dec 28, 2014 06:05:37 PM

1-25 of 877

CHAPTER 6: COMPLIANCE MANAGEMENT

Configuration Checks

indeni allows users to create baseline settings. Configurations are validated through the use of device profiles. Use this feature to define a profile that states what configurations should be set on a device, and then on which devices to apply the profile.

The system will constantly verify that each device in the profile complies with the profile or profiles assigned to it. Individual devices can have multiple profiles assigned to them.

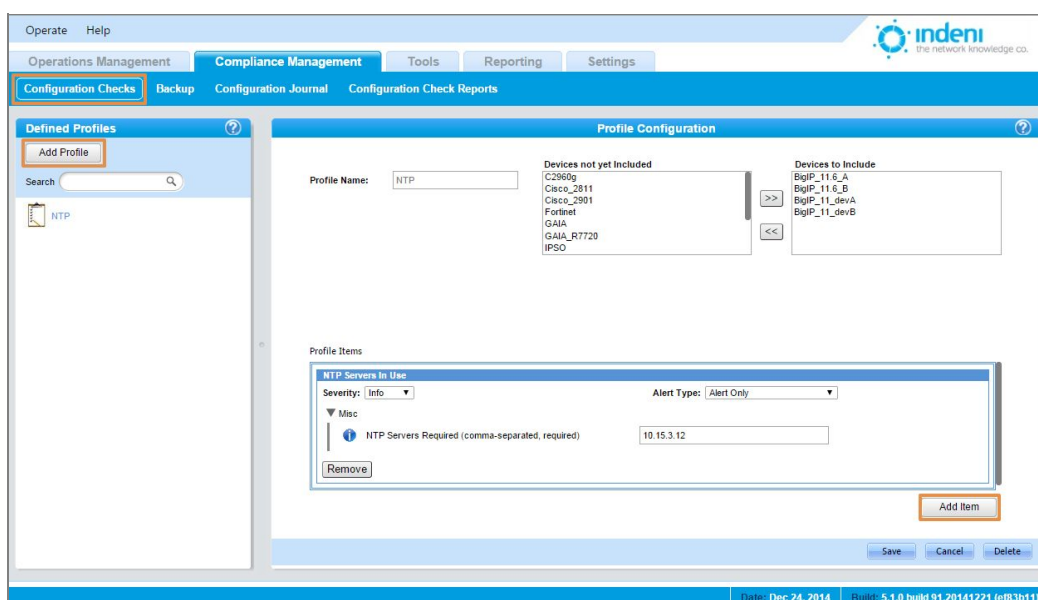
If indeni finds that a device is not in compliance with a profile, the system will issue an alert for each violation. This alert will appear in the **Current Alerts** list on the **Alerts** tab and also in the **Configuration Check Report** in the **Compliance Management** tab.

To access the Device Profiles settings:

1. Click on the **Compliance Management** tab.
2. Select the **Configuration Checks** sub-tab.

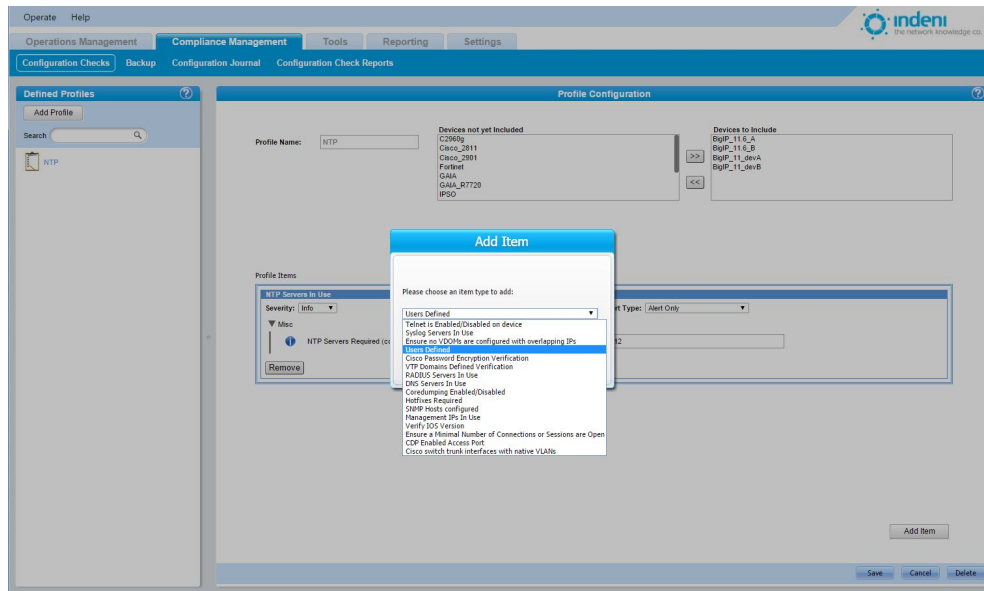
Adding a Profile

1. Add profiles using the **Add Profile** button on the left. You can add as many profiles as you wish.
2. For each profile, choose the devices you want to manage from the **Devices Not Yet Included** list on the right side of the screen under **Profile Configuration**.
3. Click the double right arrow to include the chosen device(s) for this profile.
4. Give the device profile an appropriate name in the **Profile Name** field.



To add an item to the devices to be included in the profile:

1. Click the **Add Item** button in the bottom right corner of the **Device Profiles** sub-tab screen. indeni will display the **Profile Items** dialog box, that allows users to choose which configurations to have validated, checked, and alerted in this profile.



2. Choose the item type. See the next section, **Using Item Types**, for specific information on each selection.
3. Click **OK**.
4. You may add as many items as you want. For each item, configure the settings in the **Profile Items** dialog box.
5. Once you are done configuring the profile, click **Save**.

Using Item Types

By assigning any or all of the item types in **Device Profile**, you give indeni the necessary information to validate, check, and alert if the status of a device is not according to the profile. indeni continuously analyzes the configuration profile on those devices and reports violations as an alert to system administrators.

Below you will find a few examples of items that can be enforced via a profile. For each example, we show a **Profile Item** configuration and then the resulting message that appears in alerts for affected devices under the **Alerts** tab. *Note that in each alert a reference is made to the device profile by name.*

Hotfix(es) Installed

Specific issues addressed by hotfixes are available. indeni alerts if the required hotfix has not been installed.

Hotfix(es) Installed

Severity: Warn Alert Type: SNMP + Email + Log

Basic Settings

Misc

Hotfix Required (required) HOTFIX_R71_10

Remove

		100251	R60SMC (10.3.3.152)	<p>Some hotfixes which should be installed are not</p> <p>Description: As part of the verification of the device profile "Profile-2", indeni checks that the hotfixes installed on the device match the requirement. indeni has found that some hotfixes are missing. These are listed below. indeni will re-check this alert every 5 minutes. If indeni will determine the issue has been resolved it will automatically be flagged as such.</p> <p>Missing Hotfixes: HOTFIX_R71_10 Ignore this...</p> <p>Manual Remediation Steps: Install the missing hotfixes as required by the device profile.</p>
--	--	--------	------------------------	---

NTP Servers In Use

The **Device Profile** will check that the specific NTP servers which are listed are the ones being used by the devices in the profile.

NTP Servers In Use

Severity: Error Alert Type: Alert Only

Basic Settings

Custom Settings

Misc

NTP Servers Required (comma-separated, required) 192.168.7.1

Remove

		100360	Cisco_2811 (192.168.7.1)	<p>Some NTP servers which should be defined are not</p> <p>Description: As part of the verification of the device profile "Profile-4", indeni checks that the NTP servers configured on the device match the requirement. indeni has found that some NTP servers are missing. These are listed below. indeni will re-check this alert every 5 minutes. If indeni will determine the issue has been resolved it will automatically be flagged as such.</p> <p>Missing Servers: 192.168.7.1 Ignore this...</p> <p>Manual Remediation Steps: Modify the device's configuration as required by the device profile.</p>
--	--	--------	-----------------------------	---

Users Defined

If you want to ensure there are no unexpected users defined on your devices, this item type will enable that.

Users Defined

Severity: Error Alert Type: Alert Only

Basic Settings

Automation Policy Item Autoremediate Ask Me

Custom Settings

Misc

Users Required (comma-separated, required) User-1, User-2

Remove

<input type="checkbox"/>		100280	 cpg01 (10.3.3.222)	<p>Users defined do not match expected list</p> <p>Description: As part of the verification of the device profile "Profile-1", indeni checks that the users defined on the device match the requirement. 1 users are defined and shouldn't be. These are listed below. indeni will re-check this alert every 5 minutes. If indeni will determine the issue has been resolved it will automatically be flagged as such.</p> <p>Missing or Un-needed Users: + hacker Ignore this...</p> <p>Manual Remediation Steps: Modify the device's configuration as required by the device profile.</p>
--------------------------	---	--------	---	---

Syslog Servers In Use

indeni will check that a specific Syslog server is being used by the devices in the profile.

Syslog Servers In Use

Severity: Critical

Alert Type: SNMP + Email + Log

Basic Settings

Misc



Syslog Server Hostname or IP (required)

10.3.3.75

Minimal Severity

All

Remove

<input type="checkbox"/>		100352	 cpsmc (10.3.3.225)	<p>Some syslog servers which should be defined are not</p> <p>Description: As part of the verification of the device profile "Profile-4", indeni checks that the syslog servers configured on the device match the requirement. indeni has found that some syslog servers are missing or misconfigured. These are listed below. indeni will re-check this alert every 5 minutes. If indeni will determine the issue has been resolved it will automatically be flagged as such.</p> <p>Missing or Misconfigured Servers: 10.3.3.75 with minimal severity of All Ignore this...</p> <p>Manual Remediation Steps: Modify the device's configuration as required by the device profile.</p>
--------------------------	---	--------	---	--

RADIUS Servers In Use

indeni will check that a specific RADIUS server is being used by the devices in the profile.

RADIUS Servers In Use

Severity: Critical Alert Type: SNMP + Email + Log

Basic Settings

Automation Policy Item Autoremediate Ask Me

Misc

RADIUS Server Hostname or IP (required)

Timeout

Secret

Remove

<input type="checkbox"/>		100275	cpg02 (10.3.3.223)	<p>Some RADIUS servers which should be defined are not</p> <p>Description: As part of the verification of the device profile "Profile-1", indeni checks that the RADIUS servers configured on the device match the requirement. indeni has found that some RADIUS servers are missing or misconfigured. These are listed below. indeni will re-check this alert every 5 minutes. If indeni will determine the issue has been resolved it will automatically be flagged as such.</p> <p>Missing or Misconfigured Servers: 1.2.3.4 with timeout of 0 with secret</p> <p>Manual Remediation Steps: Modify the device's configuration as required by the device profile.</p>
--------------------------	--	--------	-----------------------	--

Ensure a Minimal Number of Connections or Sessions are Open

The profile can flag a device that suddenly reports less than a set number of connections or sessions, which can occur when the device has been circumvented by other network equipment. This item will alert when this happens.

Ensure a Minimal Number of Connections or Sessions are Open

Severity: Error Alert Type: Alert and Email Only

Basic Settings

Automation Policy Item Autoremediate Never

Custom Settings

Customized Notes For Alert

Misc

Low Threshold of Number of Connections/Sessions (required)

Remove

<input type="checkbox"/>		100291	Nokia_Box_IP530-2 (10.3.3.144)	<p>Number of connections or sessions is lower than the set minimum</p> <p>Description: There are 4 concurrent connections or sessions which is less than the set minimum of 5 as defined in the device profile Profile-1. indeni will re-check this alert every 1 minute. If indeni will determine the issue has been resolved it will automatically be flagged as such.</p> <p>Manual Remediation Steps: This may be a result of a change in network topology or a limiting firewall policy. Please inspect the surrounding network equipment and its configuration to determine the cause of the problem.</p>
--------------------------	--	--------	-----------------------------------	--

DNS Servers In Use

indeni will check that the DNS server is being used by the devices in the profile.

DNS Servers In Use

Severity: Error

Alert Type: Alert and SNMP Trap Only

▼ Basic Settings

Automation Policy Item Autoremediate

Ask Me

▼ Custom Settings



Customized Notes For Alert

▼ Misc

DNS Servers Required (comma-separated, required)

23.21.4.56,1.2.3.4

Remove

<input type="checkbox"/>		100308	 cpg01 (10.3.3.222)	<p>Some DNS servers which should be defined are not</p> <p>Description: As part of the verification of the device profile "Profile-4", indeni checks that the DNS servers configured on the device match the requirement. indeni has found that some DNS servers are missing. These are listed below. indeni will re-check this alert every 5 minutes. If indeni will determine the issue has been resolved it will automatically be flagged as such.</p> <p>Missing Servers: 23.21.4.56 Ignore this... 1.2.3.4 Ignore this...</p> <p>Manual Remediation Steps: Modify the device's configuration as required by the device profile.</p>
--------------------------	---	--------	---	--

Core dumping Enabled/Disabled

When core dump files are created on the device, it may hint that certain processes have failed recently. If this item type is enabled, indeni will validate that core dumping is actually enabled on the analyzed device in the profile.

Coredumping Enabled/Disabled

Severity: Critical

Alert Type: Alert and SNMP Trap Only

▼ Basic Settings

Automation Policy Item Autoremediate

Ask Me

▼ Custom Settings

Customized Notes For Alert



Back up the media.

▼ Misc

Should Core Dumping Be Enabled

☒

Remove

<input type="checkbox"/>		100292	 cpg02 (10.3.3.223)	<p>Coredumping setting not as desired</p> <p>Description: As part of the verification of the device profile "Profile-1", indeni checks that coredumping is enabled. On this device coredumping is disabled. indeni will re-check this alert every 5 minutes. If indeni will determine the issue has been resolved it will automatically be flagged as such.</p> <p>Custom Notes: Back up the media.</p> <p>Manual Remediation Steps: Follow SK53363.</p>
--------------------------	---	--------	---	--

Deleting an Item from the Profile

- Click the **Remove** button at the bottom of the item's configuration section. You may have to scroll down to see the button.



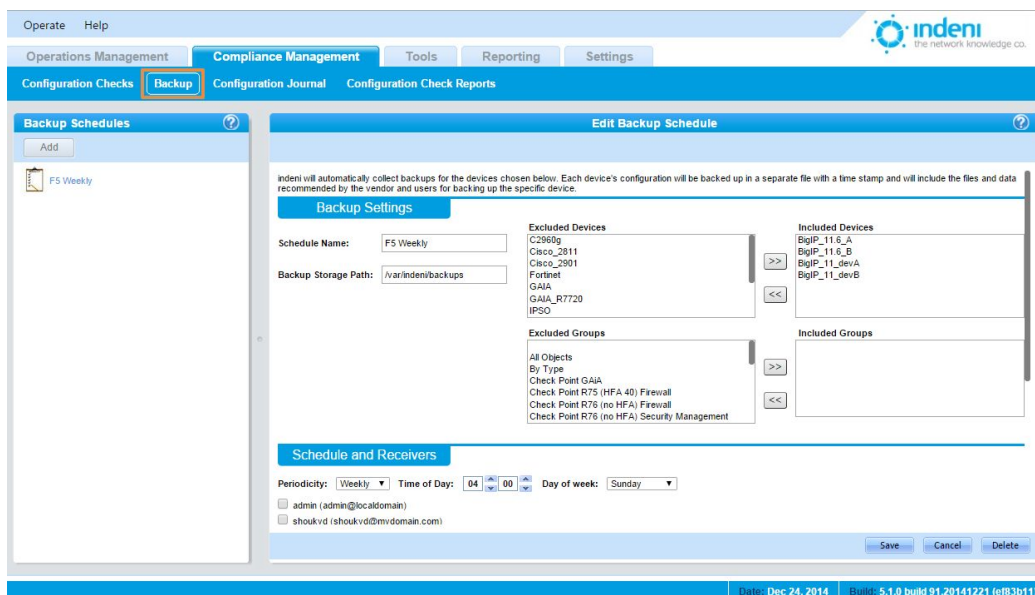
Deleting a Profile

To delete the entire device profile:

- Click the **Delete** button at the bottom of the **Profile Configuration** screen.

Backup Schedules

indeni can be set to automatically collect backup data for specified devices or groups of devices. Each device's configuration will be backed up in a separate file that includes the files and data that should be included in the backup, as recommended by the vendor and according to best practices.



Scheduling Backups

Backups can be scheduled for individual devices. You can also add a Group to the backup schedule.

- From the **Compliance Management** tab, select the **Backups** sub-tab.
- Click on the **New Backup** icon in the left panel. Use the backup settings under **Edit Backup Schedules** on the right to provide a **Schedule Name**.

3. In the **Backup Storage Path** field, provide the path where these backup files will be stored (this may be either on the indeni machine or on a remote location).
4. Choose the devices or groups you wish to back up from the **Excluded Devices/Groups** list. Use the double arrow buttons to add or remove devices in the **Included Devices/Groups** list.
5. In the **Schedules and Receivers** portion of the screen, set the time of day you want the backups to run. By default, the backups will be saved daily.
6. Choose the users who will receive notification of backups and their success or failure.
7. If desired, use the **Backup Details** field to add further instructions for use of this backup file. It will be saved as a README text file in the backup archive.

Additional Files or Directories can be backed up by providing their paths - one path in each line.



8. Click **Save** to save the new backup schedule, or **Delete** to remove it from the list.

Adding Additional Backup Schedules

1. Click the **Add** button in the left panel. A **New Schedule** will appear in the **Backup Schedules** list on the left.
2. Click on the **New Schedule** icon.
3. Follow steps 2-8 as shown in the previous section.

Configuration Journal (change tracking)

In the **Compliance Management** tab select the **Configuration Journal** sub-tab. This functionality aggregates and displays all of the changes users have made to analyzed devices, time stamped and listed by the most recent, to enable a single at-a-glance listing.

The columns include the following data:

ID: Device ID

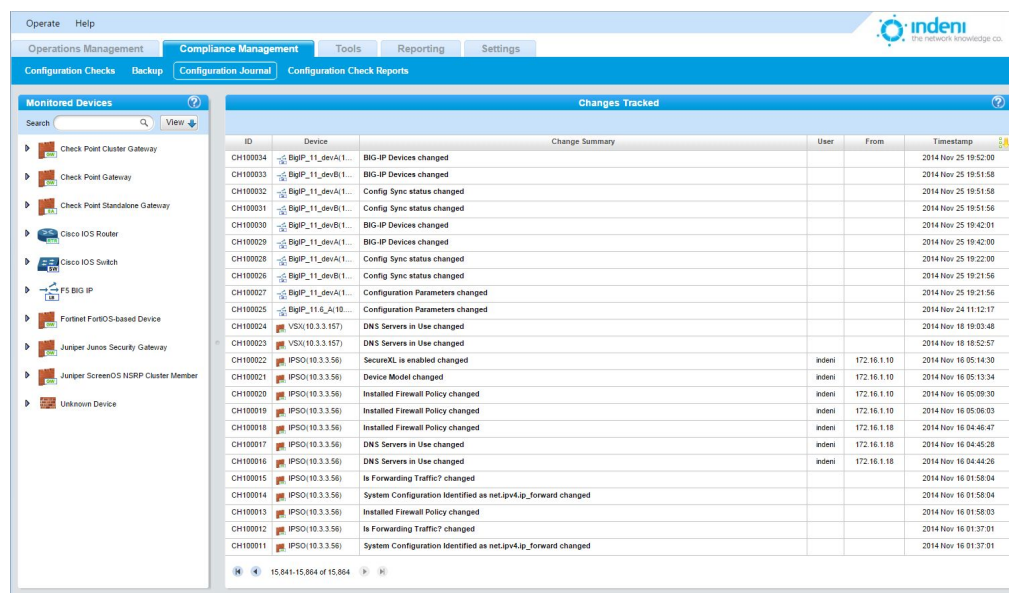
Device: Device name and IP number

Change Summary: All changes made to analyzed devices are displayed here. To access details for each change, click on each individual line to expand it. Click again to collapse it. The summary includes the exact details of the changes that were made.

User: Displays the user who made the change.

From: Displays the IP of the user who made the change.

Timestamp: The most recent changes are displayed first.



The screenshot shows the Indeni Configuration Journal interface. On the left is a sidebar with 'Monitored Devices' including categories like Check Point, Cisco, and Fortinet. The main area is titled 'Changes Tracked' and contains a table with the following columns: ID, Device, Change Summary, User, From, and Timestamp. The table lists various configuration changes such as 'BIG-IP Devices changed', 'Config Sync status changed', and 'DNS Servers in Use changed' with corresponding timestamps and user information.

ID	Device	Change Summary	User	From	Timestamp
CH100034	BIG-IP_11_devA/1...	BIG-IP Devices changed			2014 Nov 25 19:52:00
CH100033	BIG-IP_11_devB/1...	BIG-IP Devices changed			2014 Nov 25 19:51:58
CH100032	BIG-IP_11_devA/1...	Config Sync status changed			2014 Nov 25 19:51:58
CH100031	BIG-IP_11_devB/1...	Config Sync status changed			2014 Nov 25 19:51:56
CH100030	BIG-IP_11_devA/1...	BIG-IP Devices changed			2014 Nov 25 19:42:01
CH100029	BIG-IP_11_devA/1...	BIG-IP Devices changed			2014 Nov 25 19:42:00
CH100028	BIG-IP_11_devB/1...	Config Sync status changed			2014 Nov 25 19:22:00
CH100026	BIG-IP_11_devB/1...	Config Sync status changed			2014 Nov 25 19:21:56
CH100027	BIG-IP_11_devA/1...	Configuration Parameters changed			2014 Nov 25 19:21:56
CH100025	BIG-IP_11_devA/10...	Configuration Parameters changed			2014 Nov 24 11:12:17
CH100024	VSO(10.3.3.157)	DNS Servers in Use changed			2014 Nov 18 10:03:48
CH100023	VSO(10.3.3.157)	DNS Servers in Use changed			2014 Nov 18 10:52:57
CH100022	IPSO(10.3.3.56)	SecureXL is enabled changed	indeni	172.16.1.10	2014 Nov 16 05:14:30
CH100021	IPSO(10.3.3.56)	Device Model changed	indeni	172.16.1.10	2014 Nov 16 05:13:34
CH100020	IPSO(10.3.3.56)	Installed Firewall Policy changed	indeni	172.16.1.10	2014 Nov 16 05:09:30
CH100019	IPSO(10.3.3.56)	Installed Firewall Policy changed	indeni	172.16.1.10	2014 Nov 16 05:06:03
CH100018	IPSO(10.3.3.56)	Installed Firewall Policy changed	indeni	172.16.1.10	2014 Nov 16 04:46:47
CH100017	IPSO(10.3.3.56)	DNS Servers in Use changed	indeni	172.16.1.10	2014 Nov 16 04:45:28
CH100016	IPSO(10.3.3.56)	DNS Servers in Use changed	indeni	172.16.1.10	2014 Nov 16 04:44:26
CH100015	IPSO(10.3.3.56)	Is Forwarding Traffic? changed			2014 Nov 16 01:58:04
CH100014	IPSO(10.3.3.56)	System Configuration Identified as net.ipv4.ip_forward changed			2014 Nov 16 01:58:04
CH100013	IPSO(10.3.3.56)	Installed Firewall Policy changed			2014 Nov 16 01:58:03
CH100012	IPSO(10.3.3.56)	Is Forwarding Traffic? changed			2014 Nov 16 01:37:01
CH100011	IPSO(10.3.3.56)	System Configuration Identified as net.ipv4.ip_forward changed			2014 Nov 16 01:37:01

Configuration Check Reports

This report provides a detailed report of all devices that do not comply with the device profile set for that device.

1. Select the **Configuration Check Reports** sub-tab at the top of the screen.
2. Click the **Add Schedule** button in the **Defined Schedules** list.

3. A **New Report** icon will appear under **Defined Schedules**. Edit the details under **Scheduled Report Configuration** on the right:
4. Give the report a new name in the **Report Name** field.
5. Choose the devices to be included in the report from the **Excluded Devices** list and click the double arrow to add them to the **Included Devices** list.
6. You can generate the report right away by clicking on the **Create Immediately** button; otherwise, go to step 7.
7. Set the time indeni will generate and deliver the report in **Schedule and Receivers**. All alerts generated since the previous report will be included, as well as any updates to previously reported alerts.
8. Select the users to receive the report. indeni provides a list of all system users. These users will receive reports only for those devices they are allowed to see, even if the original report was set to include all devices being analyzed.
9. **Save** your changes.

CHAPTER 7: TOOLS

The **Tools** tab allows quick access to indeni's debugging tools and a debug report generator to pinpoint errors and obtain details for the analyzed devices listed in the left panel under **Debuggable Objects**. (*Debug the indeni software from the **Help** menu.*)

The **Object Debug Panel** on the right changes according to the type of device selected for debugging.

Search

With the **Search** pane, indeni users are now able to search for configurations, settings and other parameters on all analyzed devices. This tool allows free text search for things like NIC settings, patches and hotfixes, software versions, licenses, users, etc. The outcome of the search provides all the relevant results structured in a table, which can be printed.

1. Click on the **Tools** tab.
2. Select the **Search** sub-tab. Enter the relevant text in the search field and press the **Explore!** button on the right.
3. indeni will then automatically search for any parameters that meet the search criteria. Once this ends, the results will be displayed in a table.
4. Click the printer icon on the top right of the table to print results.

The screenshot shows the indeni web interface with the **Tools** tab selected and the **Search** sub-tab active. A search box contains the text 'eth0' and an **Explore!** button is to its right. Below the search box is a table with two columns: **Device Name** and **Result**. The table contains several rows of search results for the 'eth0' interface across different devices.

Device Name	Result
Name: Bgp_116_A IP: 10.3.3.134	Static Routes: 127.1.0.0/24 via tunnel 127.3.0.0/24 via mgmt_bp 192.168.3.0/24 via external 10.3.1.0/24 via internal 10.3.3.0/24 via HA 127.7.0.0/16 via tunnel 127.1.1.254 0.0.0.0/0 via external 192.168.3.1 0.0.0.0/0 via eth0 10.3.3.1
Name: Bgp_11_devA IP: 10.3.1.64	Static Routes: 19.20.21.0/27 via internal 127.1.1.0/24 via tunnel 127.3.0.0/24 via mgmt_bp 192.168.3.0/24 via external 10.0.133.0/24 via HA 10.3.1.0/24 via eth0 10.3.3.0/24 via internal 0.0.0.0/0 via external 192.168.3.1 0.0.0.0/0 via eth0 10.3.1.1
Name: Bgp_11_devB IP: 10.3.1.65	Static Routes: 127.1.0.0/24 via tunnel 127.3.0.0/24 via mgmt_bp 192.168.3.0/24 via external 10.0.133.0/24 via HA 10.3.1.0/24 via eth0 10.3.3.0/24 via internal 0.0.0.0/0 via external 192.168.3.1 0.0.0.0/0 via eth0 10.3.1.1
Name: GAAA IP: 10.3.3.34	Working ARP Entries: 7 (10.3.3.1) at 00:50:56:80:07:78 [ether] on eth0 ? (10.3.3.100) at 00:50:56:80:58:F6 [ether] on eth0 ? (10.3.3.123) at 00:50:56:80:27:DC [ether] on eth0 ? (10.3.3.154) at 00:50:56:80:25:22 [ether] on eth0 ? (10.3.3.38) a 1 00:50:56:80:58:F6 [ether] on eth0 ? (10.3.3.40) at 00:50:56:80:25:DC [ether] on eth0 ? (10.3.3.80) at 00:50:56:80:01:25 [ether] on eth0 Static Routes: 0.0.0.0/0 via eth0 10.3.3.1 10.3.3.0/24 via eth0 10.168.10.0/24 via eth0 10.255.2.0/24 via eth0 Network Interfaces: eth0 (Bandwidth: 1000Mbit, MAC Address: 00:50:56:80:25:E6, IP Address: 10.3.3.34/24) Network Interface eth0/2: eth0/2 (MAC Address: 00:10:00:00:00:00) Working ARP Entries: 10 (10.3.3.1) 00:50:56:80:07:78 [ether] on eth0/2 VLD 813 0 0 0 10.3.3.32 00:50:56:80:37:42 [ether] on eth0/2 VLD 14 0 0 0 10.3.3.33 00:50:56:80:30:48 [ether] on eth0/2 VLD 12 0 0 0 10.3.3.36 00:50:56:80:37:42 [ether] on eth0/2 VLD 1193 0 0 10.3.3.68 00:50:56:80:12C [ether] on eth0/2 VLD 1185 1 0 1 10.3.3.100 00:50:56:80:58:F6 [ether] on eth0/2 VLD 1137 0 0 0 10.3.3.123 00:50:56:80:27:DC [ether] on eth0/2 VLD 347 0 0 1 10.3.3.154 00:50:56:80:25:22 [ether] on eth0/2 VLD 959 0 0 1 10.3.3.159 00:50:56:80:58:F6 [ether] on eth0/2 VLD 151 1 0 0 10.3.3.222 00:50:56:80:25:DC [ether] on eth0/2 VLD 44 0 0 0 10.3.3.223 00:50:56:80:07:78 [ether] on eth0/2 VLD 44 0 0 0 10.3.3.224 00:50:56:80:25:DC [ether] on eth0/2 VLD 116 0 0 0 Network Interface eth0/3: eth0/3 (Bandwidth: 1000Mbit, MAC Address: 28:c3:da:c3:6180) Static Routes: 0.0.0.0/0 via eth0 10.3.3.1 1.1.0/24 via eth0 10.3.3.0/24 via eth0 192.168.1.0/24 via bgpgrp Network Interfaces: eth0/1 eth0/2 eth0/3 eth0/4 eth0/5 Network Interface eth0/1: eth0/1 (MAC Address: 00:10:00:00:00:00, IP Address: 1.1.1.0/24) Network Interface eth0/2: eth0/2 (Bandwidth: 1000Mbit, MAC Address: 28:c3:da:c3:6180, IP Address: 10.3.3.161/24) Network Interface eth0/3: eth0/3 (Bandwidth: 1000Mbit, MAC Address: 28:c3:da:c3:6180) Network Interface eth0/5: eth0/5 (Bandwidth: 1000Mbit, MAC Address: 00:10:00:00:00:00) Working ARP Entries: 7 (10.3.3.1) at 00:50:56:80:07:78 [ether] on eth0 ? (10.3.3.1) at 00:50:56:80:07:78 [ether] on eth0 ? (10.3.3.100) at 00:50:56:80:58:F6 [ether] on eth0 ? (10.3.3.123) at 00:50:56:80:27:DC [ether] on eth0 ? (10.3.3.130) at 00:50:56:80:25:22 [ether] on eth0 ? (10.3.3.140) at 00:50:56:80:01:05 [ether] on eth0 ? (10.3.3.140) at 00:50:56:80:50:03 [ether] on eth0 ? (10.3.3.154) at 00:50:56:80:25:22 [ether] on eth0 ? (10.3.3.159) at 00:50:56:80:40:48 [ether] on eth0 ? (10.3.3.222) at 00:50:56:80:62:E4 [ether] on eth0 ? (10.3.3.224) at 00:50:56:80:62:E4 [ether] on eth0 ? (10.3.3.331) at 00:50:56:80:66:3A [ether] on eth0 ? (10.3.3.36) at 00:50:56:80:37:42 [ether] on eth0
Name: JurgessSG-1 IP: 10.3.3.161	
Name: IP90	

Live Configuration

Live Configuration allows indeni users to quickly and simply access all the configurations and settings on their analyzed devices.

1. Click on the Tools tab.
2. Select the Live Configuration sub-tab.
3. Choose a specific device from the list on the left side of the screen.

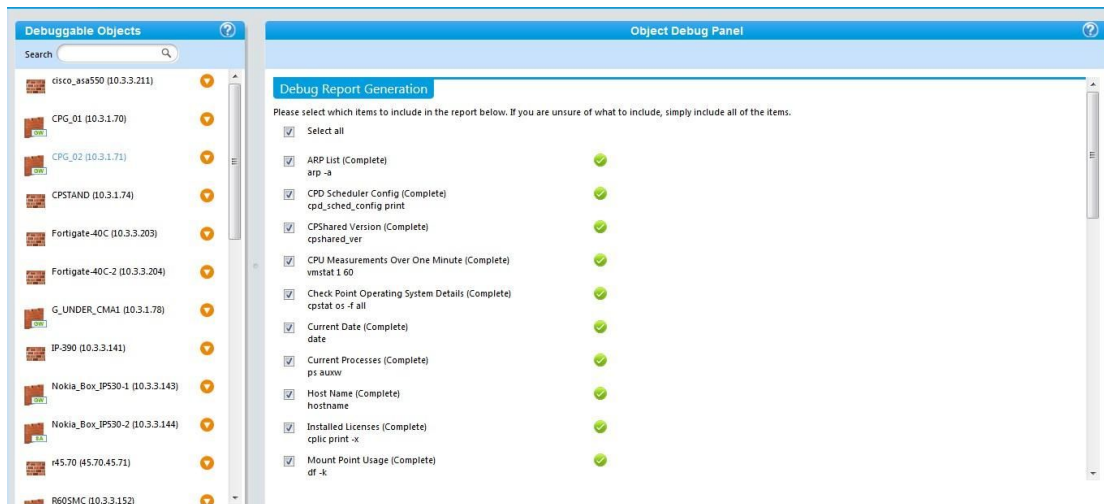
indeni will display in a table format all the configuration details of the particular device, once this device has been chosen from the list.

You can use the search field in the left panel to find specific devices either by IP or by device name.

The screenshot displays the indeni web interface. The top navigation bar includes 'Operate', 'Help', 'Operations Management', 'Compliance Management', 'Tools' (selected), 'Reporting', and 'Settings'. Below this, the 'Tools' section has 'Live Configuration' (selected) and 'Troubleshooting' tabs. On the left, the 'Monitored Devices' panel shows a search bar and a list of devices including Check Point Cluster Gateway, Check Point Gateway, Check Point Standalone Gateway, GAIA (10.3.3.34), GAIA_R7720 (10.3.3.148), Cisco IOS Router, Cisco IOS Switch, PS BIG IP, Fortinet FortiOS-based Device, Juniper Junos Security Gateway, Juniper ScreenOS NSRP Cluster Member, and Unknown Device. The main 'Live Configuration' panel shows details for the selected device, GAIA (10.3.3.34). The details are organized into sections: 'Is a Virtual Machine' (Yes), 'Device Model' (Product Name: VMware Virtual Platform Product Name: 440BX Desktop Reference Platform Warning: Can't find :CPSP-COMP-U in cp_macros. License version might be not compatible. Warning: Can't find :cpnb-comp-u in cp_macros. License version might be not compatible model name: Intel(R) Xeon(R) CPU X5570 @ 2.93GHz cpu MHz :2025.822), 'Device Component Products Installed' (Check Point Gaia, Check Point Smart Center, Check Point Security Gateway, Check Point R76 (no HFA) Firewall), 'OS Memory Usage' (68.00 %), 'Firewall Memory Usage' (3.00 %), 'Swap Memory Usage' (80.12 %), 'Average CPU Usage (%)' (40.00 %), 'CPU(s)/Cores' (80% CPU Core Usage: 94.00 %), 'Total Number of Concurrent Sessions or Connections' (22), 'Maximum Number of Supported Connections or Sessions' (25000), 'Filesystems' (boot: usage (MB) : 18.85 / 136.85 (13.00%), devfs: usage (MB) : 0 / 471.9 (0%)), and 'Device License Info' (License: 10-255-2-1-10Nov2015.dowSec83hVXatGvccCmATGCHLvkxR8avky::CK-C2FF34880B67::CP5B-COMB-U, Type: TIME_LIMITED, Expiration: Nov 16 2015, Active: true; License: 10-3-3-34-28Nov2013.al8AYG8eG5T1S2F0VAODH1MMyupXTJGzuz::CK-D08F689E46C::COMB-U, Type: TIME_LIMITED, Expiration: Nov 02 2013, Active: true; License: 10-255-2-1-12Dec2014.aDZwRMXP3aAm17YvYyzvQtdofEoPvCNK6ah::CK-C2FF34880B67::cpnb-COMB-U, Type: TIME_LIMITED, Expiration: Dec 12 2014, Active: true).

Troubleshooting

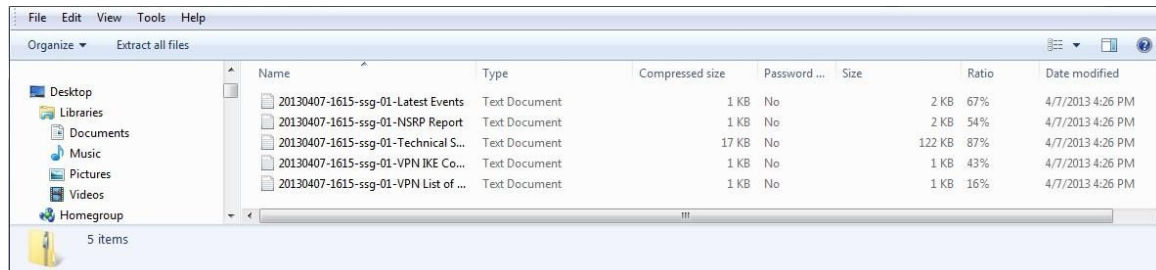
1. Select the **Troubleshooting** sub-tab to generate debug reports. The **Debug Report Generation** in the **Object Debug Panel** compiles reports by individual device. By default, all commands and variables are chosen based on vendor-specific requirements and best practices. Users may choose to remove some commands from the debug report based on specific requirements.
2. Choose the device you want to report on from the list of analyzed devices in the left panel. This will display a list of reportable items that indeni will check and report on.
3. Click on the **Generate** button to obtain the report (scroll down to access this button).



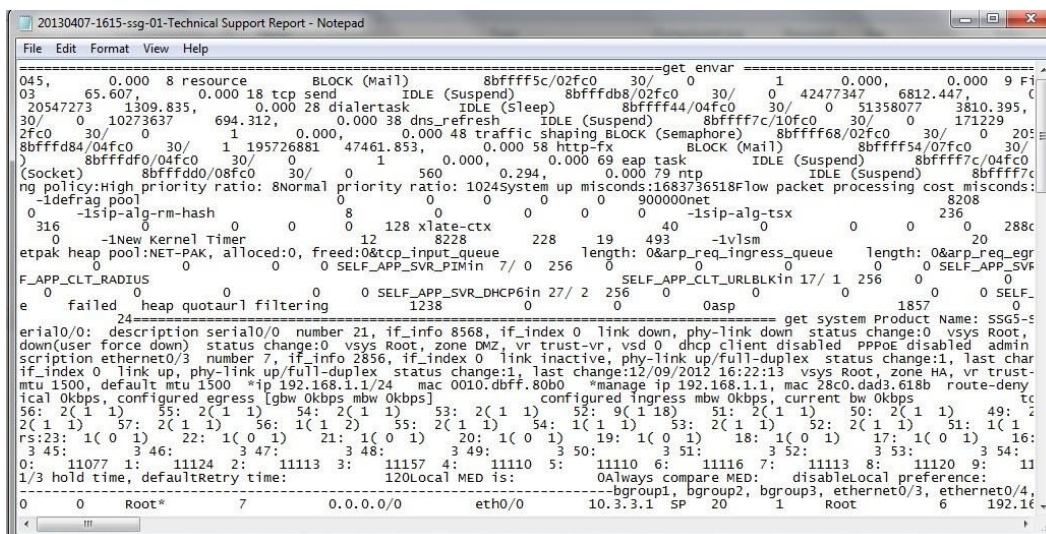
- **Green** checkmarks indicate the debug was successful.
- **Red** icons indicate errors.

To view details of the report:

1. Click the **Download Last Generated Report** button. indeni will compile a .zip file of text documents which users can download. The report includes text files of the output of all the commands which indeni ran in the debug report.



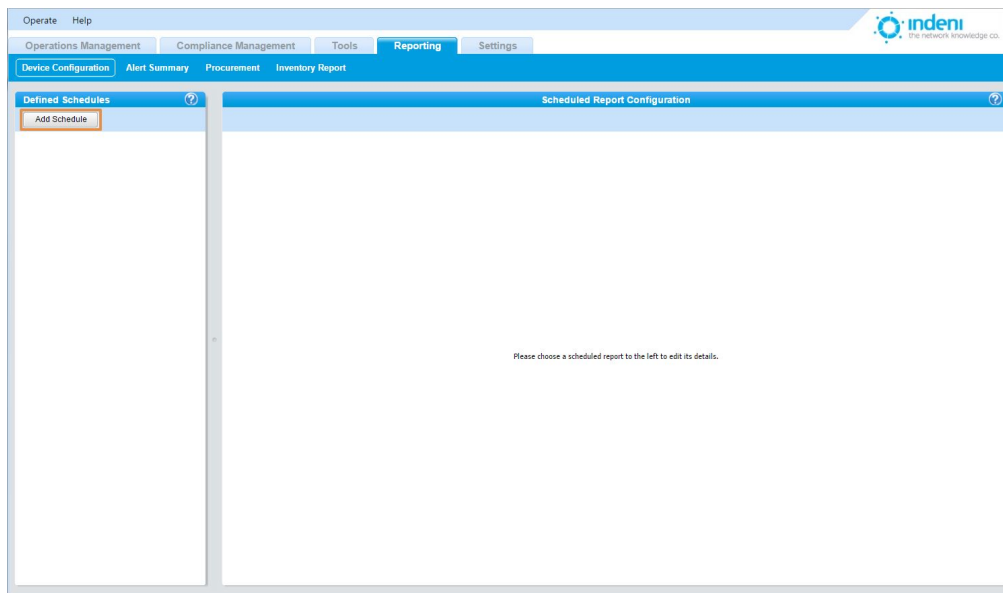
2. Double-click on any of the files to review the individual report.



- After viewing the debug report, users can change the device's internal configuration using the vendor-specification interface.
- Run the **Device Debug** report often to check for continuing errors.

CHAPTER 8: REPORTING

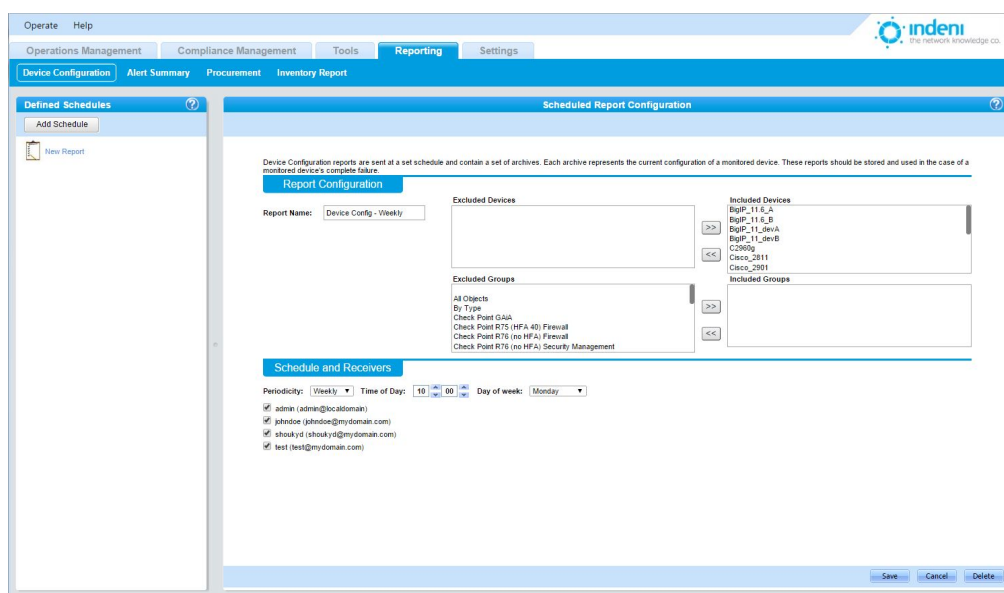
indeni's reporting function provides users with emailed reports on a user-set schedule. The **Reporting** tab lists the type of reports available in sub-tabs at the top of the screen. Currently indeni allows scheduling for four reports. Click on the appropriate sub-tab to choose the desired report to schedule.



Device Configuration Report

This consolidated report provides a separate report for each device included in the report parameters. **Device Configuration** reports are sent on a set schedule and contain a set of archives. Each archive represents the current configuration of a analyzed device

1. Click on **Reporting**, and then the **Device Configuration** sub-tab.



2. Under **Defined Schedules** on the left, click the **Add Schedule** button.
3. An icon will appear under **Defined Schedules**. Edit the details for the schedule under **Scheduled Report Configuration** on the right:
4. Give the report a new name in the **Report Name** field.
5. Choose the devices to be included in the report from the **Excluded Devices** list and click the double arrow to add them to **Included Devices**.
6. Set the time that indeni will generate and deliver the report in **Schedule and Receivers**. Currently indeni provides reports daily. Schedules are based on indeni server time.
7. Select the users to receive the report. indeni provides a list of system users. These users will receive reports only for those devices they are allowed to see, even if the original report was set to include all devices being analyzed.
8. **Save** your changes.

Alert Summary Report

The **Alert Summary** report lists all new and updated alerts that were added or modified since the previous report as well as updates to current alerts, etc.

1. Click on the **Alert Summary** sub-tab option at the top of the screen.
2. Click the **Add Schedule** button in the **Defined Schedules** list.
3. A **New Report** icon will appear under **Defined Schedules**. Edit the details under **Scheduled Report Configuration** on the right.
4. Give the report a new name in the **Report Name** field.
5. Choose the devices to be included in the report from the **Excluded Devices** list and click the double arrow to add them to the **Included Devices** list.
6. Set the time indeni will generate and deliver the report in **Schedule and Receivers**. All alerts generated since the previous report will be included, as well as any updates to previously reported alerts.
7. Select the users to receive the report. indeni provides a list of all system users. These users will receive reports only for those devices they are allowed to see, even if the original report was set to include all devices being analyzed.
8. **Save** your changes.

Note that the reports list in the left panel displays only those reports created for the individual sub-tab you have selected (**Device Configuration** or **Alerts Summary**). If multiple reports have been created under either sub-tab, select the report you want to configure from the list.

Procurement Report

Device Performance and **End of Life** reports are sent on a set schedule and contain all the information needed to assess whether a device requires upgrade or replacement. The ranking is comprised of several parameters such as CPU and memory utilization and end of supports.

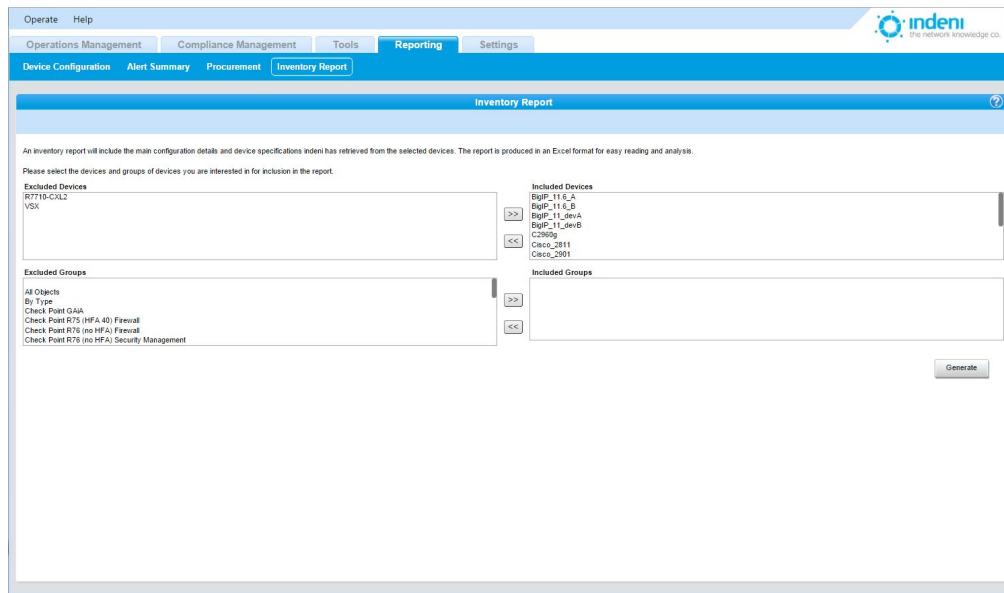
1. Select the **Procurement** sub-tab at the top of the screen.
2. Click the **Add Schedule** button in the **Defined Schedules** list.
3. Give the report a new name in the **Report Name** field.
4. Choose the devices to be included in the report from the **Excluded Devices** list and click the double arrow to add them to the **Included Devices** list.
5. Set the time indeni will generate and deliver the report in **Schedule and Receivers**. All alerts generated since the previous report will be included, as well as any updates to previously reported alerts.
6. Select the users to receive the report. indeni provides a list of all system users. These users will receive reports only for those devices they are allowed to see, even if the original report was set to include all devices being analyzed.
7. **Save** your changes.

Inventory Report

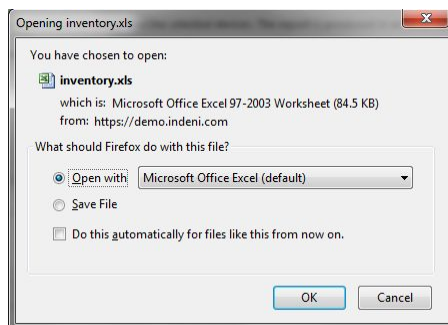
This report exports as an Excel spreadsheet with multiple tabs presenting details regarding your analyzed devices.

To access the report from the **Reporting** tab:

1. Click on the **Inventory Report** sub-tab.
2. Choose from the list of **Excluded Devices** which analyzed devices you do not wish to include in the report.
3. Choose from the list of **Included Devices** to include which analyzed devices you want to report on.



- Click the **Generate** button in the lower right corner of the screen. This generates a report entitled “inventory.xls”.



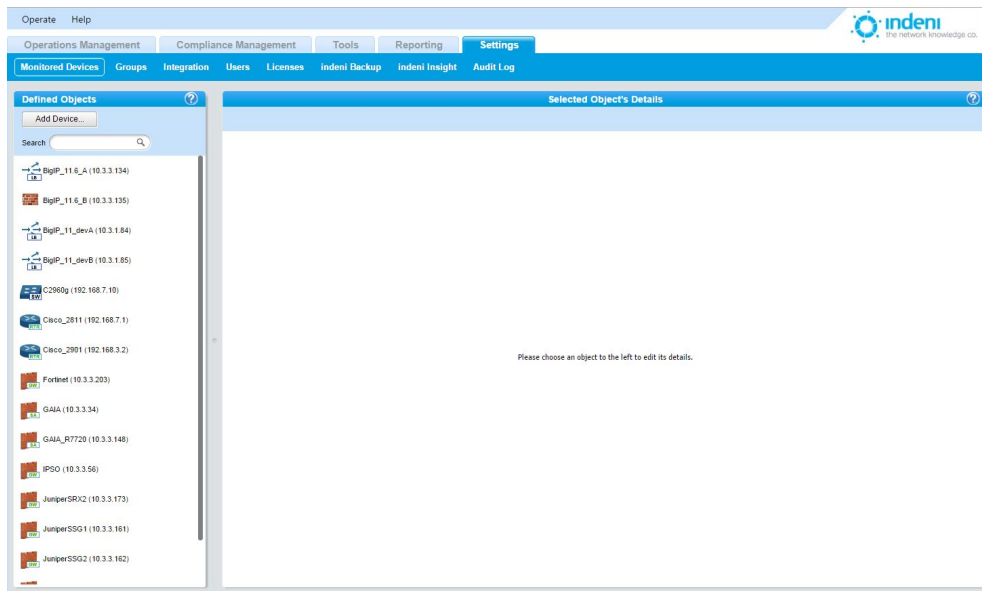
- Choose whether to save or open the file.
- Click **OK** when the **Report Generation Complete** dialog box appears.



This report generates multiple tabs. Navigate through them for detailed information on each device included in the report.

CHAPTER 9: SETTINGS TAB

The **Settings** tab provides access to a variety of functions within indeni through its sub-tabs.




Monitored Devices

This tab provides the same functionality for adding, deleting, and configuring devices as described in [Chapter 4: Getting Started](#).

Here users can change the parameters which define how indeni analyzes a device.

Connectivity

This option allows users to set and troubleshoot connection issues, change the device password, view the security key, and adjust other connection settings that may be causing network issues.

Connectivity parameters need to be set for each device. Hover over the  icon for more details about each parameter, which vary by vendor, model, and device:

- **SSH Connection Timeout:** The maximum wait time when connecting via SSH before deciding the device is not responding. Choose a value (days, hours, minutes, seconds).
- **SSH Username:** Provide the SSH name to be used to log in to the device.
- **SSH Password:** Provide the SSH password to be used to log in to the device.
- **SSH Private Key:** Provide a private key to be used, if any.
- **SSH Private Key Passphrase:** This field is required only if the private key is encrypted.

- **Max Aggregated Connection Bandwidth (in bytes):** Maximum number of bytes per second that can be sent in each direction to avoid overload. Enter the maximum bandwidth value you want the connection to allow.
- **SSH Port:** The port on which the SSH server is running. Set a port number.
- **Approved Host Key:** Allows the client to determine if the SSH server being connected to is the correct one. Only one host key is approved for use at a time. Enter the approved key.
- **SSH Connection Reestablishment Timeout:** The time to wait before attempting to reconnect. This value gives administrators time to resolve issues and ensures the device will not be overloaded with reconnection attempts. Choose a value (days, hours, minutes, seconds).
- **Require Ping Response for Alive Checks:** Forces the device to respond to ICMP ECHO and TCP Port 7 to be considered alive. Toggle On or Off.
- **Max SSH Session Count:** The maximum number of SSH alerts allowed for this device. The lower the number, the longer it will take for a particular issue to be identified and alerted upon. Choose a maximum number from the dropdown box.

Paths


During certain processes such as creating backups, indeni stores information locally on the device and then fetches it to the indeni server. Temporary files are deleted from the server when the operation is complete. Set the **Location for Temporary Paths on Device**.

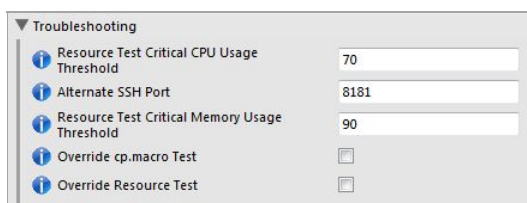


Paths

Location for Temporary Files on Device

Troubleshooting parameters

Users can set a variety of parameters for troubleshooting the individual device. Hover over the  icon for more information, as parameters change by vendor, model, and device.



Troubleshooting

Resource Test Critical CPU Usage Threshold	<input type="text" value="70"/>
Alternate SSH Port	<input type="text" value="8181"/>
Resource Test Critical Memory Usage Threshold	<input type="text" value="90"/>
Override cp.macro Test	<input type="checkbox"/>
Override Resource Test	<input type="checkbox"/>

- **Resource Test Critical CPU Usage Threshold:** Defines the critical resource usage value that triggers a slowdown in analysis operations. Enter a value.
- **Alternate SSH Port:** When communicating with a Linux or FreeBSD-based device, indeni may use an alternate SSH communications port in order to separate between indeni's actions and user-driven activities.

- **Resource Test Critical Memory Usage Threshold:** Defines the critical resource usage value that triggers a slowdown in analysis operations. Enter a value. (In the example, if memory usage is above 90%, indeni will stop analyzing the device.)
- **Override Resource Test:** indeni monitors resource usage for each device under normal analysis conditions and slows down analysis if critical levels are reached. Check the box to override this mechanism. indeni will no longer monitor resource usage as a safety mechanism for this device. This is not recommended.

Scheduled Maintenance Window

To set up a maintenance schedule for a device:

1. Click on the **Add Window** button:



2. Enter the preferred time frames.

To remove a schedule that has already been set up:

- Click on the **Remove** button.

Settings change by type of device, so not all devices will include all of the parameters listed above.

Groups

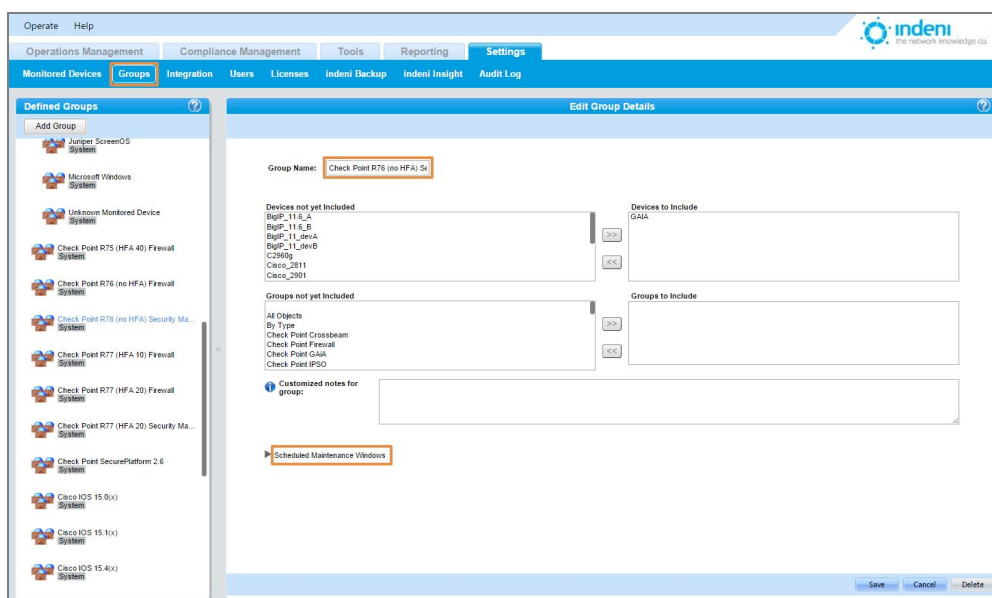
indeni allows users to group analyzed devices in order to quickly find objects of a particular type, such as all Juniper devices, or custom groups based on geographical location or organizational/network infrastructure.

To add a new group:

1. Choose the **Settings** tab, and then the **Groups** sub-tab.
2. Click the **Add Group** button on the left panel.
3. Provide a **Group Name**.
4. Choose devices to add to the new group from the **Devices Not Yet Included** list and use the double arrow icon to move them into the **Devices to Include** box.
5. Add an existing group to the new group as desired by choosing it from the **Groups Not Yet Included** box and adding it to the **Groups to Include** box.
6. Click **Save**. The new group will appear in the list of **Defined Groups** on the left.

To edit an existing group:

1. Click on its name in the **Defined Groups** list on the left side of the screen to display its current settings.
2. Make the desired changes.
3. Click **Save**.



Customized Notes: A user may choose to add custom notes that will be displayed along with other information on the alerts on specific groups and subgroups.

Scheduled Maintenance Windows

To set up a maintenance schedule for a group:

1. Click on the **Add Window** button:

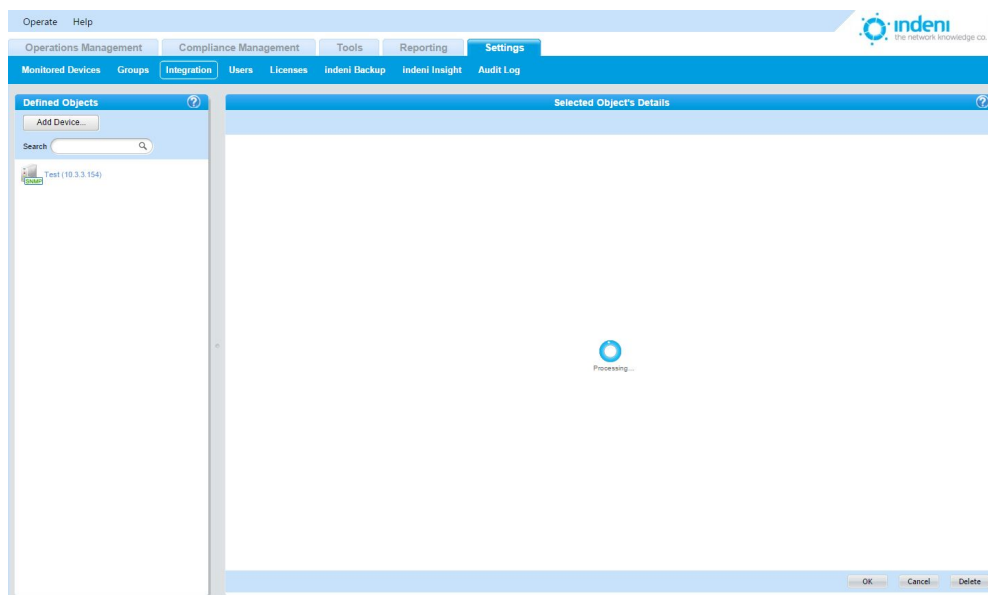
2. Enter the preferred time frames.

To remove a schedule that has already been set up:

- Click on the **Remove** button.

Integration

This tab manages a variety of objects used to notify users of alerts. indeni can be configured to send alerts via SNMP trapping, SMTP email, or by using the UDP syslog protocol. Users must add the type of server desired to indeni and configure the system to forward alerts to the desired users.



Adding an SNMP Master

SNMP trapping captures alerts, which can then be forwarded to a user's mobile phone or pager for further action. indeni supports any SNMP master.

indeni has been verified to be compatible with IBM Tivoli and has achieved the IBM Ready for Tivoli status. To request the files required to use IBM Tivoli please contact support at: <http://indeni.com/support>





indeni is also a Technology Alliance Partner of CA Technologies, providing security assurance solutions through their Technology Partner Program. Our solution helps ensure continuity of services and provides deep insight into real-time performance as well as impending issues that could impact service delivery. For more information on how to configure the integration between indeni and CA Spectrum Infrastructure Manager, please download *Integrating indeni with CA Spectrum Infrastructure Manager* at <http://indeni.com/support>

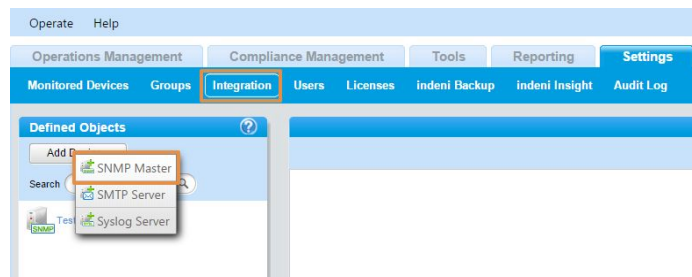


indeni participates in HP's Enterprise Management Alliance Program. The software has been validated to integrate easily with HP Operations Manager (HP OM). HP OM contains a tool to convert the indeni Management Information Base (MIB) file to a HP OM policy. The tool is not an integral part of HP OM but rather a contributed addition. The MIB file and more information on configuring indeni with HP OM can be downloaded from <http://www.indeni.com/support>.

To set up SNMP trapping for indeni you must set up a server capable of receiving SNMP traps and configure it to accept traps from indeni. *An SNMPv2 community or SNMPv3 USM setting is required for SNMP to operate correctly.*


Once the SNMP Master is set up on the server, at the **Settings** tab:

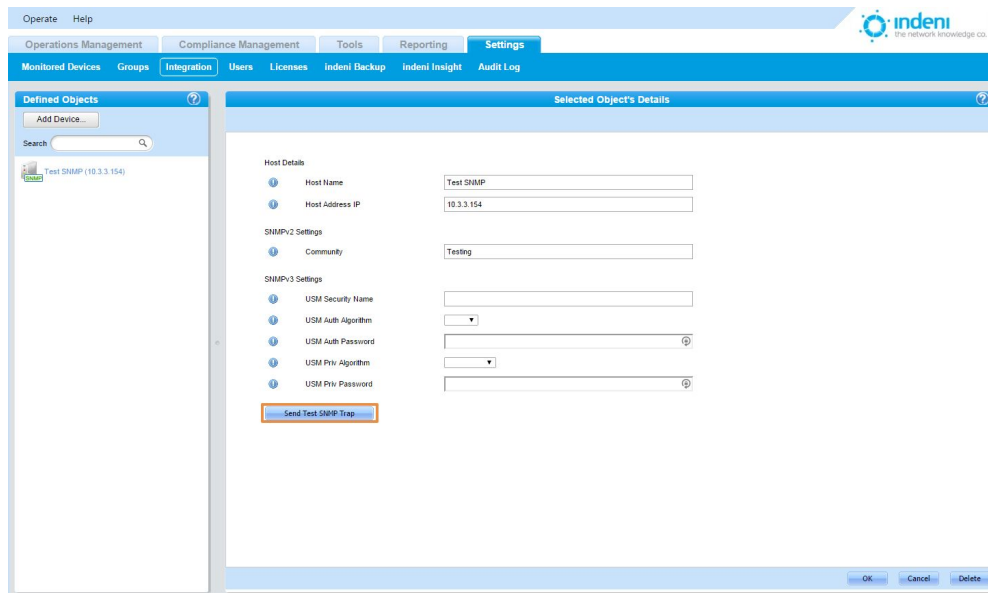
1. Select the **Integration** sub-tab.
2. Click the **Add Device** button under **Defined Objects**.
3. Select **SNMP Master**.



Use the setup screen shown on the next page to configure SNMP trapping for this master. Assign appropriate names and passwords to individual masters, and choose the security algorithm in use on your system from the dropdown lists provided. The user can do any of the following and then **Save** the changes:

- Assign only a host address IP, host name and community (that is, no SNMPV3 settings).
- Set all fields EXCEPT for community (no SNMPv2 settings).
- Set all fields.

Note: Hover over the  icon for more details about each parameter.



When finished, by default, all alerts having an Error or Critical severity will be sent via SNMP traps to this master. Users can change what alerts are trapped, logged, or sent via the [Signatures](#) sub-tab on the **Monitoring** tab.

- Use the **Send Test SNMP Trap** button to test the new configuration.

Configuring indeni as an SNMP Device in the SNMP Master

When configuring the SNMP Master, users should:

- Download the MIB file:
Accessible at <http://www.indeni.com/support>.
- Configure the SNMP Master to use the MIB to fetch data from indeni as well as receive the SNMP traps. indeni currently supports two trap formats:

indeniNewAlertTrap: This is issued when an alert is created. The trap contains all of the information pertaining to the alert, including its ID, in a trap field called `indeniAlertEntryIndex`. The trap fields are:

`indeniAlertEntryIndex:` The ID of the specific alert that was generated

`indeniAlertSeverity:` The alert's severity

`indeniAlertHeadLine:` The alert's headline

`indeniAlertDescription:` The alert's description

`indeniDeviceName:` The name of the device the alert pertains to

`indeniDeviceIp:` The IP of the device

`indeniAlertCategory:` The category the alert belongs to

indeniAlertBaseIdentifier: The type of alert

indeniAlertStatus: The alert status

UNRESOLVED: Normally the status when an alert is first generated

RESOLVED: Normally issued as part of trap type 2 below

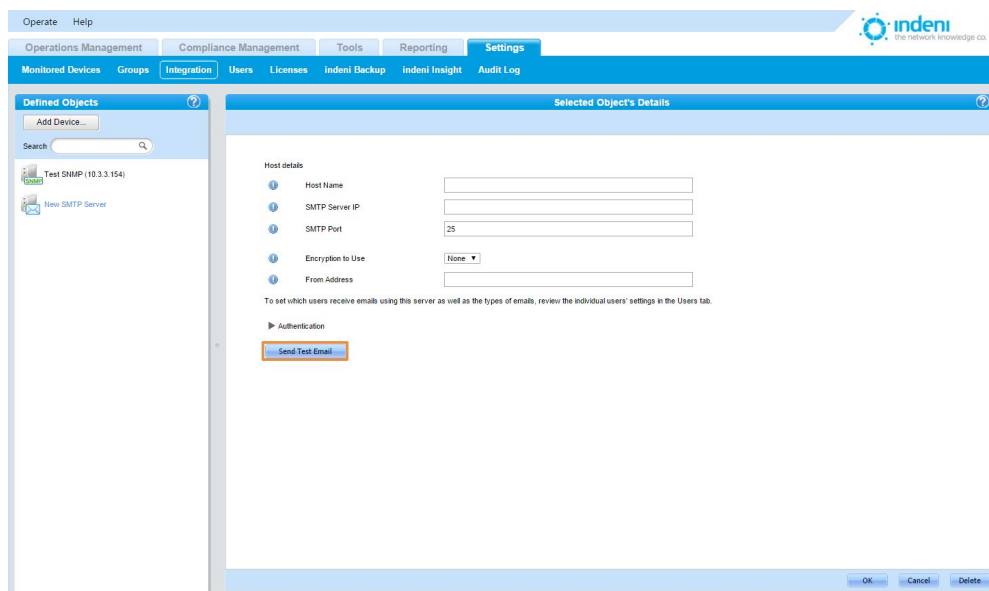
indeniAlertStatusUpdateTrap: This is issued when an alert's resolved status changes. When an alert has been remediated, indeni automatically changes the status to Resolved; however, if indeni later re-verifies and identifies it as unresolved it will remove the Resolved designation. Whenever the status changes, either from Unresolved to Resolved or vice versa, this trap will be issued with the ID of the original alert in the **indeniAlertEntryIndex** field. New values will appear in the **indeniAlertSeverity** and **indeniAlertStatus** fields.

Adding an SMTP Server

indeni provides the means to add an SMTP server to the list of managed devices to facilitate alert emailing. Once configured, Critical and Error alerts are sent through this server by default.

To add a new SMTP server:

1. Go to the **Settings** tab and select the **Integration** sub-tab.
2. Click the **Add Device** button and select **SMTP Server**.
3. Configure the new server.
4. Use the **Send Test Email** button to test that the configuration is correct.
5. **Save** the configuration. indeni will add the new SMTP server to the list of **Defined Objects**.



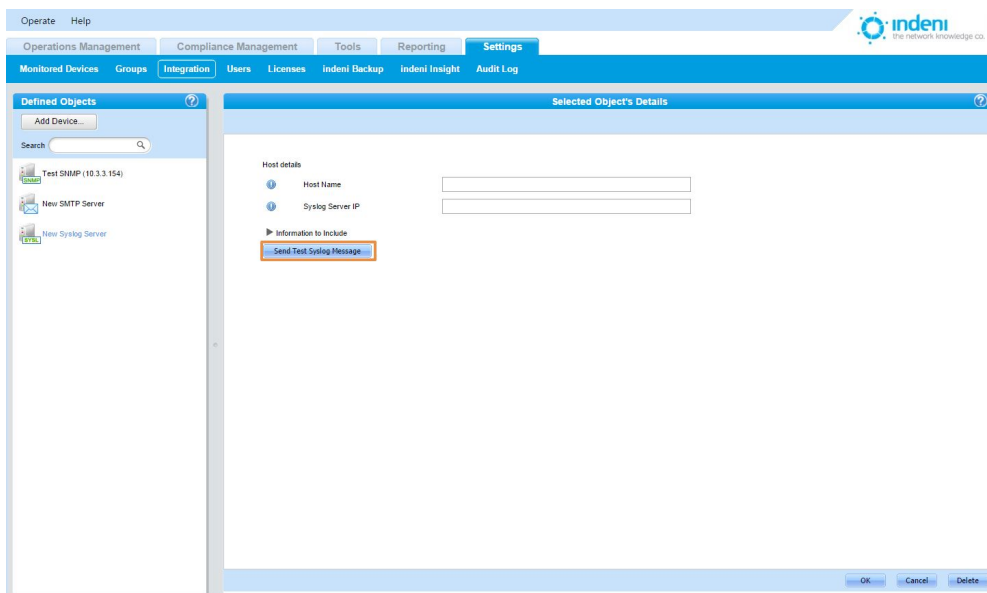
Adding a Syslog Server

indeni is also capable of sending alert information to syslog servers using the UDP syslog protocol. In order to conform to compliance requirements, administrators can also choose to have indeni send a

syslog message whenever a user attempts to access the system via the web dashboard, including whether or not such access was granted.

To add a syslog server:

1. Go to the **Settings** tab and select the **Integration** sub-tab.
2. Click the **Add Device** button under **Defined Objects** on the left side of the screen.
3. Select **Syslog Server**.
4. Configure the new syslog server.



5. Send a test message to determine if the configuration is working.
6. **Save** the configuration. indeni will add the new syslog server to the list of **Defined Objects**.

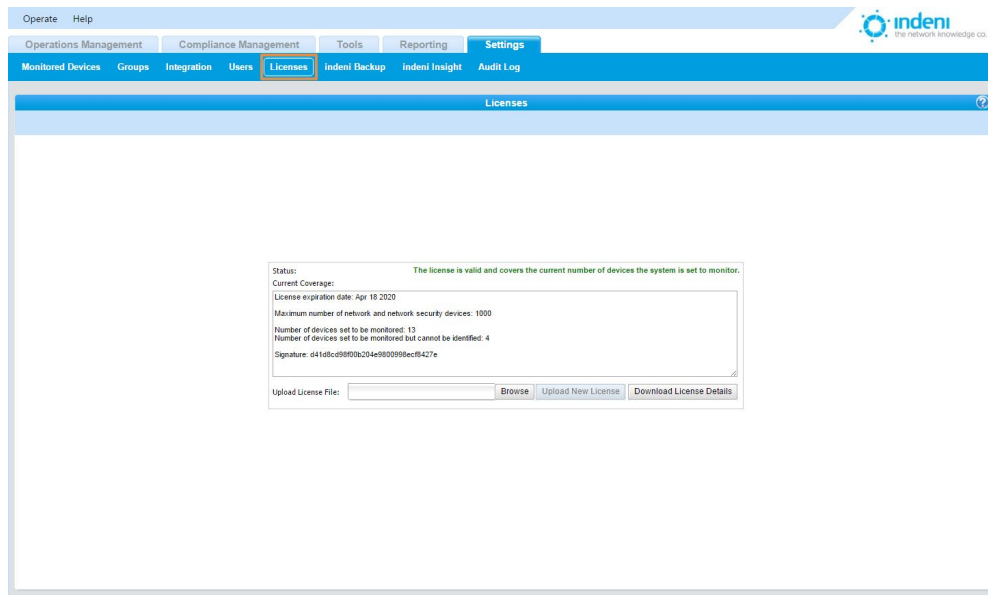
Users

Use this sub-tab to add, delete, and edit users, passwords, email settings, permissions for setting up and remediating individual devices, and permissions for group objects, as described in [Chapter 4: Getting Started](#).

Licenses

indeni's license expiration date and limitations depend on what was purchased. To determine the status of your current indeni licenses or to upload a new license, Select the **Settings** tab and then the **Licenses** sub-tab.

Licenses are obtained from an indeni reseller as a file with a “.lic” extension. Users must download the .lic file to their own hard drive and then upload to indeni. The file can then be removed from the local hard drive.



This screen displays the current status of the indeni license as well as the exact terms of the license, such as the number of devices allowed, the expiration date, etc.

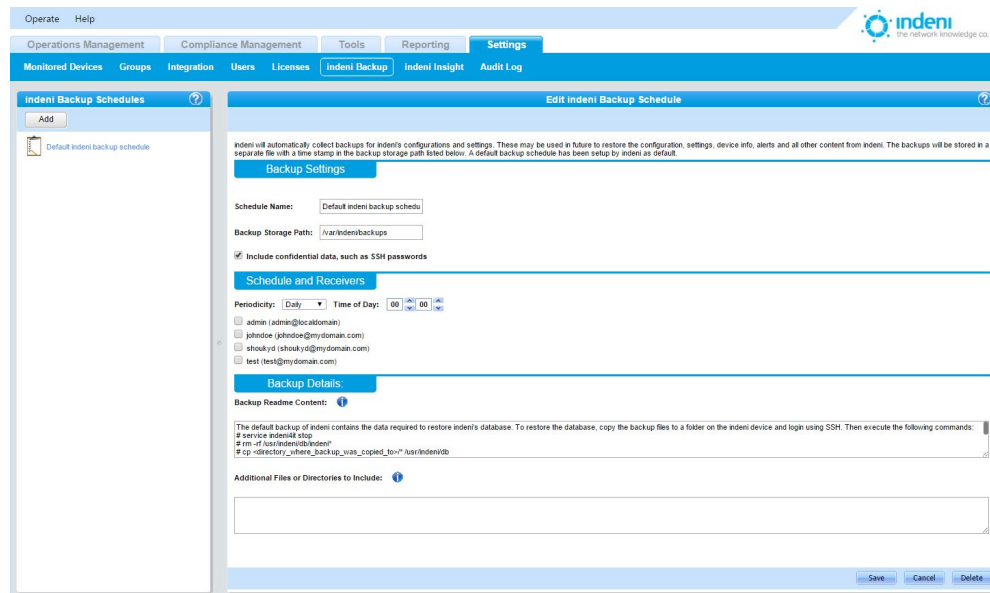
The system will notify users via an alert in the **Operations Management** tab when one of the following conditions is observed:

- If 90 days remain before the license expires.
- If the license has already expired.
- If the user is approaching the limit of allowed analyzed devices.

indeni Backup

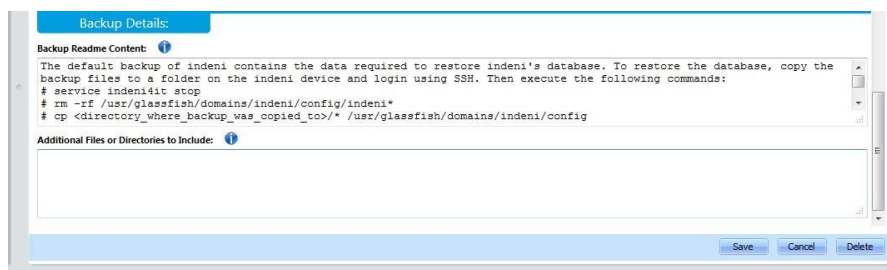
indeni will automatically collect backups for indeni's configurations and settings. These may be used in future to restore the configuration, settings, device info, alerts and all other content from indeni. The backups will be stored in a separate file with a timestamp in the backup storage path shown on the next page.

A default backup schedule has also been setup by indeni.



To schedule backups for indeni in addition to the default backup:

1. From the **Settings** tab, select the **indeni Backup** sub-tab. Note that the default indeni backup shows up predefined (out of the box).
2. Click the **Add** button. **New indeni backup** will appear in the **indeni Backup Schedules** list on the left.
3. Use the backup settings under **Edit indeni Backup Schedule** on the right to provide a **Schedule Name**.
4. In the **Backup Storage Path** field, provide the path where these backup files will be stored.
5. Check the box if desired to Include confidential data, such as SSH passwords
6. In the **Schedules and Receivers** portion of the screen, set the time of day you want the backups to run and how often. By default, the backups will be saved daily.
7. Choose the users who will receive notification of backups and their success or failure.
8. Under the heading **Backup Details**, you can include instructions on how to utilize a backup that has been created by this backup schedule. These instructions will be saved as a README file in the resulting backup archive.

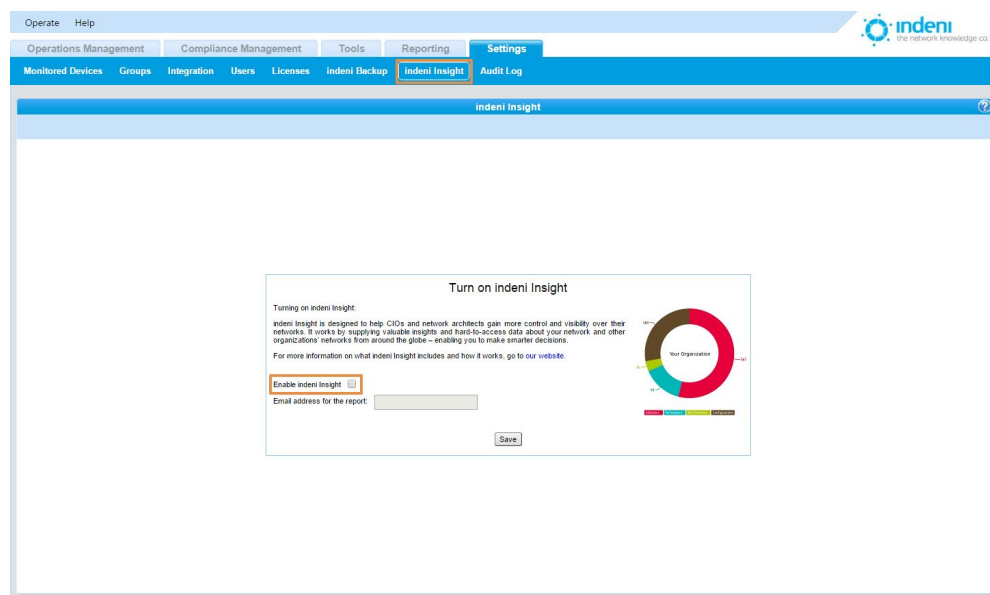


9. In the field for **Additional Files or Directories to Include**, you can add directories and files to include in the backup file. Each path should be on a separate line and its format should be compliant with the operating system installed on the devices you've chosen to back up.
10. **Save** your changes.

indeni Insight

indeni Insight is designed to help CIOs and network architects gain more control and visibility over their networks. It works by supplying valuable insights and hard-to-access data about your network and other organizations' networks from around the globe - enabling you to make smarter decisions.

For more information on what indeni Insight includes and how it works, visit [our website](#).



Audit Log

The **Audit Log** sub-tab shows a list of changes and activities that took place in the indeni application. *Its information does not apply to analyzed devices.*

Operate Help					
Operations Management Compliance Management Tools Reporting Settings					
Monitored Devices Groups Integration Users Licenses Indeni Backup Indeni Insight Audit Log					
Audit Log					
ID	Type	User	Summary	Affected Objects	Timestamp
AU100357	Configuration Change	admin	Report removed: P5 Weekly	Affects: 0 object(s)	24/12/2014 16:15
AU100356	Configuration Change	admin	Scheduled backup created	Affects: 0 object(s)	24/12/2014 16:15
AU100355	Configuration Change	admin	Report removed: Monthly Configuration Check	Affects: 0 object(s)	24/12/2014 16:14
AU100354	Configuration Change	admin	Report created	Affects: 0 object(s)	24/12/2014 16:13
AU100353	Configuration Change	admin	Report removed: Monthly Procurement	Affects: 0 object(s)	24/12/2014 16:10
AU100352	Configuration Change	admin	Report created	Affects: 0 object(s)	24/12/2014 16:10
AU100351	Configuration Change	admin	Report removed: Daily Report	Affects: 0 object(s)	24/12/2014 16:09
AU100350	Configuration Change	admin	Report created	Affects: 0 object(s)	24/12/2014 16:09
AU100349	Configuration Change	admin	Report removed: Cisco	Affects: 0 object(s)	24/12/2014 16:08
AU100348	Configuration Change	admin	Report created	Affects: 0 object(s)	24/12/2014 16:08
AU100347	Configuration Change	admin	Scheduled backup created	Affects: 0 object(s)	24/12/2014 16:08
AU100346	Configuration Change	admin	Report removed: P5	Affects: 0 object(s)	24/12/2014 16:05
AU100345	Configuration Change	admin	Report created	Affects: 0 object(s)	24/12/2014 16:05
AU100344	Configuration Change	admin	Report removed: Check Point	Affects: 0 object(s)	24/12/2014 16:04
AU100343	Configuration Change	admin	Scheduled backup created	Affects: 0 object(s)	24/12/2014 16:03
AU100342	Login Successful	admin	User login successful	Affects: 0 object(s)	24/12/2014 15:54
AU100341	Login Successful	admin	User login successful	Affects: 0 object(s)	23/12/2014 11:58
AU100340	Login Successful	admin	User login successful	Affects: 0 object(s)	21/12/2014 08:25
AU100339	Login Successful	admin	User login successful	Affects: 0 object(s)	20/12/2014 11:18
AU100338	Login Failure	admin	User login failed	Affects: 0 object(s)	19/12/2014 22:28
AU100337	Login Successful	admin	User login successful	Affects: 0 object(s)	19/12/2014 23:52
AU100336	Login Successful	admin	User login successful	Affects: 0 object(s)	18/12/2014 14:54
AU100335	Informational	admin	Indeni stop monitoring started by user	Affects: 0 object(s)	18/12/2014 14:50
AU100334	Configuration Change	admin	Device removed: JuniperSRX2 (10.3.3.172)	Affects: 0 object(s)	18/12/2014 14:02
AU100333	Configuration Change	admin	Monitored device added	Affects: 1 object(s)	18/12/2014 14:01

ID

Indeni assigns a unique number to each entry as it is added to the log. By default, items in the **Audit Log** display in descending order of occurrence.

Type

This column displays the type of action that took place. You can set these by clicking on the filter icon, which brings up the available choices. All of the action types can be selected for viewing in the report:

☒ Login Successful
☒ Configuration Change
☒ Login Failure
☒ Informational

Clear Apply

User

This column displays the name of the user who performed the action. You can set this for one or more users by clicking on the filter icon and making your selections.

☒ admin

Clear Apply

Summary

This column displays the actual outcome of the action, such as “User’s permissions updated.”

Affected Objects

This column displays the number of objects that have been affected by the action.

Timestamp

This column allows users to display individual items in the **Audit Log** by date range. (See **Last Update** under [Columns and Functionality](#) in Chapter 5 for more detail.)

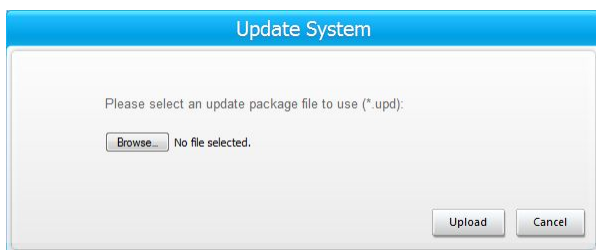
CHAPTER 10: UPGRADES AND SUPPORT

Upgrades

Products offered by indeni, like networking itself, are constantly evolving. New capabilities and functionality, including indeni's ability to recognize and configure new devices and identify and resolve additional errors, are being added on a regular basis. When you update your version of indeni by downloading the current release (available by contacting support at <http://www.indeni.com/support>), you will automatically receive the upgraded functions.

indeni is constantly adding to the list of devices the product can recognize and manage. Upon receipt of notification from indeni that an update is available, download the update from indeni.com to your workstation.

1. Select **Operate** at the top of the indeni Web Dashboard.
2. Select **Update System**.



3. On the Update System screen, use the **Browse** button to find the downloaded file.
4. Use the **Upload** button to launch the upgrade. indeni will update the system files and restart automatically. The process takes several minutes. A progress bar is provided.
5. To log off the system, select **Operate, Logout <name>**.

Support

The Support section of www.indeni.com is available 24/7. Documentation, including updated editions of this user manual, is available via .pdf download.

Additional support is also available via:

Toll-free: +1-877-778-8991

Online support: <http://www.indeni.com/support>

Email: support@indeni.com

APPENDIX A: TERMINOLOGY

Cluster Member

A network device which takes part in a cluster using one of the known clustering protocols (VRRP, ClusterXL, NSRP, JSRP, HSRP, etc.).

Analyzed Device

A device the indeni application connects to and analyzes. indeni may possibly use its data to assist with the analysis of other devices. Check Point Security Gateway, Cisco Router, Juniper Firewall and F5 LTM are examples of such devices.

APPENDIX B: SYSTEM SECURITY AND SAFEGUARDS

Database Structure

indeni stores its information locally on the hard drive on which it is installed. The database contains different types of information with two general classifications: *highly confidential* and *confidential*. The highly confidential information is stored within an encrypted file (using two types of encryption employing industry standards and best practices). The confidential information is sorted in non-encrypted files.

The database files are not accessible via the web interface and can only be retrieved by logging into the system via SSH and downloading them using standard protocols (SCP, SFTP, etc.). The SSH service is the standard sshd application, which has a long track record of being safe so long as the passwords selected by the user are strong ones. Refer to your organization's password policies for more information on choosing a strong password.

Underlying Operating System

The operating system supplied with the system is CentOS 6.x 64-bit, with most packages removed. By default, the set of services accessible via the network has been reduced to the absolute minimum required, further hardening the operating system. These services are:

SSH (OpenSSH_4.3p2)

HTTP and HTTPS (Jetty)

Device Access Credentials Storage

The credentials used to access devices, such as the SSH Username and Password, are stored within the database described above. The username is stored in the confidential store, while the password is stored in the highly confidential store (and is encrypted). By protecting the database files, an organization is protecting this information from being compromised.

Password Security of Users Defined in the System

All users defined in the system (allowed to access the system itself via the web interface) are required to use strong passwords as defined by PCI DSS requirements 8.5.10, 8.5.12, 8.5.13, and 8.5.14. Passwords are stored as salted hashes within the encrypted database. This protects the original passwords from being recovered.

Protecting Analyzed Devices

The commands executed on analyzed devices (routers, firewalls, load balancers, management servers, etc.) are defined by the internal logic of the product and cannot be modified by a user. This is to limit the commands that can be executed by indeni on analyzed devices to those which have been tested and approved by indeni.

indeni also monitors the resource usage (CPU, RAM, etc.) on each analyzed device and reduces the analysis work to an absolute minimum if it notes that the resource usage has crossed certain thresholds. This is in order to avoid placing an extra load on an unstable device that may result in its failure. Once the resource usage returns to normal levels, full analysis operations are resumed.

No Change Policy

indeni has a very strict no change policy, meaning no changes will be made on the devices indeni analyzes. The only writing actions indeni executes is to write temporary files to /tmp and to initiate an additional instance of SSHD when needed.

APPENDIX C: BASIC TROUBLESHOOTING

Below are some basic troubleshooting procedures which may be used to verify and initial setup or any communication errors between indeni and the analyzed devices:

Accessing the Web UI

When accessing the web UI, please verify that the URL format is `https://<indeni_ip>:8181/` (example: `https://10.3.1.87:8181/`) and that port 8181 is open and not restricted by any firewall rules.

Adding Devices to indeni



The following pages address common scenarios of problems users encounter when adding a device to indeni. Note in the following examples that there is a further explanation of the problem within each alert shown, which can assist you in finding the solution. In most cases, the content of the alert will provide the user with all the required details. Please make sure to expand the alert so that the alert's content becomes available.

Verify SSH connectivity between indeni and the analyzed device by connecting to indeni over SSH and initiating an SSH session into the analyzed device using indeni's designated username and password.

In some cases, as indicated in the alert's details, management servers require their superior management server to be analyzed before they can be analyzed (for example, MDS needs to be analyzed before a CMA can be, in the case of Check Point). If indicated, please make sure to analyze the superior management servers.

1. Failed to communicate - No response on port 22

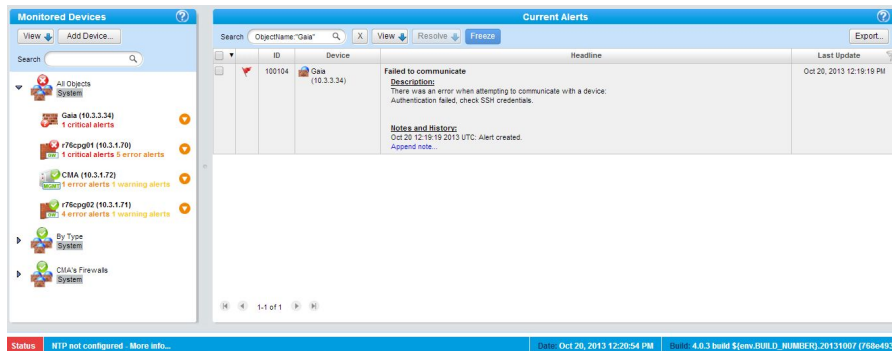
a. This is how the alert would appear:

<input type="checkbox"/>		108415	 R75.40_-_VRRP_-_Member1 (10.3.3.44)	Failed to communicate Description: There was an error when attempting to communicate with a device: Device at 10.3.3.44: No response on port: 22 Notes and History: Oct 09 14:58:36 2013 BST: Alert created. Append note...	Oct 9, 2013 02:58:36 PM	Oct 9, 2013 02:58:36 PM
--------------------------	---	--------	--	--	-------------------------	-------------------------

b. As a first step to assess where the issue lies, try to SSH from the indeni server to the analyzed device. If this fails, try to understand why this happens and this will lead to solving this issue. Make sure that port 22 is opened in your firewall. Please check the rule base of any firewalls involved in the path between indeni and this device to ensure this port is allowed.

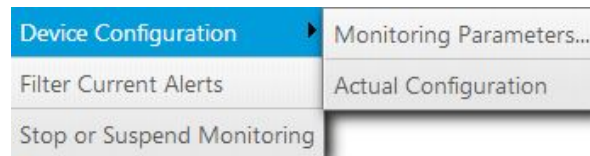
2. Failed to communicate - SSH Credentials

a. This is how the alert would appear:

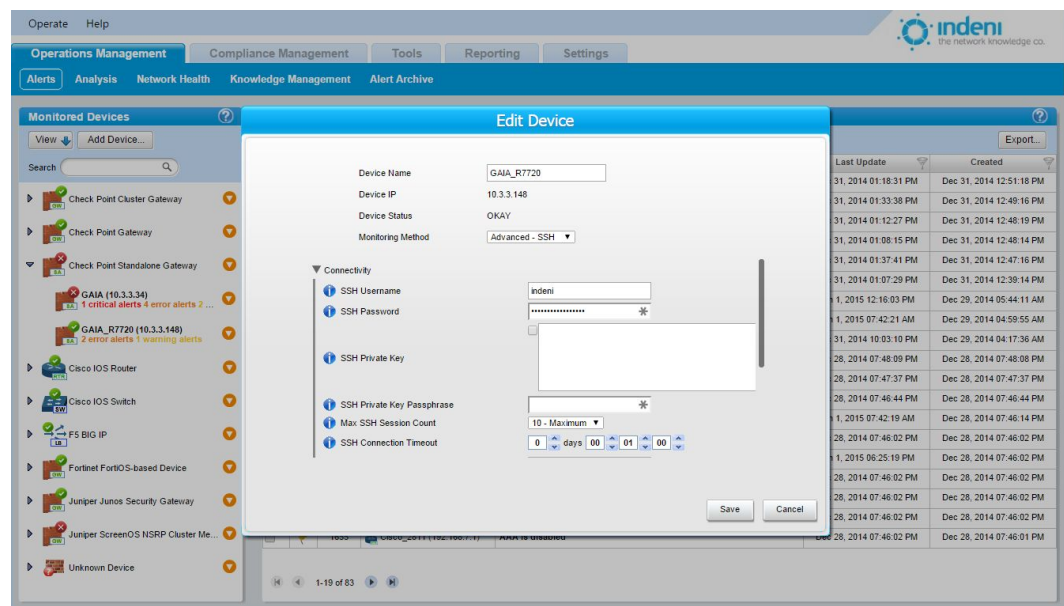


b. Authentication failed. Please update the SSH credentials as follows.

- i. Find the device ID in the list on the left panel of the **Monitoring/Current Alerts** screen. Click on the orange circle beside the device to change its settings. From the pop-up, select **Device Configuration/Monitoring Parameters**.



- ii. The **Edit Device** window opens. Scroll down the **Edit Device** screen and update "SSH Password" or "SSH username" field. Click on **Save**.



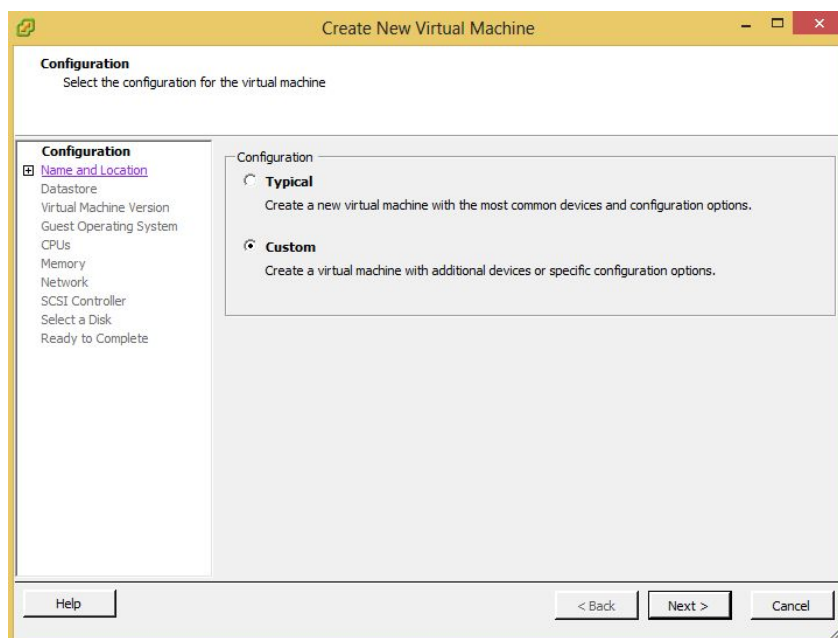
APPENDIX D: SETTING UP INDENI ON VMWARE ESX

indeni can run on a number of virtual environments. This appendix takes you through the Create New Virtual Machine wizard, providing the steps necessary to set up an indeni server on VMware ESX.

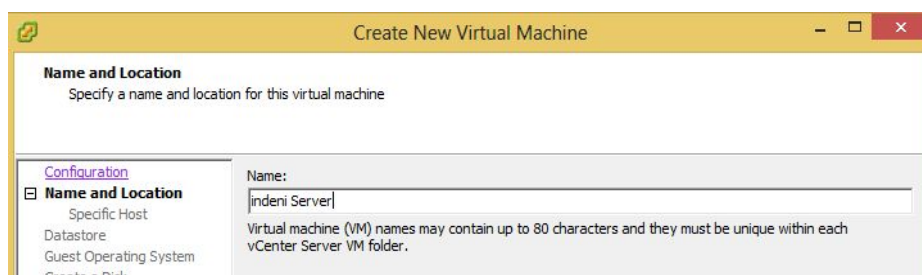
IMPORTANT NOTE: When defining the network interfaces of a VM in a VMware environment, please choose E1000 as the adapter type and not vmxnet.

Creating a New Virtual Machine

1. Open the VMware ESX configuration wizard. Choose the **Custom** radio button to create the virtual machine and click **Next**:



2. Enter a **Name** for the server and click **Next**:



3. Select a specific host for your virtual machine from the list under **Host Name**:

Create New Virtual Machine

Specify a Specific Host
On which host within the cluster should the virtual machine run?

Configuration

- Name and Location**
 - Specific Host**
 - Datastore
 - Guest Operating System
 - Create a Disk
 - Ready to Complete

Choose a specific host within the cluster.
On clusters that are configured with VMware HA or Manual mode VMware DRS, each virtual machine must be assigned to a specific host, even when powered off.
Select a host from the list below:

Host Name

Compatibility:
Validation not applicable this time.

Help < Back Next > Cancel

4. Select a **Datastore** from the list provided and click **Next**:

Create New Virtual Machine

Datastore
Select a datastore in which to store the virtual machine files

Virtual Machine Version: 7

Configuration

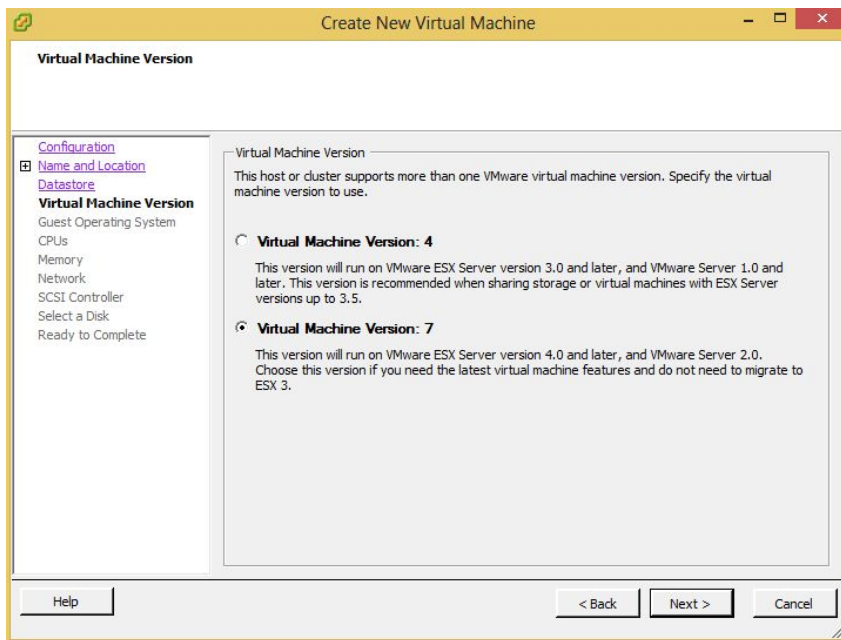
- Name and Location**
 - Datastore**
 - Guest Operating System
 - Create a Disk
 - Ready to Complete

Select a datastore in which to store the virtual machine files:

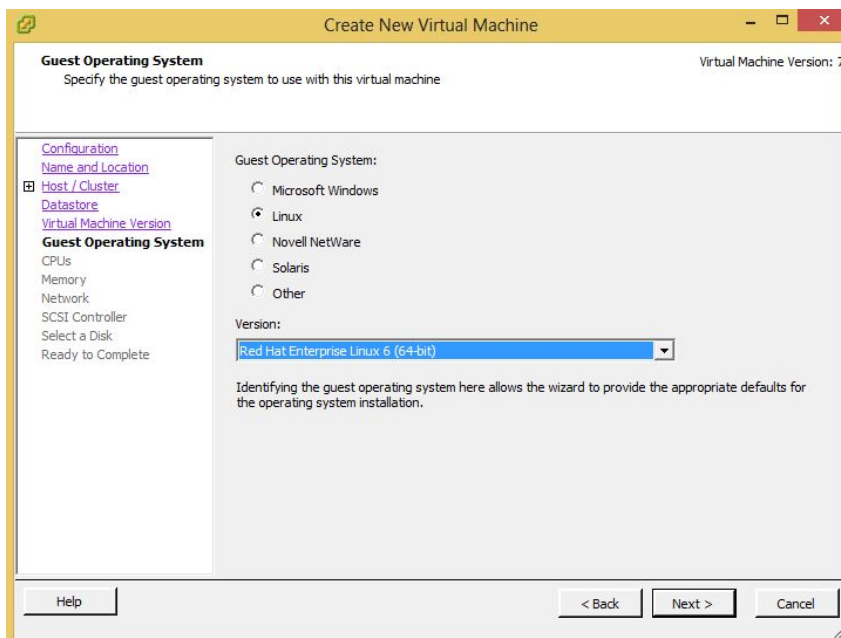
Name	Capacity	Provisioned	Free	Type	Thin Provisioning	Access
------	----------	-------------	------	------	-------------------	--------

< >

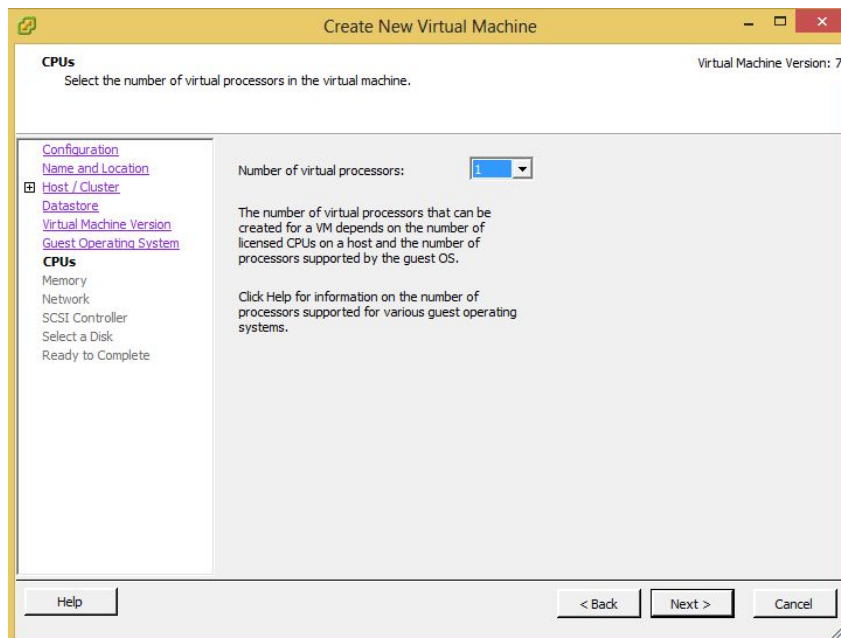
5. Specify which **Virtual Machine Version** to use if the host or cluster supports multiple versions:



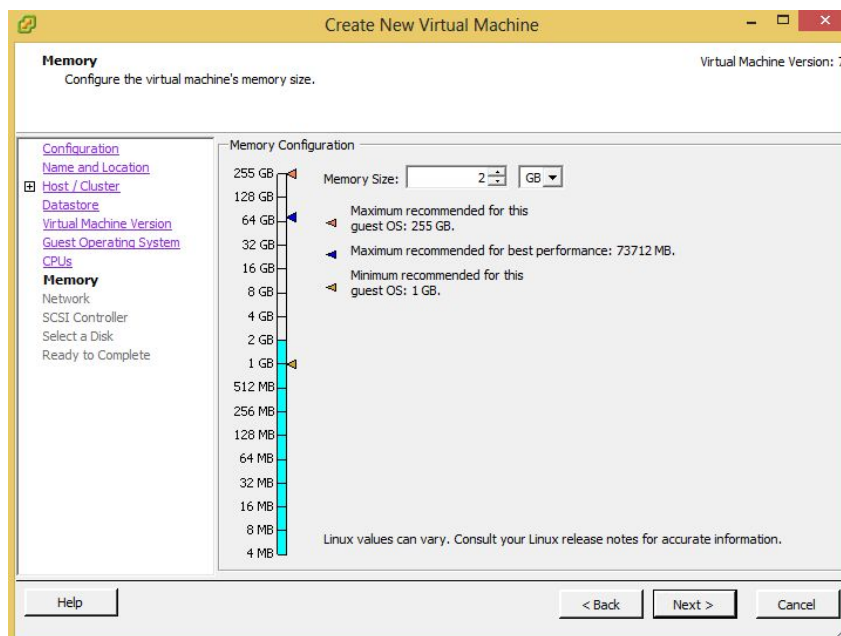
6. Choose which **Guest Operating System** to use with the virtual machine. For **Version** be sure to select **Red Hat Enterprise Linux 6 (64-bit)** from the drop-down menu. Click **Next**:



7. Select the **Number of virtual processors** to create for the VM. Use the **Help** button for additional information. Click on **Next**:

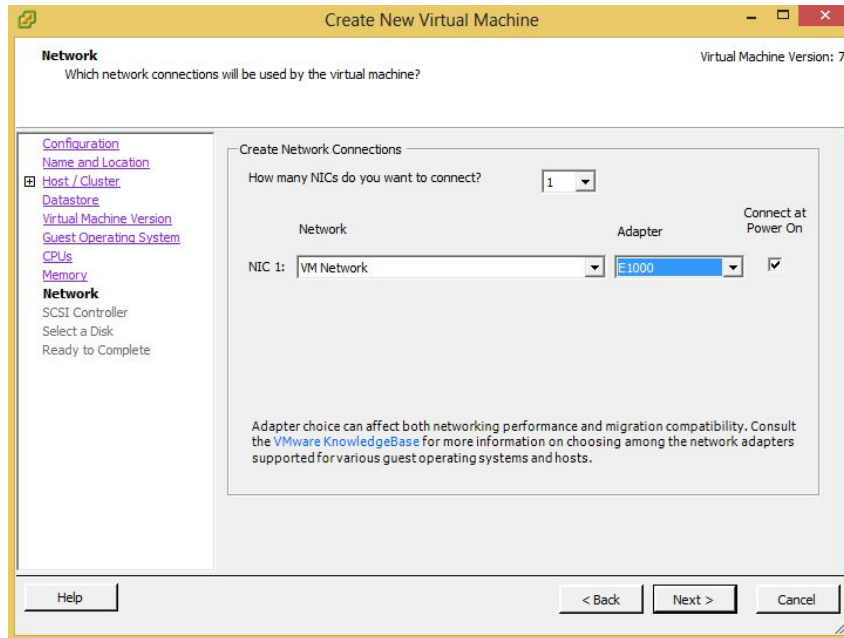


8. **Memory Size must be 2 GB or greater** to ensure there is enough memory to run indeni.

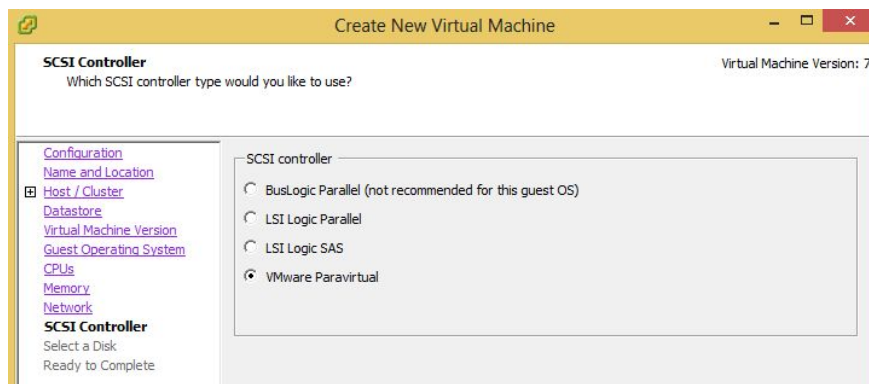


See also indeni [Hardware Requirements](#) in Chapter 1 of this user guide for a description of how to calculate the needed memory for your indeni implementation

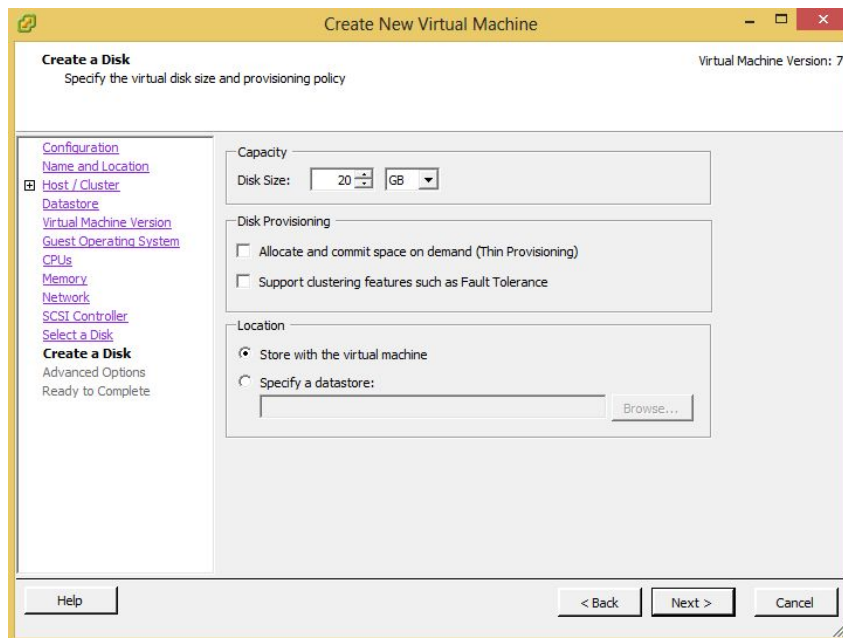
9. To **Create Network Connections**, select how many NICs you want to connect from the drop-down menu. Select the VM Network for **NIC 1**. From the **Adapter** drop-down list select the adapter type **E1000**. Check the box for **Connect at Power On**. Click **Next**:



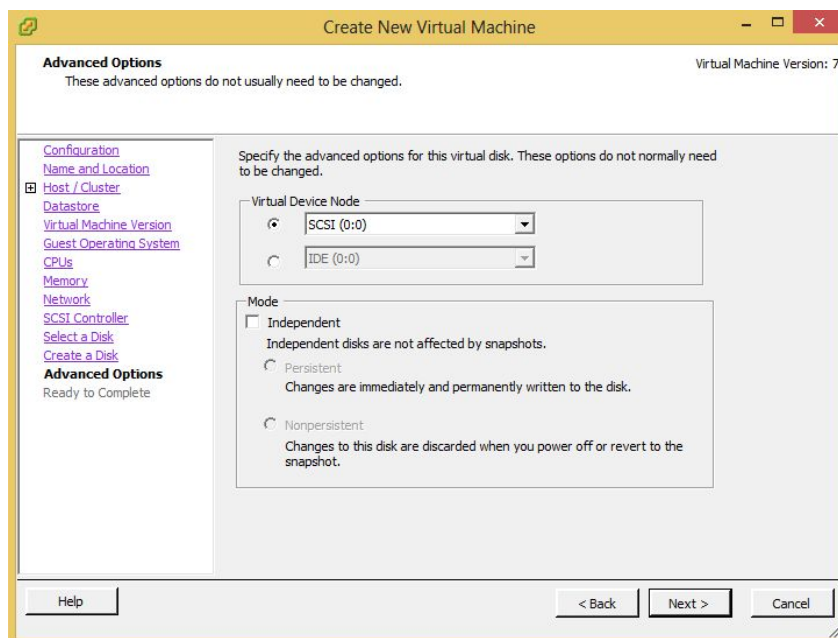
10. Choose **VMware Paravirtual** as the **SCSI controller**. Click **Next**:



11. Create a disk by setting **Capacity**, **Disk Provisioning**, and **Location**. Click **Next**:



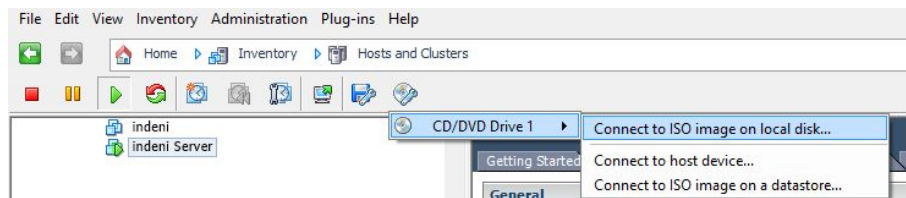
12. **Advanced Options** are available but are not usually required. Click **Next**:



13. Power on the virtual machine using the **Power** button.



14. Click on **CD/DVD Drive 1** -> **Connect to ISO image on local disk**, shown highlighted on the screen below. Locate the ISO file downloaded from indeni website.



15. The indeni setup for VMware ESX is complete. See [Chapter 2](#) in this user guide for the installation and configuration of indeni.

About indeni

Founded in 2009 by a team of network security experts, indeni is revolutionizing networking with the world's first future-proof network management tool. Built on a game-changing platform that combines crowd-sourced knowledge with device-agnostic automated error checking, indeni gives enterprises the high-resolution visibility to preempt costly downtime and service disruption in their networks - while freeing up vital IT resource.

indeni is entrusted by Global and Fortune 100 companies, government agencies and SMBs, to keep their networks running smoothly 24/7/365.

For more information about indeni, visit www.indeni.com or email us at sales@indeni.com.

This product includes software developed by The Apache Software Foundation (<http://www.apache.org/>).

Apache Commons Codec

Copyright 2002-2009 The Apache Software Foundation

This product includes software developed by

The Apache Software Foundation (<http://www.apache.org/>).

src/test/org/apache/commons/codec/language/DoubleMetaphoneTest.java contains
test data from <http://aspell.sourceforge.net/test/batch0.tab>.
Copyright (C) 2002 Kevin Atkinson (kevin@gnu.org). Verbatim copying
and distribution of this entire article is permitted in any medium,
provided this notice is preserved.

Apache Commons Collections Copyright 2001-2008 The Apache Software Foundation
Apache Commons Configuration Copyright 2001-2008 The Apache Software Foundation
Apache Commons IO Copyright 2001-2008 The Apache Software Foundation
Apache Commons Lang Copyright 2001-2008 The Apache Software Foundation
Apache Commons Logging Copyright 2003-2007 The Apache Software Foundation
Cglib Copyright 2002-2004 cglib

Licensed under the Apache License, Version 2.0 (the "License");

you may not use this file except in compliance with the License. You may obtain a copy of the License at
<http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

Logback: the reliable, generic, fast and flexible logging framework. Copyright (C) 1999-2009, QOS.ch. All rights reserved.

This program and the accompanying materials are dual-licensed under either the terms of the Eclipse Public License v1.0 as published by the Eclipse Foundation or (per the licensee's choosing) under the terms of the GNU Lesser
General Public License version 2.1 as published by the Free Software Foundation.

SLF4J Copyright (c) 2004-2008 QOS.ch All rights reserved. Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the
Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be
included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND
NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE
LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION
WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Apache Commons Pool Copyright 1999-2009 The Apache Software Foundation

Ganymed-SSH2 Copyright (c) 2006 - 2010 Christian Plattner. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions
are met:

a.) Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

b.) Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.

c.) Neither the name of Christian Plattner nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS
FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING,
BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software includes work that was released under the following license:

Copyright (c) 2005 - 2006 Swiss Federal Institute of Technology (ETH Zurich), Department of Computer Science (<http://www.inf.ethz.ch>),
Christian Plattner. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions
are met:

a.) Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

b.) Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.

c.) Neither the name of ETH Zurich nor the names of its contributors may be used to endorse or promote products derived from this software
without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS
FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING,
BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The Java implementations of the AES, Blowfish and 3DES ciphers have been taken (and slightly modified) from the cryptography package released by "The Legion Of The Bouncy Castle". Their license states the following:
Copyright (c) 2000 - 2004 The Legion Of The Bouncy Castle (<http://www.bouncycastle.org>)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the
rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN
THE SOFTWARE.

AspectJ Copyright (c) 2007, Eclipse Foundation, Inc. and its licensors. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the Eclipse Foundation, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS
FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING,
BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Jaxen Copyright 2003-2006 The Werken Company. All Rights Reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are
met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.

* Neither the name of the Jaxen Project nor the names of its contributors may be used to endorse or promote products derived
from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER
OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF
LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

JZlib 0.0.* were released under the GNU LGPL license. Later, we have switched over to a BSD-style license.

Copyright (c) 2000,2001,2002,2003 ymnk, JCraft,Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
 3. The names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.
- THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL J-CRAFT, INC. OR ANY CONTRIBUTORS TO THIS SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Lappy Copyright (c) 2010 Kris A. Dover

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Apache log4j Copyright 2007 The Apache Software Foundation

Commons Beanutils Copyright 2007 The Apache Software Foundation

Commons Collections Copyright 2007 The Apache Software Foundation

Commons Digester Copyright 2007 The Apache Software Foundation

Commons Jelly Copyright 2007 The Apache Software Foundation

Commons Launcher Copyright 2007 The Apache Software Foundation

Commons Logging Copyright 2007 The Apache Software Foundation

Commons Modeler Copyright 2007 The Apache Software Foundation

Ant Copyright 2007 The Apache Software Foundation

JavaDB Copyright 2007 The Apache Software Foundation

Fastinfoset Copyright 2007 The Apache Software Foundation

JXTA Copyright 2007 The Apache Software Foundation

Commons Lang Copyright 2007 The Apache Software Foundation

GWT Mosaic Copyright 2010 ???

AppFuse Copyright 2003-2010 AppFuse Team Members

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License.

You may obtain a copy of the License at

<http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

Google Web Toolkit, GIN, Juice Copyright 2010 Google

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License.

You may obtain a copy of the License at

<http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

Spring Copyright 2010 SpringSource

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License.

You may obtain a copy of the License at

<http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

ehcache Copyright 2003-2010 Terracotta, Inc.

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License.

You may obtain a copy of the License at

<http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

Joda Time Copyright 2002-2010 Joda.org

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License.

You may obtain a copy of the License at

<http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

```
=====
== NOTICE file corresponding to the section 4 d of ==
== the Apache License, Version 2.0, ==
== in this case for the SNMP4J distribution. ==
=====
```

This product includes software developed by SNMP4J.org (<http://www.snmp4j.org/>). Please read the different LICENSE files present in the root directory of this distribution.

The names "SNMP4J", "SNMP4J-Agent" and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact info@snmp4j.org (SNMP4J) or apache@apache.org.

XPP3 Indiana University Extreme! Lab Software License Version 1.1.1

Copyright (c) 2002 Extreme! Lab, Indiana University. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment:

"This product includes software developed by the Indiana University Extreme! Lab (<http://www.extreme.indiana.edu/>)."

Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.
4. The names "Indiana University" and "Indiana University Extreme! Lab" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact <http://www.extreme.indiana.edu/>.
5. Products derived from this software may not use "Indiana University" name nor may "Indiana University" appear in their name, without prior written permission of the Indiana University.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS, COPYRIGHT HOLDERS OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

XStream (BSD Style License) Copyright (c) 2003-2006, Joe Walnes Copyright (c) 2006-2007, XStream Committers All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of XStream nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.