



## **5.9 User Guide**

# Table of Contents

## [Chapter 1: Overview](#)

### [Requirements](#)

#### [Indeni Server Requirements](#)

#### [Web User Interface Access Requirements](#)

#### [Analyzed Device Requirements](#)

## [Chapter 2: Installation](#)

### [Installations on Virtual Machines](#)

#### [Configuring the Indeni virtual appliance](#)

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

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

## [Chapter 3: Overview](#)

### [Operations Management](#)

### [Tools](#)

### [Settings](#)

## [Chapter 4: Getting Started](#)

### [Managing Users](#)

#### [Adding a User](#)

### [Adding Devices to the System](#)

#### [Check Point](#)

##### [GAiA](#)

##### [61000 Security System](#)

##### [Provider-1/MDS/MDM - GAiA](#)

##### [Check Point running Embedded GAiA](#)

#### [Cisco](#)

##### [Nexus Switches](#)

##### [F5 BIG-IPs](#)

##### [Palo Alto](#)

## [Adding a Device in the Web UI](#)

### [Upload List of Devices](#)

### [Choosing Credentials](#)

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

### [Vendor Specific](#)

## [Editing Devices](#)

## [Chapter 5: Operations Management](#)

### [The Alerts Sub-Tab](#)

#### [Monitored Devices](#)

#### [Current Alerts](#)

#### [Searching Alerts](#)

#### [Filtering Alerts](#)

#### [Columns and Functionality](#)

#### [Resolving Alerts](#)

##### [Using the Resolve Button](#)

#### [Resolving Multiple Alerts](#)

#### [Annotating Alerts](#)

### [The Analysis Tab](#)

### [Using Signatures in Alerts](#)

#### [Managing the Signatures](#)

##### [Configure](#)

### [Alert Archive](#)

## [Chapter 6: Tools](#)

### [Live Configuration](#)

## [Chapter 7: Settings Tab](#)

### [Monitored Devices](#)

#### [Connectivity](#)

#### [Paths](#)

#### [Troubleshooting parameters](#)

#### [Scheduled Maintenance Window](#)

## [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 Insight](#)

## [Chapter 8: Upgrades and Support](#)

### [Upgrades](#)

### [Support](#)

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

## [Appendix B: Basic Troubleshooting](#)

[Accessing the Embedded GAIa](#)

[Adding Devices to Indeni](#)

# 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](http://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) and be familiar with how to use the command line interface (CLI) for the chosen software.

### Indeni Server Requirements

Indeni supports virtual servers such as VMware. Please contact Indeni support if you have questions regarding your virtual environment. The following server requirement rely on a parameter **N** which represents the number of network devices you plan to analyze with Indeni.

- CPU: 64-bit capable CPU (minimum of 2 cores, with additional one core per every 20 devices in **N**)
- Hard drive:  $170\text{GB} + (2\text{GB} * N)$ . For example, for 10 devices, a total of 190GB is required.
- RAM: The formula is  $50\text{MB} \times N + 2\text{GB}$ , with the minimum being 4GB. For example, for 50 devices a total of 4.5GB is required. For a production setup, Indeni requires the use of at least 4GB.

- **Connectivity:** the server should be able to access all of the required devices via TCP/IP. The server will also need Internet access to retrieve software updates. These can be done via an HTTPS proxy as well.

The installation file includes 64-bit Ubuntu 14.04 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 a local network during the OVA installation. Lack of connectivity may result in the setup script hanging during network configuration. If it's not possible to connect to the network then please contact [support@Indeni.com](mailto:support@Indeni.com)

## Web User Interface Access Requirements

The Indeni GUI is accessible via Web UI. Supported Internet browsers include: Microsoft Internet Explorer, Mozilla Firefox and Google Chrome. The browser's pop-up blocker needs to be disabled.

NOTE: Experience shows that Google Chrome has the best performance of the above listed browsers and should be preferred.

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.
- HTTPS over TCP 8181 – Nonstandard port used for accessing the Indeni Web UI 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.
  - HTTPS (TCP 443)
  - 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**.

# CHAPTER 2: INSTALLATION

As stated in the previous chapter, Indeni runs on a virtual server or on a physical server. Users will need to download the latest version of Indeni from **www.Indeni.com**.



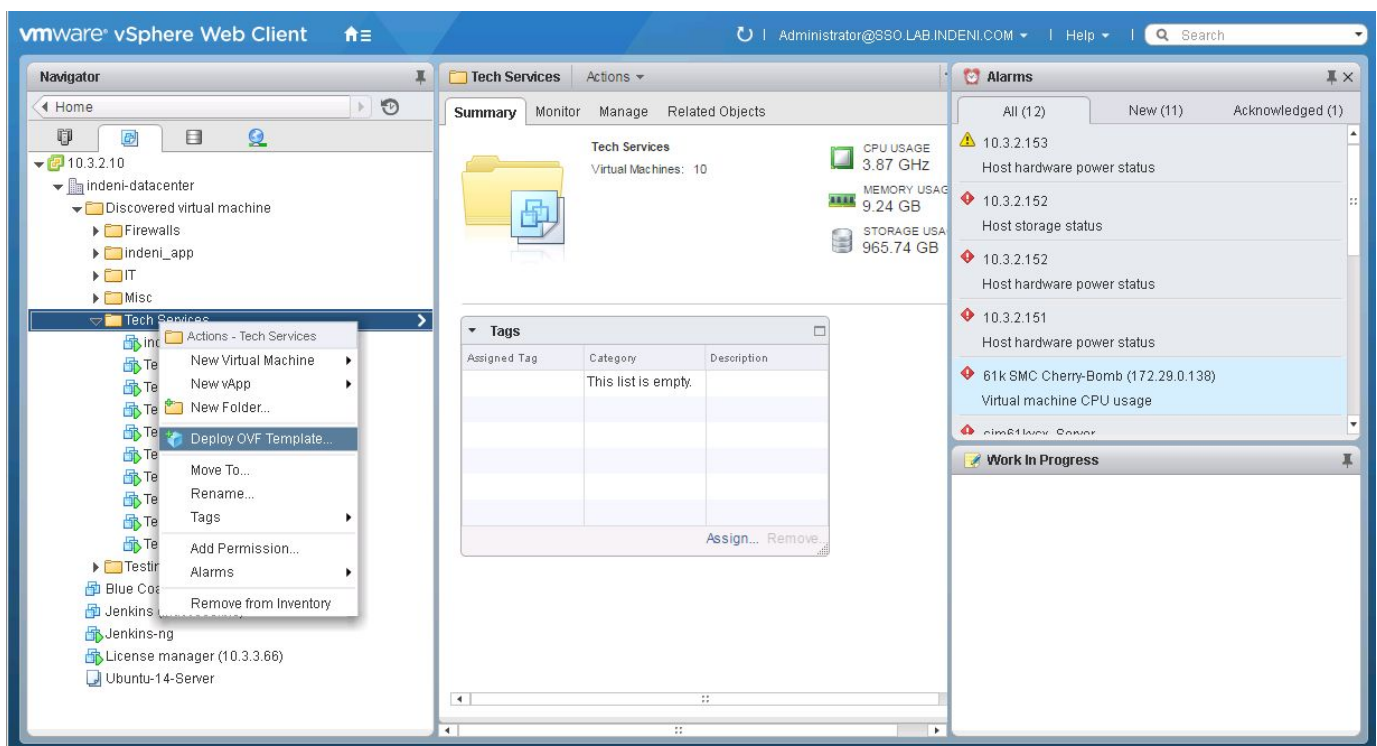
## Installations on Virtual Machines

The Indeni OVA is used for deploying the system in virtualization environments as a virtual appliance.

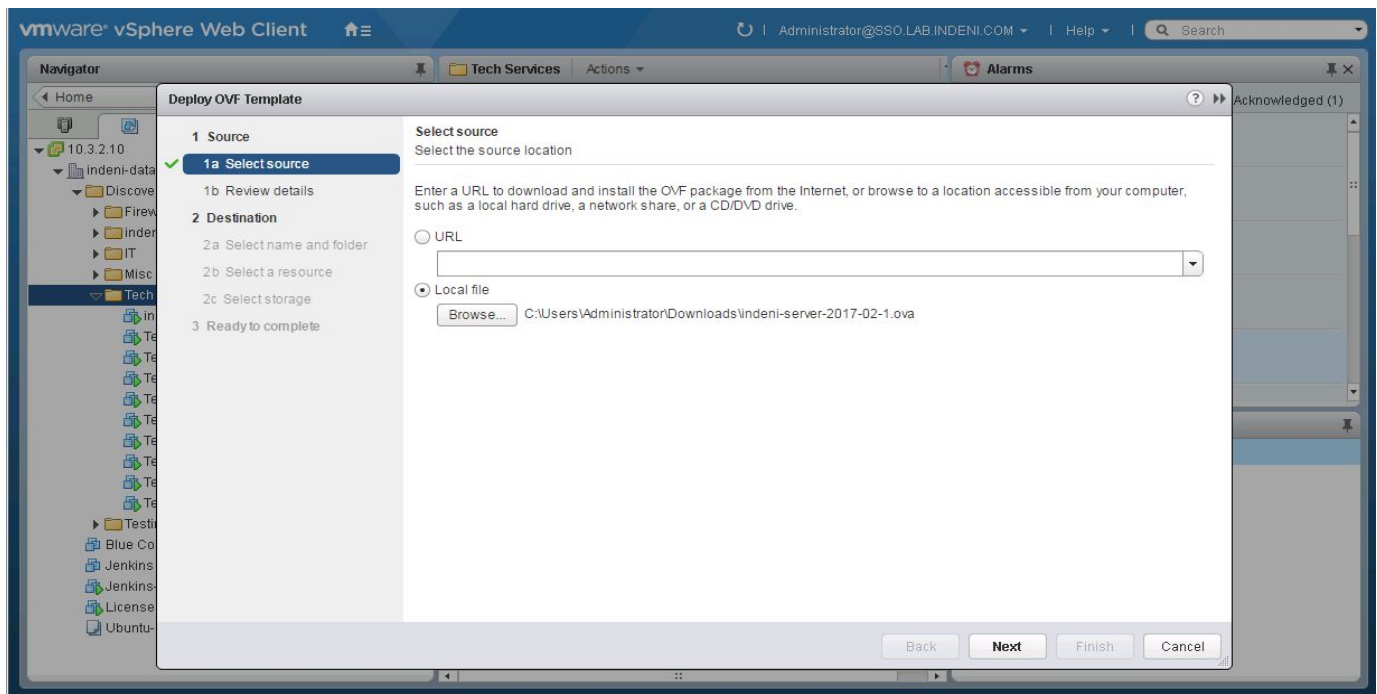
1. Access the download page at <http://offers.Indeni.com/install-Indeni> to download the Indeni OVA.
2. Supply the downloaded OVA to your virtualization environment's administrator for deployment.

## Configuring the Indeni virtual appliance

Log into the VMware interface, such as vSphere Web Client, and select "Deploy OVF Template"

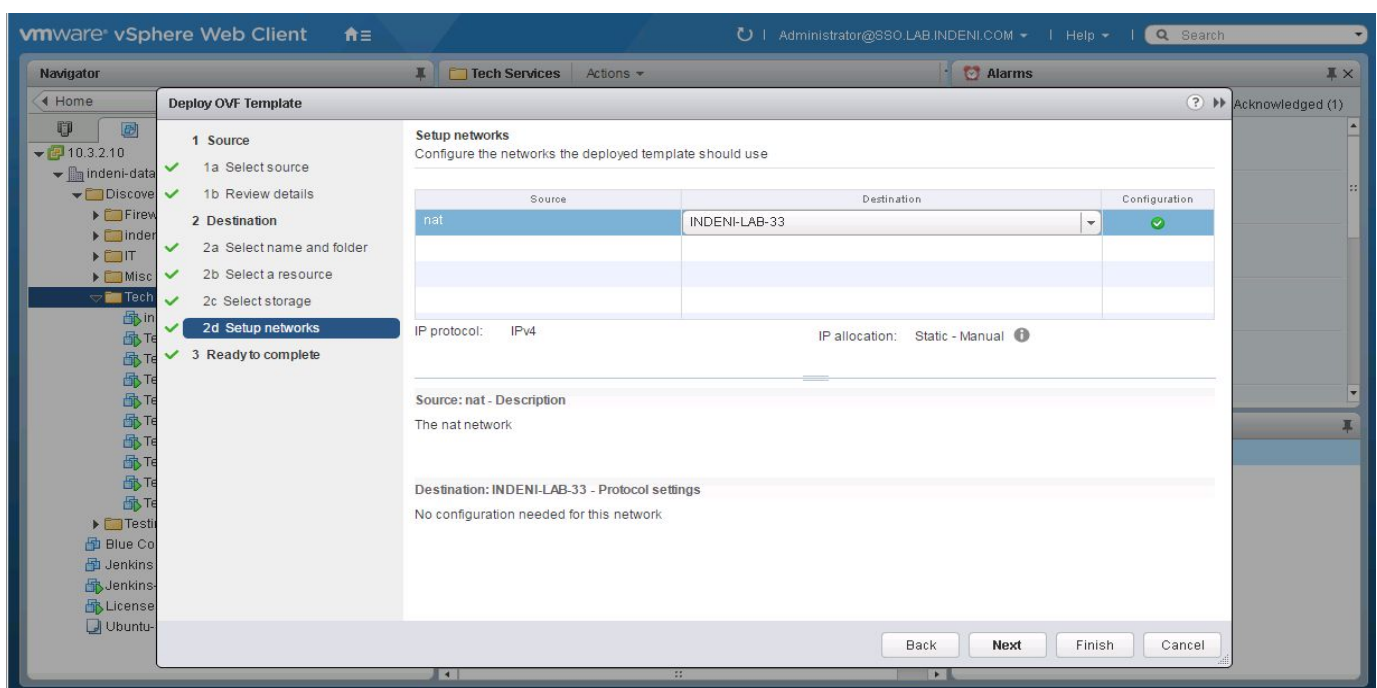


Select the OVF file and proceed to run the wizard



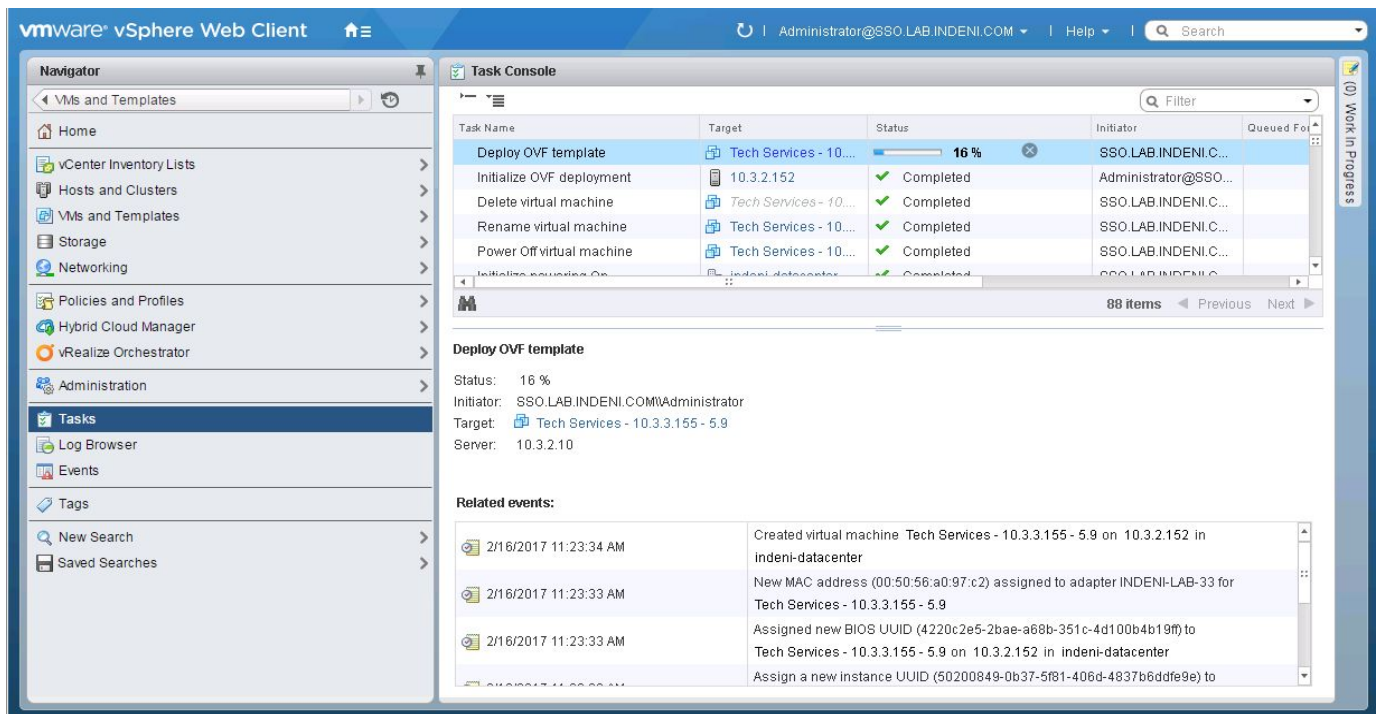
The wizard will ask for the:

1. Name and folder of the new VM
2. VMware resource to use for the VM
3. Storage device
4. Select the relevant network (see below)



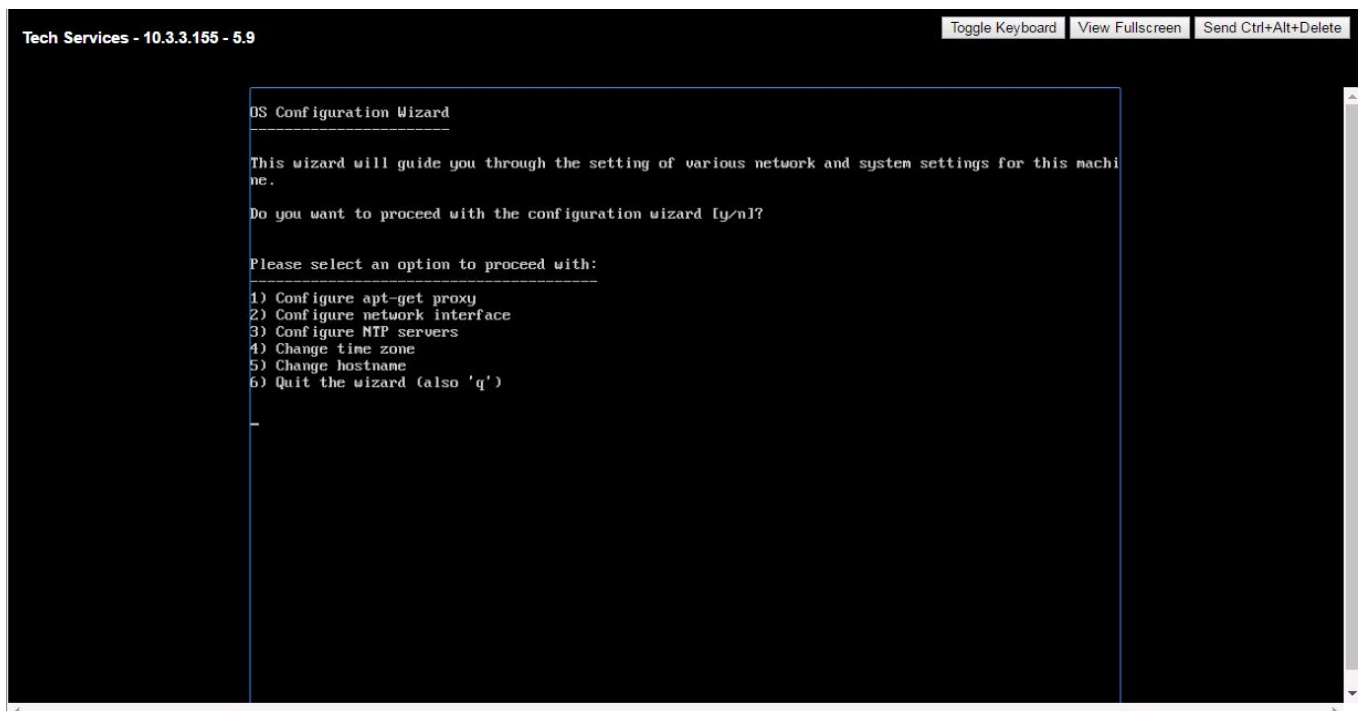
After clicking on Finish, wait for the OVA deployment to complete.





Use the VMware interface to power up the VM and access its console. The initial login will present a wizard to configure the device's apt-get proxy, static IP, NTP server, time zone and hostname.

The "apt-get proxy" should be configured if this VM is required to access the Internet via a proxy, instead of directly. "apt-get" is used to update the Indeni software installed on the VM.



## Logging in to the System - Console

You can log in to the system after reboot, as shown in the previous section:

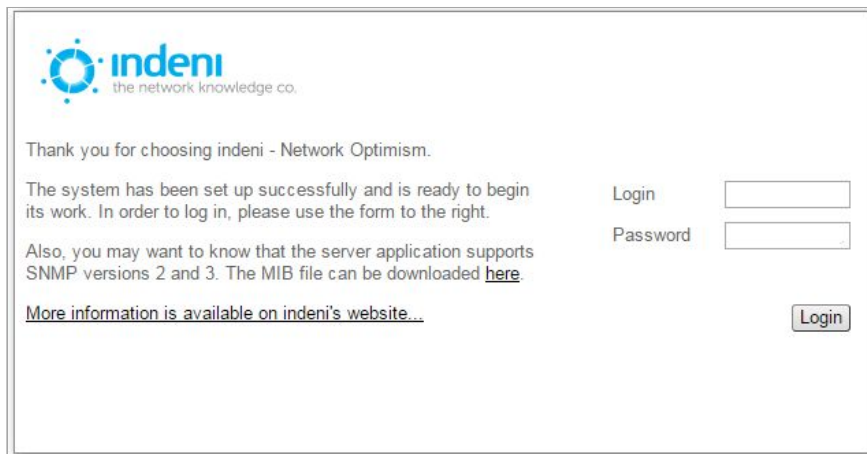
Username: **indeni**  
Password: **indeni4it**

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/](https://<Indeni_ip>:8181/)
3. Substitute your server's IP address for <Indeni\_ip> (example:  
<https://10.3.1.87:8181/>).
4. Log in to the Indeni web dashboard:

Username: **admin**  
Password: **admin123!**



The screenshot shows the Indeni web dashboard login page. At the top left is the Indeni logo with the tagline 'the network knowledge co.'. Below the logo, a message reads: '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.' To the right of this text is a login form with two input fields: 'Login' and 'Password'. Below the 'Login' field is a 'Login' button. A link at the bottom left says '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...'

## CHAPTER 3: OVERVIEW

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

- **Operations Management**
- **Tools**
- **Settings**

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

### 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**, **Knowledge Management**, and **Alert Archive**) to access further functionality as described on the next page.

The screenshot displays the Indeni Operations Management interface. The top navigation bar includes 'Operate' and 'Help' links, and the Indeni logo. Below this, the 'Operations Management' tab is selected, with sub-tabs for 'Alerts', 'Analysis', 'Knowledge Management', and 'Alert Archive'. The 'Alerts' sub-tab is active.

The interface is divided into two main panels:

- Monitored Devices:** Located on the left, it features a search bar and an 'Add Device...' button. A list of devices is shown, including 'checkpoint', 'checkpoint VMware Virtual Platform', 'fs BIG-IP Virtual Edition', 'paloaltonetworks PA-VM', and 'paloaltonetworks Panorama'.
- Current Alerts:** Located on the right, it features a search bar and buttons for 'View', 'Resolve', 'Freeze', and 'Export...'. A table lists current alerts with columns for ID, Device, Headline, and Last Update.

The table of Current Alerts contains the following data:

ID	Device	Headline	Last Update
34	PAN15 (10.3.1.15)	High memory usage	Feb 17, 2017 10:09:03 AM
33	VSX (10.3.3.38)	DNS lookup failure(s)	Feb 16, 2017 01:05:19 PM
32	Montezuma (10.3.3.38)	DNS lookup failure(s)	Feb 16, 2017 12:59:19 PM
31	Arkhan (10.3.3.61)	DNS lookup failure(s)	Feb 16, 2017 12:59:19 PM
30	PAN14 (10.3.1.14)	High memory usage	Feb 16, 2017 12:51:03 PM
29	Knight (10.3.3.62)	Communication issues with certain log servers	Feb 16, 2017 12:46:20 PM
28	Arkhan (10.3.3.61)	Communication issues with certain log servers	Feb 16, 2017 12:45:20 PM
27	VSX (10.3.3.38)	License usage limit approaching	Feb 16, 2017 12:35:32 PM
26	Metal (10.3.3.72)	License usage limit approaching	Feb 16, 2017 12:35:32 PM
25	Metal (10.3.3.72)	Phote(s) down	Feb 16, 2017 12:33:14 PM
24	Knight (10.3.3.62)	Phote(s) down	Feb 16, 2017 12:30:29 PM
23	Knight (10.3.3.62)	Cluster down	Feb 16, 2017 12:30:07 PM

The bottom status bar shows the date 'Feb 19, 2017 02:37:01 PM' and the build version '5.9.0 build 189.20170216 (d59f488)'.

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:

<b>Alerts</b>	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).
<b>Analysis</b>	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.
<b>Knowledge Management</b>	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.
<b>Alert Archive</b>	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](#).

## 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.

The screenshot shows the Indeni web interface. At the top, there are tabs for 'Operate', 'Help', 'Operations Management', 'Tools' (selected), and 'Settings'. Below the 'Tools' tab, there is a 'Live Configuration' sub-tab. The main content area is divided into two panels. The left panel, titled 'Monitored Devices', contains a search bar and a list of devices: Arkhan (10.3.3.61), F5 (10.3.3.134), Hideo (10.3.3.75), Knight (10.3.3.62), Kojima (10.3.3.76), Metal (10.3.3.72), Montezuma (10.3.3.148), and P1 (10.3.3.150). The right panel, titled 'Live Configuration', shows the configuration for the selected device 'Arkhan/OS (10.3.3.61)'. It contains a table with the following data:

Device: Arkhan/OS (10.3.3.61)	
Overview	: Value: Gaia Value: Check Point Value: VMware Virtual Platform
ARP Cache - Limit	4096.0
CCP Mode	broadcast
CPU	<u>cpu-id-0:</u> Value: 2.02% <u>cpu-id-1:</u> Value: 29.29% <u>cpu-id-all-average:</u> Value: 15.74%
Cluster Member State (this)	DOWN/INACTIVE
ClusterXL Devices	<u>name-fwd:</u> Value: UP/ACTIVE <u>name-Interface Active Check:</u> Value: DOWN/INACTIVE <u>name-Filter:</u> Value: UP/ACTIVE <u>name-Discovery Delay:</u>

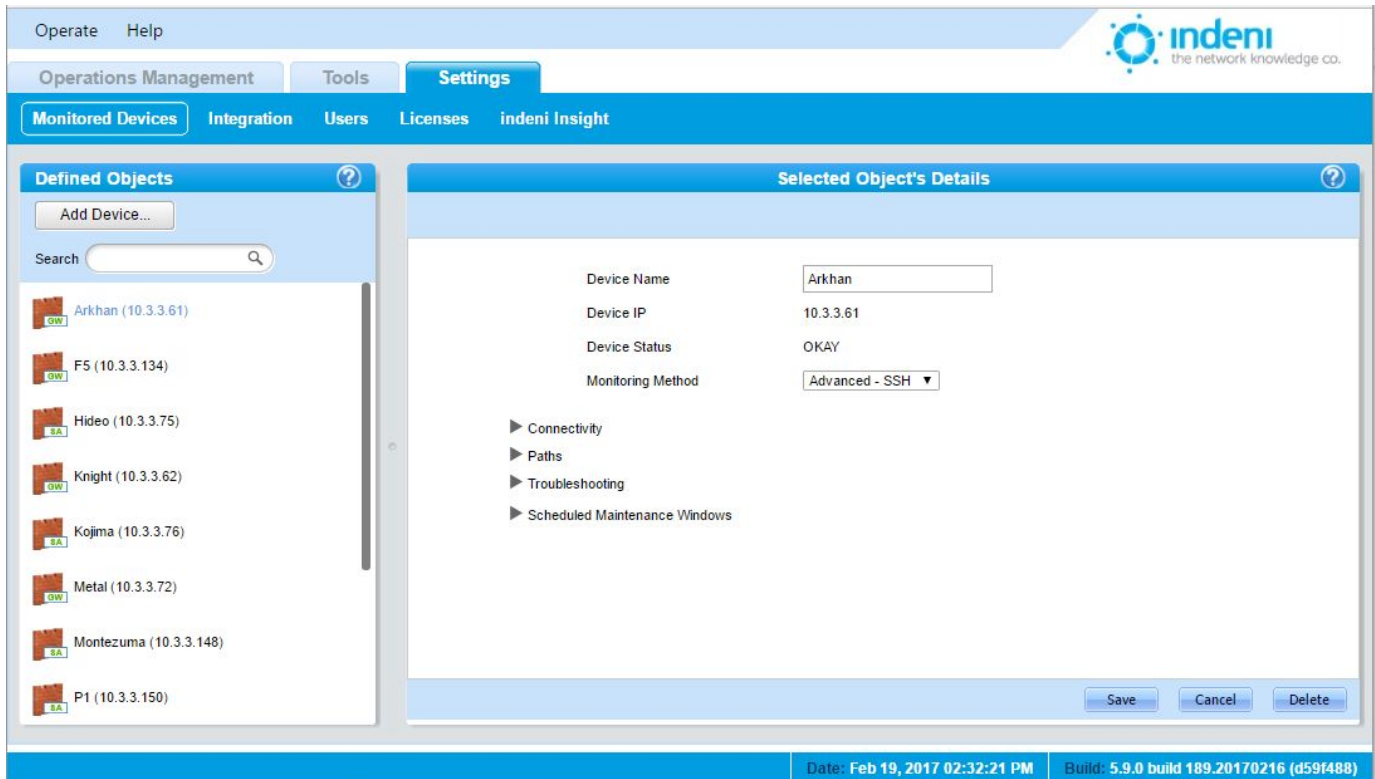
At the bottom of the interface, there is a status bar showing 'Date: Feb 19, 2017 02:31:31 PM' and 'Build: 5.9.0 build 189.20170216 (d59f488)'.

### 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

# 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.

**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.

## 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.

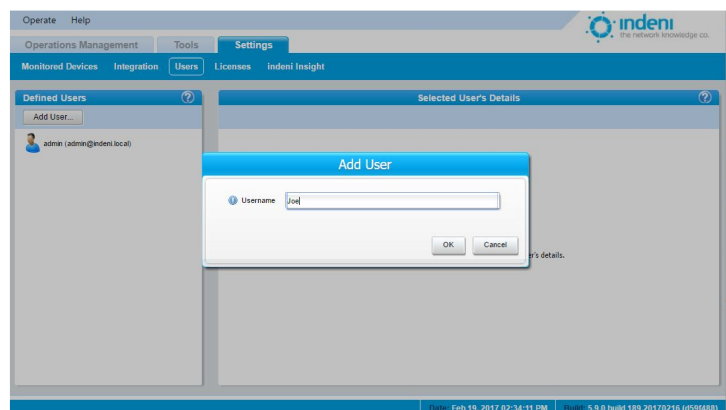
### Managing Users

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**.

**NOTE:** If more than one user is to access the Indeni Web UI at one time, then additional users must be created. Indeni will not allow concurrent users to have the same login.

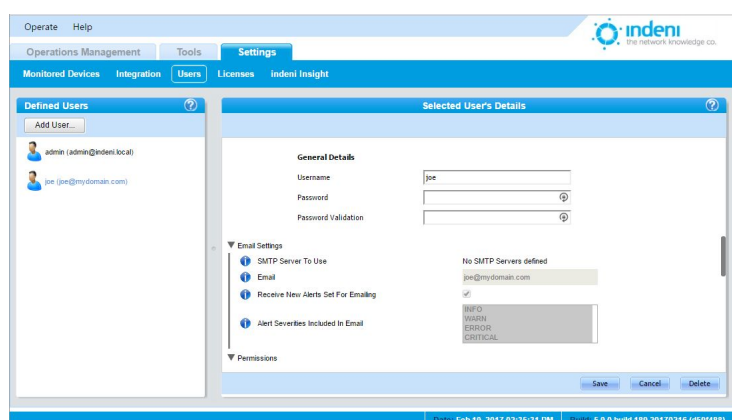
#### Adding a User

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

### GAiA

#### Adding a User to GAiA via the Portal

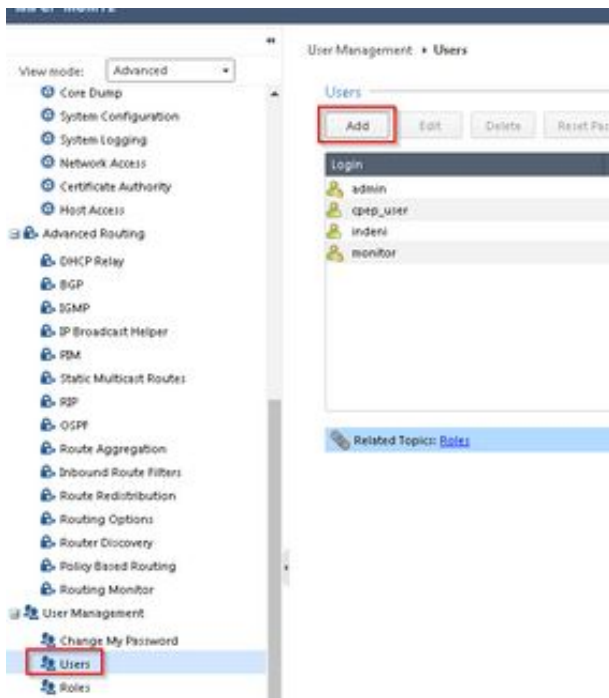
1. Log in to the Web UI.
2. Navigate to User Management -> Users
3. Select the ADD button in the viewing pane.
4. Add a user and select OK. Be sure to select the **/bin/bash** shell and the **adminRole**.

The screenshot shows the 'Add User' dialog box with the following details:

- Login Name:** indeni
- Password:** [masked] (Strength: Good)
- Confirm Password:** [masked]
- Real Name:** Indeni
- Home Directory:** /home/indeni
- Shell:** /bin/bash
- Available Roles:** monitorRole
- Assigned Roles:** adminRole
- Access Mechanisms:**
  - ☒ Web
  - ☒ Command Line
- Buttons:** Add >, < Remove, OK, Cancel

NOTE: Check Point R80 Management Web UI screenshot below.





## 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/MDS/MDM - 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.

## Check Point running Embedded GAIa

1. Login to the Embedded GAIa device via CLI
2. Type “expert” to enter expert mode
3. Run: bashUser on

## Cisco

### Nexus Switches

To add a local user:

```
username user-id [ password password ] [ expire date ] [ role role-name ]
```

The role can be **network-operator** which has complete read access to the Nexus Switch refer to the relevant configuration guide for further information:

[http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/sec\\_rbac.html](http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/sec_rbac.html)

## F5 BIG-IPs

In the Web UI, navigate to System -> User

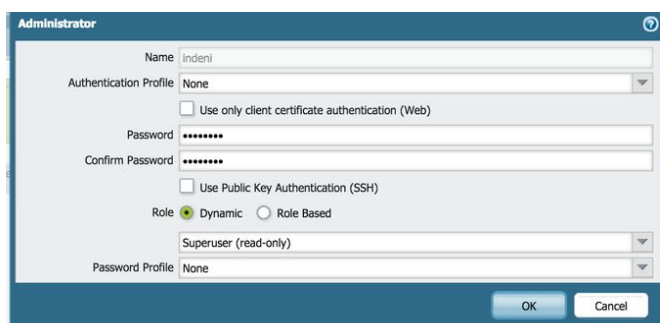
NOTE: For more information about why administrative privileges are needed, please refer to this article:

<http://Indeni.com/how-to-select-script-monitoring-authentication-types/>

Please note that when using the local admin account it is required to configure SSH access manually as this is not enabled by default.

## Palo Alto

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



The screenshot shows the 'Administrator' user creation form in the Palo Alto firewall's web interface. The form includes the following fields and options:

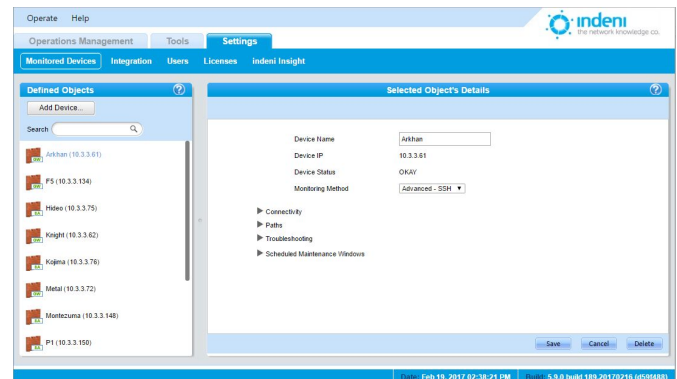
- Name:** indeni
- Authentication Profile:** None
- ☐ Use only client certificate authentication (Web)
- Password:** [masked with dots]
- Confirm Password:** [masked with dots]
- ☐ Use Public Key Authentication (SSH)
- Role:** Dynamic (selected), Role Based
- Role:** Superuser (read-only) (selected from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


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


## Adding a Device in the Web 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.

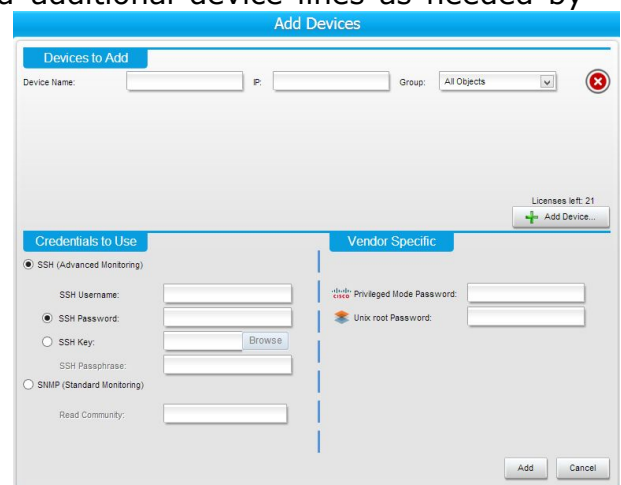


Indeni supports adding multiple devices at once. If two or more devices are to be added at once, add additional device lines as needed by clicking the  button in the dialog box.

Delete unneeded blank boxes by clicking on the  symbol.

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

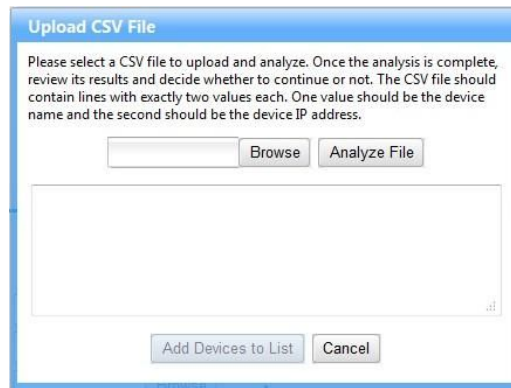
**Device Name: Cluster\_Member1**  
**IP: 10.3.1.88**



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.

## 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: DEVICE NAME, DEVICE IP,

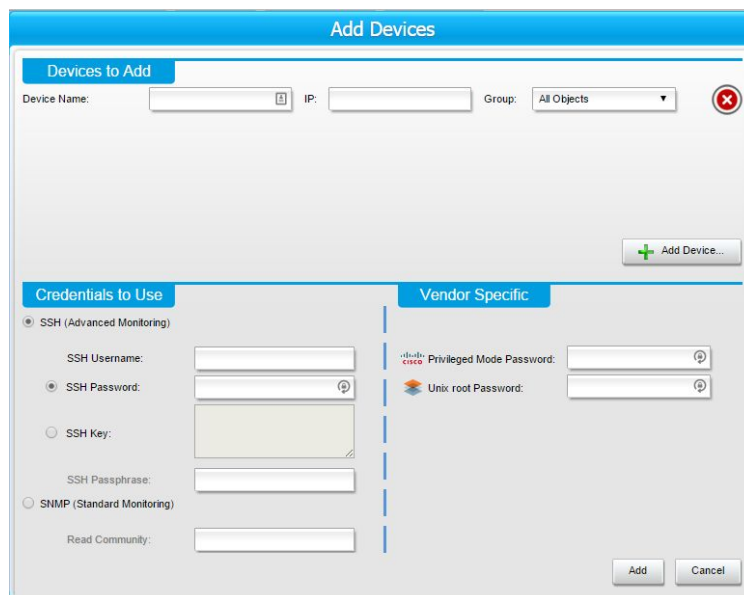


**Upload CSV File**

Please select a CSV file to upload and analyze. Once the analysis is complete, review its results and decide whether to continue or not. The CSV file should contain lines with exactly two values each. One value should be the device name and the second should be the device IP address.

## 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)**.



**Add Devices**

**Devices to Add**

Device Name:  IP:  Group:

**Credentials to Use**

☒ SSH (Advanced Monitoring)

SSH Username:

☒ SSH Password:

☐ SSH Key:

SSH Passphrase:

☐ SNMP (Standard Monitoring)

Read Community:

**Vendor Specific**

☐ Privileged Mode Password:

☐ Unix root Password:

## 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 (GAiA, Secure Platform, PAN-OS, 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.

## 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.



The screenshot shows a 'Vendor Specific' section with two password input fields. The first field is labeled 'Privileged Mode Password' and has a Cisco logo icon to its left. The second field is labeled 'Unix root Password' and has a Linux logo icon to its left. Both fields are empty text boxes.

## 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**.

# CHAPTER 5: OPERATIONS MANAGEMENT

## The Alerts Sub-Tab

Indeni was designed to simplify management of networks and to free an administrator's 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 screenshot shows the Indeni Operations Management interface. The top navigation bar includes 'Operate' and 'Help'. Below it, the 'Operations Management' tab is active, with sub-tabs for 'Alerts', 'Analysis', 'Knowledge Management', and 'Alert Archive'. The 'Alerts' sub-tab is selected, displaying the 'Current Alerts' pane. On the left, the 'Monitored Devices' pane shows a list of devices with a dropdown menu for filtering by Group, Cluster, Type, or Management Hierarchy. The 'Current Alerts' pane displays a table of alerts with columns for ID, Device, Headline, Last Update, and Created. The table lists various alerts such as 'Packet drop counters increasing', 'Configuration changed but not saved', and 'NTP sync failure(s)'.

ID	Device	Headline	Last Update	Created
57	PAN15 (10.3.1.15)	Packet drop counters increasing	Feb 20, 2017 10:18:54 AM	Feb 20, 2017 01:16:31 AM
66	V5X (10.3.3.38)	Configuration changed but not saved	Feb 20, 2017 09:49:57 AM	Feb 20, 2017 09:49:57 AM
65	Montezuma (10.3....)	Configuration changed but not saved	Feb 20, 2017 09:40:57 AM	Feb 20, 2017 09:40:57 AM
64	Knight (10.3.3.62)	Configuration changed but not saved	Feb 20, 2017 09:39:57 AM	Feb 20, 2017 09:39:57 AM
63	Arkhan (10.3.3.61)	Configuration changed but not saved	Feb 20, 2017 09:39:57 AM	Feb 20, 2017 09:39:57 AM
61	Montezuma (10.3....)	NTP sync failure(s)	Feb 20, 2017 09:30:09 AM	Feb 20, 2017 09:30:09 AM
60	Hideo (10.3.3.75)	NTP sync failure(s)	Feb 20, 2017 09:30:09 AM	Feb 20, 2017 09:30:09 AM
59	Kojima (10.3.3.76)	NTP sync failure(s)	Feb 20, 2017 09:30:09 AM	Feb 20, 2017 09:30:09 AM
58	Metal (10.3.3.72)	Network port(s) down	Feb 20, 2017 09:28:27 AM	Feb 20, 2017 09:28:27 AM
49	Hideo (10.3.3.75)	SIC to certain managed devices not working	Feb 19, 2017 03:58:29 PM	Feb 19, 2017 03:58:29 PM
48	Kojima (10.3.3.76)	SIC to certain managed devices not working	Feb 19, 2017 03:58:29 PM	Feb 19, 2017 03:58:29 PM
47	P1 (10.3.3.150)	SIC to certain managed devices not working	Feb 19, 2017 03:56:29 PM	Feb 19, 2017 03:56:29 PM
46	PAN15 (10.3.1.15)	DNS lookup failure(s)	Feb 19, 2017 03:56:06 PM	Feb 19, 2017 03:56:06 PM
45	Hideo (10.3.3.75)	High disk space utilization	Feb 19, 2017 03:45:48 PM	Feb 19, 2017 03:45:48 PM
44	Kojima (10.3.3.76)	High disk space utilization	Feb 19, 2017 03:45:48 PM	Feb 19, 2017 03:45:48 PM
43	PAN15 (10.3.1.15)	Clock set incorrectly	Feb 19, 2017 03:41:43 PM	Feb 19, 2017 03:41:43 PM
41	Montezuma (10.3....)	High disk space utilization	Feb 19, 2017 03:35:48 PM	Feb 19, 2017 03:35:48 PM

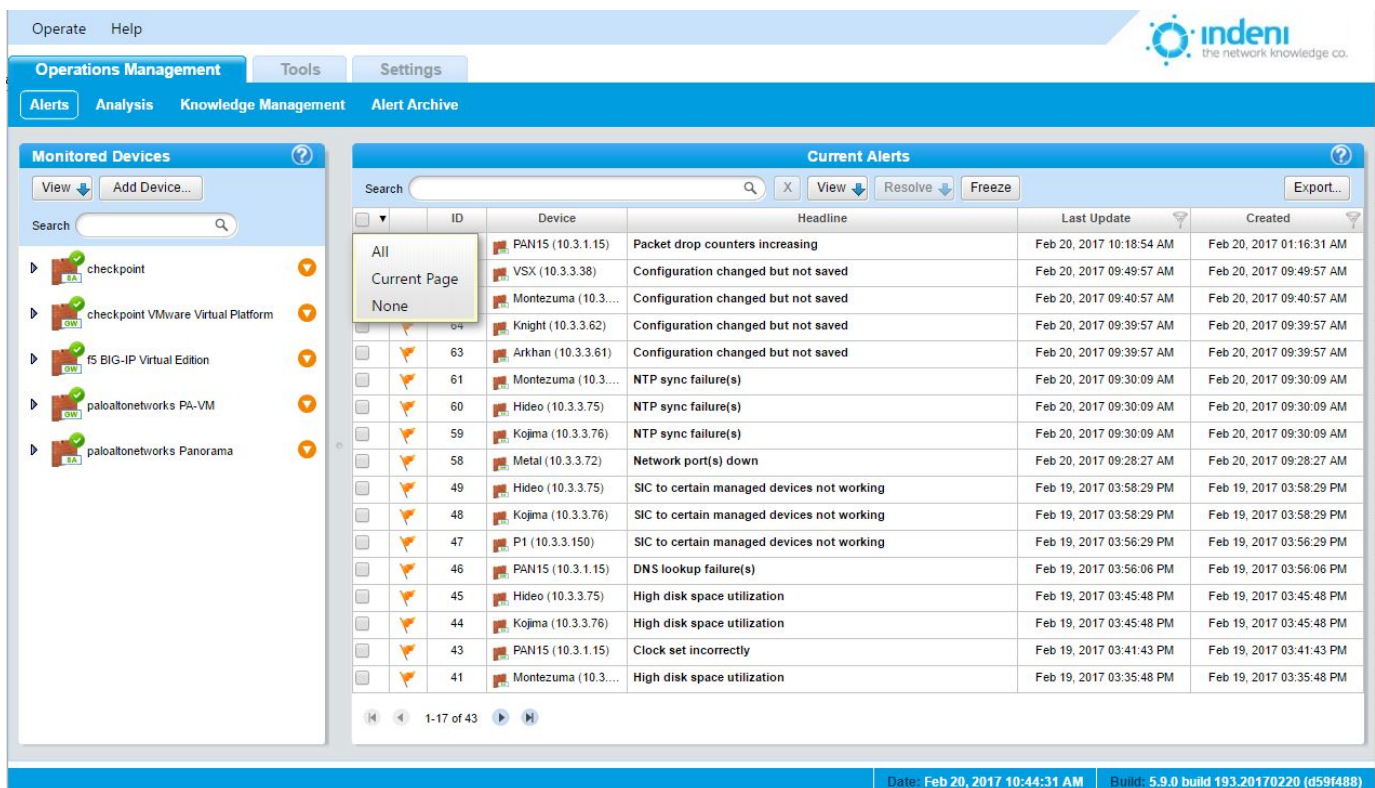
The bottom status bar shows the date 'Feb 20, 2017 10:43:41 AM' and the build version 'Build: 5.9.0 build 193.20170220 (d59f488)'.

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 screenshot shows the Indeni Operations Management interface. The 'Current Alerts' pane is active, displaying a table of alerts. The table has columns for ID, Device, Headline, Last Update, and Created. A dropdown menu is open over the 'All' checkbox, showing options: 'All', 'Current Page', and 'None'. The table contains 17 alerts, with the first few showing configuration changes and NTP sync failures. The bottom status bar indicates the date as Feb 20, 2017 10:44:31 AM and the build as 5.9.0 build 193.20170220 (d59f488).

ID	Device	Headline	Last Update	Created
	PAN15 (10.3.1.15)	Packet drop counters increasing	Feb 20, 2017 10:18:54 AM	Feb 20, 2017 01:16:31 AM
	VSX (10.3.3.38)	Configuration changed but not saved	Feb 20, 2017 09:49:57 AM	Feb 20, 2017 09:49:57 AM
	Montezuma (10.3....)	Configuration changed but not saved	Feb 20, 2017 09:40:57 AM	Feb 20, 2017 09:40:57 AM
	Knight (10.3.3.62)	Configuration changed but not saved	Feb 20, 2017 09:39:57 AM	Feb 20, 2017 09:39:57 AM
	Arkhan (10.3.3.61)	Configuration changed but not saved	Feb 20, 2017 09:39:57 AM	Feb 20, 2017 09:39:57 AM
63	Montezuma (10.3....)	NTP sync failure(s)	Feb 20, 2017 09:30:09 AM	Feb 20, 2017 09:30:09 AM
61	Hideo (10.3.3.75)	NTP sync failure(s)	Feb 20, 2017 09:30:09 AM	Feb 20, 2017 09:30:09 AM
60	Kojima (10.3.3.76)	NTP sync failure(s)	Feb 20, 2017 09:30:09 AM	Feb 20, 2017 09:30:09 AM
59	Metal (10.3.3.72)	Network port(s) down	Feb 20, 2017 09:28:27 AM	Feb 20, 2017 09:28:27 AM
58	Hideo (10.3.3.75)	SIC to certain managed devices not working	Feb 19, 2017 03:58:29 PM	Feb 19, 2017 03:58:29 PM
49	Kojima (10.3.3.76)	SIC to certain managed devices not working	Feb 19, 2017 03:58:29 PM	Feb 19, 2017 03:58:29 PM
48	P1 (10.3.3.150)	SIC to certain managed devices not working	Feb 19, 2017 03:56:29 PM	Feb 19, 2017 03:56:29 PM
47	PAN15 (10.3.1.15)	DNS lookup failure(s)	Feb 19, 2017 03:56:06 PM	Feb 19, 2017 03:56:06 PM
46	Hideo (10.3.3.75)	High disk space utilization	Feb 19, 2017 03:45:48 PM	Feb 19, 2017 03:45:48 PM
45	Kojima (10.3.3.76)	High disk space utilization	Feb 19, 2017 03:45:48 PM	Feb 19, 2017 03:45:48 PM
44	PAN15 (10.3.1.15)	Clock set incorrectly	Feb 19, 2017 03:41:43 PM	Feb 19, 2017 03:41:43 PM
43	Montezuma (10.3....)	High disk space utilization	Feb 19, 2017 03:35:48 PM	Feb 19, 2017 03:35:48 PM
41				

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.

- 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.

The screenshot shows the Indeni Operations Management interface. The top navigation bar includes 'Operate', 'Help', 'Operations Management', 'Tools', and 'Settings'. Below this is a sub-navigation bar with 'Alerts', 'Analysis', 'Knowledge Management', and 'Alert Archive'. The main content area is divided into two panels: 'Monitored Devices' on the left and 'Current Alerts' on the right.

The 'Monitored Devices' panel shows a list of devices under the 'checkpoint VMware Virtual Platform' category. The devices listed are: Arkhan (10.3.3.61) with 6 error alerts, Hideo (10.3.3.75) with 3 error alerts, Knight (10.3.3.62) with 4 error alerts, Kojima (10.3.3.76) with 3 error alerts, Metal (10.3.3.72) with 3 error alerts, Montezuma (10.3.3.148) with 5 error alerts, VSX (10.3.3.38) with 3 error alerts, and F5 BIG-IP Virtual Edition. The 'F5 (10.3.3.134)' device is also listed.

The 'Current Alerts' panel shows a table of alerts for the selected device 'Arkhan (10.3.3.61)'. The table has columns for 'ID', 'Device', 'Headline', 'Last Update', and 'Created'. The alerts are as follows:

ID	Device	Headline	Last Update	Created
63	Arkhan (10.3.3.61)	Configuration changed but not saved	Feb 20, 2017 09:39:57 AM	Feb 20, 2017 09:39:57 AM
31	Arkhan (10.3.3.61)	DNS lookup failure(s)	Feb 16, 2017 12:59:19 PM	Feb 16, 2017 12:59:19 PM
28	Arkhan (10.3.3.61)	Communication issues with certain log servers	Feb 16, 2017 12:45:20 PM	Feb 16, 2017 12:45:20 PM
18	Arkhan (10.3.3.61)	Routes defined in clish/webUI are missing	Feb 16, 2017 12:29:01 PM	Feb 16, 2017 12:29:01 PM
16	Arkhan (10.3.3.61)	Pnote(s) down	Feb 16, 2017 12:28:29 PM	Feb 16, 2017 12:28:29 PM
	Arkhan (10.3.3.61)	Cluster down	Feb 16, 2017 12:28:07 PM	Feb 16, 2017 12:28:07 PM

A context menu is open over the 'Arkhan (10.3.3.61)' device in the 'Monitored Devices' panel, showing options: 'Device Configuration', 'Filter Current Alerts', and 'Stop or Suspend Monitoring'. The 'Filter Current Alerts' option is highlighted.

The bottom status bar shows the date 'Date: Feb 20, 2017 10:45:21 AM' and the build version 'Build: 5.9.0 build 193.20170220 (d59f488)'.

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

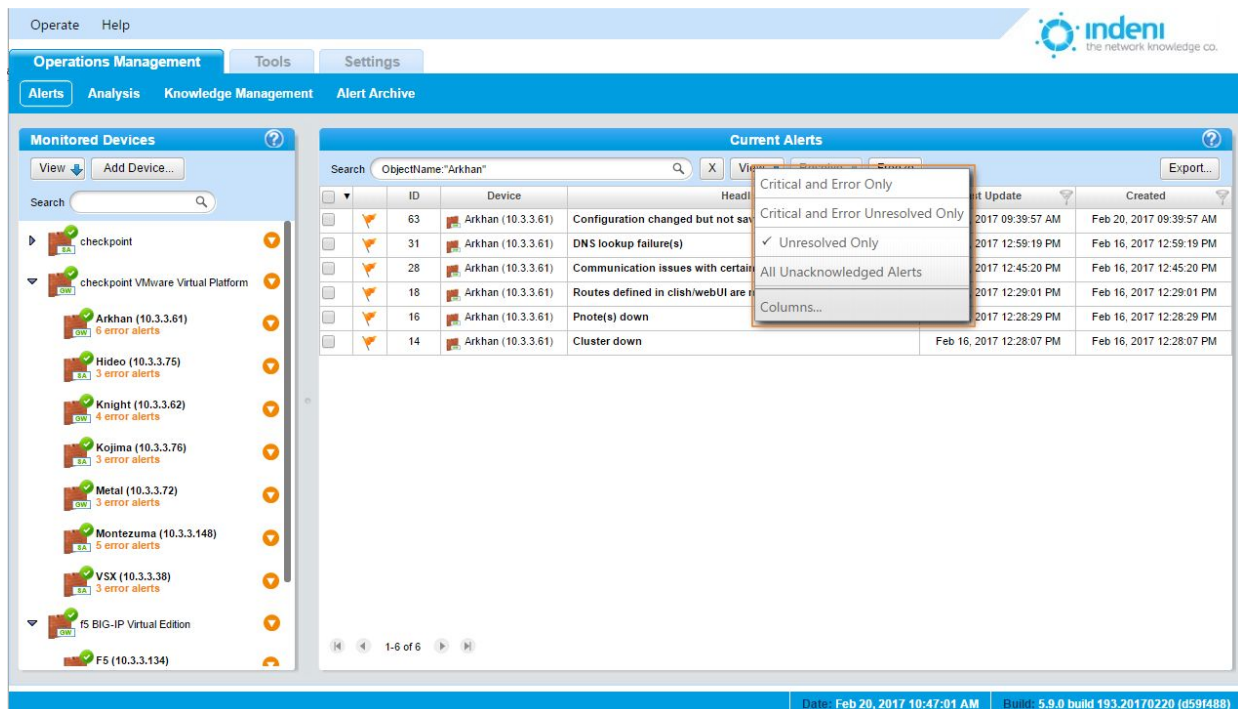
This column displays a colored flag for each alert. Colors range from red to blue to distinguish critical warnings from less severe alerts. This allows users to find and resolve alerts most likely to cause imminent downtime and to visually assess the type of alert and remedial action required.



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	

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

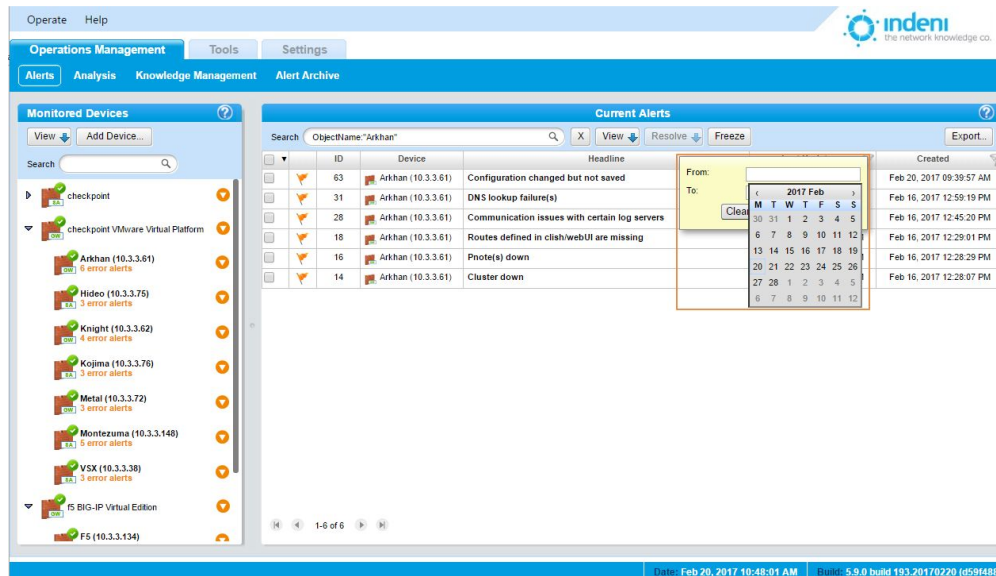
This column displays the actual alert information: a brief description of the condition Indeni has observed as well as its status.

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**.

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.

## Reviewing Alert Details

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.

The screenshot displays the Indeni Operations Management web interface. The top navigation bar includes 'Operate' and 'Help' menus, and the 'indeni' logo with the tagline 'the network knowledge co.'. Below this, a secondary navigation bar contains 'Operations Management', 'Tools', and 'Settings'. A third bar highlights 'Alerts', 'Analysis', 'Knowledge Management', and 'Alert Archive'.

The main content area is divided into two panels. The left panel, titled 'Monitored Devices', shows a tree view of devices under 'checkpoint' and 'checkpoint VMware Virtual Platform'. Devices listed include Arkhan (10.3.3.61), Hideo (10.3.3.75), Knight (10.3.3.62), Kojima (10.3.3.76), Metal (10.3.3.72), Montezuma (10.3.3.148), VSX (10.3.3.38), and F5 BIG-IP Virtual Edition (F5 (10.3.3.134)). Each device has a status icon and a count of error alerts.

The right panel, titled 'Current Alerts', shows a table of alerts filtered by 'ObjectName: Arkhan'. The table has columns for 'ID', 'Device', 'Headline', 'Last Update', and 'Created'. The 'Freeze' button is visible in the top right of the alerts table.

ID	Device	Headline	Last Update	Created
63	Arkhan (10.3.3.61)	Configuration changed but not saved	Feb 20, 2017 09:39:57 AM	Feb 20, 2017 09:39:57 AM
31	Arkhan (10.3.3.61)	DNS lookup failure(s) <b>Description:</b> One or more DNS servers configured on this device are not responding or are failing to resolve www.indeni.com. <b>DNS Servers Affected:</b> 10.3.3.1 <b>Remediation Steps:</b> Review the cause for the DNS resolution not working. <b>Notes and History:</b> Feb 16 12:59:19 2017 IST: Alert created. Feb 16 12:59:19 2017 IST: Associated item added: 10.3.3.1 <a href="#">Append note...</a>	Feb 16, 2017 12:59:19 PM	Feb 16, 2017 12:59:19 PM
28	Arkhan (10.3.3.61)	Communication issues with certain log servers	Feb 16, 2017 12:45:20 PM	Feb 16, 2017 12:45:20 PM
18	Arkhan (10.3.3.61)	Routes defined in cliish/webUI are missing	Feb 16, 2017 12:29:01 PM	Feb 16, 2017 12:29:01 PM
16	Arkhan (10.3.3.61)	Probe(s) down	Feb 16, 2017 12:28:29 PM	Feb 16, 2017 12:28:29 PM
14	Arkhan (10.3.3.61)	Cluster down	Feb 16, 2017 12:28:07 PM	Feb 16, 2017 12:28:07 PM

The bottom status bar shows the date 'Feb 20, 2017 10:49:01 AM' and the build version '5.9.0 build 193.20170220 (d59f488)'.

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.

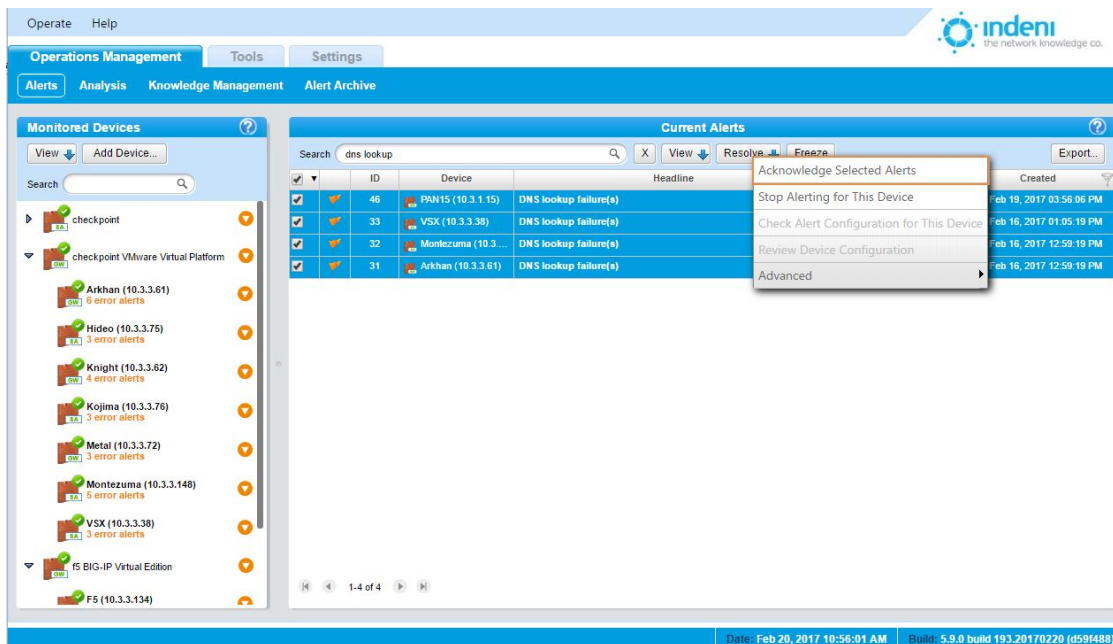
The screenshot displays the Indeni Operations Management interface. On the left, the 'Monitored Devices' panel lists various devices under categories like 'checkpoint' and '15 BIG-IP Virtual Edition'. The main area shows 'Current Alerts' for the selected device 'Arkhan (10.3.3.61)'. The alerts table includes columns for ID, Device, Headline, Last Update, and Created. One alert is selected, showing details for a 'DNS lookup failure(s)'. The 'Resolve' button is visible above the 'Headline' column.

ID	Device	Headline	Last Update	Created
63	Arkhan (10.3.3.61)	Configuration changed but not saved	Feb 20, 2017 09:39:57 AM	Feb 20, 2017 09:39:57 AM
31	Arkhan (10.3.3.61)	DNS lookup failure(s) Description: One or more DNS servers configured on this device are not responding or are failing to resolve www.indeni.com DNS Servers Affected: 10.3.3.1 Remediation Steps: Review the cause for the DNS resolution not working Notes and History: Feb 16 12:59:19 2017 IST: Alert created. Feb 16 12:59:19 2017 IST: Associated item added: 10.3.3.1 Append more...	Feb 16, 2017 12:59:19 PM	Feb 16, 2017 12:59:19 PM
28	Arkhan (10.3.3.61)	Communication issues with certain log servers	Feb 16, 2017 12:45:20 PM	Feb 16, 2017 12:45:20 PM
18	Arkhan (10.3.3.61)	Routes defined in clish/webUI are missing	Feb 16, 2017 12:29:01 PM	Feb 16, 2017 12:29:01 PM
16	Arkhan (10.3.3.61)	Phote(s) down	Feb 16, 2017 12:28:29 PM	Feb 16, 2017 12:28:29 PM
14	Arkhan (10.3.3.61)	Cluster down	Feb 16, 2017 12:28:07 PM	Feb 16, 2017 12:28:07 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 leave only the active alerts present in the current alert list. 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.

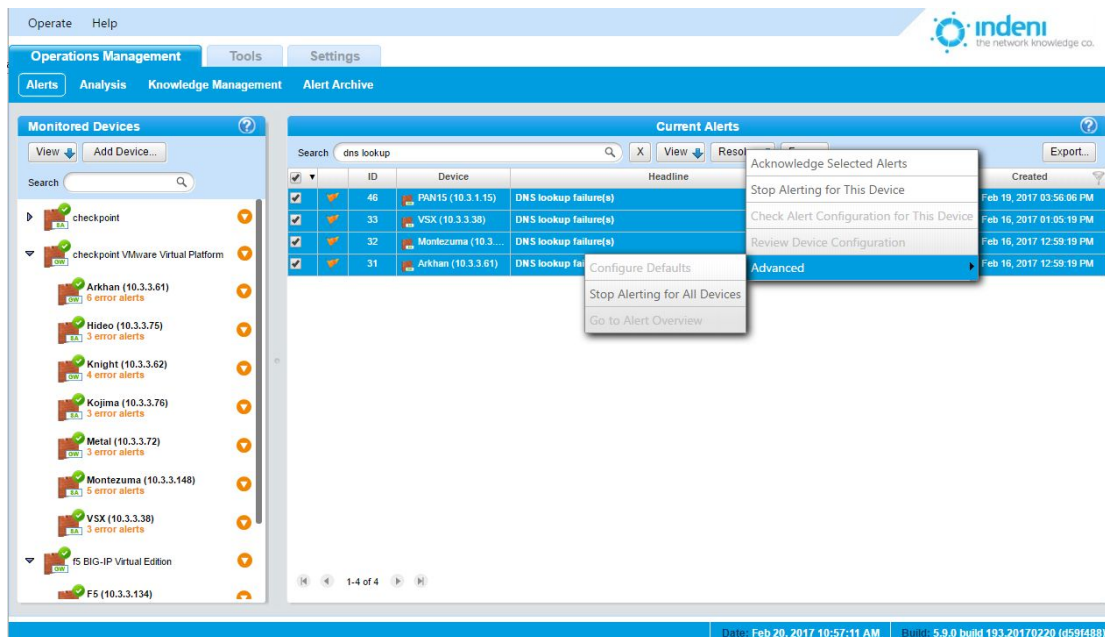
### Review Device Configuration

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.

The screenshot shows the Indeni web interface. On the left is a sidebar for 'Monitored Devices' with a search bar and a list of devices. The main area is titled 'Current Alerts' and contains a table of alerts. The first alert is expanded, showing details for 'Knight (10.3.3.62)'. The alert message is 'Configuration changed but not saved'. Below the message is a 'Description' section, a 'Status Description' section, and a 'Remediation Steps' section. At the bottom of the expanded alert is a 'Notes and History' section with an 'Append note' button. The table lists 17 alerts in total, with the first 16 shown. The bottom status bar shows the date 'Feb 20, 2017 10:57:51 AM' and build version '5.9.0 build 193.20170220 (d59f488)'.

Alert ID	Device	Alert Message	Timestamp	Timestamp
64	Knight (10.3.3.62)	Configuration changed but not saved <b>Description:</b> The configuration has been changed on this device, but has not yet been saved. This may result in the loss of the new configuration during a power cycle or device reboot. <b>Status Description:</b> <b>Remediation Steps:</b> Log into the device and save the configuration. In cli, run "save configuration". <b>Notes and History:</b> Append note	Feb 20, 2017 09:39:57 AM	Feb 20, 2017 09:39:57 AM
63	Arkhan (10.3.3.61)	Configuration changed but not saved	Feb 20, 2017 09:39:57 AM	Feb 20, 2017 09:39:57 AM
61	Montezuma (10.3.3.148)	NTP sync failure(s)	Feb 20, 2017 09:30:09 AM	Feb 20, 2017 09:30:09 AM
60	Hideo (10.3.3.75)	NTP sync failure(s)	Feb 20, 2017 09:30:09 AM	Feb 20, 2017 09:30:09 AM
59	Kojima (10.3.3.76)	NTP sync failure(s)	Feb 20, 2017 09:30:09 AM	Feb 20, 2017 09:30:09 AM
58	Metal (10.3.3.72)	Network port(s) down	Feb 20, 2017 09:28:27 AM	Feb 20, 2017 09:28:27 AM
49	Hideo (10.3.3.75)	SIC to certain managed devices not working	Feb 19, 2017 03:58:29 PM	Feb 19, 2017 03:58:29 PM
48	Kojima (10.3.3.76)	SIC to certain managed devices not working	Feb 19, 2017 03:58:29 PM	Feb 19, 2017 03:58:29 PM
47	P1 (10.3.3.150)	SIC to certain managed devices not working	Feb 19, 2017 03:56:29 PM	Feb 19, 2017 03:56:29 PM
46	PAN15 (10.3.1.15)	DNS lookup failure(s)	Feb 19, 2017 03:56:06 PM	Feb 19, 2017 03:56:06 PM
45	Hideo (10.3.3.75)	High disk space utilization	Feb 19, 2017 03:45:48 PM	Feb 19, 2017 03:45:48 PM
44	Kojima (10.3.3.76)	High disk space utilization	Feb 19, 2017 03:45:48 PM	Feb 19, 2017 03:45:48 PM

## 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.





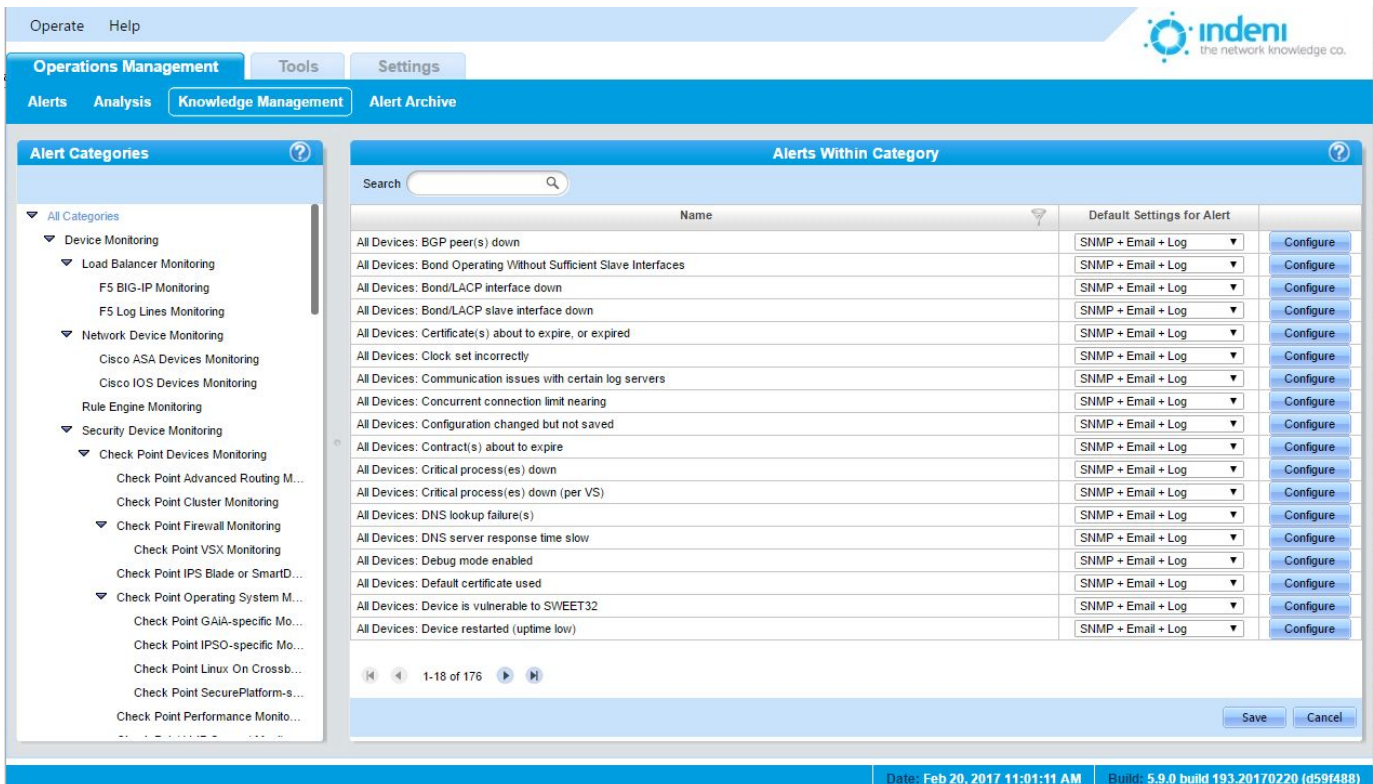
The analysis tab allows for easy control of the data that is presented:

- 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 “lollipops” at the bottom of the graph.

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

## 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. This list is updated and expanded regularly.



The screenshot shows the Indeni Knowledge Management interface. On the left, under 'Alert Categories', there is a tree view with 'Device Monitoring' expanded, showing sub-categories like 'Load Balancer Monitoring', 'Network Device Monitoring', and 'Security Device Monitoring'. The main area, 'Alerts Within Category', displays a table of alerts. Each row includes the alert name, its default settings (e.g., 'SNMP + Email + Log'), and a 'Configure' button. The table lists 17 alerts, including 'All Devices: BGP peer(s) down', 'All Devices: Bond Operating Without Sufficient Slave Interfaces', and 'All Devices: Device restarted (uptime low)'. At the bottom right, there are 'Save' and 'Cancel' buttons. The footer shows the date 'Feb 20, 2017 11:01:11 AM' and build information '5.9.0 build 193.20170220 (d591488)'.

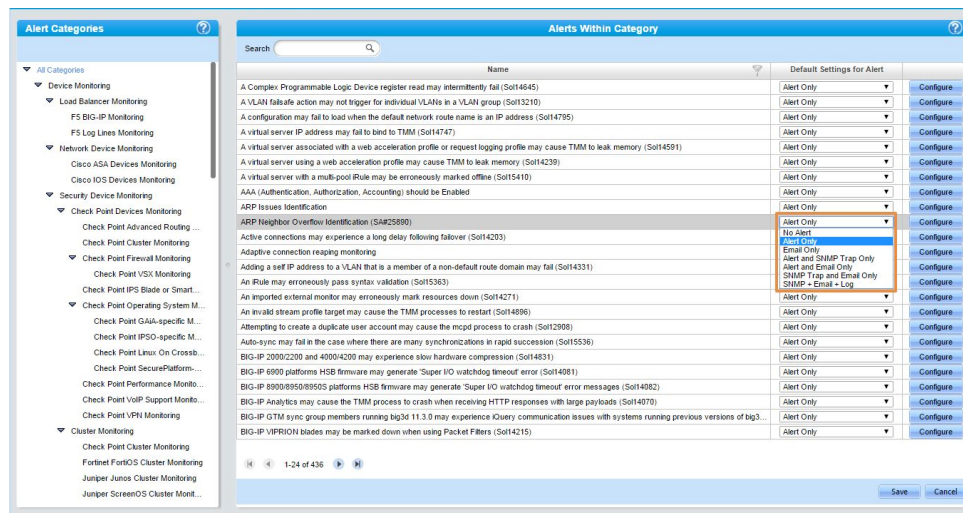
Name	Default Settings for Alert	
All Devices: BGP peer(s) down	SNMP + Email + Log	Configure
All Devices: Bond Operating Without Sufficient Slave Interfaces	SNMP + Email + Log	Configure
All Devices: Bond/LACP interface down	SNMP + Email + Log	Configure
All Devices: Bond/LACP slave interface down	SNMP + Email + Log	Configure
All Devices: Certificate(s) about to expire, or expired	SNMP + Email + Log	Configure
All Devices: Clock set incorrectly	SNMP + Email + Log	Configure
All Devices: Communication issues with certain log servers	SNMP + Email + Log	Configure
All Devices: Concurrent connection limit nearing	SNMP + Email + Log	Configure
All Devices: Configuration changed but not saved	SNMP + Email + Log	Configure
All Devices: Contract(s) about to expire	SNMP + Email + Log	Configure
All Devices: Critical process(es) down	SNMP + Email + Log	Configure
All Devices: Critical process(es) down (per VS)	SNMP + Email + Log	Configure
All Devices: DNS lookup failure(s)	SNMP + Email + Log	Configure
All Devices: DNS server response time slow	SNMP + Email + Log	Configure
All Devices: Debug mode enabled	SNMP + Email + Log	Configure
All Devices: Default certificate used	SNMP + Email + Log	Configure
All Devices: Device is vulnerable to SWEET32	SNMP + Email + Log	Configure
All Devices: Device restarted (uptime low)	SNMP + Email + Log	Configure

## 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**.



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.

**ARP Issues Identification**  
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.

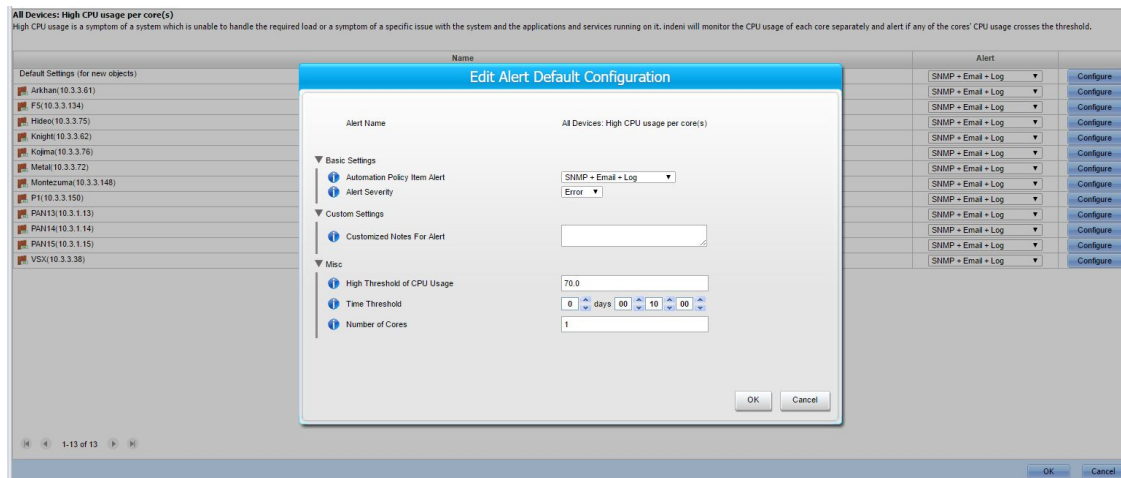
Check interval: 0 days 00:01:00

Name	Alert	Autoremediate	
Default Settings (for new objects)	Alert Only	Ask Me	Configure
SRX-02(10.3.3.172)	Alert Only	Ask Me	Configure
ssg-01(10.3.3.161)	Alert Only	Ask Me	Configure
ssg-02(10.3.3.162)	Alert Only	Ask Me	Configure

1-4 of 4

## 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 custom 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

Tools





















Settings

Alerts

Analysis

Knowledge Management

Alert Archive

	ID	Device	Headline	Last Update	Created
	30	PAN14 (10.3.1.14)	RESOLVED: High memory usage	Feb 20, 2017 11:06:43 AM	Feb 16, 2017 12:51:03 PM
	40	PAN15 (10.3.1.15)	RESOLVED: Packet drop counters increasing	Feb 20, 2017 11:06:43 AM	Feb 19, 2017 03:35:31 PM
	52	PAN14 (10.3.1.14)	RESOLVED: High memory usage	Feb 20, 2017 11:06:43 AM	Feb 19, 2017 07:51:15 PM
	62	VSX (10.3.3.38)	RESOLVED: NTP sync failure(s)	Feb 20, 2017 11:06:43 AM	Feb 20, 2017 09:36:09 AM
	57	PAN15 (10.3.1.15)	RESOLVED: Packet drop counters increasing	Feb 20, 2017 11:06:43 AM	Feb 20, 2017 01:16:31 AM
	55	PAN14 (10.3.1.14)	RESOLVED: High memory usage	Feb 20, 2017 11:06:43 AM	Feb 19, 2017 10:59:15 PM
	34	PAN15 (10.3.1.15)	RESOLVED: High memory usage	Feb 20, 2017 11:06:43 AM	Feb 17, 2017 10:09:03 AM
	53	PAN14 (10.3.1.14)	RESOLVED: High memory usage	Feb 20, 2017 11:06:43 AM	Feb 19, 2017 07:56:15 PM
	56	Arkhan (10.3.3.61)	RESOLVED: DNS server response time slow	Feb 20, 2017 11:06:43 AM	Feb 20, 2017 12:59:08 AM
	51	PAN14 (10.3.1.14)	RESOLVED: High memory usage	Feb 20, 2017 11:06:43 AM	Feb 19, 2017 04:52:15 PM
	50	PAN14 (10.3.1.14)	RESOLVED: High memory usage	Feb 20, 2017 11:06:43 AM	Feb 19, 2017 04:35:15 PM
	42	PAN15 (10.3.1.15)	RESOLVED: High memory usage	Feb 20, 2017 11:06:43 AM	Feb 19, 2017 03:38:15 PM
	54	PAN14 (10.3.1.14)	RESOLVED: High memory usage	Feb 20, 2017 11:06:43 AM	Feb 19, 2017 08:07:15 PM
	5	Hideo (10.3.3.75)	RESOLVED: Failed to communicate	Feb 16, 2017 12:30:19 PM	Feb 16, 2017 12:26:33 PM
	12	Knight (10.3.3.62)	RESOLVED: Failed to communicate	Feb 16, 2017 12:28:53 PM	Feb 16, 2017 12:27:33 PM
	8	Metal (10.3.3.72)	RESOLVED: Failed to communicate	Feb 16, 2017 12:28:25 PM	Feb 16, 2017 12:27:05 PM
	11	PAN14 (10.3.1.14)	RESOLVED: Failed to communicate	Feb 16, 2017 12:28:17 PM	Feb 16, 2017 12:27:23 PM
	7	VSX (10.3.3.38)	RESOLVED: Failed to communicate	Feb 16, 2017 12:28:13 PM	Feb 16, 2017 12:26:53 PM
	6	F5 (10.3.3.134)	RESOLVED: Failed to communicate	Feb 16, 2017 12:27:40 PM	Feb 16, 2017 12:26:50 PM
	2	Montezuma (10.3.3.134)	RESOLVED: Failed to communicate	Feb 16, 2017 12:27:21 PM	Feb 16, 2017 12:26:19 PM

1-20 of 20

Date: Feb 20, 2017 11:05:51 AM

Build: 5.9.0 build 193 20170220 rd59f68a

1-20 of 20

Date: Feb 20, 2017 11:05:51 AM Build: 5.9.0 build 193.20170220 (d59f488)

## CHAPTER 6: TOOLS

The **Tools** tab allows quick access to a device's general details.

### Live Configuration

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

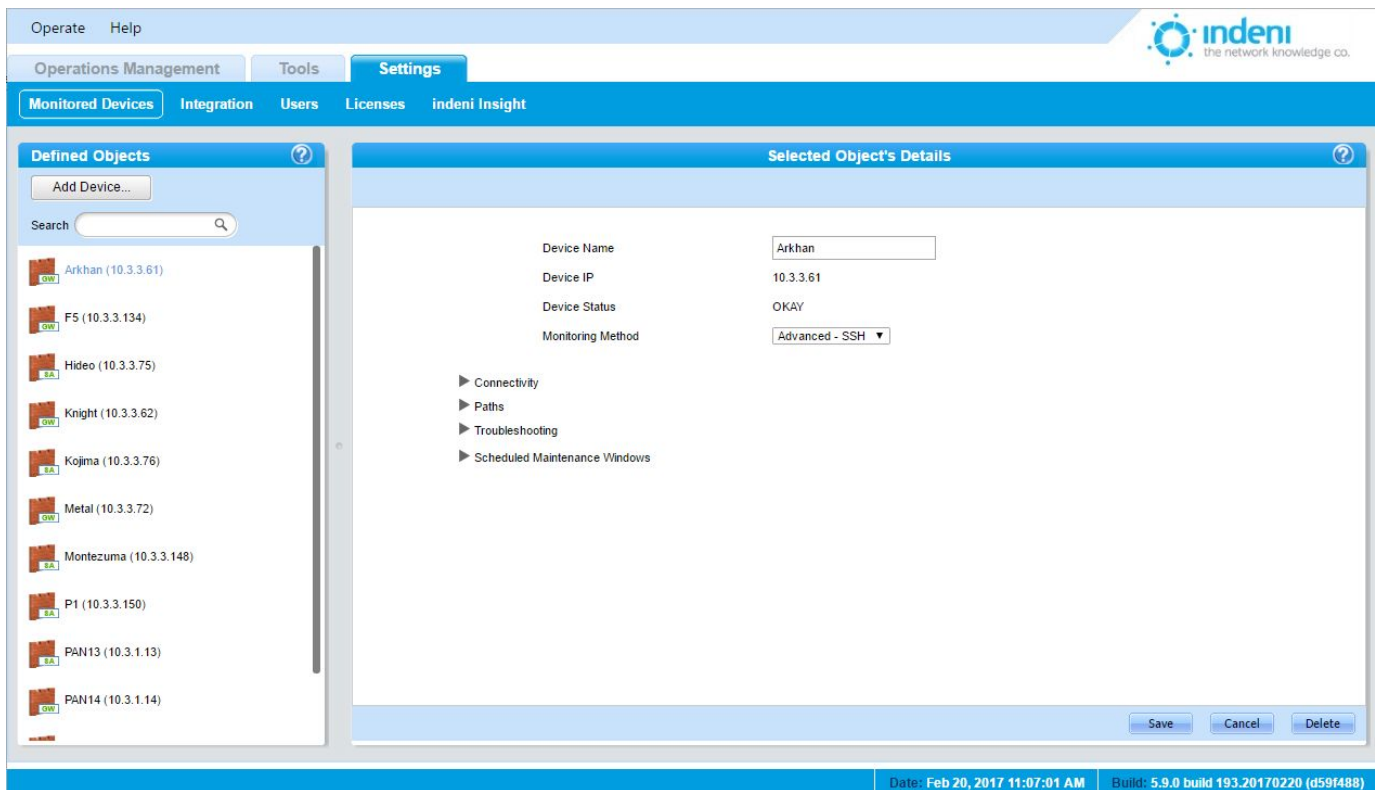
1. Click on the Tools tab.
2. Select the Live Configuration sub-tab.
3. Choose a specific device from the list on the left side of the screen.

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.

# CHAPTER 7: 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**.



## 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	70
Alternate SSH Port	8181
Resource Test Critical Memory Usage Threshold	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:

Scheduled Maintenance Windows

Add window

On Sunday From 0 : 0 For 1 hour(s) Remove

Maintenance window set to 2 days 1 hour 17 minutes from now

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.

## 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.

The screenshot displays the Indeni web interface, specifically the 'Settings' tab under 'Integration'. The interface is divided into two main sections: 'Defined Objects' on the left and 'Selected Object's Details' on the right.

**Defined Objects:** This section contains a search bar and a list of defined objects. The objects listed are:

- SNMP-host (192.168.1.109)
- gmail (64.233.166.28)
- sadasdas (192.168.1.109)
- Syslog Server (192.168.1.109)

**Selected Object's Details:** This section shows the configuration details for the selected 'SNMP-host' object.

**Host Details:**

- Host Name: SNMP-host
- Host Address IP: 192.168.1.109

**SNMPv2 Settings:**

- Community: public

**SNMPv3 Settings:**

- USM Security Name: (empty field)
- USM Auth Algorithm: (dropdown menu)
- USM Auth Password: (password field with eye icon)
- USM Priv Algorithm: (dropdown menu)
- USM Priv Password: (password field with eye icon)

At the bottom of the 'Selected Object's Details' section, there is a button labeled 'Send Test SNMP Trap'.

The bottom status bar of the interface shows the date and time: 'Date: Feb 20, 2017 11:08:35 AM' and the build information: 'Build: 5.9.0 build 193.20170220 (d59f488)'.

## 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>

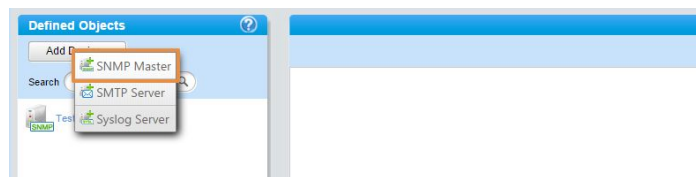


Indeni participates in HP's Enterprise Management Alliance Program. The software has been validated to integrate easily with HP Operations Manager (HP OM). HP OM contains a tool to convert the Indeni Management Information Base (MIB) file to a HP OM policy. The tool is not an integral part of HP OM but 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 drop down lists provided. The user can do any of the following and then **Save** the changes:

- Assign only a host address IP, hostname 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.

The screenshot shows the Indeni web interface. The top navigation bar includes 'Operate', 'Help', and the Indeni logo. Below this is a secondary navigation bar with 'Operations Management', 'Tools', and 'Settings'. The 'Settings' tab is active, and within it, the 'Integration' sub-tab is selected. The main content area is divided into two panels. The left panel, titled 'Defined Objects', contains a search bar and a list of objects: 'SNMP-host (192.168.1.109)', 'gmail (64.233.166.28)', and 'Syslog Server (192.168.1.109)'. The right panel, titled 'Selected Object's Details', shows the configuration for the selected 'SNMP-host'. It includes sections for 'Host Details' (Host Name: 'SNMP-host', Host Address IP: '192.168.1.109'), 'SNMPv2 Settings' (Community: 'public'), and 'SNMPv3 Settings' (USM Security Name, USM Auth Algorithm, USM Auth Password, USM Priv Algorithm, USM Priv Password). A 'Send Test SNMP Trap' button is located at the bottom of the configuration section. At the bottom of the interface, a status bar shows the date 'Feb 20, 2017 11:12:21 AM' and the build version '5.9.0 build 193.20170220 (d59f488)'.

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.

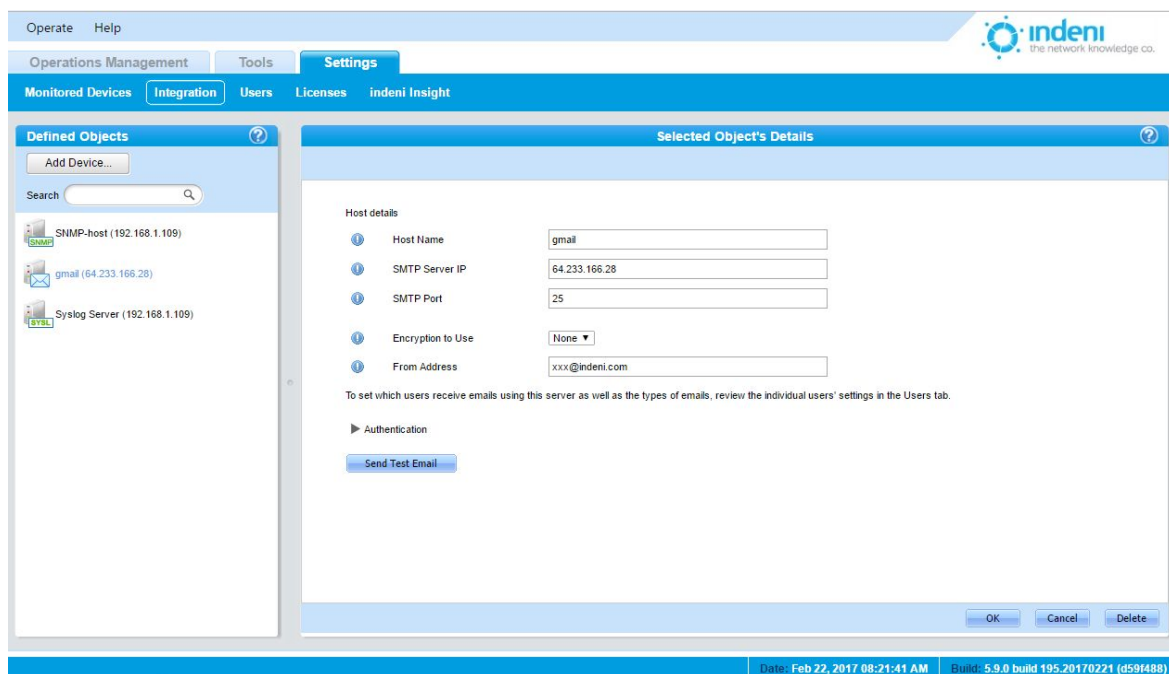
## Adding an SMTP Server

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**



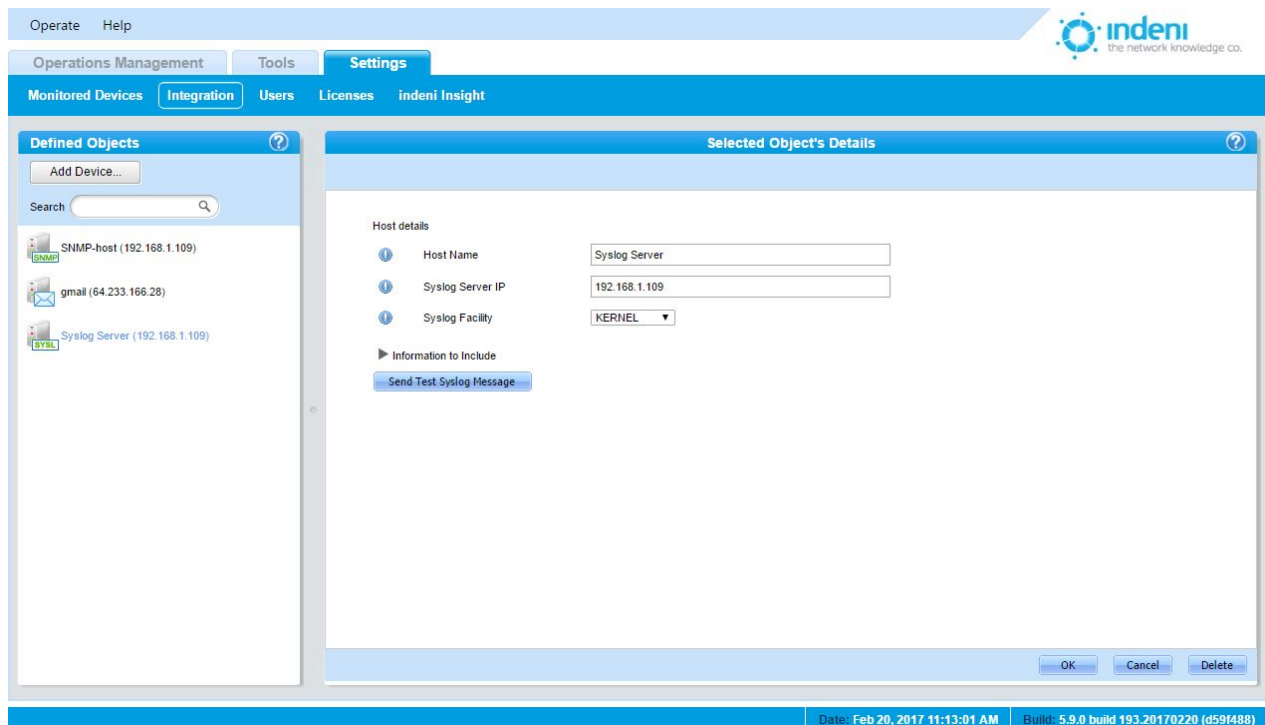
**Objects.**

## 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

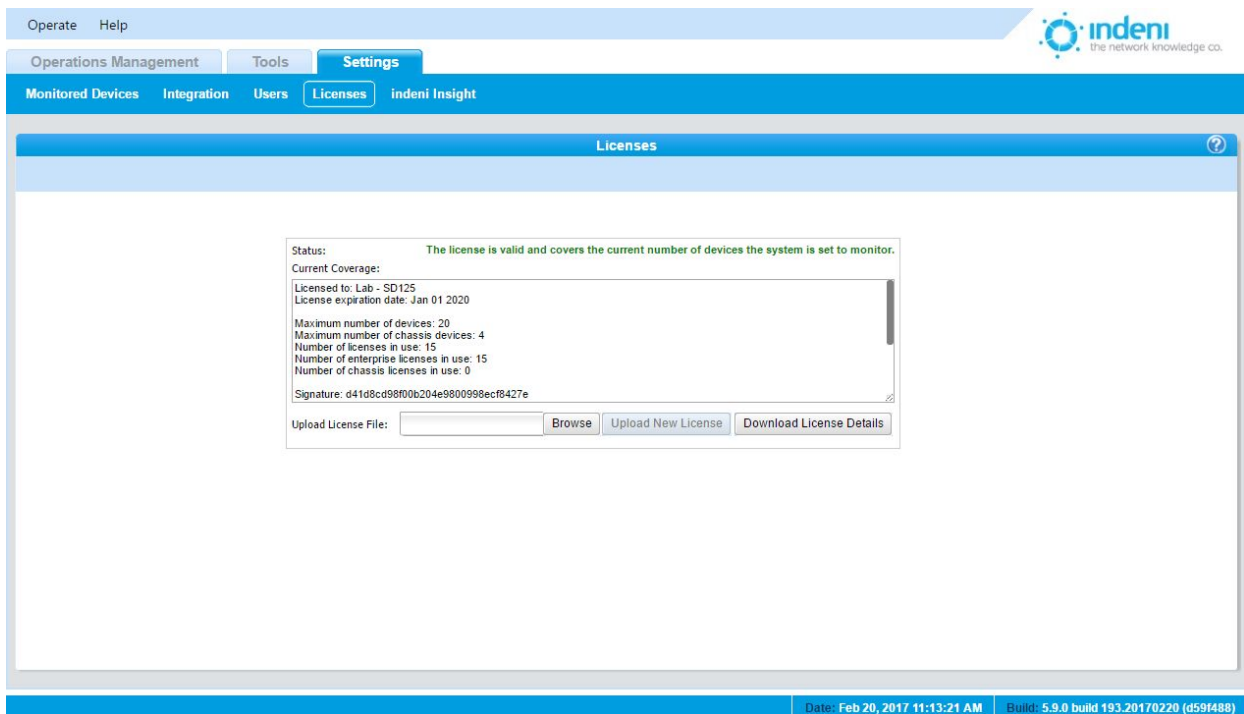
Use this subtab to add, delete, and edit users, passwords, email settings, permissions for setting up and remediating individual devices, and permissions for group objects, as described in [Chapter 4: Getting Started](#).

## 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 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](#).

The screenshot shows the Indeni Insight settings page. The top navigation bar includes 'Operate', 'Help', 'Operations Management', 'Tools', and 'Settings'. Below this, a sub-navigation bar contains 'Monitored Devices', 'Integration', 'Users', 'Licenses', and 'Indeni Insight'. The main content area displays a dialog box titled 'Turn on Indeni Insight'. The dialog box contains the following text:

Turning on 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, go to [our website](#).

Below the text, there is a checkbox labeled 'Enable Indeni Insight' which is checked. To the right of the checkbox is a donut chart titled 'Your Organization' with four segments: red (labeled '14'), yellow (labeled '15'), green (labeled '16'), and blue (labeled '17'). Below the chart is a legend with four categories: 'Networks', 'Infrastructure', 'Security', and 'Configuration'. Below the checkbox and chart, there is a text input field labeled 'Email address for the report:' with the value 'yarin@indeni.com'. A 'Save' button is located at the bottom right of the dialog box.

The footer of the page displays the date and time: 'Date: Feb 20, 2017 11:13:41 AM' and the build information: 'Build: 5.9.0 build 193.20170220 (d59f488)'.

# CHAPTER 8: 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.

Updates are performed by running the "apt-get" Linux from Indeni's server CLI.

Note: Updates require access to Indeni's repositories residing on Amazon's Web Services at [s3.amazonaws.com](https://s3.amazonaws.com)

1. Log into Indeni's server using an SSH console
2. Run the following commands:  
`sudo apt-get update`  
`sudo apt-get upgrade`

## Support

The Support section of [www.Indeni.com](http://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](mailto:support@Indeni.com)

# APPENDIX A: 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 Ubuntu 14.04 Server. 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

HTTP and HTTPS (the Indeni server's web interface, hosted inside Jetty)

TCP Ports 9009, 9912 used by Indeni's Server component

## 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 B: 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 Embedded GAIa

When accessing the Embedded GAIa , 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

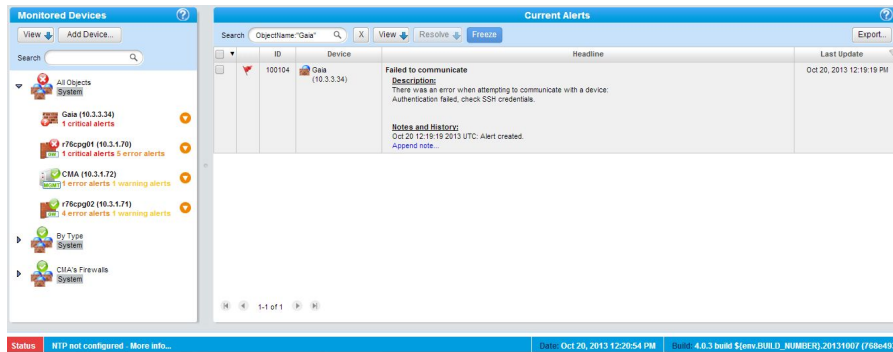
a. This is how the alert would appear:

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

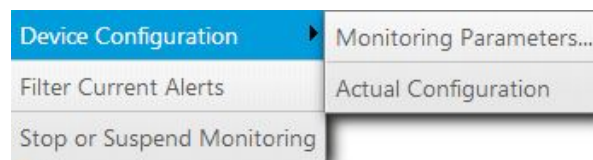
## 2. Failed to communicate – SSH Credentials

a. This is how the alert would appear:

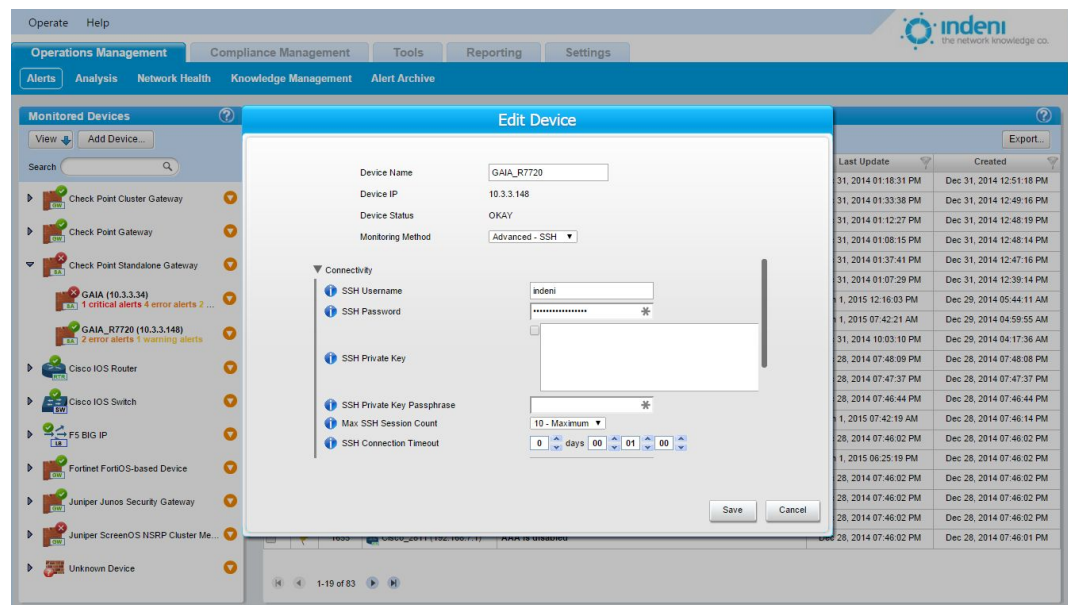


b. Authentication failed. Please update the SSH credentials as follows.

- 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**.





## About Indeni

Indeni makes it easy to manage the infrastructure of digital businesses. With Indeni Knowledge™ and Indeni Insight™ companies can create an infrastructure that is adaptable to change. Our deep set of integrations to critical devices, built-in automation, and easy to read remediation instructions arm IT with the knowledge they need to move from reactive to proactive infrastructure management. By analyzing billions of data points per day, and gathering knowledge from thousands of IT professionals, Indeni minimizes business disruption and maximizes their contribution. For more information, contact an Indeni partner or visit [www.indeni.com](http://www.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 JCRRAFT, 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](mailto:info@snmp4j.org) (SNMP4J) or [apache@apache.org](mailto: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.