



Indeni 6 User Guide

Indeni 6 User Guide

[Part 1: Understanding the Basics](#)

[1.1 Requirements](#)

[1.2 Installation](#)

[1.3 Indeni Insight](#)

[Part 2: Getting Started](#)

[2.1 Creating Users on Vendor Devices](#)

[2.2 Device Communication](#)

[Part 3: Navigating the User Interface](#)

[3.1 Summary Tab](#)

[3.2 Current Tab](#)

[3.3 Archived Tab](#)

[3.4 Rules Tab](#)

[Part 4: Analysis and Reporting](#)

[4.1 Custom Reports](#)

[Part 5: Device Management](#)

[5.1 Credential Sets](#)

[5.2 Adding Devices](#)

[5.3 Device Backup](#)

[Part 6: Settings](#)

[6.1: Centralized Authentication](#)

[6.2: Role Based Access Control](#)

[6.3: Configuring a Proxy Server to access Indeni Insight](#)

[6.4: SNMP Integration](#)

[Part 7: Security](#)

[Open Source Credits](#)

Part 1: Understanding the Basics

This Introductory Guide is geared towards technical users with a strong working knowledge of networking and network security administration. Users should have the ability to set up network devices on their own, and also be familiar with how to use the various **Command Line Interfaces (CLI)**.

The guide is designed to take you from start to finish, in an order that will help you succeed. If you are a first time Indeni user, you will want to go through each step of the guide, and at the end, you should be able to add devices with a good understanding of how to use the system successfully.

We highly encourage interested users, students, and IT professionals testing new technologies to [download](#) and use Indeni for **free**! If you do not have networking devices to test with, but are interested in trying out our system, you can use other tools such as [GNS3](#), since Indeni works with both physical and virtual devices.

We also encourage users interested in test driving Indeni to [join our community](#)! There are many benefits in doing so, such as connecting with other IT professionals who are interested in learning to code and script, but you can also extend your free license in perpetuity by participating. If you encounter any problems along the way, your first port of call is the Indeni community.

1.1 Requirements

Server Requirements

The Indeni installation file comes in an **Open Virtualization Appliance** (.OVA) format and is ready for import. Indeni supports installation of virtual servers on a variety of **Virtual Machines** (VM's). Please contact Indeni Support if you have questions regarding installation on an alternative environment.

The .OVA file includes **64-bit Ubuntu 14.04** with the required packages, so there is no need to pre-install an operating system on the virtual server. The .OVA file comes pre-configured with **6 GB RAM, 4 Cores** and **146.5 GB Hard drive**.

Indeni 6 is certified for installation on **VMware ESXi** releases 6.0, 6.5 and 6.7.

Minimum system requirements based on the connection of 5 network devices:

- **CPU:** 4 x 64-bit capable processors
- **Disk Space:** 150 GB
- **Memory:** 6 GB RAM
- **NIC:** 1 x 10/100 Gb ethernet
- **Connectivity:** The Indeni server needs Internet access to retrieve software updates. This may be done directly or via HTTPS proxy. While not recommend for Production Environments, you do have the option to use DHCP.

Please Note:	The server must be connected a local network during the installation process. Lack of connectivity may result in the setup script hanging during network configuration. If it is not possible to connect to the network then please contact support@indeni.com .
---------------------	--

Web User Interface Access Requirements

The Indeni GUI, or Indeni Dashboard, is accessible via Web UI. So you can now 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, through a single web browser.

Supported Internet browsers include Microsoft Internet Explorer, Mozilla Firefox and Google Chrome. The browser's pop-up blocker needs to be disabled.

Please Note: We have seen the best performance on Google Chrome and should be preferred.

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** (443) – 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.

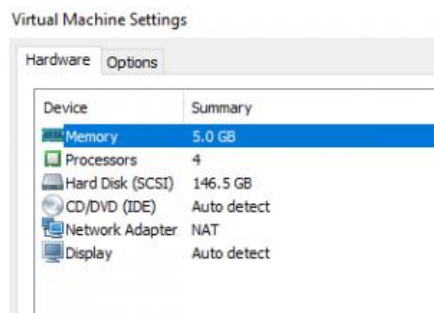
Please Note: The ping test can be deactivated in the individual device's configuration at the Monitored Devices sub-tab under Settings.

1.2 Installation

We strongly recommend that you check and ensure that you meet the minimum systems requirements outlined below, and understand the server requirements.

Installation

The Indeni .OVA file is preconfigured to launch with **6 GB of RAM, 4 Cores and 146.5 GB of hard drive space**. A new install of the Indeni Virtual Lab will use 3.19 GB. For a **live production environment**, we recommend the use of 5 – 8GB of RAM.



Please Note: As you continue to use the Indeni server, memory volume will start to increase, so it is best to monitor memory usage as you go. If you run a virtualized Indeni environment and max out your system resources, you may encounter severe performance issues.

To check your hardware settings on Windows:

1. Go to **Start** > right click on **Computer** and go to **Properties**.
2. You will see system settings under the performance rating. Look for **System** > **Processor and Installed Memory**.
3. Go to **Window Explorer** > **Computer** > Look under your Main Drive to find the amount of free storage.

To check your hardware settings on Mac OS X:

1. Click on the **Apple Icon** (top left corner) > **About this Mac** > **Systems Report**

Software Options:

Virtual Machine: [VMware Workstation](#), ESX or other VM offering such as [Virtual Box](#). [VMware Workstation 12.5](#) was used in this documentation. It is **free** to use for home, or educational purposes, when you register with a valid email address.

Please Note: Production certification has been done exclusively on VMware's ESXi releases 6.0, 6.5 and 6.7.

- **Network Monitoring:** [Wireshark](#)
- **CLI** (command-line-interface): [Putty](#) for PC users, [Terminal](#) for Mac OS X users.
- **File Transfer:** [WinSCP](#) for PC users and [Cyberduck](#) for Mac users.

Loading the .OVA

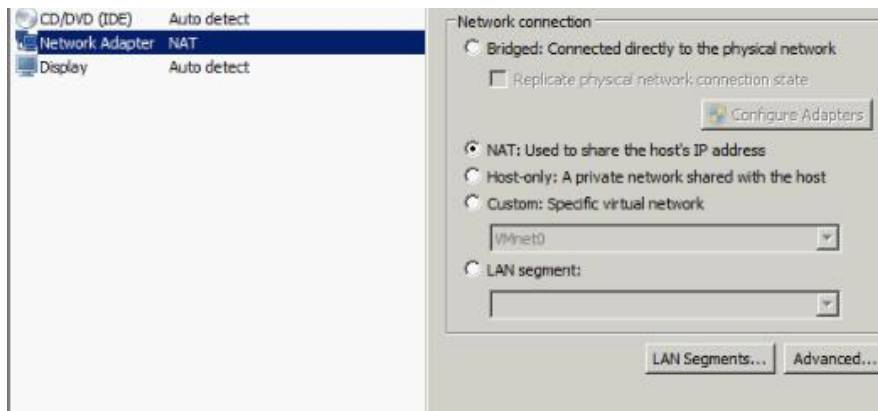
Indeni supports a wide variety of virtual machines, including freeware versions. However, [VMware Workstation](#) was preferred for this exercise due to the ease of DHCP assignment to the Indeni server and connectivity to devices over a VPN.

To Load the OVA, proceed as follows:

1. Launch VMware Workstation Player, or preferred virtual machine, and select **Open a virtual machine**.

Please Note: Typically, the default file type VMware looks for is .ISO. You might need to change the file type from .ISO to All Support File Types to find and load the .OVA. Also, if you load multiple images of the .OVA for testing purposes, be sure to delete them in VMware and then check that they have also been removed from the directory.

2. Before launching the OVA click on **Player > Manage > Virtual Machine Settings > Network Adapter**. Make sure that *NAT* is selected, then load/play the instance.



Installing Indeni on a Virtual Instance

When you launch the Indeni Server, you should see the service highlighted in red start:

```
* Starting Bridge socket events into upstart [ OK ]
* Starting Mount network filesystems [ OK ]
* Stopping Mount network filesystems [ OK ]
* Starting configure network device [ OK ]
* Stopping Failsafe Boot Delay [ OK ]
* Starting System V initialisation compatibility [ OK ]
* Starting configure virtual network devices [ OK ]
Skipping profile in /etc/apparmor.d/disable: usr.sbin.rsyslogd
* Starting AppArmor profiles [ OK ]
* Stopping System V initialisation compatibility [ OK ]
* Starting System V runlevel compatibility [ OK ]
* Starting regular background program processing daemon [ OK ]
* Starting save kernel messages [ OK ]
* Starting CPU interrupts balancing daemon [ OK ]
* Stopping save kernel messages [ OK ]
* Starting OpenSSH server [ OK ]
* Starting PostgreSQL 9.5 database server [ OK ]
Starting indeni-backup
Starting indeni-cognito
Starting indeni-collector
Starting indeni-ds
Starting indeni
Starting indeni-vigile
Starting indeni-walt
```

Once the instance launches, login with User: **indeni** Password: **indeni4it**:

```
Ubuntu 14.04.5 LTS indeni-server tty1
indeni-server login: indeni
Password:
```

Once you have logged in, it will ask you to continue with the *Configuration Wizard*. To access the configuration after initial setup, type in **'isetup'**:

Please Note: It is good to get in the habit of [changing default passwords](#) after you have logged in. But do not forget it because Indeni support cannot reset or recover your password after it has been changed. If this happens, please see the following [thread on how to reset your admin password](#) in askubuntu.com.

Once the *Configuration Wizard* continues, you are prompted to choose from one of the following options:

- 1) Configure Network Interface
- 2) Configure NTP servers
- 3) Configure Proxy
- 4) Change TimeZone
- 5) Change HostName
- 6) Quit

Network Interface: configure the static IP network settings by providing the following values: **address, netmask, gateway. dns-nameservers**

NTP: change the server's **NTP server**.

Proxy: If you manage your own network, then input the appropriate settings for Proxy, *if necessary*, and open the following ports (8181, 443, 8080) on any firewalls you may have running.

TimeZone: change the server's **timezone**.

HostName is optional, but you will need to adjust the time zone and make sure the virtual machine clock is correct. Once you have your preferred settings, select (6) *Quit* to exit the setup.

Please Note: It is best practice to also check the system time on Ubuntu since issues may occur if times are not in sync. To check, type in `date + "%:z %Z"`.
To reset the timezone, type in `sudo dpkg-reconfigure tzdata`.

After you exit the Configuration Wizard, you should see the currently installed versions. It is okay if the versions differ on your system, the process is still the same:

```
Installed indeni packages:
indeni-backup      6.4.0.36
indeni-cognito     6.4.0.36
indeni-collector   6.4.0.36
indeni-ds          6.4.0.36
indeni-server      6.4.0.36
indeni-triton      6.4.0.36
indeni-vigile      6.4.0.36
indeni-walt        6.4.0.36
stable
indeni@indeni-server:~$ _
```

Please Note: Indeni will not work properly if the collector and server versions do not match.

Typing '**imanage**' [enter] will take you to Indeni tools, where you can perform the following functions:

```
Please select an option to proceed with:
-----
1) Display installed Indeni packages
2) Upgrade all installed Indeni packages
3) Restart Indeni services
4) Change Indeni source packages
5) Enable/Disable watchdog
6) Send logs to Indeni technical support
7) Backup & Restore
8) Set Cold Standby server
9) Setup DataDog integration
0) Quit
```

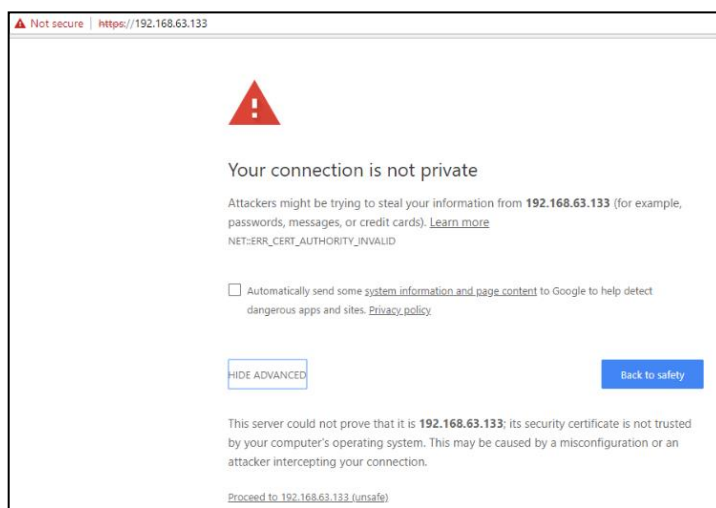
The most common option will be [6] Send logs to Indeni technical support. It is not recommended to Restart Indeni services without good reason since doing so can disrupt device interrogation.

Next, in the command line, type in **'ifconfig'** to find the IP address that was assigned to the virtual machine. It should be assigned to **eth0**. Once you have the IP address, make sure and take note of it.

```
indeni@indeni-server:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:43:94:80
          inet addr:192.168.63.133  Bcast:192.168.63.255  Mask:255.255.255.0
```

Launch a browser and enter in the following into the address bar:

[https://\[YOUR-eth0-IP\]/](https://[YOUR-eth0-IP]/)



If you're using Chrome, go to Advance and Proceed. You should be presented with the login page. The default login is **Username: admin** and **Password: admin123!**



After you log in, accept the License Agreement.



Enter an Email for Indeni Insights and SAVE.

Turning on Indeni Insight:

Indeni Insight gives you network intelligence by improving the predictability and analysis of your network. It enables us to help you with your network issues and deliver faster solutions.

For more information on what Indeni Insight includes and how it works, go to [our website](#)

Enable Indeni Insight ☒

Enter Email address for the report

Save

Congratulations! You have now successfully setup your Indeni Virtual Lab!
You are now ready to add devices to monitor.



Looks like you don't have any devices yet

[Click To Add Some Devices](#)

1.3 Indeni Insight

Indeni Insight is a continuously updated database that provides the global network and security community with the data to understand how devices behave in the real world. By democratizing this data, Indeni enables engineers and architects to make better decisions, and write better code.

How it Works

Each installation of the Indeni Automation Platform collects millions of metrics in its on-going operation – from basic CPU and Memory usage to in-depth device type-specific metrics. These metrics are then analyzed by a rule engine for the generation of issues.

The Indeni Insight component of the platform collects issues, metrics and additional device data, and sends it to a central database. All of the data collected by Indeni Insight is non-confidential – it has **no** personally identifiable information, **no** company-identifying information, **no** devices names, and **no** IP addresses. This allows us to give everyone access to the data, without posing a risk to any Indeni user.

Please Note that Insight requires access to “***service.indeni-ops.com***” over ports 80 (HTTP) and 443 (HTTPS).

Indeni Overview

The top of each report gives an overview of the current license utilization, version in use, best practices followed and work hours saved.

Device Overview

Whether you are evaluating new network or security devices, or looking to lower the TCO of your existing infrastructure, with Indeni Insight you can benchmark your performance across your peers and make informed decisions.

The device overview section shows the models and versions of software used in your environment, compared to other users connected to Indeni Insight. It is a great way to know if you are in line with other users of the same devices.

Technical Architecture

Data Collection, Transfer and Storage within each instance of Indeni, there is an **Insight Data Collection** component which injects itself into specific data write functions within the systems. When a configuration change is done in Indeni, or when an issue is generated, this component saves a copy of the data. The component collects only specific types of data and specific fields. It particularly selects data that we know is not confidential. This is essentially a white-list concept, where only data that is allowed will actually be collected. It ensures that no confidential data is collected by accident.

The data is saved locally on the hard drive of the machine running the Indeni server. Once an hour, the data is compressed and sent to a dedicated S3 bucket in Amazon Web Services. This bucket is write-only externally, which means data can only be written to it, but not retrieved from it. A series of AWS Lambda Functions are triggered when data is uploaded. They process the data, verify it, and insert it into the global MySQL database described below.

Database Structure

The Indeni Insight database is a MySQL database running in Amazon Web Services. To access it, please click [here](#).

Please Note: Actual End-Users will need to replace "me@indeni.com" with your email. Make sure you use the same email you are using to access Indeni Crowd (<http://community.indeni.com>) and that you have at least 1000 points in the community. You should receive an email within minutes with the database access information. The database has a series of related tables, and then views that are built on top of them to make querying easier.

How to Get Started

As a new Indeni customer simply follow the Indeni Insight set up instructions during system installation.

Turn on indeni Insight

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](#).

Enable indeni Insight ☒

Email address for the report:

Note: You may change this setting at any time by accessing the "Settings" tab.

Ok



If still have outstanding questions, please let us know in our [community](#)!

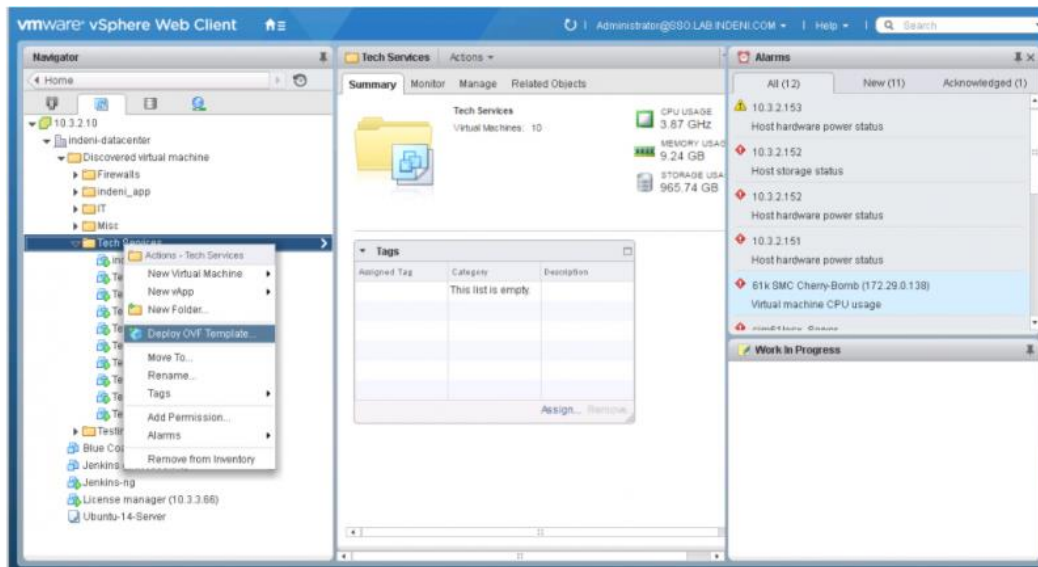
Part 2: Getting Started

Installations on Virtual Machines

The Indeni OVA is used for deploying the system in virtualization environments as a virtual appliance. You can access the download page at <http://offers.Indeni.com/download-Indeni> to download the Indeni OVA. You can then supply the downloaded OVA to your virtualization environment's administrator for deployment. Please see the [Virtual Lab Installation](#) for more detailed installation instructions, or visit the [install video guide](#).

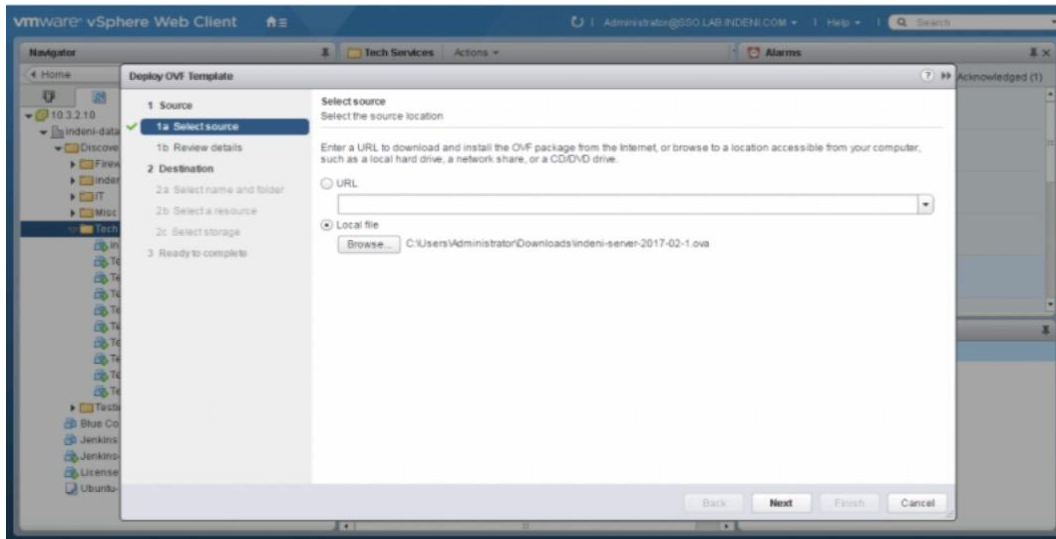
Configuring the Indeni Virtual Appliance

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



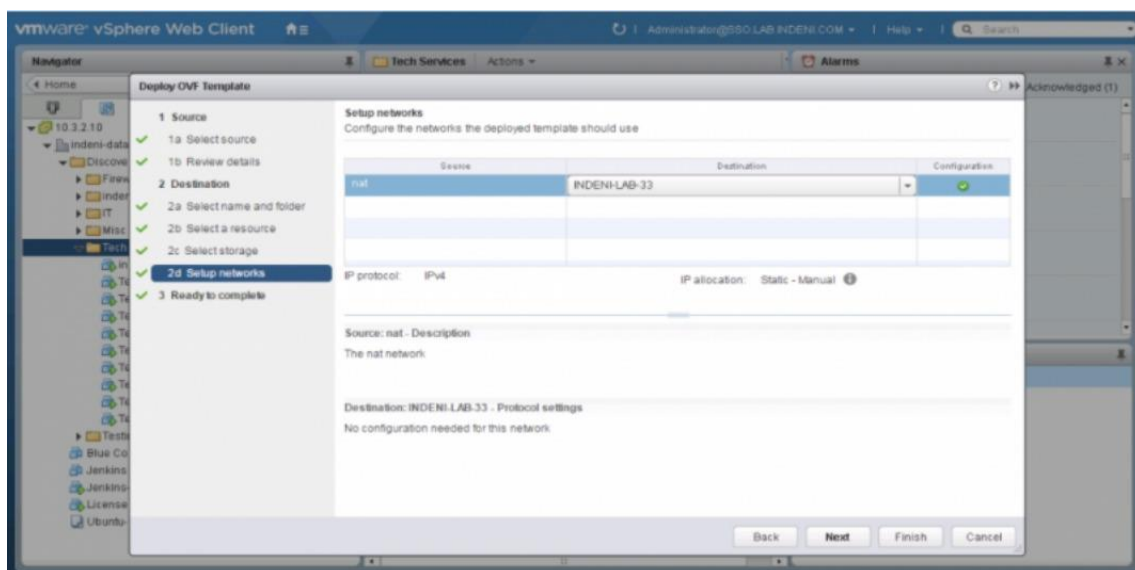
2. Configure Indeni VMware

3. Select the OVF file and proceed to run the wizard

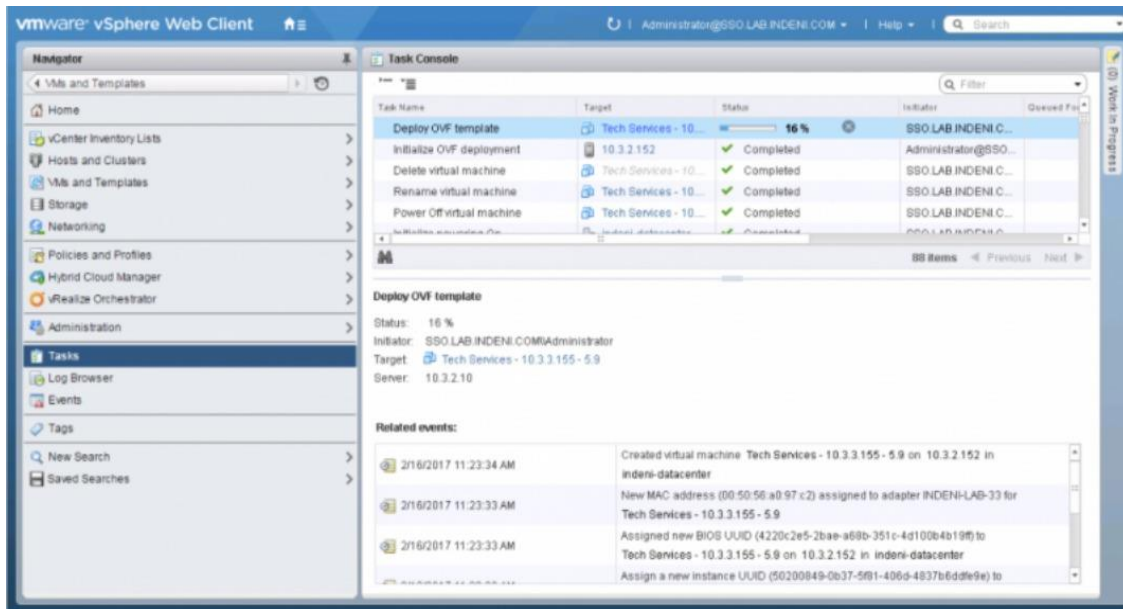


The wizard will ask for the following:

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.



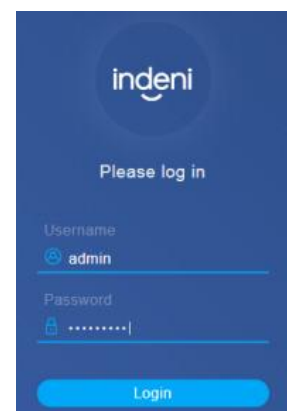
Use the VMware interface to power up the VM and access its console.

Logging in to the System – Console

You can log in to the system with **Username:** *indeni* and **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 User Interface at: [https://\[your-server-ip-address\]](https://[your-server-ip-address])
3. Log in to the Indeni UI:
4. Username: admin
5. Password: admin123!



2.1 Creating Users on Vendor Devices

In order for full automation to take place, a unique Indeni user must first be created and assigned the proper permissions by an administrator of the device. The created Indeni user must then be added to a **Credential Set** in your webUI. By leveraging credential sets and IP subnets you can enter credentials in one time, for multiple devices, which makes managing credentials for clusters and device vendors a breeze.

While we **always recommend** a system administrator defer to the vendor's official documentation on credential creation, we have outlined the user creation steps we took for successful addition, and automation of supported devices in the Indeni platform for those who might not be administrators themselves, or unfamiliar with the process.

Creating Users by Vendor

- [Blue Coat](#)
- [Check Point](#)
- [Cisco ASA](#)
- [F5](#)
- [FireEye](#)
- [Fortinet](#)
- [Juniper](#)
- [Gigamon](#)
- [Palo Alto Networks](#)
- [Radware](#)
- [Symantec](#)

Blue Coat

We always recommend a system administrator defer to the vendor's official documentation on credential creation. Please follow the vendor's instructions for configuring the device for access with an SSH key, and then use the Indeni WebGUI to store the Private key in the relevant Credential Profile.

The Blue Coat proxy running SGOS uses the default User ID of admin to access the GUI and SSH CLI of the box. The password of admin is setup during the time of install.

All other Users and Groups are created in either the CLI for the local realm or through other authentication realms (ex. *Radius, Window Domain, IWA, SAML, etc.*). There are two roles, **read-only access** and **read-write access**.

Local Authentication Realm

1. Login to the web-based Management Console.
2. Browse to the **Configuration Tab > Authentication > Local**
3. Click **New**, located in the **Local Realms** tab.
4. Enter a name for the Local Realm. For this example, "**Local**" will be used as the *Realm Name*.
5. Click the **Local Main** tab. Make note of the *Local User List* name, as it will be necessary in the next section.
6. Click **Apply**.

Creating Users and Groups

1. Log in to the CLI and enter enable and **Configuration Terminal Mode**.
2. At the (config) prompt, type: "*security local-user-list edit local_user_database*"
3. **Add a Group** with the following command: "*group create users*"
Optional: Add another group with the following command: "group create administrators"
4. **Create User Accounts** with the following command: "*user create user1*"

5. Type the following to **edit the User Account** and define the *Password* and *User Group* details for the User Account: *"user edit new_user"*
6. **Create a password** for the account by entering: password 1234 (*Replace 1234 with an appropriate password*)
Optional: Associate this user account with a Local User Group with the command: *"group add administrators"*. Repeat this process for all local user accounts you want to create.

Policy Controlled Admin Access

You can use the policy rules to control administrator access to the management console and to the CLI.

Using policy rules, you can require administrators to identify themselves by entering a username and password and specify whether read-only or read-write access is given. You can make this policy contingent on IP address, user name, group membership (if credentials were required), and many other conditions.

This solution assumes you have already configured users and groups for authentication using RADIUS, LDAP, Microsoft Active Directory, or other authentication servers, and created a realm on the ProxySG to connect to these servers.

Please see the below to create a policy for ProxySG administrator access:

1. Launch the Visual Policy Manager.
2. Create an Admin Authentication layer. **Policy > Add Admin Authentication Layer.**
3. In the Admin Authentication layer, specify the Authentication Realm that will be used to authenticate administrative users of the ProxySG.
4. Right-click in the Action column and choose Set. **Select New > Authenticate.**
5. Select the authentication mode and realm. (See *ProxySG Authentication Modes*)
6. Close the dialogs.
7. Create an Admin Access layer. **Policy > Add Admin Access Layer.**

8. In the Admin Access layer, define who is allowed to access the ProxySG:
 - a. Right-click in the Source column and choose Set.
 - b. Select New.
 - c. Select the entity (*for example, Client IP Address/Subnet, User, Group*) and configure the specifics.
 - d. Close the dialogs.
9. Specify the type of Administrator Read/Write Access:
 - a. Right-click the Action column and select Allow Read-only
 - b. Access or Allow Read/Write Access.
 - c. By default, the policy applies to any service (*HTTP/HTTPS in the Management Console and SSL in the CLI*). Do the following if you want to control access to just the Management Console or the CLI:
 - a. Right-click in the Service column and choose Set.
 - b. Select **New > Service Name**.
 - c. Select the service you want the rule to apply to (*HTTP-Console, HTTPS- Console, or SSH-Console*).
 - d. Close the dialog
10. Install the policy.

Check Point

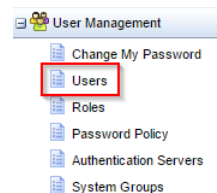
We always recommend a system administrator defer to the vendor's official documentation on credential creation. Please follow the vendor's instructions for configuring the device for access with an SSH key, and then use the Indeni WebGUI to store the Private key in the relevant Credential Profile.

In order for Indeni to run its full set of discovery and interrogation scripts, a **/bin/bash** user with a role of administrator needs to be used to connect your device. It is highly recommended that a unique Indeni user is created for auditing and security purposes.

Creating User on GAIa WebUI Portal

1. Log in to the Check Point WebUI.
2. Go to **User Management** → **Users** → **Add**
3. Fill in the required information.

It is important to set the Shell to **/bin/bash** and set the role to **adminRole**.

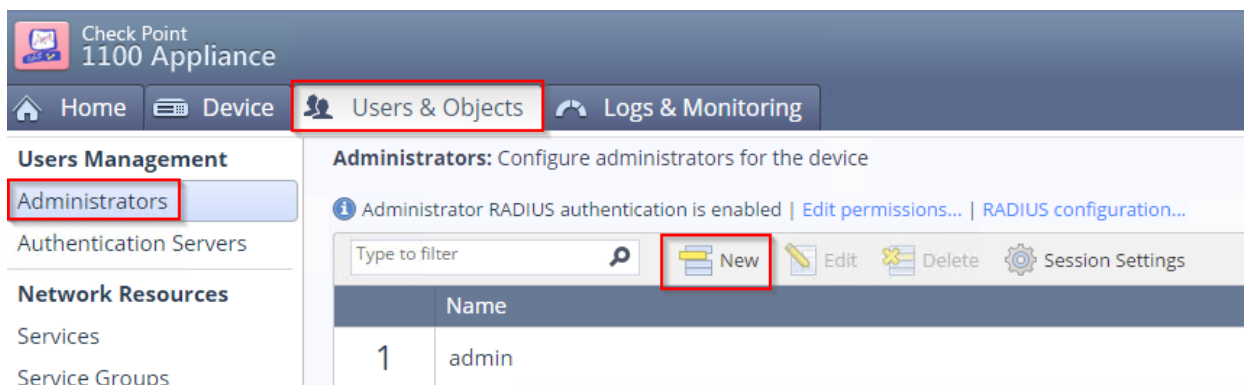
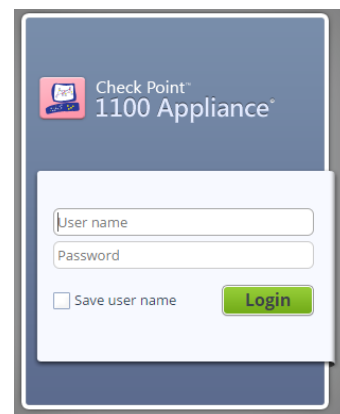
A screenshot of the 'Add User' dialog box in the Check Point WebUI. The dialog has several fields: 'Login Name' (indeni), 'Password' (masked with dots), 'Confirm Password' (masked with dots), 'Real Name' (Indeni), 'Home Directory' (/home/indeni), 'Shell' (/bin/bash), 'User must change password at next login' (unchecked), and 'UID' (0). There are also 'Available Roles' and 'Assigned Roles' lists. The 'Assigned Roles' list contains 'adminRole'. The 'Access Mechanisms' section has 'Web' (unchecked) and 'Command Line' (checked) options. The 'Login Name' and 'Shell' fields are highlighted with red boxes. The 'Assigned Roles' list is also highlighted with a red box. The dialog has 'OK' and 'Cancel' buttons at the bottom right.

Creating Users via CLI

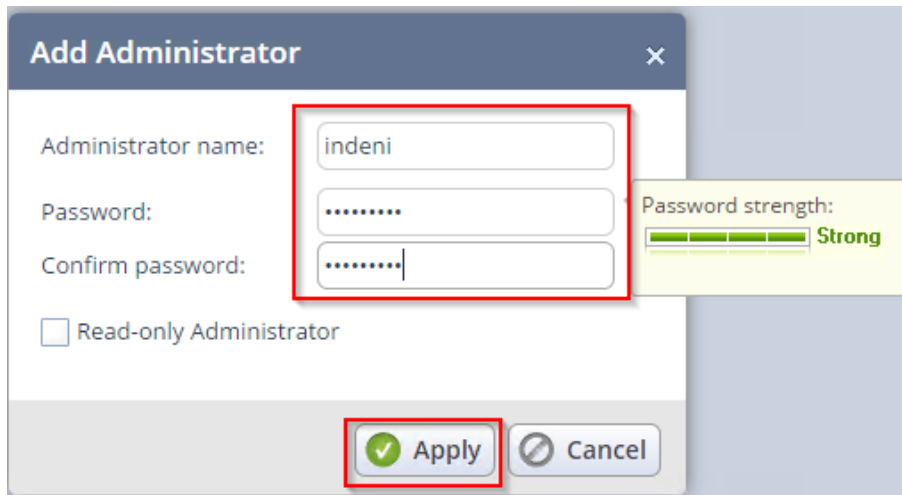
1. Log in to the Check Point device using SSH
2. Make sure you are in Clish. If you have the shell set to **/bin/bash**, run the command **clish**
3. Add the user (in the example we are using the username **indeni**):
add user indeni uid 0 homedir /home/indeni
4. Set the password for the user:
set user indeni password
New password: [xxxx]
Verify new password: [xxxx]
5. Type the following to add the access role adminRole:
add rba user indeni roles adminRole
6. Type the following to set the shell to /bin/bash:
set user indeni shell /bin/bash

Creating via GAIa Embedded

1. Login to the webUI
2. Go to **Users & Objects** → **Administrators** → **New**



3. Fill in the username and password and click Apply



Add Administrator

Administrator name:

Password:

Confirm password:

☐ Read-only Administrator

Password strength: Strong

4. Login with the user using SSH and type the command **expert** followed by the command **"bashUser on"**:

```
[Expert@indeni]# bashUser on
user: admin

Bash login enabled.
Scp access enabled.

Note:
  Your default shell will now be bash,
  and when you login you will enter expert mode.
  We recommend that you use clish as your default shell,
  and move to expert mode only when necessary.
  You can move from bash to clish using the "clish" command.
  To restore your default shell to clish run "bashUser off"

[Expert@indeni]#
```

Connect using public/private SSH Keys

The SSH key is stored within the Indeni application and not in the typical Linux OS location, therefore, device keys will need to be entered individually into the WebUI which can be done by performing the following:

1. Log into the remote device
2. Make a note of which user Indeni will connect with. This will be needed later. In our example below the username will be "indeni"

3. To create a public/private key pair, type the following:
"ssh-keygen -t rsa -b 4096 -f indeni-ssh -N"
4. Create a folder called **".ssh"** in the home folder of the user which will use Indeni, by typing in the following:
"mkdir /home/indeni/.ssh"
5. Move the public key to the .ssh folder, and rename it to **authorized_keys** and set the correct permissions by typing the following:
"mv indeni-ssh.pub /home/indeni/.ssh/authorized_keys"
"chmod 700 /home/indeni/.ssh"
"chmod 600 /home/indeni/.ssh/authorized_keys"

OPTIONAL: For increased security, perform the following to render the password for the "indeni" account useless, allowing only the SSH key to login:

dbset passwd:indeni:passwd "*" "dbset save".

6. Get the output the private key by typing the following:

"cat indeni-ssh"

OUTPUT EXAMPLE

– --BEGIN RSA PRIVATE KEY– –MIIJJQIBAAKCAgEAp5UbPfn36Y1NIqbvJLPWvd128lfZ1FH5gt/E=.....
– --END RSA PRIVATE KEY– –.

Checkpoint Private Key Example

```
-----BEGIN RSA PRIVATE KEY-----
MIIEJQIBAAKCAgEAp5UbPfn36Y1
NIqbvJLPWvd128lfZ1FH5gt/E=.....
wylUUt/ORHb390tp1ay0fnGebR9a7
rgsSzUr02exi0juLDPEgfmTBzNQFI
hav13EZw2F32KibUR63HLgJSTS6
WEhBd7AolH+Nrl1/zGINSBLYBMK
uxAdM/Yy1ZR+A9wDKYrKml/kn8
fDRWWLVaizCQmWstHcxQvLM1L2
+ZKu+Q+EuhH1sAZip7UtmA6eda
945e1F7aTDDU000QcSuzsCBk...
```

7. When adding the device into Indeni, select **"SSH Key"** and input the entire content (including the dashes)
"--BEGIN RSA PRIVATE KEY – and – END RSA PRIVATE KEY --"
of the RSA output.

Frequently Asked Questions

I've setup the user as described, but I cannot add the device

The most common issue is that the user configured has the incorrect shell, and/or the incorrect permissions. Make sure that the shell is set to **/bin/bash**, the role is **adminRole**, has the **correct password** set and that the **Uid** is '0' (zero). To verify this run, the following Clish command: "**show user <username>**" and "**show rba user <username>**"

```
lab-CP-GW1-R7730> show user indeni

```

Uid	Gid	Home Dir.	Shell	Real Name
0	0	/home/indeni	/bin/bash	Indeni

```
lab-CP-GW1-R7730> show rba user indeni
User
  indeni
  access-mechanism CLI
  access-mechanism Web-UI
  role adminRole
lab-CP-GW1-R7730>
```

Cisco ASA

We always recommend a system administrator defer to the vendor's official documentation on credential creation. Please follow the vendor's instructions for configuring the device for access with an SSH key, and then use the Indeni WebGUI to store the Private key in the relevant Credential Profile.

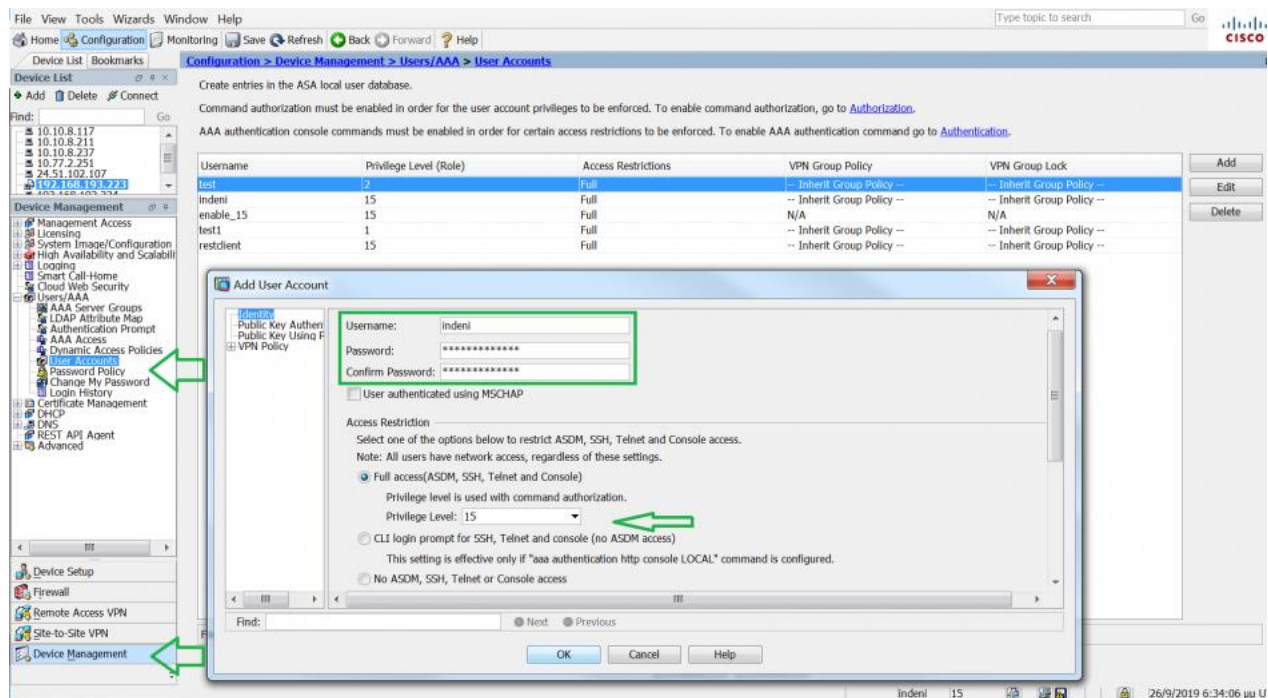
In order for Indeni to run its full set of interrogation and monitoring scripts, an SSH and SNMP user with a role of administrator needs to be used to connect your device. It is highly recommended that a unique Indeni user is created for auditing and security purposes. Before adding any ASA device, make sure both SSH and SNMP credentials are provided in Credentials Set.

Creating a SSH User in local database via CLI

1. Log in to the Cisco ASA device via SSH
2. **# enable**
3. **# config t**
4. **# username <username> password <password> privilege 15**
5. This command will create a new user with privilege level 15
6. After admin user is created, apply the following command to allow the local admin users to enter **enable** mode by default. This step is required in order for all the scripts to run successfully.
7. **# aaa authorization exec LOCAL auto-enable**

NOTE: The ASA support two Diffie-Hellman key exchange methods which are the DH Group 1 (768-bit) and DH Group 14 (2048-bit). By default, the ASA is set to use Diffie-Hellman Group 1. The command "**ssh key-exchange group dh-group14-sha1**" was introduced in 8.4(4.1) and 9.1(2). It can be used to set the default SSH key exchange method to dh-group14-sha1 (recommended).

Creating an SSH User in local database via ASDM



Creating a SNMPv3 User via CLI

1. The following example creates a SNMPv3 user with authentication and privacy passwords and limits the SNMP access to a range of IPs. Make sure the Indeni server IP is included in the IP range configured on the device, otherwise Indeni will NOT be able to interrogate the device.
2. Log in to the Cisco ASA device via SSH
3. **# enable**
4. **# config t**
5. **# object network indeni-server**
6. **# range 192.168.250.0 192.168.250.255**
7. **# exit**
8. **# snmp-server group SNMPv3Group v3 priv**
9. **# snmp-server user indeni SNMPv3Group v3 auth SHA <AuthPassword> priv AES 128 <PrivPassword>**
10. **# snmp-server host-group management indeni-server version 3 indeni**
11. **# exit**

F5

We always recommend a system administrator defer to the vendor's official documentation on credential creation. Please follow the vendor's instructions for configuring the device for access with an SSH key, and then use the Indeni WebGUI to store the Private key in the relevant Credential Profile.

User Requirements

The created user will require Administrative privileges. Also, depending on TMOS version and method of authorization the local admin account may be required.

Determining Account Type

To help determine what's right for your device, please consult the table below.

Version	Authentication	Authorization	Required User Type
BIG-IQ	Remote or Local	Remote or Local	Administrator role
11.6.0 and later	Remote	Remote	Local Administrator account with Advanced shell
11.6.0 and later	Local	Local	Any user with an Administrator role with shell set to Advanced shell
11.6.0 and later	Remote	Local	Any user with an Administrator role with shell set to Advanced shell

Setting up the Indeni User Account

Once you have identified the Version, Authentication, Authorization and User Type based on the chart above, please see the below examples of how to setup the User Account to be used for the Device Credentials when adding devices.

Configuring for LTM Administrator

1. Log in to the F5 web interface.
2. Navigate to **System** → **Users** → **User List**.
3. Click on **Create**.
4. Enter a **User Name** and a **Password**, configure role **Administrator** across **All** partitions and grant terminal access **Advanced shell**.
5. Click on **Finished**.

Account Properties

User Name: indeni

Password: New: [password], Confirm: [password]

Role: Administrator

Partition: All

Terminal Access: Advanced shell

Buttons: Cancel, Repeat, Finished

Configuring for Local Admin

1. Log in to the F5 web interface.
2. Navigate to **System** → **Users** → **User List**.
3. Click on the local admin account.
4. Change the **Terminal Access** from **Disabled** to **Advanced shell**.
5. Click on **Update**.

Account Properties

User Name: admin

Password: New: [password], Confirm: [password]

Role: Administrator

Partition: All

Terminal Access: Advanced shell

Buttons: Cancel, Repeat, Finished

Configuring for BIG-IQ

1. Log in to the BIG-IQ web interface.
2. Navigate to **System Management**.
3. Navigate to **User Management** → **Users**.
4. Click on **Add**.
5. Fill in the details and make sure that the user has the role **Administrator**.
6. Click **Save**.



... / New User*

User Properties

Auth Provider: local (Local)

User Name: indeni

Full Name: indeni

Password: [password]

Confirm Password: [password]

User Groups: Select...

User Roles: Administrator

Frequently Asked Questions

Why does Indeni need Administrator Access and Advanced Shell?

- Certain versions of F5 require that any user accessing the REST interface must have a role of administrator.
- The Indeni user needs to access bash to perform all smart monitoring checks.

Why does Indeni have to use the Local Administrator Account?

- When remote authorization is used there is no way of setting the Shell of remote users to Advanced Shell. More information on this can be found [here](#).
- In version 11.5.4 the only user that has access to the REST interface is the local admin account.

What is Remote Authorization?

- This is when a remote service (e.g. RADIUS, LDAP) defines the role a user has after they have successfully logged in to the device.

How does Indeni communicate with the BigIP?

- Indeni uses SSH (Advanced shell), and the iControl REST-API to pull data from the device.

What does Indeni do to ensure that it is not negatively impacting the performance of the device?

- If there is more than one way to script for an issue we will compare, and choose the one that uses less resources.
- We do not run scripts more often than needed. Each script interval is chosen to ensure that you get the Indeni Rules you need, when you need them.
- When gathering data, we try to minimize the size of the payloads from the device in order to make sure that minimal bandwidth is used.

These factors combined ensures that the device resources (CPU, Memory, and Bandwidth) used by Indeni are minimally impacted.

If you have additional questions, please feel free to hop on over to our community site and join the discussion!

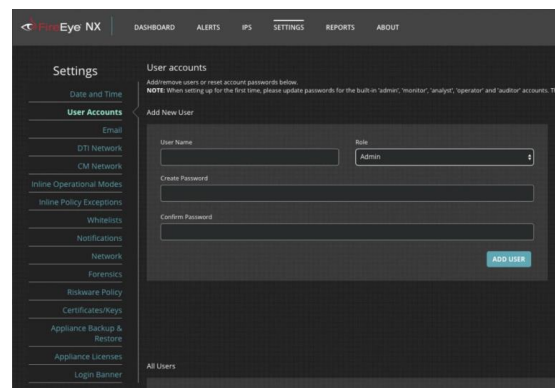
FireEye

We always recommend a system administrator defer to the vendor's official documentation on credential creation. Please follow the vendor's instructions for configuring the device for access with an SSH key, and then use the Indeni WebGUI to store the Private key in the relevant Credential Profile.

In order for Indeni to run its full set of discovery and interrogation scripts, a SSH user with a role of administrator needs to be used to connect your device. It is highly recommended that a unique Indeni user is created for auditing and security purposes.

Creating User via WebUI

1. Log in to the FireEye NX WebUI.
2. Go to **Settings** → **User Accounts**
3. Enter user name and password.
Select **Admin** for Role.
4. Click **ADD USER**.
5. Confirm new user account was created successfully by viewing all active users on **User Accounts**



All Users									
	User Name	Role	Account Status	Subnet	Mask	VLAN	Last Login	Login Count	Last Action
Permanent	admin	admin	Password set				11/08/19 01:52:20	3	11/08/19 01:52:20
Permanent	analyst	analyst	Local login disabled				None Yet	0	None Yet
Permanent	api_analyst	api_analyst	Local login disabled				None Yet	0	None Yet
Permanent	api_monitor	api_monitor	Local login disabled				None Yet	0	None Yet
Permanent	auditor	Auditor	Local login disabled				None Yet	0	None Yet
Permanent	crl_node	crl_node	Local password login disabled				None Yet	0	None Yet
Permanent	crl_sensor	crl_sensor	Local password login disabled				None Yet	0	None Yet
Permanent	cmcranda	cmcranda	Local password login disabled				None Yet	0	None Yet
Permanent	fx_services	fx_services	Local login disabled				None Yet	0	None Yet
Permanent	haagent	haagent	Local password login disabled				None Yet	0	None Yet
Self	indeni	admin	Password set				04/14/19 03:49:04	8	04/14/19 03:49:04
Permanent	monitor	monitor	Account locked out				None Yet	0	None Yet
Permanent	operator	operator	Account locked out				None Yet	0	None Yet
Regist	reject	reject	Account locked out				None Yet	0	None Yet
<input type="checkbox"/>	test	api_analyst	Password set				None Yet	0	None Yet

Creating Users via CLI

1. Log in to the FireEye NX device using SSH
2. **> *enable***
3. **# *configure terminal***
4. **# *username <username> password 0 <password>***
5. **# *username <username> role admin***

Fortinet

We always recommend a system administrator defer to the vendor's official documentation on credential creation. Please follow the vendor's instructions for configuring the device for access with an SSH key, and then use the Indeni WebGUI to store the Private key in the relevant Credential Profile.

Understanding Access Profiles and Users

Access Profiles

Fortinet Firewall Software uses the concept of **Access Profiles** to define the access level of a user. Access profiles control which CLI commands an administrator account can access. Access profiles can assign either read, write, or no access to each area of the FortiGate software. **You need read access level rights** in order **to view configurations**. To make configuration changes, you must have **write** access level rights. **Write Access is required** in order **to view configurations & troubleshoot** using the **get, diagnose** and **exec commands**.

Unlike other Administrator Accounts, the Default Administrator account named **"admin"** exists by default and cannot be deleted. The **"admin"** account is *similar* to a *root administrator account*. This administrator account always has full permission to view and change all FortiGate configuration options, including viewing and changing all other administrator accounts. However, its name and permissions cannot be changed.

Setting up the Indeni User

The Indeni User can be assigned to the predefined **super_admin level profile** to execute all the required **"get <x>"**, **"exec <x> "** and **"diagnose <x>"** FortiOS CLI commands currently supported by Indeni 6.0. It should be noted that the **"get"** and

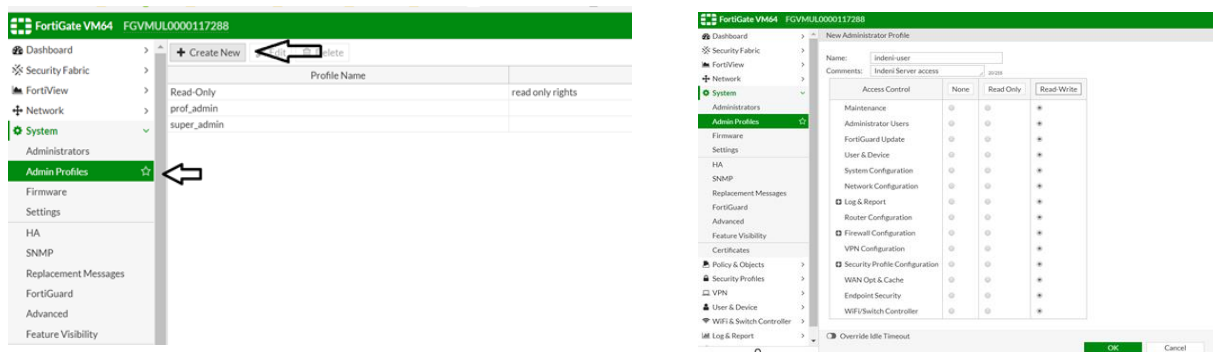
“exec” FortiOS commands **can be executed with a Read-Only user** but **not** the “diagnose” commands. Therefore, it is strongly recommended to create, or use an existing account, with admin (*read-write*) level rights so the Indeni Monitoring platform can provide more content around potential issues and remediation steps for all Fortinet Rules.

Configuring the Indeni User

This example adds a new FortiGate administrator account that uses a new **administrative** access profile with **full read-write access**. Account access to the firewall will be limited to connections from a specific IP subnet. The configuration is applied via https access to the Fortinet firewall so a user with admin privilege rights is required to perform the following steps (e.g. *the default admin user*). Finally, it should be noted that an existing user account can be reused by the Indeni Monitoring Platform; such as the default admin account name “admin” for example.

Step 1: Creating a New Administrative Profile

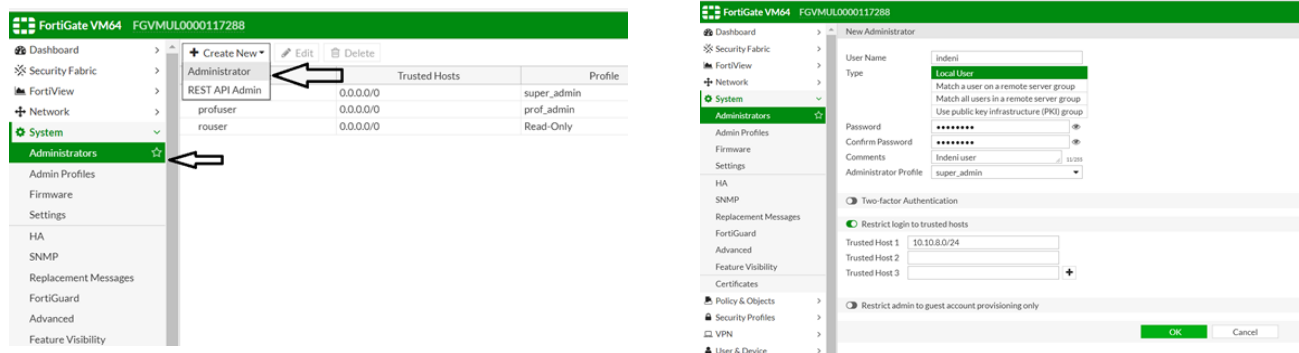
Go to **System > Admin > Admin Profile**. Create a new **Administer Profile** that allows the Indeni User with this profile to run all the “get”, “exec” and “diagnose” FortiOS CLI commands currently supported by the Indeni 6.0.



PLEASE NOTE: Read-Write should be selected for all the fields in order for the Indeni Platform to run exec, get and diagnostic commands via CLI. The default *prof_admin* and *super_admin* can also be used.

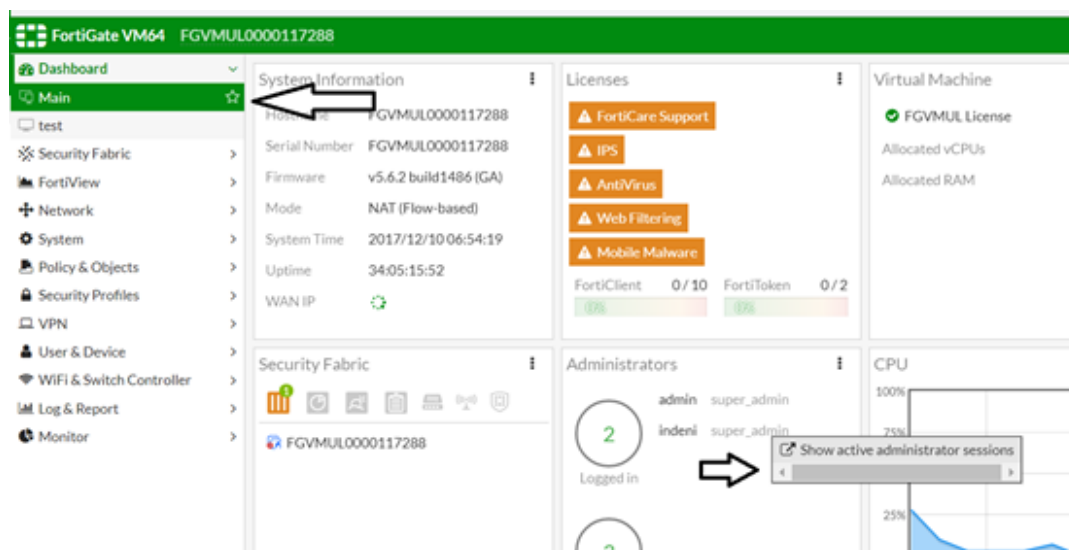
Step 2: Creating and Assigning a New User

A new administrator is added and assigned to the new admin-profile by going to **System > Admin > Administrators**. Create a new administrator account for the Indeni User and assign it to the profile that was just created (i.e. *indeni-user*). You can restrict access to the firewall to login from **Trusted Hosts Only** by adding the IP address range to one of the **Trusted Host fields**. You can use the IP address of the Indeni Server in case that this account is used only by Indeni.



Step 3: Verification & Results

Once you have successfully added the credentials and successfully interrogated a device, login to the FortiGate unit using an account with admin rights such as the default admin account. Go to **System > Dashboard > Status**, and view the **System Information widget**.



Select **Details** for the Current Administrator to view all administrators logged in. You should note that the Indeni server has logged in to the Fortinet firewall by using the newly created user and an SSH session.

Refresh Disconnect				
Username	Profile	Method	Source Address	Connected
admin	super_admin	SSH	10.10.8.116	53 minutes 39 seconds
admin	super_admin	HTTPS	10.10.8.244	13 minutes 47 seconds
indeni	super_admin	SSH	10.10.8.244	2 minutes 37 seconds

Go to **Log & Report > Event Log > System**. Look at the upper pane so see more activity, such as the successful login of the Indeni account. Select the entry for the new administrator login to get more detailed information to be displayed in the lower pane. The details show that the new administrator account logged in from an IP address that is within the ranges specified in the Trusted Hosts field.

FortiGate VM64 FGVML0000117288					
Dashboard	>	Refresh	Download	Add Filter	
#	Date/Time	Level	User	Message	
1	06:52:53	Success	indeni	Administrator indeni logged in successfully from ssh(10.10.8.244)	
2	06:52:33	Success	admin	Add system.admin indeni	
3	06:52:29	Failure	indeni	Administrator indeni login failed from ssh(10.10.8.244) because of invalid user name	
4	06:52:25	Failure	indeni	Administrator indeni login failed from ssh(10.10.8.244) because of invalid user name	
5	06:43:10	Success	admin	Fortigate update now fcni=yes fdni=yes fsci=yes virdb(53.00620) etdb(53.00620) exdb(1.00)	
6	06:41:43	Success	admin	Administrator admin logged in successfully from https(10.10.8.244)	
7	06:41:39	Failure	admin	Administrator admin login failed from https(10.10.8.244) because of invalid password	
8	06:39:31	Success	admin	Delete 19 old report files	
9	06:29:38	Success	rouser	Administrator rouser timed out on ssh(10.10.8.244)	
10	06:29:08	Success	admin	Configuration is changed in the admin session	
11	06:29:08	Success	admin	Administrator admin logged out from https(10.10.8.244)	
12	06:24:28	Success	rouser	Administrator rouser logged in successfully from ssh(10.10.8.244)	
13	06:24:12	Success	profuser	Administrator profuser logged out from ssh(10.10.8.244)	
14	06:24:07	Success	admin	Edit system.acprofile Read-Only	
15	06:22:08	Success	admin	Fortigate scheduled update fcni=yes fdni=yes fsci=yes from 173.243.138.68:443	
16	06:21:49	Success	profuser	Administrator profuser logged in successfully from ssh(10.10.8.244)	
17	06:21:31	Success	admin	Add system.admin profuser	
18	06:20:40	Success	admin	Fortigate update now fcni=yes fdni=yes fsci=yes from 173.243.138.79:443	

Frequently Asked Questions

Does Indeni support Fortinet Management Servers?

No. Indeni currently only support Fortigate Firewalls.

How does Indeni communicate with FortiGate firewalls?

The Indeni platform collects the information from the Fortinet Firewalls via direct SSH access to the devices. Now, let's see that in action:

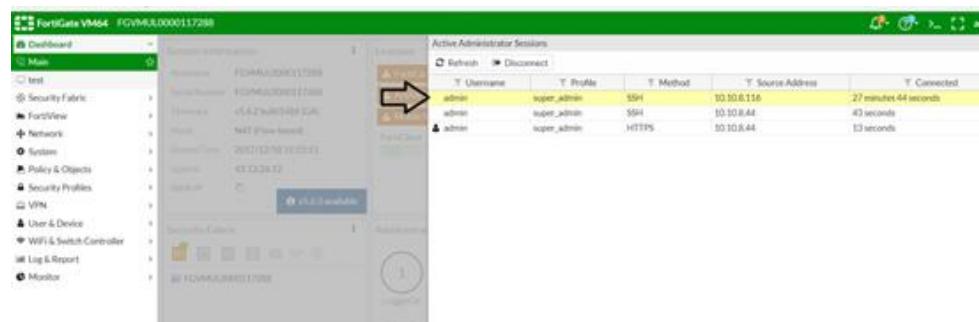
```
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic x86_64)

* Documentation:  https://help.ubuntu.com/
Last login: Sat Dec 16 19:01:44 2017 from 10.10.8.244

Installed indeni packages:

indeni-collector 6.0.70.1.330-RC
indeni-ds        6.0.50.173
indeni-server   6.0.70.1.330-RC
indeni-tools     1.0.1.40
indeni@indeni-server:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:56:a2:4b:1f
          inet addr:10.10.8.116 Bcast:10.10.8.255 Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fea2:4b1f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:11557059 errors:0 dropped:357 overruns:0 frame:0
          TX packets:5696255 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4510057672 (4.5 GB)  TX bytes:433499720 (433.4 MB)
```

As is illustrated above, Indeni has been installed and configured with the private IP address **10.10.8.116**.



Here we see that a Fortigate VM64 has been discovered and is now being monitored by the Indeni platform. Remember, Indeni uses the **admin** Fortinet **user** to get direct access via SSH to the Fortigate. As a result, an **admin user** with the source IP address of 10.10.8.116 is logged in to the firewall.

To summarize, Indeni collects all the required information for analysis via SSH access to a Fortinet Firewall, so a user with **super-admin** rights should be assigned to the Indeni user.

What does Indeni do to ensure that it is not negatively impacting the performance of the device?

Thorough testing has been performed at the Indeni Lab to determine the recommended minimum **CPU** and **Memory** requirements of a Fortinet firewall required to be monitored by the Indeni platform.

It was noted that an increased demand for *Memory* and *CPU* utilization was recorded during the discovery (*interrogation*) of the Fortinet firewall by the Indeni platform. **This is expected behavior**. We recorded a drop, and stabilization, of systems resources after discovery and normal Rule interrogation against the devices began.

It is **strongly recommended** that the Fortinet Firewall have a minimum 4 CPU cores and 4GB RAM to ensure peak device performance. All mid-range Fortinet Firewalls, starting from the FG-100E Series, have the minimum hardware requirements to be effectively monitored by Indeni. You can review the CPU/RAM resources and utilization of a firewall by running the following command: “*get system performance status*”

```
FG100D3G15809339 (global) # get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU1 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU2 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU3 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 4050664k total, 982712k used (24%), 3067952k free (76%), 141356k buffers
Average network usage: 10 / 3 kbps in 1 minute, 8 / 1 kbps in 10 minutes, 7 / 0 kbps in 30 minutes
Average sessions: 79 sessions in 1 minute, 65 sessions in 10 minutes, 63 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last 10 minutes, 0 sessions per second in 1
minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 194 days, 13 hours, 4 minutes
```

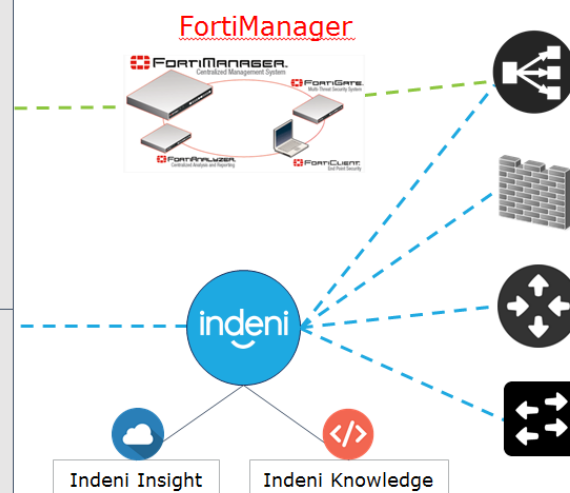
If I already have FortiManager, why do I still need Indeni?

FortiManager

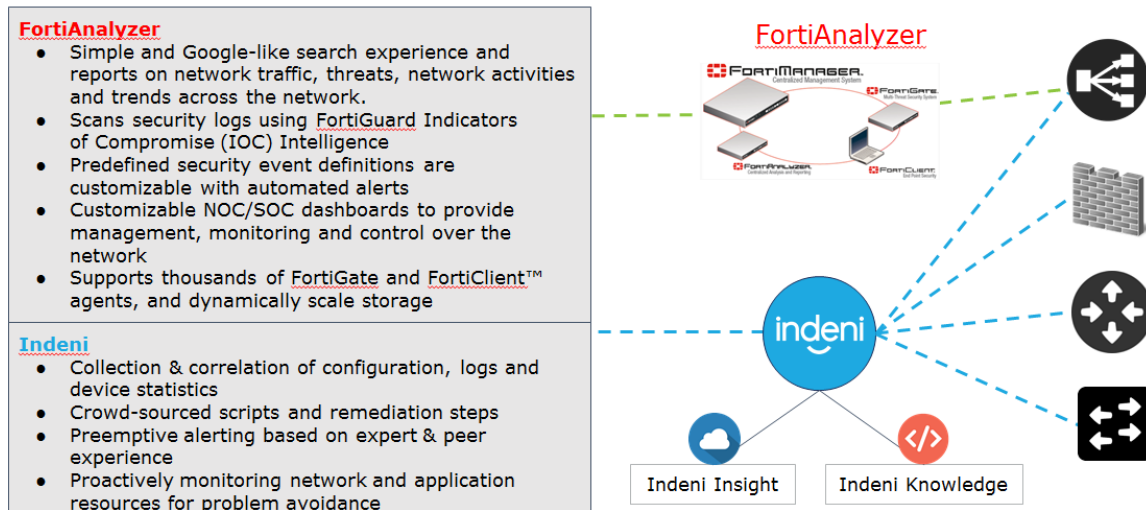
- Simplified policy management, device provisioning and configuration management for large scale Fortinet Enterprise deployments from one central place
- Ensure common security baseline is enforced and shared among multiple ADOMs required for audit and compliance.
- Dynamic security updates and end-to-end security management for Fortinet products.
- VPN manager to simplify the deployment, monitoring and allowing centrally provisioned VPNs
- API for Automation and Orchestration

Indeni

- Collection & correlation of configuration, logs and device statistics
- Crowd-sourced scripts and remediation steps
- Preemptive alerting based on expert & peer experience
- Proactively monitoring network and application resources for problem avoidance



If I already have FortiAnalyzer, why do I still need Indeni?



Fortigate has a number of licenses, which licenses do you check for expiration?

The Indeni Platform regularly checks the status of the Fortinet licenses and triggers a message either when the license is near expiration, or has expired. This information is also easily accessible from the dynamic configure tab of each Fortinet firewall. Once you have a device connected navigate to the **Devices icon** > search for the Fortinet device > Once selected, click on **More Device Info**. Here you can get a full list of your Certificates and Licenses Status; e.g. Anti-Spam AV definitions, IPS, etc.

As soon as the status of a license is either expired or close to expiration, a message is triggered and delivered to the Indeni platform.

If you have additional questions, feel free to hop on over to our community and post your question there!

Juniper

We always recommend a system administrator defer to the vendor's official documentation on credential creation. Please follow the vendor's instructions for configuring the device for access with an ssh key, and then use the Indeni WebGUI to store the Private key in the relevant Credential Profile.

In order for the Indeni User to monitor a Juniper SRX properly, two steps must be completed on the SRX.

STEP 1: *Enable SSH* for Scripting Access.

STEP 2: Create a ***Locally Authenticated*** Indeni User with ***Administrator Rights***.

How to Enable SSH for Scripting Access

First, verify SSH is configured via the CLI by entering the following command: *"show configuration system services"*

You should see the following SSH protocol present:

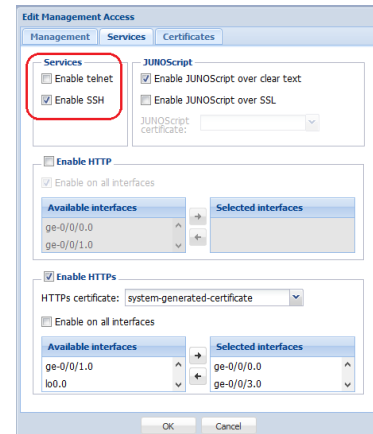
```
ssh {  
protocol-version v2;  
}
```

If SSH is not configured correctly, then enter the following commands in ***configuration mode***: *"set system services ssh protocol-version v2"; "commit"*.

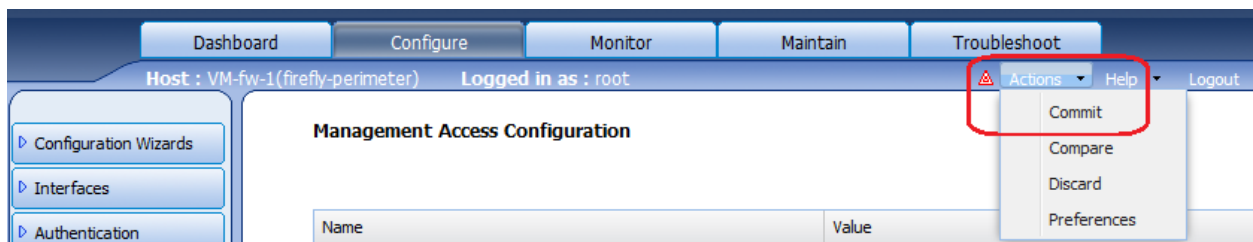
PLEASE NOTE: If access to the SRX is firewalled, SSH must be allowed from the Indeni server via the firewall.

To verify and/or enable SSH is enabled via the J-Web interface, please see the following:

- Configure → System Properties → Management Access
- Click Edit button on the right upper corner
- Check Enable SSH box (*if not already checked*)
- Click OK



Select commit from Actions pull down menu to activate the configuration.



How to Create a User with Administrator Rights

A locally authenticated User account with administrative privileges is required for Indeni to access SRX devices. Please note that the **“root”** account **cannot be used** for this purpose.

Creating the User Account via the CLI

Enter the following commands in configuration mode:

“set system login user indeni-user class super-user”

“set system login user indeni-user authentication plain-text-password”

New password: *****

Retype new password *****

“commit”

To verify that the user configuration is completed, enter the following in operational mode:

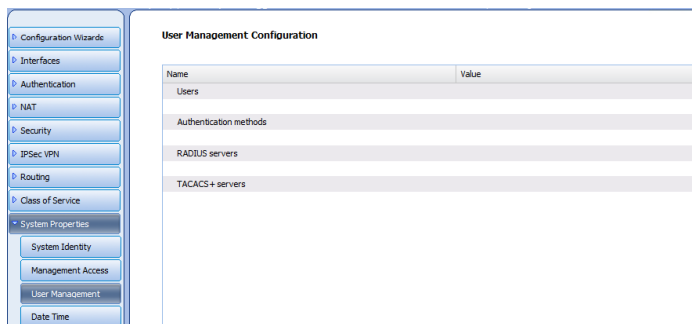
“show configuration system login”

Below is the expected output:

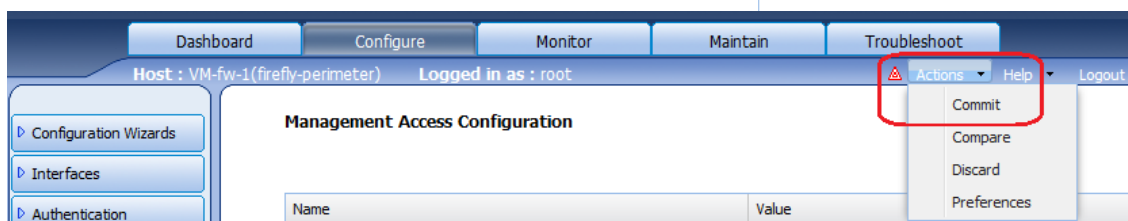
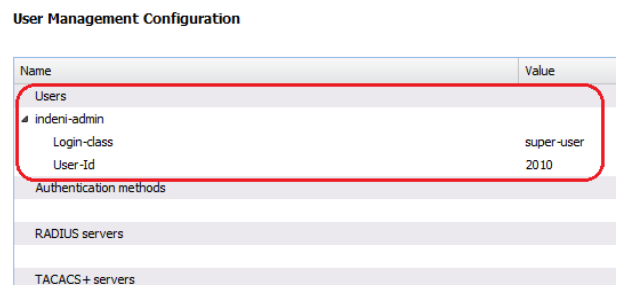
```
user indeni-user {  
  uid XXXX;  
  class super-user;  
  authentication {  
    encrypted-password “XXXXXXXXXXXX”; ## SECRET-DATA  
  }  
}
```

Creating a User Account via J-Web

1. Select **Configuration** → **System Properties** → **User Management**
2. Click Edit on the right upper corner:



3. Click Add button to add a new account.
4. Ensure that the **“Login class”** is **“super-user”**.
5. Click OK to add the new account.
6. Verify the account appears as below:



7. Select commit from Actions pull down menu to activate the configuration.
8. Test the newly created account from a remote system, then enter the following command: `ssh indeni-admin@srx-jfw`. Below is the expected output:

```
UNAUTHORIZED USE OF THIS SYSTEM
IS STRICTLY PROHIBITED!
Password: *****
- JUNOS 12.1X46-D65.4 built 2016-12-30 01:34:30 UTC
indeni-admin@SRX-JFW>
```

Frequently Asked Questions

We currently **do not have** FAQ's generated around this device at this time. If you have questions, or suggestions for FAQ's, please join us on our Community and ask there. Your feedback is greatly appreciated!

Gigamon

We always recommend a system administrator defer to the vendor's official documentation on credential creation. Please follow the vendor's instructions for configuring the device for access with an SSH key, and then use the Indeni WebGUI to store the Private key in the relevant Credential Profile.

In order for Indeni to run its full set of discovery and interrogation scripts, a SSH user with a role of administrator needs to be used to connect your device. It is highly recommended that a unique Indeni user is created for auditing and security purposes.

Accounts can be locally or externally authenticated by TACACS+, RADIUS, or LDAP servers. Local users are added directly to the device, while remotely authenticated users will need to be mapped (local user account to external login).

There are 3 predefined roles – Admin, Default, and Monitor. The Indeni user needs to be an admin as the role provides access to all command modes, including Standard, Enable, and Configure. Admin users also have access to all commands and all ports. They are also members of all groups.

Users can be created via the H-VUE web interface or via CLI. This article covers the creation of local users via CLI.

Creating Users via CLI

1. Log in to the Gigamon GigaVUE device using SSH
2. **> enable**
3. **# configure terminal**
4. **# username <username> password 0 <password>**
5. **# username <username> role replace admin**

Palo Alto Networks

We always recommend a system administrator defer to the vendor's official documentation on credential creation. Please follow the vendor's instructions for configuring the device for access with an SSH key, and then use the Indeni WebGUI to store the Private key in the relevant Credential Profile.

Indeni connects to Palo Alto Network Devices (Log Collector excepted) via PAN-OS XML API/HTTPS and SSH. We recommend assigning the Dynamic role of **Superuser** or **Superuser (read-only)** to the Indeni user, with standard session timeouts configured. This leverages Palo Alto Networks' fixed privileges and is a scalable option for future automation scripts to be successfully utilized by the Indeni system.

In the event that a Custom role need to be defined, it is preferred to include privileges that allow for flexibility and growth when Indeni's Knowledge scripts expand to include more enhanced functionality. However, the following are minimum access requirements and must be enabled within the profile.

WebUI: No minimum requirements (*all disabled*)

XML API: Operational Request

Command Line: devicereader

If you need assistance creating a user on your Palo Alto Networks device, please refer to [Palo Alto's website](#).

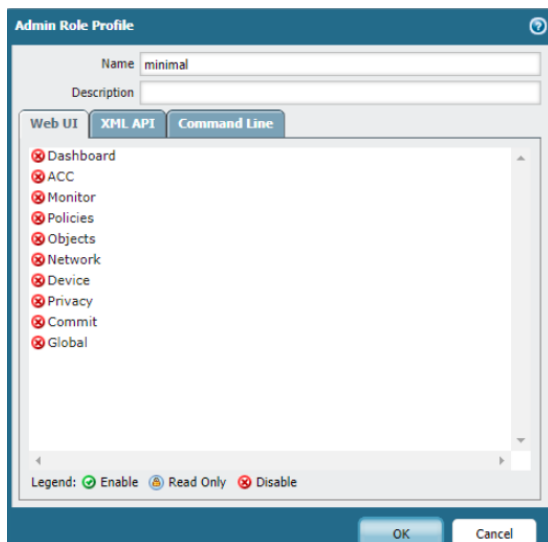
Indeni recommends that credentials set for Palo Alto Network devices are left with the default privilege of **Superuser (Read-Only)**, and **dynamic-based control**. Indeni is read-only and **does not** make any changes to the device's configurations or policies. The reason we recommend the above role configuration for the user is because as the product continues to expand its knowledge base, the Indeni credentials will need enough flexibility to facilitate any new scripts that may require access to API and SSH commands; which are otherwise strictly defined with custom roles.

Configuring Custom Roles

Should internal policies require that Indeni utilize the minimum available privileges required to collect and analyze data from the devices, we recommend to follow the guidance below in terms of creating custom credentials:

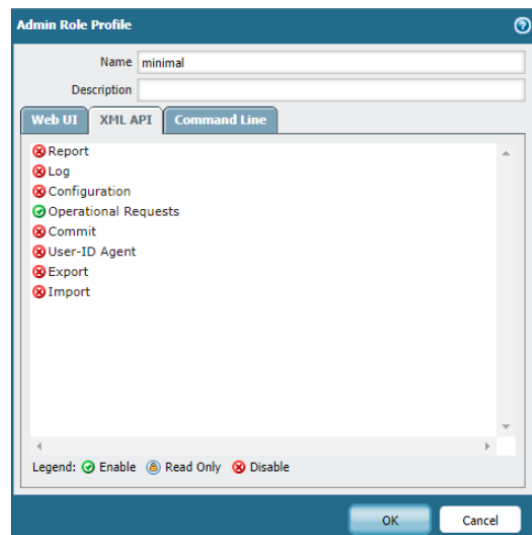
The enabled/disabled options should be set as follows:

Web UI – Disable All



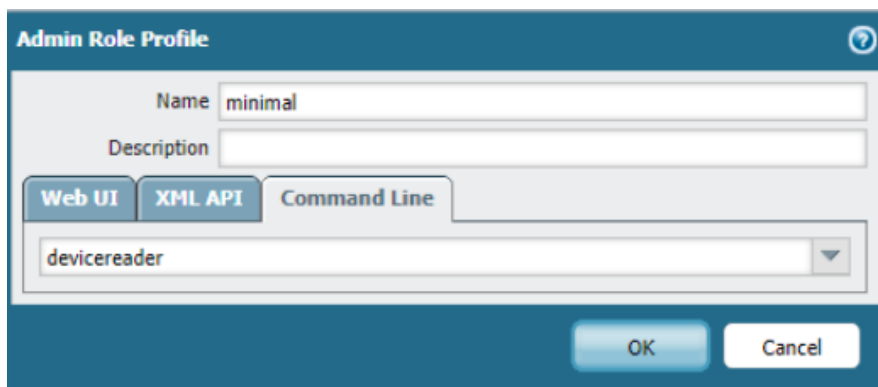
The 'Admin Role Profile' dialog shows the 'Web UI' tab selected. The 'Name' field is 'minimal' and the 'Description' field is empty. The list of permissions includes: Dashboard, ACC, Monitor, Policies, Objects, Network, Device, Privacy, Commit, and Global. All permissions are disabled, indicated by a red 'X' icon. A legend at the bottom shows: Enable (green checkmark), Read Only (blue circle), and Disable (red X).

XML API – Operational Requests



The 'Admin Role Profile' dialog shows the 'XML API' tab selected. The 'Name' field is 'minimal' and the 'Description' field is empty. The list of permissions includes: Report, Log, Configuration, Operational Requests, Commit, User-ID Agent, Export, and Import. 'Operational Requests' is enabled, indicated by a green checkmark icon. All other permissions are disabled, indicated by a red 'X' icon. A legend at the bottom shows: Enable (green checkmark), Read Only (blue circle), and Disable (red X).

Command Line: "devicereader"



The 'Admin Role Profile' dialog shows the 'Command Line' tab selected. The 'Name' field is 'minimal' and the 'Description' field is empty. The 'Command Line' dropdown menu is open, showing 'devicereader' as the selected option. The 'OK' and 'Cancel' buttons are visible at the bottom.

Radware

We always recommend a system administrator defer to the vendor's official documentation on credential creation. Please follow the vendor's instructions for configuring the device for access with an SSH key, and then use the Indeni WebGUI to store the Private key in the relevant Credential Profile.

Determining which Account Type to Set Up

By default, admin privileges are created for all Alteon devices. However, please see the below on recommended configuration for the Indeni user.

Version	Authentication	Authorization	Required User Type
Alteon- OS 29.0 and later	Remote or Local	Remote or Local	Administrator role

Setting up the Indeni User Account:

Please Note: Up to 10 users can be created at any time.

Creating a Local Account via CLI:

1. To enter into user configuration, type the following: `/cfg/sys/access/user/uid <#>`
 - a. Create the user name: **"name"**
 - b. Change the password: **"pswd"**
 - c. Establish the privilege level: **"cos admin"**
2. Type **"enable"**
3. Type **"apply"**

Creating a New Local Administrator Account in Alteon:

1. In the directory on the left, select “Users” → “Local Users”. Select the ‘+’ symbol

Alteon 172.16.20.33

Type: VA (Standalone)
Mgmt IP: 172.16.20.33
HA Status: Master
Version: 31.0.0.0
MAC: 00:0C:29:02:79:E4

Configuration Monitoring

Overview

System

Management Access

Users

Local Users

Remote Authentication

SNMP

Logging and Alerts

DNS Client

Time and Date

Licenses

VM Resource Allocation

Version Management

Configuration Management

Geo Location Database Import

Memory Management

APM Server

Device Performance Monitoring

Reset/Shutdown

Network

Application Delivery

Local Users

User Role: Administrator

Current Admin Password:

New Administrator Password:

Verify New Administrator Password:

Language Display: English

Local Users

+ -

State	User ID	User Name	Certificate Management Permissions	Language Display	RADIUS/TACACS Fallback
Enabled	2	indeni	Enable	English	Disable

Submit

Syslog Messages Note: The filter on the alert table can be set in its maximized view.

Time and Date	Severity	Message
Dec 26 02:42:19	NOTICE	mgmt: indeni login from host 192.168.197.12 via Telnet/SSH
Dec 26 02:42:18	NOTICE	mgmt: Failed login attempt via SSH from host 192.168.197.12, user ind...
Dec 26 02:42:18	NOTICE	mgmt: Failed login attempt via SSH from host 192.168.197.12, user ind...

2. To create the correct user for Indeni, you need to:
 - a. Enable the User.
 - b. Define the User ID, User Name, User Roles (*administrator only*) and define the new password.
 - c. **Optional Configuration:** You can enable fallback to RADIUS/TACACS should the local database fail at any point. This allows Radware to communicate with the RADIUS/TACACS server configured for authentication/authorization. Please read the [Alteon application user guide](#) to properly configure this.

Please Note: Up to 11 credentials can be defined at a time.

3. After configuring the user, click on “**Submit**”

- Click on **"Apply"** and **"Save"** to save your configurations. Make sure you are not accidentally making any additional changes to the devices. You can identify this by clicking on the **"Diff"** button on the top right.

Alteon 172.16.20.33

Type: VA (Standalone)
Mgmt IP: 172.16.20.33
HA Status: Master
Version: 31.0.0.0
MAC: 00:0C:29:D2:79:E4

Configuration Monitoring

Overview

System

Management Access

Users

Local Users

Remote Authentication

SNMP

Logging and Alerts

DNS Client

Time and Date

Licenses

VM Resource Allocation

Version Management

Configuration Management

Geo Location Database Import

Memory Management

APM Server

Device Performance Monitoring

Reset/Shutdown

Apply Save Revert Sync

Local Users Add New Local User*

☐ Enable User

User ID: Valid range: 1 ... 11

User Name:

User Role: Administrator

Current Admin Password:

New Password:

Confirm New Password:

Certificate Management Permissions: Enable

Language Display: English

RADIUS/TACACS Fallback: Disable

Submit Cancel

Configuring the administrator account for remote authentication (RADIUS/TACACS)

For both RADIUS and TACACS:

- To configure the Alteon to communicate with a RADIUS and TACACS server over the web GUI, select **"Remote Authentication"** which is just below **"Local Users"**

radware

Alteon 172.16.20.33

Type: VA (Standalone)
Mgmt IP: 172.16.20.33
HA Status: Master
Version: 31.0.0.0
MAC: 00:0C:29:D2:79:E4

Configuration Monitoring

Overview

System

Management Access

Users

Local Users

Remote Authentication

SNMP

Logging and Alerts

DNS Client

Time and Date

Licenses

VM Resource Allocation

Version Management

Configuration Management

Geo Location Database Import

Memory Management

APM Server

Device Performance Monitoring

Reset/Shutdown

Apply Save Revert Sync

Remote Authentication

☐ Enable RADIUS ☐ OTP Enable

TACACS+

Primary IP Address

IP Version: IPv4 IPv6

IP Address: 0.0.0.0

Secondary IP Address

IP Version: IPv4 IPv6

IP Address: 0.0.0.0

Port: 1645

Timeout: 3 Sec.

Retries: 3

Primary Server Secret:

Secondary Server Secret:

Allow Local User Fallback: Disable

Submit

2. Make sure to configure the fields required for your RADIUS/TACACS server as the only way to test if the server connected is SSH using the new configurations.

The screenshot shows the Alteon radware web interface for configuring Remote Authentication. The left sidebar contains a navigation menu with options like System, Management Access, Users, Local Users, Remote Authentication (highlighted), SNMP, Logging and Alerts, DNS Client, Time and Date, Licenses, VM Resource Allocation, Version Management, Configuration Management, Geo Location Database Import, Memory Management, APM Server, Device Performance Monitoring, and Reset/Shutdown. The main content area is titled 'Remote Authentication' and has tabs for 'Apply', 'Save', 'Revert', and 'Sync'. Below these tabs, there are checkboxes for 'Enable TACACS+' and 'OTP Enable'. The 'RADIUS' tab is selected, showing configuration for a RADIUS server. It includes fields for 'Primary IP Address' and 'Secondary IP Address', both set to '0.0.0.0' with 'IPv4' selected. Other fields include 'Port' (49), 'Timeout' (4 Sec.), 'Retries' (3), 'Primary Server Secret', 'Secondary Server Secret', and 'Command Authorization' (Disable). A 'Submit' button is at the bottom.

Radius Authentication Only:

Ensure that the credentials used have the correct RADIUS attribute. For administrator privileges, the default attribute “6” works just fine.

TACACS Authentication Only:

TACACS+ uses the AAA architecture, which separates **A**uthentication, **A**uthorization, and **A**ccounting. This allows separate authentication solutions that can still use TACACS+ for authorization and accounting.

For example, with TACACS+, it is possible to use Kerberos authentication and TACACS+ authorization and accounting. After Alteon authenticates a user on a Kerberos server, it requests authorization information from a TACACS+ server without requiring re-authentication. Alteon informs the TACACS+ server that it has successfully authenticated the user on a Kerberos server and the server then provides authorization information.

TACACS Disclaimer

Alteon supports ASCII inbound logins, however, the following **are not supported**:

1. **PAP, CHAP, and ARAP** login methods.
2. TACACS+ change password requests.
3. One-time password authentication

For TACACS Authorization, **privilege level differs** in the following scenarios:

- Disabled Privilege Level Mapping. TACACS+ Level should be set to 6
- Enabled Privilege Level Mapping. TACACS+ Level should be set to 14 or 15

Frequently Asked Questions

Why does Indeni need administrator access?

The Alteon devices are heavily restricted from viewing data outside each privilege levels. Privileges are designed around what may be configured on the load balancers.

For example, networking has only access to L2-L3 configurations of the Alteon while the “server operator” privileges can only view configurations involving the application servers that Indeni is connected to. This separation makes it difficult to utilize one account to view all level of data unless utilizing administrator privilege.

Indeni is strictly **read-only**. We **do not** execute any changes against the device.

Symantec

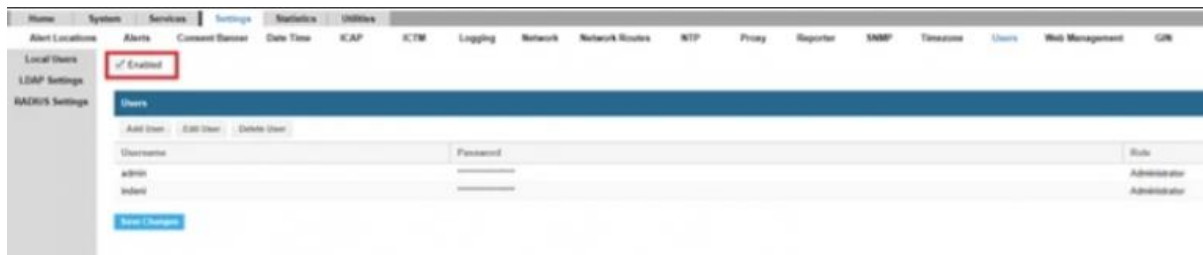
We always recommend a system administrator defer to the vendor's official documentation on credential creation. Please follow the vendor's instructions for configuring the device for access with an SSH key, and then use the Indeni WebGUI to store the Private key in the relevant Credential Profile.

In order for Indeni to run its full set of discovery and interrogation scripts, a SSH user with a role of administrator needs to be used to connect your device. It is highly recommended that a unique Indeni user is created for auditing and security purposes.

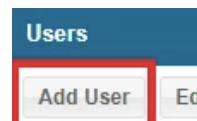
On Indeni, please make sure to provide the **Privileged password** in the **Credential Set** associated with this device.

Creating User via WebUI

1. Log in to the Symantec CAS WebUI.
2. Go to **Settings** → **Users** → **Local Users**
3. Make sure the **Enabled** check box is selected.



4. Click **Add User** to add a new user.
5. Fill in the user name and password and set the Role to **Administrator**.
6. Click **Add** to finish adding the new user.

A screenshot of the 'Add User' dialog box. It contains the following fields: 'Username:', 'Password:', 'Confirm Password:', and 'Role:'. The 'Role' field is a dropdown menu. At the bottom, there are 'Add' and 'Cancel' buttons.

2.2 Device Communication

In order for Indeni to run its full set of intelligent knowledge checks, you need to Create a User in the management system for the device you want to add, then add that user to a Credential Set (see [Section 5.1](#)). We recommend creating a unique Indeni user for auditing and security purposes.

The privilege level required varies depending on the device type. When possible, we avoid the need to use an administrative account for accessing the device, but in some cases, it cannot be avoided due to limitations to the network device. If communication between Indeni and the analyzed devices passes through a firewall, please allow the following:

- **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.

Please see the below chart for vendor port requirements:

DEVICE VENDOR	SSH PORT	HTTP PORT
Blue Coat	22	8082
Check Point	22	x
Cisco	22	x
F5	22	443
FireEye	22	x
Fortinet	22	x
Gigamon	22	x
Juniper	22	x
Palo Alto Networks	22	443
Radware	x	443
Symantec	22	x

Part 3: Navigating the User Interface

After login, the site will land you on the **Summary Page** by default. On the left side of the page, we have the 4 Icons which are your main menu options:



ISSUES: This is where you can find **Current** and **Archived** issues (formerly known as “alerts”), and configure your **Indeni Rules**.



ANALYSIS: This is where you can get a **historical analysis** of managed devices.

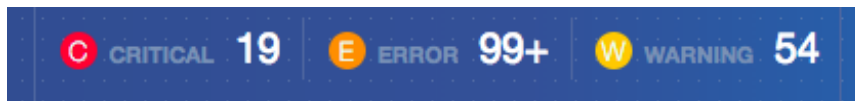


DEVICES: This is where you can manage **Devices**, run **Device Reports**, **Device Backup**, create **Labels** and also manage your **Credential Sets**.



SETTINGS: This is where you can view your **License** details, setup **Integrations** and **Manage Users**.

You can change the severity of issues in **Indeni Rules**. The icons to the left of the issue types continue to represent the severity throughout the WebUI:

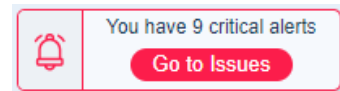


These menu links are always present along the border of all the main sections within Indeni, so you never miss an issue while operating inside the WebGUI.

3.1 Summary Tab

The Summary Tab is the first place you land after logging in. This is where you can get a quick overview of the issues Indeni has uncovered.

The first thing to take note of is the **Critical Issue** alarm in the center of the page.

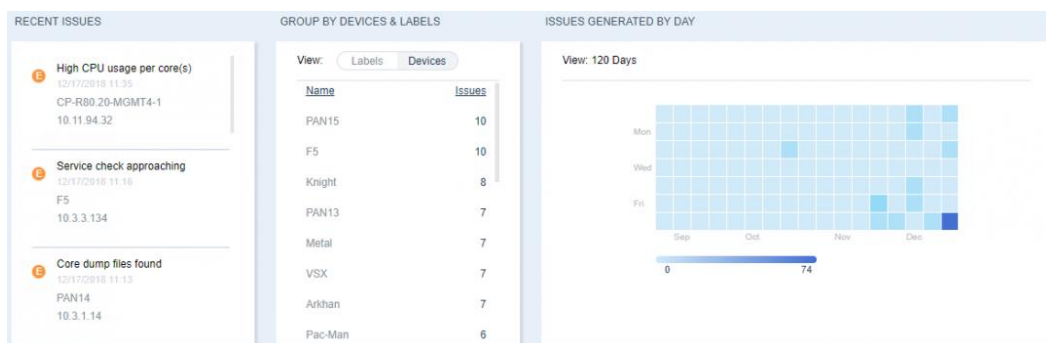


This is updated real time as Critical issues are being found. You can jump to the Critical Issue details by clicking on **Go to Issues**.

Under the Critical Alarm tab, you can review your **Top 10 Issues**. Click on the blue arrow (*highlighted in green*) to scroll and view the rest of the issues. There is also a **Pie** chart that shows the most common type of issues generated.



At the bottom of the page you can find the most **Recent Issues** generated, Group them by **Labels** or **Devices** and a **Heat Map** of the last 120 days so you can see when you had that most issues. A color code is provided at the bottom of the heat map, but you can see more granular details by hovering your cursor over a day of interest.



3.2 Current Tab

The **Current** sub-tab displays all current issues as well as the complete list of all analyzed devices and their associate issues. Users can filter by **Devices**, **Severities**, **Labels** and **Issues Status**. You can even **Export** issue data in CSV format.

Summary	Current	Archived	Indeni Rules			
All Issues	All Devices	All Severities	All Labels	All Statuses	Export	
<input type="checkbox"/>	ID	Headline	Device IP	Device	Created	Updated

Use the blue arrows (*names highlighted above in green*) to edit or filter issues for individual devices, group of devices, type of issues, type of severity, resolved or unresolved issues. You can also sort by **Created** and **Updated** timestamps.

Please Note: When issues have been successfully resolved (*greyed out*) it will remain on display until the user acknowledges and archives it, or filters by unresolved issues.

<input type="checkbox"/>	ID	Headline	Device IP	Device	Created	Updated
<input checked="" type="checkbox"/>	32957	Routes defined in clish/webUI are missing	192.168.194.30	LAB-CP-MGMT1-1	21 minutes ago	21 minutes a...
<input type="checkbox"/>	32956	RESOLVED Debug mode enabled	172.16.20.30	ipso	27 minutes ago	21 minutes a...
<input checked="" type="checkbox"/>	32955	RESOLVED Debug mode enabled	172.16.20.30	ipso	37 minutes ago	31 minutes a...
<input checked="" type="checkbox"/>	32954	RESOLVED Debug mode enabled	172.16.20.30	ipso	an hour ago	an hour ago

The check boxes in the left column allow users to manage multiple issues. The topmost checkbox (*in the header row*) will allow you to check or uncheck all boxes at once.

The **ID column** will display the severity type based on the color flag and initial of each issue.

Colors range from red to blue to distinguish critical warnings from less severe issues. This allows users to find and resolve issues most likely to cause imminent downtime and to visually assess the type of issue and remedial action required.

	Severity
	Critical
	Error
	Warning
	Info

Indeni assigns a unique ID number to each issue as it occurs.

By default, issues display in descending order of severity and by date modified. The **Headline** displays the actual issue information and a brief description of the condition Indeni has observed. The **Device IP** column displays the device management IP address assigned to each device for which an issue has been flagged. **Device** column displays the device name assigned to each device for which an issue has been flagged, followed by when it was **Created** and last **Updated**.

<input type="checkbox"/>	ID	Headline	Device IP	Device	Created ▾	Updated ▾
<input checked="" type="checkbox"/>	32957	Routes defined in clish/webUI are missing	192.168.194.30	LAB-CP-MGMT1-1	21 minutes ago	21 minutes a...
<input type="checkbox"/>	32956	RESOLVED Debug mode enabled	172.16.20.30	ipso	27 minutes ago	21 minutes a...
<input checked="" type="checkbox"/>	32955	RESOLVED Debug mode enabled	172.16.20.30	ipso	37 minutes ago	31 minutes a...
<input checked="" type="checkbox"/>	32954	RESOLVED Debug mode enabled	172.16.20.30	ipso	an hour ago	an hour ago

Detailed Issue Review

To review a reported issue in more detail, simply click on an issue of interest to update the **Issue Summary** page on the right-hand side. You do not need to use the check box to expand the issue.

ALERT SUMMARY

VPN TUNNEL(S) DOWN
 checkpoint R77.30 - gaia, VMware Virtual Platform

DESCRIPTION

One or more VPN tunnels are down.

VPN TUNNELS AFFECTED:

VPNisDown2 (2.2.2.2) - This tunnel is down

VPNisUp2 (192.168.194.49) - This tunnel is down

VPNisUp3 (192.168.194.38) - This tunnel is down

REMEDIATION STEPS:

Review the cause for the tunnels being down. Indeni uses the "vpn tu" command on the firewall to determine gateway status. Open SmartView Tracker and look for recent logs pertaining to the VPN peers listed above. Consider reading: [How to Troubleshoot Check Point Firewall VPN Connection](#)

NOTES: New

3/15/2018 13:20	Associated item added: VPNisDown2 (2.2.2.2)
3/15/2018 13:20	Associated item added: VPNisUp3 (192.168.194.38)
3/15/2018 13:20	Associated item added: VPNisUp2 (192.168.194.49)
3/15/2018 13:20	Alert created.

More Alert Info
Archive
⌵

The **Description** section will give you a general description overview and explanation of the problem. Just below that you will see **Issue Items** relating to the reported problem, like the actual VPN tunnels that are down. If you want to remove a specific item, and keep others, you can do so by hovering over an item and click the x mark. This will effectively Archive that specific issue.

You can also provide **Custom Instructions** that gives users the option to add their own notes, which are a great way to supplement the **Remediation Steps** (*recommended*) and actionable direction to address the issue.

You can select **More Issue Info** for more details, **Archive** it, or by clicking on the up-arrow reveal **Disable** options. You can also send the details to **Support** if you have questions around the issue.

and look for recent logs pertaining to the VPN peers listed above. Consider reading: [How to Troubleshoot Check Point Firewall VPN Connection](#)

NOTES: New

3/15/2018 13:20	Associated item added: VPNisDown2 (2.2.2.2)	Email Indeni Support
3/15/2018 13:20	Associated item added: VPNisUp3 (192.168.194.38)	Disable Entirely
3/15/2018 13:20	Associated item added: VPNisUp2 (192.168.194.49)	Disable for this Device
3/15/2018 13:20	Alert created.	Change Threshold

More Alert Info
Archive
⌵

Issues with Multiple Items

Click on **More Info** to get a better view of reoccurring and consistent issues. For example, **VPN Tunnel(s) down** issue has multiple VPN tunnels affected, as indicated below:

- *VPNisDown2 (2.2.2.2) – This tunnel is down*
- *VPNisUp2 (192.168.194.49) – This tunnel is down*
- *VPNisUp3 (192.168.194.38) – This tunnel is down*

**VPN TUNNEL(S) DOWN**
LAB-CP-GW2 192.168.194.37
checkpoint R77.30 - gaia, VMware Virtual Platform

ALERT SUMMARY

DESCRIPTION

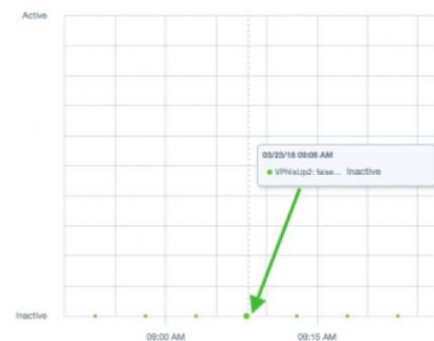
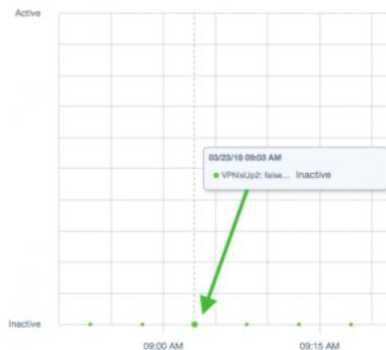
One or more VPN tunnels are down.

VPN TUNNELS AFFECTED:

VPNisDown2 (2.2.2.2) - This tunnel is down
VPNisUp2 (192.168.194.49) - This tunnel is down
VPNisUp3 (192.168.194.38) - This tunnel is down

REMEDATION STEPS

The graph to the right gives you a visual view of when the issue was generated, helping the end user get a better understanding of when the system is reporting it. In this particular example, you see an up/down on/off state triggering at the intervals which the script is set to run:



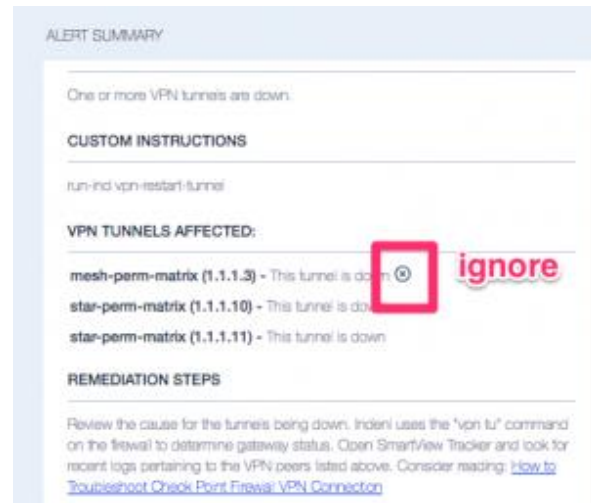
As you can see the dots are coming in at 5-minute intervals (09:03 AM to 09:08 AM) at the bottom (*Inactive*). You are not going to see a consistent line graph here because we also want to make sure the interrogation is happening at the intervals it should. Gaps in normal intervals could be indicators of other issues.

Acknowledge an Issue Item

The user can acknowledge (*aka ignore*) an item within an issue. The acknowledgement of issues is meant for physical intervention from a user. Typically, acknowledge functions gives the user an audit trail of physical intervention.

Its purpose is to prevent multiple people from working on the same issue. When you acknowledge an issue item, it effectively archives it.

For example, you want to acknowledge one of the **VPN Tunnels Down** issue because it is not a permanent tunnel, therefore it is often down.



To acknowledge the 1.1.1.3 tunnel, click on the **x** button. Ignoring this item effectively means that the item is excluded (*or archived*) from the issue.



At this point, the VPN Tunnel(s) down issue is still in active state, but now with two items. When the **1.1.1.10** and **1.1.1.11** tunnels go back up, this particular issue would be marked **resolved**. Note: the **1.1.1.3** tunnel remains inactive, since the item was ignored, Indeni will mark the entire issue as resolved.

3.3 Archived Tab

Clicking the **Archive** button from the **Current** tab acknowledges and archives the issue and removes it from the current list. Indeni stores all resolved issues. These are placed under **Current Issues** until they are manually acknowledged. There is no aging algorithm. To review issues acknowledged, go to the **Archived** sub-tab.

Summary

Current

Archived

Indeni Rules




All Issues

All Devices

All Severities





All Labels

Export

<input type="checkbox"/>	ID	Headline	Device IP	Device	Created	Updated
<input type="checkbox"/>	 25	RESOLVED User-ID agent(s) down	10.3.1.15	PAN15	2 months ago	an hour ago
<input type="checkbox"/>	 52	RESOLVED Pnote(s) down	10.3.3.62	Knight	2 months ago	an hour ago
<input type="checkbox"/>	 17	RESOLVED Core dump files found	10.3.1.14	PAN14	2 months ago	an hour ago

Use the blue arrow to edit or filter issues for individual devices, group of devices, type of issues, type of severities, resolved or unresolved issues. Issues that are resolved are greyed out.

The checkboxes in the left column allow users to manage multiple issues. Use the topmost checkbox (in the header row) to check or uncheck all boxes at once. You can archive multiple issues. The general functionality is the same as Current Issues. The **ID column** will display the severity type(s) based on the color flag and initial of each of the issues.

	Severity
	Critical
	Error
	Warning
	Info

Colors range from red to blue to distinguish critical warnings from less severe issues. This allows users to find and resolve issues most likely to cause imminent downtime and to visually assess the type of issue and remedial action required. Indeni assigns unique number to each issue as it occurs.

By default, issues display in descending order of severity and by date modified. The **Headline** displays the actual issue information and a brief description of the condition Indeni has observed. The **Device IP** column displays the device management IP address assigned to each device for which an issue has been flagged. **Device** column displays the device name assigned to each device for which an issue has been flagged, followed by when it was **Created** and last **Updated**.

Summary

Current

Archived

Indeni Rules

All Issues

All Devices

All Severities

All Labels

Export

<input type="checkbox"/>	ID	Headline	Device IP	Device	Created	Updated
<input type="checkbox"/>	<div><div>E</div>25</div>	RESOLVED User-ID agent(s) down	10.3.1.15	PAN15	2 months ago	an hour ago
<input type="checkbox"/>	<div><div>E</div>52</div>	RESOLVED Pnote(s) down	10.3.3.62	Knight	2 months ago	an hour ago
<input type="checkbox"/>	<div><div>E</div>17</div>	RESOLVED Core dump files found	10.3.1.14	PAN14	2 months ago	an hour ago

Unarchive an issue

The user can **Unarchive** an issue in the Issue Summary. The issue will return to the **Current** issue list.

SUMMARY

USER-ID AGENT(S) DOWN (RESOLVED)
paloaltonetworks 6.1.0 - panos, PA-VM

DESCRIPTION

One or more User-ID agents are down.

USER-ID AGENTS:

my-down-agent(vsys: vsys1) Host: 10.1.3.1:2323 -
The User-ID agent is not responsive.

REMEDIALTION STEPS:

A User-ID Agent being down may cause improper User-ID mappings to your firewall traffic and URL logs for example. Not having a proper User-ID mapping may even cause failure to access resources because they cannot be identified as a member of a group in a user/group based policy.
How to Troubleshoot User-ID Agent Problems:
<https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/user-id/verify-the-user-id-configuration.html>

More Info
Unarchive

3.4 Rules Tab

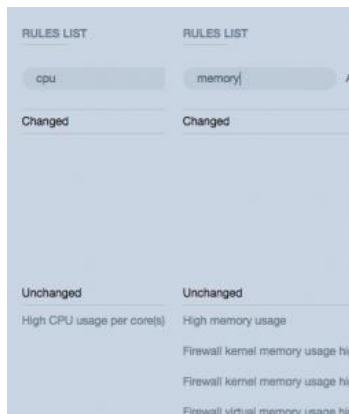
The Rules Tab is where you can modify and tune issues, email notifications and disable automation tasks. You should take note that all rules will default to the **Global Configuration** and behave on the **Thresholds** and **Actions** defined therein. This means that a critical issue may be generated around a Hard Disk which is 80% full. This is not a mistake. These thresholds were set to show you the results of the script automation and let you adjust from the rules from there.

Best Practices for Beginners

1. We would recommend downloading and installing on a lab to get a feel for how Indeni will operate and practice tuning.
2. We would recommend that Email notifications are to be suppressed, especially if adding multiple devices.
3. We would recommend tuning the system and leveraging device labels to maximize your experience with how the system will automate issue messaging.
4. We encourage you to participate, review, and ask questions on the **Crowd** should you have any questions that may not have been answered in the guide.

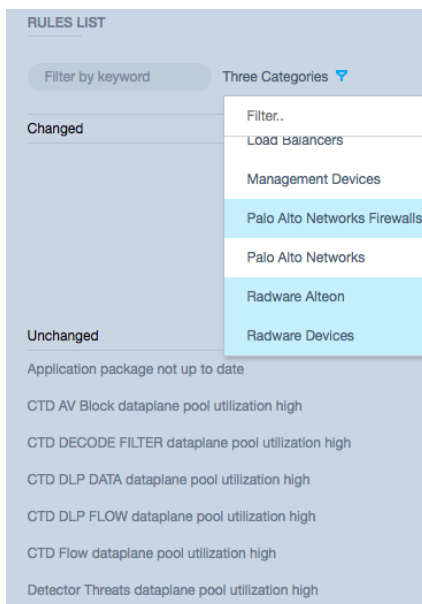
Navigating Indeni Rules

Since many rules exist, it will be best to filter by **keyword** or **All Categories**, to drill down to device specific rules. It's also best to try and search for generic words, such as **memory** or **CPU**, which will give you all rules in the system that contain those words.

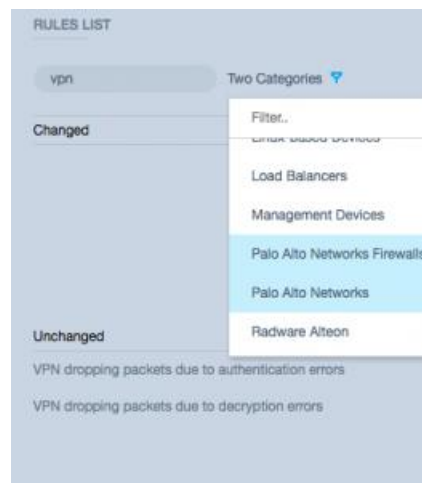


You can keep track of what Rules have been modified if they transition from **Unchanged** to **Changed**.

If you select by **Category**, you can see the rules we have around a device. For example, what Rules exist to check for CPU issues in a Radware Alteon. You can also select multiple categories by simply clicking on and highlighting them. **Shift+left** click will remove a single selection.



You can also add a search word to further filter the **Category Selection**.



Overview **Configurations** Disabled

Name

High CPU usage per core(s)

☒ Rule enabled, deselect to disable

Category

All Devices

Summary

High CPU usage is a symptom of a system which is unable to handle the required load or a symptom of a specific issue with the system and the applications and services running on it. Indeni will monitor the CPU usage of each core separately and alert if any of the cores' CPU usage crosses the threshold.

Once you have selected a rule to configure, you will land on the **Overview Sub-Tab** and should make note of the **Category**. If it is for **All Devices**, it will be marked as such. If it is a device specific rule, you will see that indicated there. It is also good to read the **Summary** of what the rule is attempting to do and how it can help. Under the **Name** of the rule, you will see a check mark. This means that the **Issue is Active**. If you uncheck this option, it will **Disable the Rule entirely**.

Please Note: You cannot delete the Global Configuration, however, once you create a new Configuration by clicking on New, it will override the Global Configuration settings.

CONFIGURATION New

Global Configuration

CONFIGURATION VALUES

Name

Global Configuration

Thresholds

High Threshold of CPU Usage:

70.0

Number of Cores:

1

Time Threshold:

Days: 0 hh: 0 mm: 10 ss: 0

Actions

☒ ISSUE ☒ SNMP ☒ EMAIL

Custom Instructions

Severity

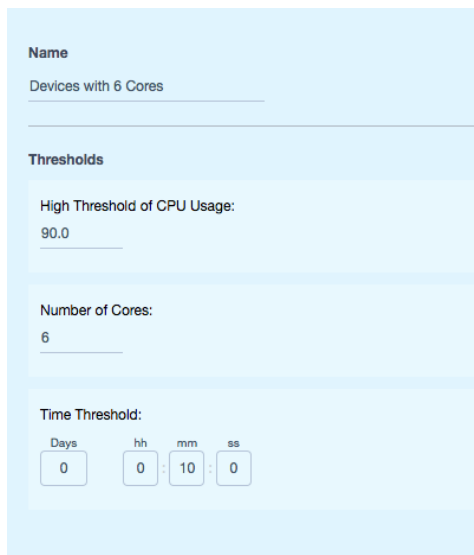
Not all rules are the same, but the structure will be. All rules will have **Name** (what is this), **Thresholds** (when should it trigger), **Time Threshold** (when you want to be notified), **Actions** (what notification to receive), **Custom Instructions** (what to do), and **Severity** (issue impact).

Multiple Rule Configuration

You can create as many rules as you want by leveraging **Labels** and **Devices**. In fact, we advise clients that have large deployments to utilize labels to better manage and tune your system. The reason you would want to have multiple rules is for situations where you would benefit from an escalating notification procession, or require more nuanced rules to uncover issues.

CPU and Multiple Rule Configuration

The best example of this is with CPU monitoring. Some devices have different number of cores, making CPU notification more nuanced than a Hard Disk that is 96% full. So how would you want to handle this situation? We have seen the best results by end-users creating labels for devices by number of cores, then adjusting the CPU Threshold to something like 90%.

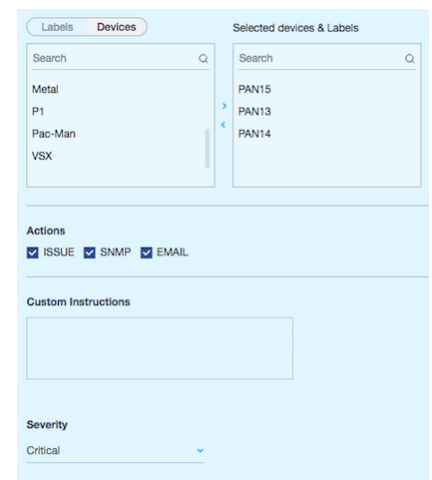


The screenshot shows a configuration form for a rule named "Devices with 6 Cores". Under the "Thresholds" section, the "High Threshold of CPU Usage" is set to 90.0. The "Number of Cores" is set to 6. The "Time Threshold" is set to 0 days, 0 hours, 10 minutes, and 0 seconds.

Here the **Name** of the issue was changed to **Devices with 6 Cores**, to help the operator know what this new issue is for.

The **Threshold** was changed to 90.0 because that is when someone should look into it. The Number of Cores was changed to 6, because 1 core is not concerning. The **Time Threshold** is same, since 6 cores running at 90% for **10 minutes** is a bit concerning.

Towards the bottom you can move the devices **Devices/Labels** you want to automate from left to right in the configuration values. The severity is set to **Critical**. It is always good to include instructions on how to validate and escalate.



The screenshot shows the "Selected devices & Labels" section of the configuration form. It displays a list of devices: Metal, P1, Pac-Man, and VSX. The "Actions" section is checked for ISSUE, SNMP, and EMAIL. The "Custom Instructions" field is empty. The "Severity" is set to Critical.

Please Note: New rule configurations will not work if you do not move devices or labels over.

Escalating Notification Process

Unlike the CPU, where it is helpful to create multiple rules for different types of devices, there are times when want to be made aware of an issue as an FYI, but then need an alarm to go off because it is about to boil over into a critical status. We have seen great success in organizations averting an outage by creating an escalating notification process around **Device Temperatures**.

High Temperature Escalation Configuration

In this example you can start by creating the minimum threshold you want the issue to trigger at; e.g., a **Warning Notification** when the devices reach 85% of the temperature at which they would probably shut down.

The screenshot shows the Indeni configuration interface. On the left, under 'CONFIGURATION', a list of items includes 'C_Heat Nearing Shutdown', 'E_Overheating', 'Global Configuration', and 'W_Over Min Value', which is selected. On the right, under 'CONFIGURATION VALUES', the configuration for 'W_Over Min Value' is shown. It includes a 'Name' field with the value 'W_Over Min Value'. Below this is a 'Thresholds' section with a 'High Threshold of Usage' set to '85.0'. Further down, there are two panels: 'Labels' and 'Selected devices & Labels'. The 'Labels' panel has a search bar and a list containing 'Test-SD' and 'Test'. The 'Selected devices & Labels' panel also has a search bar and a list containing 'All'. At the bottom, an 'Actions' section shows three checkboxes: 'ISSUE' (checked), 'SNMP' (checked), and 'EMAIL' (unchecked).

For a **Warning**, you might want to **uncheck email** to limit noise. We would suggest keeping **Log** and **SNMP checked**, so you can leverage the reporting feature in **Current** and **Archive** sub-tabs to create an audit around what devices are reaching that threshold. If you have a large number of devices to manage, this kind of quick audit reporting can be invaluable! You can start to see important trends that you might miss in your traditional vendor logs like:

“Is this happening in a particular data center all the time?”

“Is this happening on the same devices?”

“How long did it take for the temperature to come down?”

Please Note: This Rule does not have a time threshold because it triggers as soon as the device reaches the minimum threshold defined. If the temperature does not come down, the issue will stay unresolved until it falls below the thresholds you set.

Next, create another rule to trigger an **Error** with an email message, so agents are immediately notified when the device not only breached the minimum acceptable heat threshold, but increased by 5%. You could then add **custom instructions** for the agent to open an operations ticket to review the device, since they are receiving an email.

The screenshot shows the 'CONFIGURATION' tab for a rule named 'E_Overheating'. On the left, a sidebar lists configuration options: 'C_Heat Warning Shutdown', 'E_Overheating' (selected), 'Global Configuration', and 'W_Over Min Value'. The main area is titled 'CONFIGURATION VALUES' and contains several sections:

- Thresholds:** A section with a label 'High Threshold of Usage:' and a value of '90.0'.
- Labels and Devices:** Two side-by-side lists. The 'Labels' list on the left includes 'Metal', 'P1', 'Pac-Man', and 'VSX'. The 'Selected devices & Labels' list on the right includes 'PAN15', 'PAN14', and 'PAN13'. Arrows indicate the relationship between the two lists.
- Actions:** A section at the bottom with three checkboxes: 'ISSUE' (checked), 'SNMP' (checked), and 'EMAIL' (checked).

Finally, create a third rule to send a **Critical** email when the device has reached a temperature nearing shut down. You can change the custom instructions to have the agent to call the Data Center directly to have the device reviewed immediately.

The screenshot shows the 'CONFIGURATION' tab on the left with a list of rules: 'C_Heat Nearing Shutdown', 'E_Overheating', 'Global Configuration', and 'W_Over Min Value' (which is selected). The main area is titled 'CONFIGURATION VALUES' and contains the following fields:

- Name:** W_Over Min Value
- Thresholds:** High Threshold of Usage: 85.0
- Labels:** A list of labels including Metal, P1, Pac-Man, and VSX.
- Selected devices & Labels:** A list of selected devices including PAN13, PAN14, and PAN15.
- Actions:** A section with checkboxes for 'ISSUE', 'SNMP', and 'EMAIL', all of which are checked.

Please Note: Arbitrary numbers were used for this exercise so we would not recommend creating these exact rules in your live environment. Also, the All Devices label was used, but you can create labels based on data center location, device type, etc.

Disabled Tab

Here you can disable the rule by **Label** or **Device**. This allows you to get even more granular in how you want the Rule to automate your devices.

The screenshot shows the 'Disabled' tab in the Indeni interface. The top navigation bar includes 'Overview', 'Configurations', and 'Disabled' (which is selected). Below the navigation bar, there are tabs for 'Labels' and 'Devices'. The main area is titled 'DISABLED DEVICES AND LABELS' and contains two search bars. The left search bar is for 'Labels' and shows a list of 10 disabled labels, each with a unique ID. The right search bar is for 'Devices' and is currently empty. Between the two search bars, there are two blue buttons: '>>' and '<<'. The list of disabled labels is as follows:

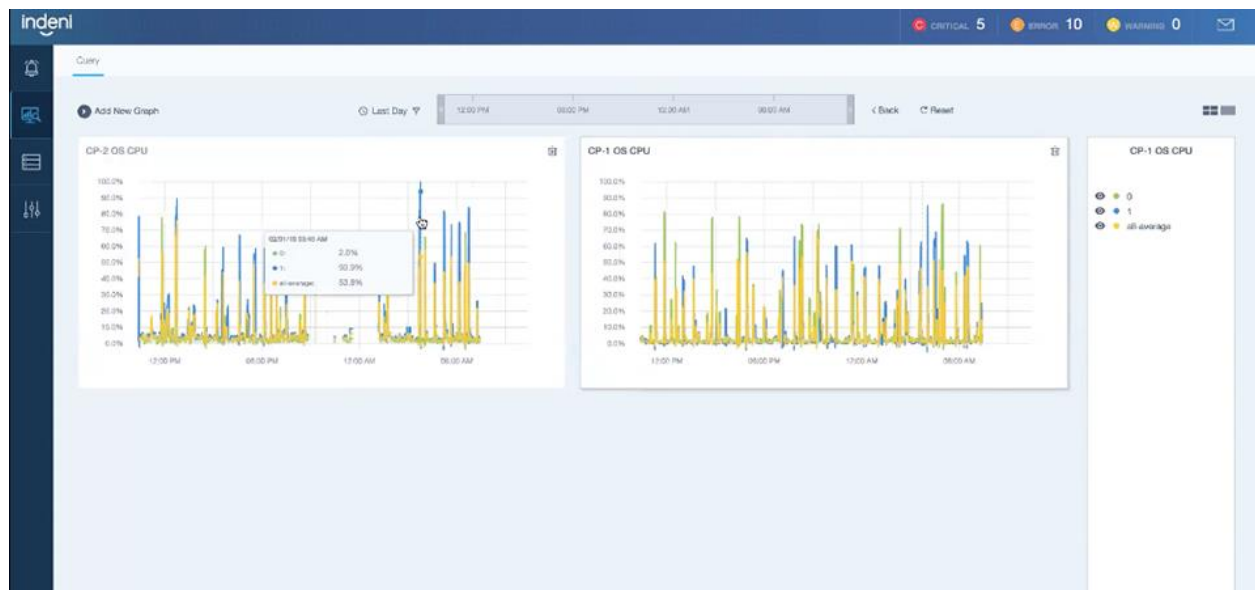
Label ID
079c226c-515e-4f08-adff-5343e4f203c7
3bd62e53-85db-431e-97e1-5f96c1276dff
3e813da8-192c-472b-bc29-f53d57a4c7ec
4c7cd3ac-8507-43b9-b9b2-710fb70a92f9
55ef0d9d-b322-48d0-aa00-db822b4baf1c
62766408-7aaa-4d3f-ad4f-e86eae65ef3b
6ad7d7c-83bb-45ba-8220-2b6100feb736
78a98b62-fafa-41ff-b900-738ffd07802e
7b6c86aa-2bde-4176-b07d-de298030561b
7ffa826d-cb6f-4431-a427-893aa1fa9ca
80140853-bf44-4265-ba15-ded3b26a5a57

Part 4: Analysis and Reporting

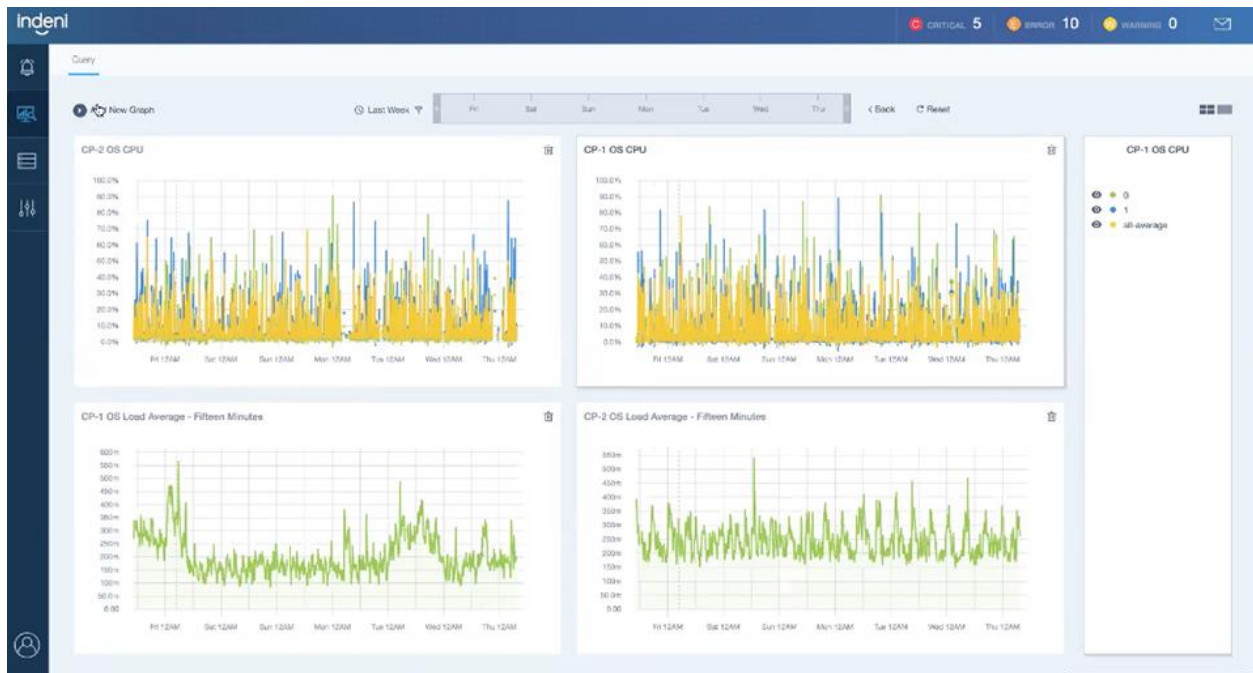
The **Analysis Tab** allows users to graph certain metrics over time, view historical values and correlate the data with issues raised by Indeni. Indeni collects data from network elements and it stores the data in a time series data store. A **Time Series** is a series of numeric data points of some particular metric over time. A **Metric** is any particular piece of data that you wish to track over time.

For the purpose of graphing, it would only make sense to graph data that is numerical in value and the value changes over time. For example, CPU utilization, number of concurrent sessions, etc. This is the reason why only certain metrics are graphable. Indeni **keeps up to a year's worth** of historical data!

An example of why you would use the analysis tab. If you have a pair of devices that form a cluster for high availability or load balancing, it often helps to visualize and compare their resources such as CPU usage for a particular time period. If the configuration is active/standby, you would expect the standby device to have low CPU utilization



CP-2 is the standby gateway and CP-1 the active gateway. In this case, CP-2 is showing high CPU spikes that do not appear to be normal for a standby device that is idle for the most part. Next, you may want to add more metrics for correlation and further analysis. You can add load average, concurrent connections, memory usage, just to name a few. The analysis tab allows you to correlate multiple metrics across multiple devices.

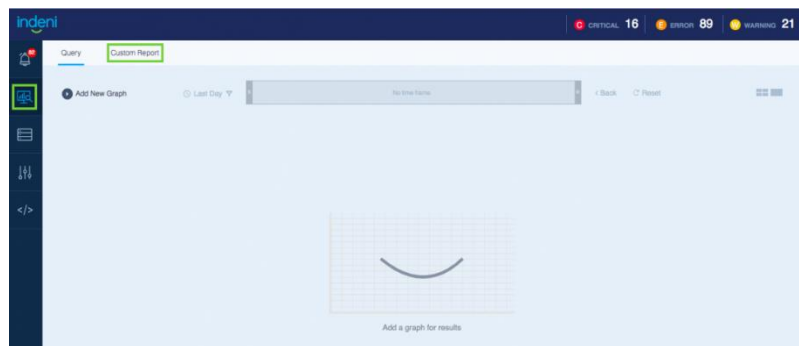


4.1 Custom Reports

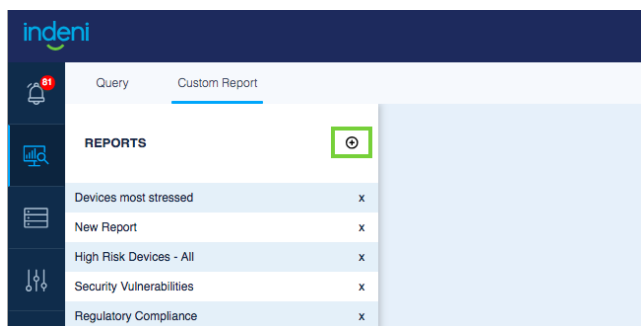
Indeni **Custom Reporting** gives you more dynamic engagement with historical data that allows you to quickly visualize trends in order to understand the overall health of your environment. It also gives you an understanding of where your organization falls within **Industry Best Practices** and **Compliance** for greater insights into the health posture of your security infrastructure. You can also schedule your **Policy Reports** to be sent to your stakeholder daily, weekly, or monthly; ensuring compliance deadlines are never missed.

Where Can I get the Custom Reports?

First, go to **Analysis Tab** and then choose **Custom Report**, where you can build your new report.



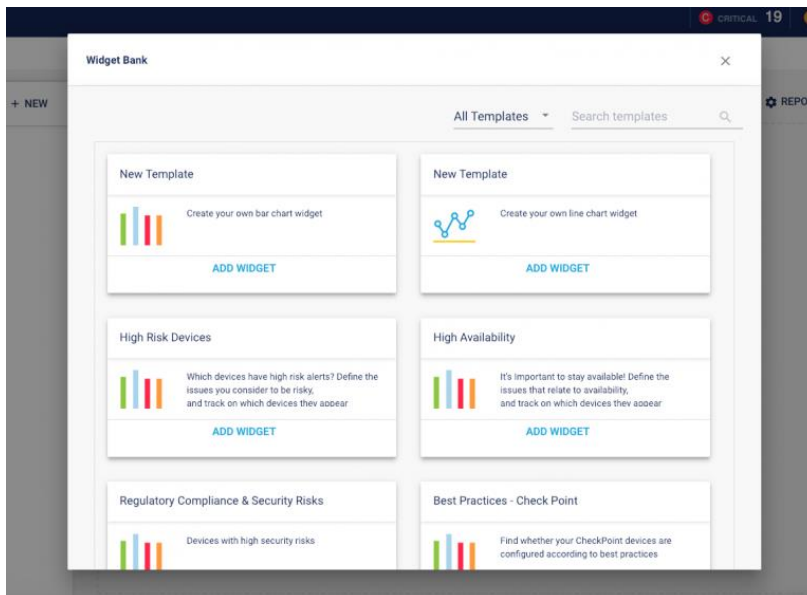
Then Click + to create a new report. You will want to give it a meaningful name by replacing **New Report**.



Afterward, select the blue **Add a Widget** button.



The system will present a number of widgets you can use to build your report. See [Which Reports Can I Build](#) (below) for a list of default templates. Select a widget, then select **Add This Widget** to continue.



Next, click on edit to add and remove rules for your report.



You will want to select a time range to restrict the data that appears in the report. For example, if you want a weekly report that includes data from a month back, select **Relative Time** then **Last Month**. The weekly reports will include issues from a month ago. Alternatively, you can create a one-time report using the **Absolute Date Range**.

WIDGET CONFIG [High Risk Devices](#)

Choose time

Relative Time

Last month

Last day

Last week

Last month

Last three months

Choose devices

No Item Selected

Choose labels

1 Item Selected

system-all

Choose issues

7 Items Selected

All Statuses

High disk space utilization

Device not responding

Failed to communicate

High load average

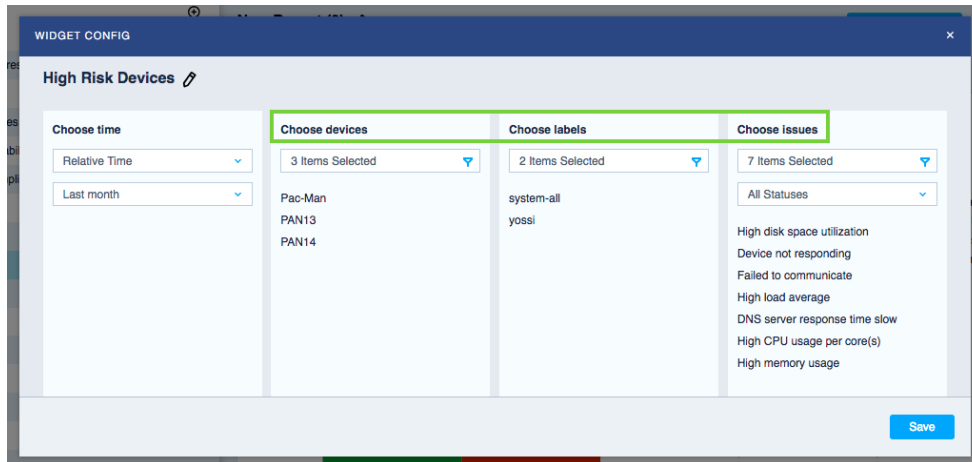
DNS server response time slow

High CPU usage per core(s)

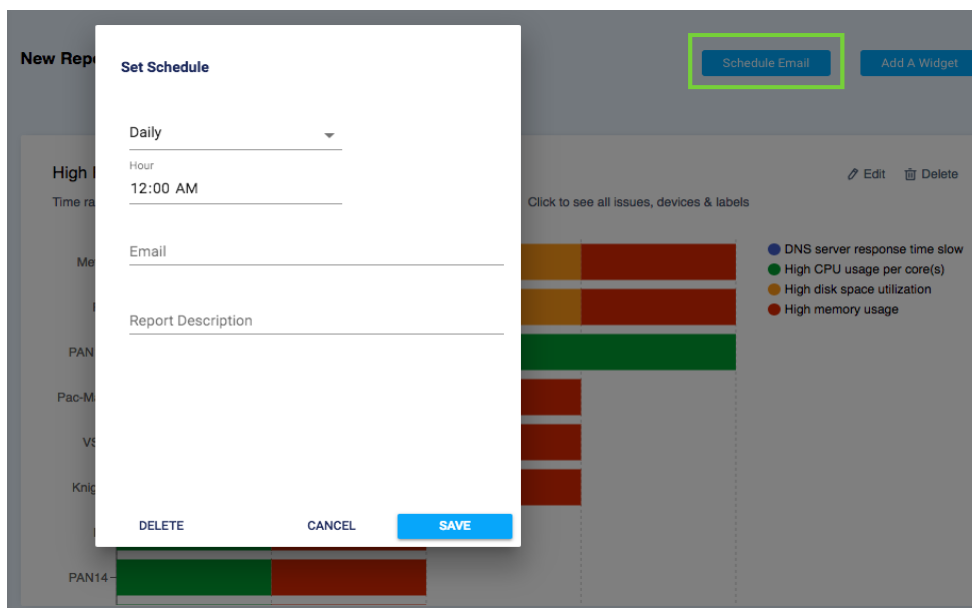
High memory usage

[Save](#)

You can select **Devices**, **Labels** and **Issues** to restrict the data that appears in the report. The system will produce a report consisting of devices you selected plus the list of devices defined in the label. For example, you may only care about your data center devices. In this case, select the label you created for you data center. Be sure to define your dimensions!



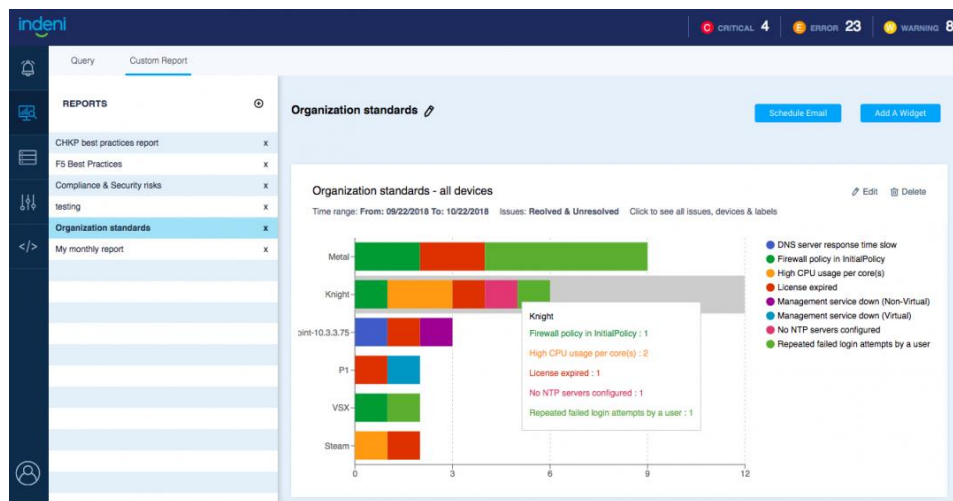
While not required, you always have the option to click the blue **Schedule Email** button if you want the report to be sent on a regular basis; either **daily**, **weekly** or **monthly**.



You can also use this option to modify the recipient list, change the frequency of the report, or remove the report from being sent. To send the report to more than one user, use comma to separate the email addresses. Once you have your desired settings configured, save your settings!

Which Reports Can I Build?

Daily Reports show the list of devices that had issues generated within the last month, and if the issues are still outstanding. This report will help you focus on addressing your most critical issues.



High Availability (HA) Configuration Reports are a key element for achieving business continuity 24/7. A highly available infrastructure involves multiple components working together. Gaining insight into the readiness of your HA infrastructure is important to achieving uninterrupted service.

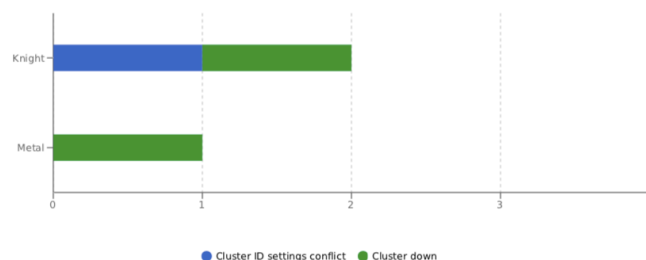
High Availability Readiness

Indeni Report

Please review to ensure the cluster members are synchronized.

Check Point HA Readiness

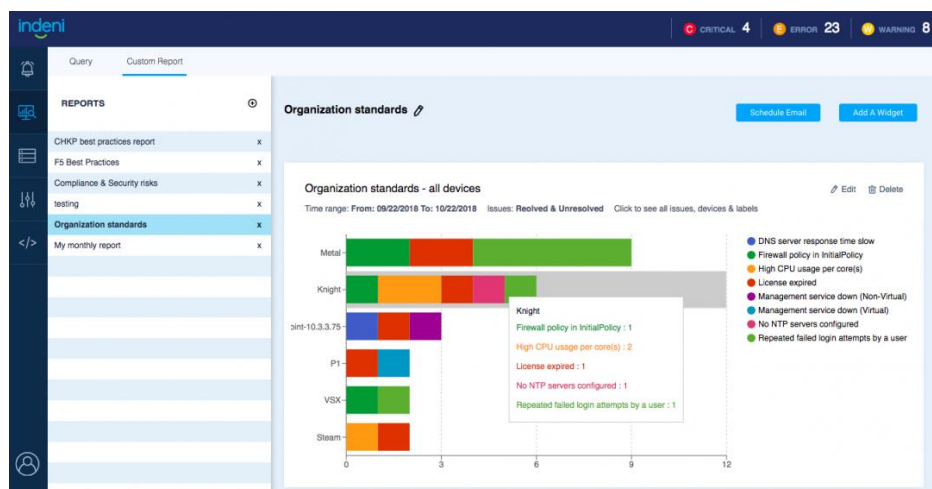
Time range: From: 09/24/2018 To: 10/24/2018 Issues: Unresolved See all issues, devices & labels on appendix



Here is the list of rules used to build the HA Readiness report as shown above:

High Availability Readiness			Indeni Report
Widget: Check Point HA Readiness			
All the relevant issues:	All the relevant devices:	All the relevant labels:	
<ul style="list-style-type: none">Cluster has preemption enabledCluster downCluster member no longer ActiveCluster members' domain names mismatchClusterXL CCP mode mismatch across cluster membersConnected networks do not match across cluster membersCoreXL cores-enabled mismatch across cluster membersCritical configuration files mismatch across cluster membersDNS servers used do not match across cluster membersFeatures enabled do not match across cluster membersJumbo Hotfix Take mismatch across cluster membersLogin banner mismatch across cluster membersModel mismatch across cluster membersNTP servers used do not match across cluster membersNetwork interface duplex does not match across cluster membersNetwork interface ipv4 subnet does not match across cluster members		<ul style="list-style-type: none">system-checkpoint	

Organization Standards Report are a monthly recurring report that can help you adhere to the company's "golden" standards for the myriad devices you have. This helps to reduce unnecessary errors from ad-hoc changes.



The Compliance & Security Risks Report can be run periodically to prepare for any regulatory audits. These reports can be sent directly to the auditors every month to demonstrate that the best security measures are observed on an ongoing basis.

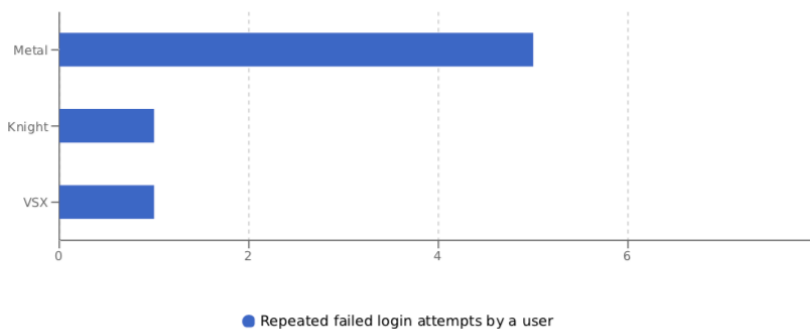
Compliance & Security risks

Indeni Report

Our compliance audit is coming up shortly. Attaching a report to get us prepared

Security risks

Time range: **From: 09/23/2018 To: 10/23/2018** Issues: **Resolved & Unresolved** See all issues, devices & labels on appendix



Here is the list of rules used to build the compliance & security report as shown above:

Compliance & Security risks

indeni Report

Widget: Security risks

All the relevant issues:

- NTP servers configured do not match requirement
- DNS servers configured do not match requirement
- OS/Software version does not match requirement
- Users defined do not match requirement
- LDAP fingerprint not trusted
- Telnet is enabled on the device
- An HTTP server is enabled on the device
- SNMPv2c/v1 used
- Repeated failed login attempts by a user
- SNMP configured with community public
- Hotfixes installed do not match requirement
- SNMPv3 is not enabled
- SNMPv3 is not configured according to the best security practices
- Device is vulnerable to SWEET32
- SSL Ticketbleed vulnerability (CVE-2016-9244)
- Spectre and Meltdown vulnerable

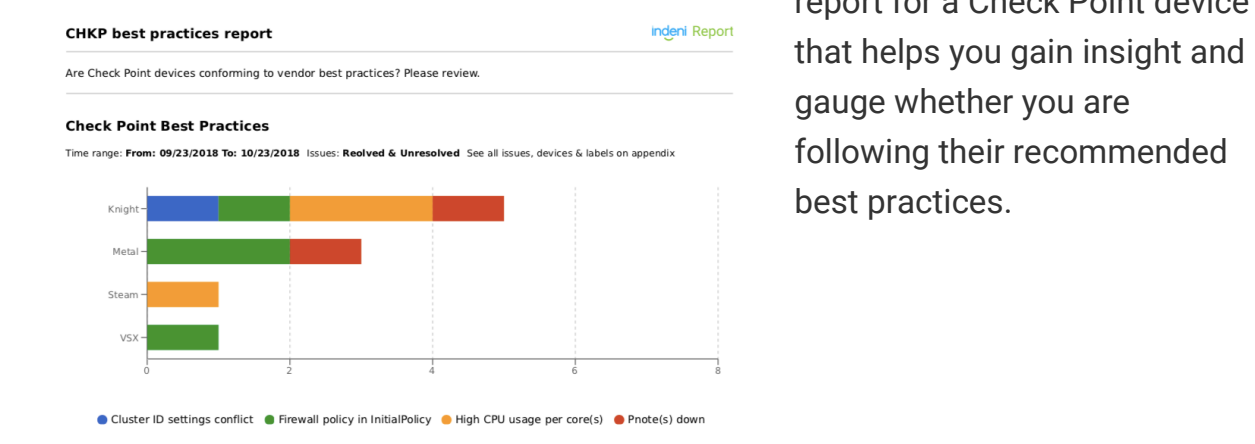
All the relevant devices:

All the relevant labels:

- system-all

The **Vendor Best Practices Report** allows engineers to ensure that they are within the recommended operational best practices defined by them. Here is a sample

report for a Check Point device that helps you gain insight and gauge whether you are following their recommended best practices.



Here is the list of Check Point best practices rules used to create the report:

CHKP best practices report

indeni Report

Widget: Check Point Best Practices

All the relevant issues:

- High CPU usage per core(s)
- Aggressive Aging enabled
- Pnode(s) down
- Signature update status
- PBR rules mismatch across cluster members
- Errors found in \$FWDIR/conf/ipassignment.conf
- CoreXL cores-enabled mismatch across cluster members
- In CoreXL a single core shouldn't handle both interface interrupts and fw worker
- Firewall policy in InitialPolicy
- No firewall policy loaded
- Policy mismatch across cluster members
- Policy-map is not configured to the control-plane
- SecureXL configuration mismatch across cluster members
- Cluster ID settings conflict
- Routes defined in dish/webUI are missing
- RADIUS server uid is not 0
- RADIUS servers used do not match across cluster members
- CPU Soft Lockup-test2

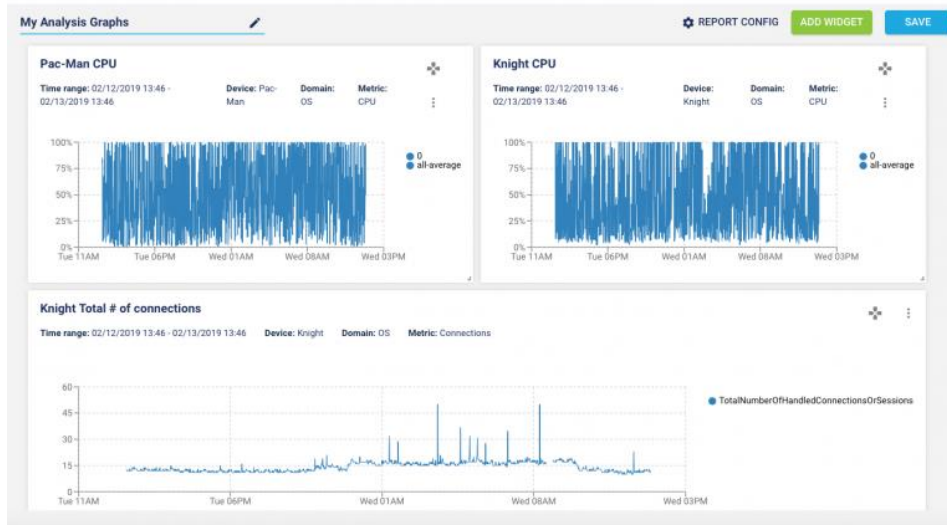
All the relevant devices:

All the relevant labels:

- system-checkpoint

Include Graphs in your report

When you migrate from a previous release to 6.5.3, you can include graphs in your report. These are same graphs from the [Analysis Tab](#). You can save your favorite graphs or send them to your colleagues regularly.



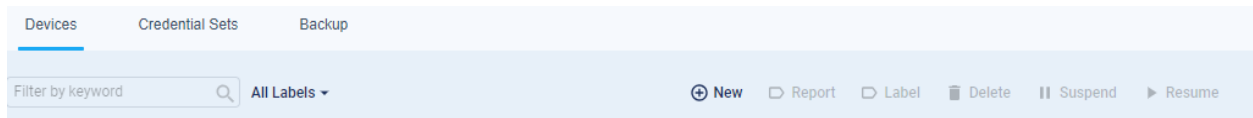
You can even combine a list of issues with historical graphs as part of your report.



If you have any other questions around Custom Reporting feel free to [Join our Community](#) discussion and ask us there!

Part 5: Device Management

As we [reviewed previously](#), adding devices requires that you first create an [Indeni User](#) in the management system for the device you want to add. Once you have completed that you will then need to add the Indeni User to the [Credential Set](#), which can be done by clicking on the tab located to the right of [Devices](#) located in the border above the filter bar.



Once you have successfully added devices, you can **Filter** the devices by [Keyword](#) or [Labels](#). You can sort by [Device Name](#) or [Issue](#) severities. You can also generate device [Report](#), create [Labels](#), [Delete](#) devices or [Suspend](#) them if you're doing maintenance and then [Resume](#) automation later.

In order to activate the device options, a device must first be added and selected.

	Device Name	IP Address	Device Vendor	Software Version	Software Model	Issues	Issues
<input type="checkbox"/>	VSX	10.3.3.38				10	92
<input checked="" type="checkbox"/>	Pac-Man	10.3.3.56	checkpoint	secureplatform R75.40	N/A	10	63
<input checked="" type="checkbox"/>	PAN15	10.3.1.15	paloaltonetworks	panos 6.1.0	PA-VM	7	26
<input checked="" type="checkbox"/>	PAN14	10.3.1.14	paloaltonetworks	panos 6.1.0	PA-VM	5	18
<input type="checkbox"/>	PAN13	10.3.1.13				149	23
<input type="checkbox"/>	P1	10.3.3.150	checkpoint	gaia R77.10	N/A	7	10

In this example all devices were selected, which activated the device options and also gives a quick count overview in **Device Summary**. Device Summary is where you can review the issue details.

The screenshot shows the 'Devices' page in the Indeni interface. At the top, there are tabs for 'Devices', 'Credential Sets', and 'Backup'. Below the tabs is a search bar and a 'Filter by keyword' dropdown. A table lists various devices with columns for 'Device Name', 'IP Address', 'Device Vendor', 'Software Version', 'Software Model', and 'Issues'. The 'Issues' column has two sub-columns: 'Issues' (with a red icon) and 'Issues' (with a yellow icon). The table is sorted by 'Issues' (red icon) in descending order. The 'DEVICE SUMMARY' sidebar on the right shows details for the selected device 'CP-R80.10-GWS-1' (IP: 10.11.94.11). It includes a 'LABELS' section with 'system-all', 'system-checkpoint', and 'Test' buttons. The 'MOST RECENT ISSUES' section lists two issues: 'Contract(s) expiration nearing' and 'Repeated failed login attempts by a user'. The 'LAST BACKUP' section shows a successful backup on Mon Dec 17, 2018.

Device Name	IP Address	Device Vendor	Software Version	Software Model	Issues (Red)	Issues (Yellow)
CP-R80.10-MDS3-CMA1-3	10.11.94.37	checkpoint	gaia R80.10	VMware Virtual Platform	1	7
CP-R80.10-GWS-1	10.11.94.11	checkpoint	gaia R80.10	VMware Virtual Platform	4	11
CP-R80.10-GWS-2	10.11.94.12	checkpoint	gaia R80.10	VMware Virtual Platform	1	7
CP-R80.10-MDS3-CMA2-3	10.11.94.38	checkpoint	gaia R80.10	VMware Virtual Platform	1	7
CP-R77.30-MGMT1-1	10.11.94.30				3	5
CP-R80.10-MGMT3-1	10.11.94.31	checkpoint	gaia R80.10	VMware Virtual Platform	1	5
P1	10.3.3.150	checkpoint	gaia R77.10	N/A	7	10
Arkhan	10.3.3.61	checkpoint	gaia R77.20	VMware Virtual Platform	3	21
CP-R80.10-MDS2-CMA1-2	10.11.94.34	checkpoint	gaia R80.10	VMware Virtual Platform	1	7
CP-R80.10-MDS3	10.11.94.36	checkpoint	gaia R80.10	VMware Virtual Platform	1	8
F5	10.3.3.134	f5	BIG-IP 11.6.0	BIG-IP Virtual Edition	8	25
Pac-Man	10.3.3.56	checkpoint	secureplatform R75.40	N/A	10	63
Metal	10.3.3.72				64	116
PAN14	10.3.1.14	paloaltonetworks	panos 5.1.0	PA-VM	5	18

You cannot get device issues to show in Device Summary with multiple devices checked. Also, you do not need to have a device checked to see a more detailed issue review.

Clicking on an issue within **Device Summary** will take you to the **Current Tab > Issue Summary**.

The screenshot shows the 'Issue Summary' page for the alert 'NETWORK PORT(S) RUNNING IN HALF DUPLEX'. The alert details include the source 'srnx100-1 172.16.20.54' and the target 'juniper 12.3X48-D45.6 - junos, srnx100h2'. The 'DESCRIPTION' section explains that one or more ports are set to half duplex, which is usually an error. The 'PORTS AFFECTED' section lists the affected ports: fe-0/0/0, fe-0/0/2, fe-0/0/3, and fe-0/0/4. The 'REMEDiation STEPS' section is currently empty. The 'ALERT SUMMARY' section shows a graph with the title 'No available data'.

Selecting **More Device Info** will give you a detailed review of the device details, including systems running in a container.

The screenshot shows the 'DEVICE INFO' page for device CP-R80.10-GW5-1. The sidebar on the left contains a search bar and a list of navigation items: Overview, Network Interfaces - rx overruns, Mount Points - Total, Memory - Total, Network Interfaces - IPv4 Address, ClusterXL Devices, Network Interfaces - rx packets, Network Interfaces - tx overruns, Memory - Usage, and DNS Response Time (Average). The main content area displays a table of system metrics:

Metric	Value
ARP Cache - Limit	4096
CCP Mode	
Cluster State	Active
Configuration Unsaved?	NO
Core Dump	true
Current Date/Time	Monday, December 17, 2018 12:59:38 PM +02:00
DNS Servers	ipaddress=8.8.8.8
Directly Connected Networks	mask=24, network=10.11.94.0
Firewall Policy	UP/ACTIVE
Firewall Policy - Last Modified	Wednesday, November 28, 2018 2:19:22 PM +02:00
Installed Hotfix Take	0
Installed Hotfixes	
Kernel Dump	true
Kernel Memory	6.00%
Load Average (1 Minute)	0.05
Load Average (15 Minutes)	0.08
Load Average (5 Minutes)	0.08
Local cluster member state (this device)	Active
NTP Servers	ipaddress=pool.ntp.org, type=primary, version=1
SecureXL - State	on
Static routes	mask=0, network=0.0.0.0, next-hop=10.11.94.254

A 'CLOSE MORE DEVICE INFO' link is located at the bottom right of the main content area.

Device Report

The report has many options, so it is best to review them after you add a device. You can scroll through, or search by an area of interest, check multiple options and then export.

The screenshot shows the 'INVENTORY REPORT - CHOOSE METRICS' dialog box. It features a search bar at the top and a list of metrics with checkboxes. The metrics listed are:

- ☒ ARP - Total Entries
- ☒ ARP Cache - Current Entries
- ☒ ARP Cache - Limit
- ☒ ARP Table
- ☒ Application Packages - Acceptable Lag
- ☒ Application Packages - Currently Installed Package
- ☒ Application Packages - Update Action
- ☒ CCP Mode
- ☒ CDP Neighbors
- ☒ CPS

An 'Export' button is located at the bottom right of the dialog box.

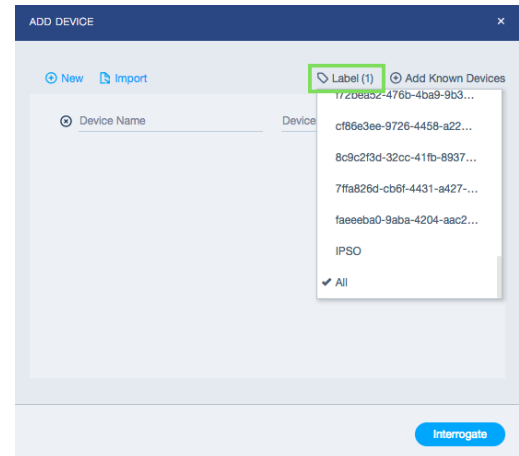
The screenshot shows the 'INVENTORY REPORT - CHOOSE METRICS' dialog box with the search term 'cpu' entered. The metrics listed are:

- ☒ CPU
- ☒ CPU Usage
- ☒ CPU per VS

An 'Export' button is located at the bottom right of the dialog box.

Label Management

Labels allow you to group your devices together, making them easier to manage when you are changing thresholds, backing up devices, viewing issues, or creating reports. Label names can be based on the structure of your organization, or on the criticality of your operation. Devices can belong to multiple labels that meet your organization needs.



You also have the ability to apply **Labels** to new devices before adding, letting you take advantage of the tuning you have already done. This means that you will not generate messages around all the Indeni Rules that exist, which means **less noise** for your team.

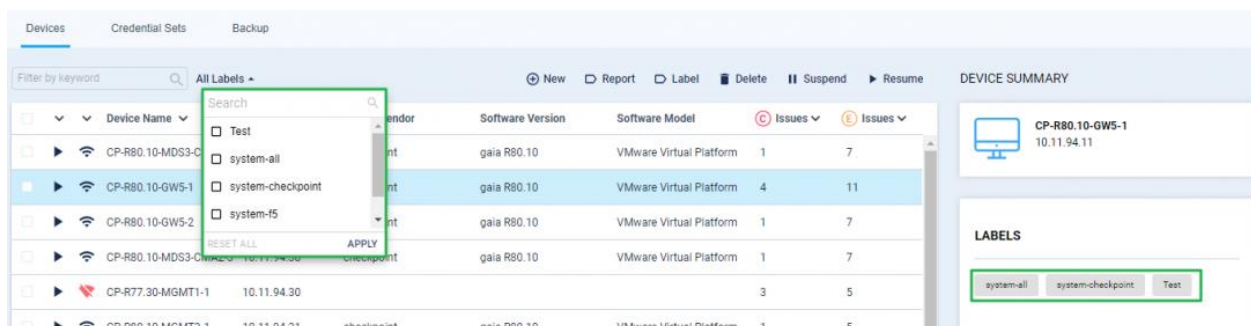
System Labels

Release Version 6.4.1

System labels are prefixed with “system-” and are automatically applied.

For example:

1. System-all
2. System-<vendor> e.g. system-checkpoint, system-F5, etc.



The **system-all** label consists of all the devices managed by Indeni. When a new device is added, the label system-all is automatically applied. Conversely, when a device is removed, the system will automatically update all relevant system labels. System labels **cannot** be modified manually.

When a new vendor device is added for the first time, “**system-<vendor-name>**” label is created automatically. The new device will be added to both the “system-all” and “system-<vendor-name>” labels.

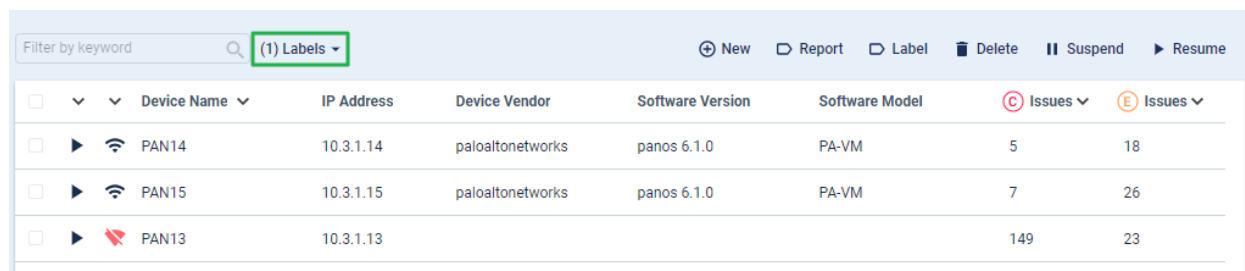
For **auditing** and debugging purpose, a log entry is added to indicate whenever a new label is created or a label is updated with the relevant information.

Labels and Migration

When you migrate from a previous Indeni release to 6.4.1, new system labels will automatically be created and applied to the relevant devices during the process. After the successful completion of a system migration, you will see the dynamic system-labels, in addition to any of your existing custom labels.

Helpful Hints

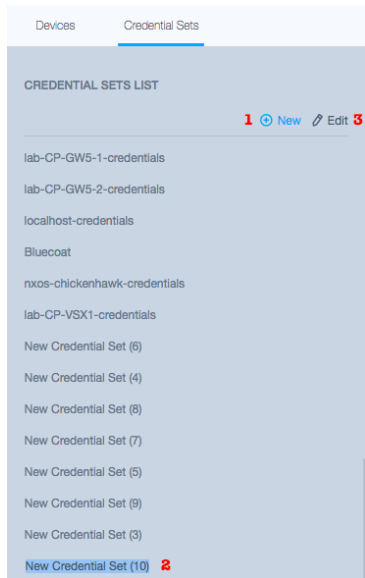
If you leverage filters to search through issues and devices, be sure to reset the filters once you are done. It could appear as though the system is not showing all the data.



The screenshot shows the Indeni web interface. At the top, there is a search bar with the text "Filter by keyword" and a dropdown menu currently set to "(1) Labels". To the right of the search bar are several action buttons: "New", "Report", "Label", "Delete", "Suspend", and "Resume". Below the search bar is a table with the following columns: "Device Name", "IP Address", "Device Vendor", "Software Version", "Software Model", "Issues", and "Issues". The table contains three rows of data:

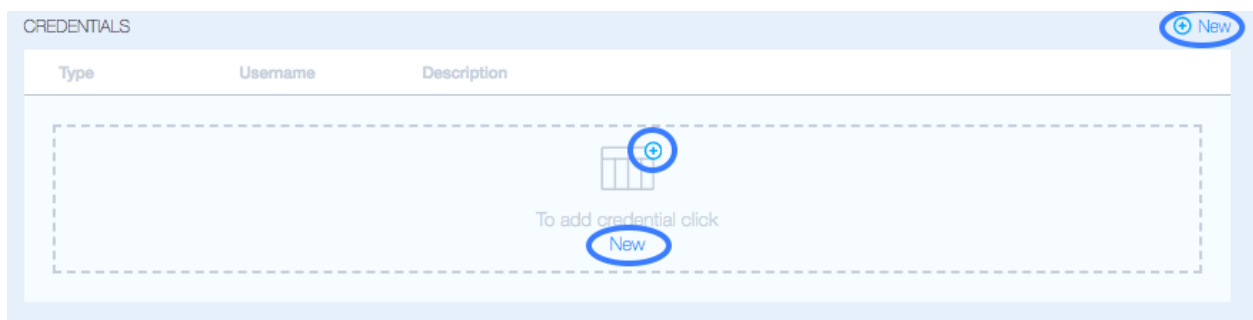
Device Name	IP Address	Device Vendor	Software Version	Software Model	Issues	Issues
PAN14	10.3.1.14	paloaltonetworks	panos 6.1.0	PA-VM	5	18
PAN15	10.3.1.15	paloaltonetworks	panos 6.1.0	PA-VM	7	26
PAN13	10.3.1.13				149	23

5.1 Credential Sets



After you have created an [Indeni User](#) for the device you want to add, (1) click on **Credential Sets**. Once you do, (2) it would be good to name it immediately because once you click out of it, it will save the name as is. If that should happen, simply select the credential set you want to rename and (3) click **Edit**, and you should be able to rename it.

After you have added the Set name in the List, you should then *add the device credentials* by clicking on **New**, which can be found in 3 places.



After you have added the **credentials**, and the connection type, add the **subnet** you want to associate with the credentials.

Please Note: If you have created the same Indeni credential across all device vendors you want to add to the system, we recommend using 0.0.0.0/0 subnet with SSH + HTTP (API) selected. This way you do not have to enter multiple credential sets with relevant connection types and the related IP subnet for every cluster you may have. This will greatly reduce complexity and time required when adding devices to the system.

SUBNETS TO USE CREDENTIALS WITH	
Network	Mask
192.168.193.0	24

Please Note: If you have devices that are not on the same subnet, but share the same credentials, we would recommend that you *add the additional* subnets in list, **NOT** create a user for each device. For ease of use it is always better to limit the number of credentials being used and instead leverage the subnet feature.

5.2 Adding Devices

After you have added the **Credential Set** you are ready to add the device(s). Navigate back to the **Devices** tab and click on **New**.



Accept the Device Requirements and Effects by selecting **Continue**:

IMPORTANT:

DEVICE REQUIREMENTS AND EFFECTS

When you add a device(s), there is a potential resource impact on every device connected

NOTE: indeni is a read-only system, it will not make any lasting changes to a device or any changes that may impact its behavior. As a responsible vendor, indeni tests its solutions to ensure safe use with even the most critical devices.

Adding Devices

Please review the indeni User Guide for a detailed list of requirements that must be followed to ensure a seamless integration with your devices. This includes adding a dedicated user for indeni, setting the correct permissions and type of shell (if applicable), etc.

The effects of analyzing with indeni

indeni uses an SSH connection and vendor-specific commands, as well as vendor-provided APIs to collect information. Some of these commands may result in CPU and/or memory use on the device. indeni goes to great lengths to minimize any resource utilization on the device(s). To this extent, indeni will:

- Keep an eye on the CPU and memory usage of a device and suspend all activities on the device automatically if critical levels are reached. Once the resource utilization normalizes, indeni will resume analysis. The thresholds for this suspension behavior are configurable.
- Limit the number of concurrently executing commands based on the type of device (vendor and model). For example, lower-memory devices will only have one command run at any given moment, while with more high-powered devices indeni can run several commands in parallel. This can be manually tuned on a per-device basis as well.
- With devices that support running commands at a lower priority (known as "nice" in the Unix world), indeni will ensure all commands are run at such a priority.
- Look at core specific utilization and also run a command ("top", "show system resources", etc.) to understand what is causing the high utilization. With devices like Palo Alto Networks and Juniper firewalls, indeni would look specifically at the management/control plane CPU utilization and adjust behavior accordingly.
- indeni also "blacklists" any OS that is prone to issues when accessed via SSH frequently. When connecting to any of the mentioned devices indeni will alert and NOT run commands against it.

Having read the above notice, would you like to continue?

Continue

You will then land on a screen where you can add the device name and IP address.

Please note that you can add multiple devices by selecting **New** or by **Importing** a list. You also have the ability to **Add** previously **Known Devices**.

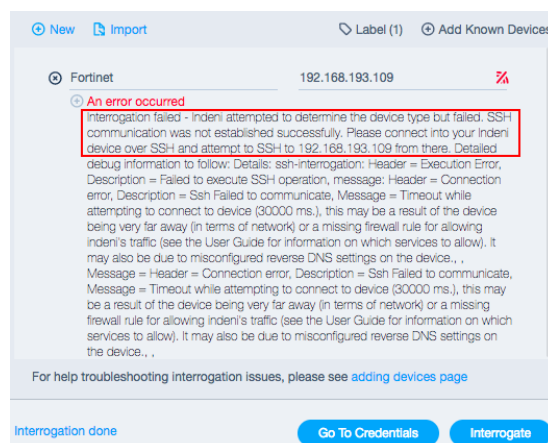


After you have added the Name, IP address and Labels (*if applicable*), click on **Interrogate**.

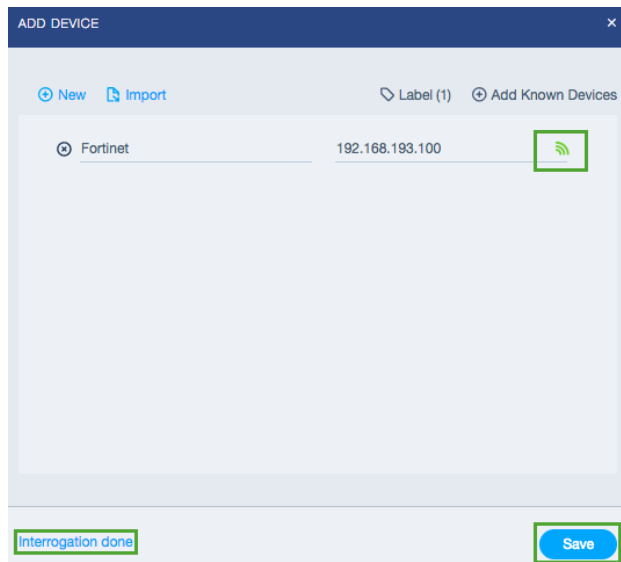
Please Note: You can only enter letters and digits. The name field is also *space sensitive*. If you notice here, no letters or numbers have been used but there's still an error. After highlighting the area, you see the extra space.



After you click on **Interrogate**, it should reach out and connect to the device via the **credential set** you created for the device(s) subnet. If it fails, it is very important to read the message that was delivered back. It contains the details that you need to remediate the issue.



Following the steps suggested, SSH connection to the device as listed did not work. After taking another look at the **credential sets**, and other testing, it is realized that the IP address of the device is incorrect. After correcting the IP and clicking interrogate again we see a successful add, indicated by the **Green Signal** icon.



Once **Interrogation** is done, you need to **Save** the device to add it to dashboard. After it is saved, you might need to wait a few moments for Indeni to run through all the Rules that can be applied to the added device. Once it does, you will be presented with issues and device details.

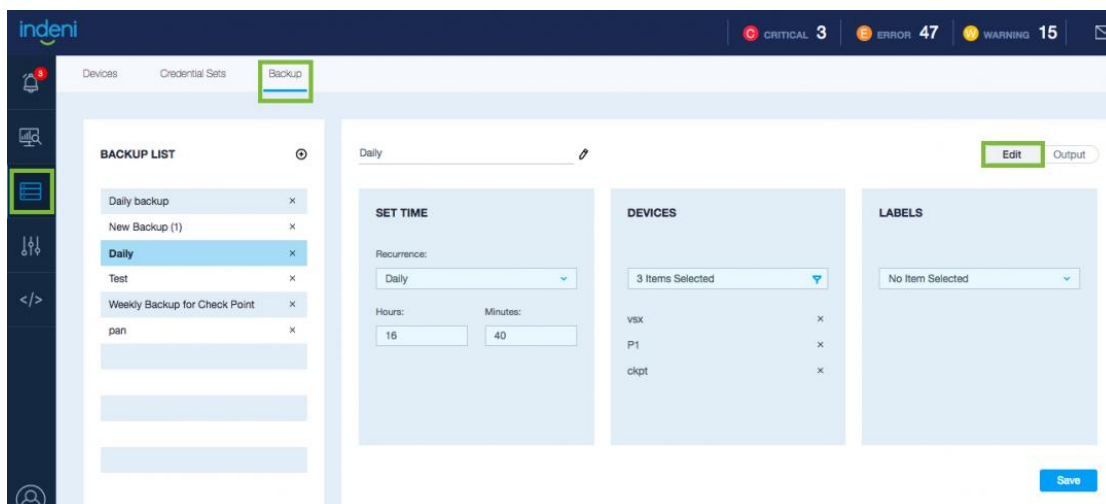
5.3 Device Backup

Indeni can be set to automatically collect backup data across multi-vendor equipment. Typically, you want to automate network device configuration backup for a group of devices. Indeni backups are fully automated. You can define a recurring task, which lets you set up a schedule and target devices. The configuration backup can be scheduled hourly, daily, weekly, monthly and also on demand. Indeni uses securely managed credentials and secure transports to access each device and retrieve configurations to a central data store.

Creating a Device Backup

Open the **Devices** tab from the left, select the **Backup** option to open the backup configuration wizard then perform the following steps:

1. Create your backup by clicking on the + sign.
2. Provide a meaningful name for your backup. The name cannot exceed 128 characters.
3. Choose the frequency (*Daily, Weekly, Monthly*).
4. Select the devices you wish to backup. In GA 6.4.9 and up, you will receive an error message if you select a device where backup is not supported.
5. Select **Labels** for the group of devices you wish to backup. You can also perform the 'and' operator by selecting **Devices** along with **Labels**.
6. Click on the blue Save button to save the configuration.



This completes the backup configuration task and the configuration will be listed under the **Backup List**. On point-click, it displays the schedule and the configuration on the right panel.

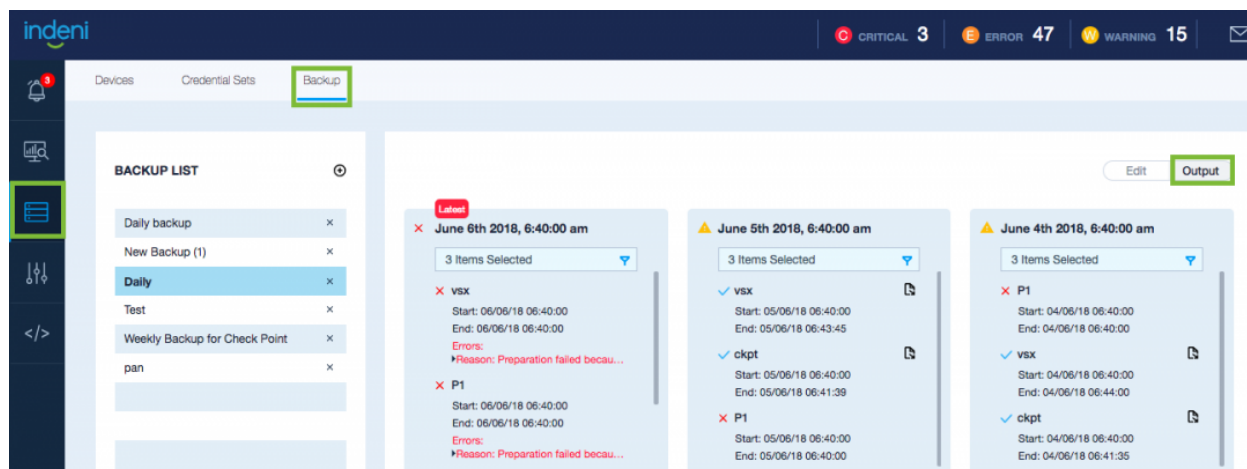
Please Note: You cannot schedule a backup for the same device at the same time even though the device may be in two different labels. In this case, one of the scheduled backups will fail.

Modifying the Backup Configuration

From the Backup List, mouse over to the backup configuration you want to modify. To change the name of the backup configuration, press the pencil icon and change the backup list name. Modify the backup configuration information (*schedule, devices or labels*) and click on save, to save your changes.

Configuring the Backup Files

Device configurations can be easily retrieved in case of emergencies. Open the **Devices** tab from the left, select the Backup option to open the backup configuration wizard. Choose **Output** to obtain the list of backup files.



Select the job you want to review from the backup. You can **store up to 10 versions** of backups. The job outputs are listed in chronological order. To retrieve the backup file, you can select the version you want to retrieve, click on the file icon associated with the device. The system will prepare the file by compressing the backup file and the file will be downloaded to your computer.

There are three possible outcomes of the backup:

- ✓ Indicates a successful backup;
- ✗ Indicates that the backup failed;
- 🕒 Indicates that the backup is pending, likely in a transient state.

A backup job may consist of multiple devices. If backup fails for one of the devices, the job is considered a “**partial success**” (*yellow*). If backup passes for all devices, the job is considered a “**success**” (*green*). If backup fails for all devices, the job has “**failed**” (*red*), in which case, manual intervention may be required.

Please Note: In GA 6.4.9 and up, the system will automatically retry backup three time. The system will wait for 10 minutes between each retry.

Scroll down to select the version you want to retrieve. All outputs contain the timestamps when the backup was run along with the statuses.

Please Note: The system does not provide issue notifications should a backup fail at this time, therefore the users are encouraged to check the Backup tab regularly.

To remove a backup configuration

From the Backup List, mouse over to the backup configuration you want to remove, click **✗**. The configuration along with the backup files will be removed from the system.

Retrieving the Backup Files

The other option to retrieve the configuration file is to select the Device(s), located under the **Devices** icon in the left menu pane.

Check off the device you want the backup for and look to the right, under **Device Summary**. You can only **select one device per backup** at this time. If there was a last successful backup associated with that device, you will see a check mark next to **LAST BACKUP**. In this case, a Check Point VSX had a successful backup, which has a **file** icon with start and end dates noted for your convenience. You can mouseover to the **file** icon and click to download the backup file.

The screenshot displays the Indeni web interface. At the top, there are status indicators for CRITICAL (3), ERROR (47), and WARNING (15). The left sidebar shows the 'Devices' tab selected. The main area contains a table of devices with columns for Device Name, IP Address, Device Vendor, Software Version, Software Model, and Issues. The 'vsx' device is selected, and its details are shown in the 'DEVICE SUMMARY' panel on the right. The 'LAST BACKUP' section in the summary panel shows a checkmark and a file icon, indicating a successful backup.

Device Name	IP Address	Device Vendor	Software Version	Software Model	Issues
vsx	10.3.3.36	checkpoint	gaia R77.20	VMware Virtual Platfo...1	3
pan3	10.3.1.15	paloaltonetworks	panos 6.1.0	PA-VM	5
pan2	10.3.1.14	paloaltonetworks	panos 6.1.0	PA-VM	3
pan1	10.3.1.13	paloaltonetworks	panos 6.1.3	Panorama	4
Pac-Man	10.3.3.56	checkpoint	secureplatform R75.40	N/A	4
P1	10.3.3.150	checkpoint	R77.10	N/A	0
Kojima	10.3.3.76	checkpoint	gaia R77.30	N/A	3
Knight	10.3.3.62	checkpoint	gaia R77.20	VMware Virtual Platfo...0	5
F5	10.3.3.134	f5	BIG-IP 11.6.0	BIG-IP Virtual Edition	9
ckpt	10.3.3.72	checkpoint	gaia R77.30	VMware Virtual Platfo...0	5
Arkhan	10.3.3.61	checkpoint	gaia R77.20	VMware Virtual Platfo...0	6

DEVICE SUMMARY

VSX
10.3.3.36

test

MOST RECENT ISSUES

- Device not responding
- Software end of support nearing
- Core dump files found
- High load average

LAST BACKUP ✓

Weekly Backup for Check Point
Start: Wed Jun 06 2018
End: Wed Jun 06 2018

[More Device Info](#)

Part 6: Settings

The **Settings** tab offers a variety of options for configuring Indeni. Generally, 'Admin' level permissions are required to access this tab. Users with 'Admin' level permissions use this tab to add users, assign privileges, view audit log, update your indeni version, configure integrations, application settings and proxy settings.

About is where you can view and update your Indeni version.

We highly recommend you check the [Release Notes](#) before Installing available updates. New rules can be introduced that may generate unwanted notifications. You can turn on and off notifications in **Settings > Users**.

VERSIONS INFO

Indeni-collector:	6.1.6.12	Available Update:	6.1.6.15
Indeni-server:	6.1.6.12	Available Update:	6.1.6.15

Install Updates

License is where here you can view and update your license information. You can also reveal your **Challenge Code**, which is what you will want to provide to Indeni if you need to renew your license.

LICENSE INFO

This Product is Licensed To:	Indeni KD Lab 192.168.197.15
License Type:	Enterprise
Customer ID:	65d480b2-8d72-4cb3-8b73-532c330fa1b1
Expiration Date:	Thu Dec 31 2020 00:00:00 GMT-0800 (PST)
Number of Standard Devices:	33 / 100
Number of Special Devices:	0 / 100

Hide Challenge Code

Upload License

rd2x3a3V0w8S36eekLQ9TO2GATeq+Z8091qUqUB/RGBJANu3MS0Gw9gyTvsAeL34lWepG1+flcrkaTOLUGZEMTr9KcJp3nLB6ob7pPUGTO9yag8pf0W0LVfaJh/A7w123H0tpj81raB0/LPmb49TveayVFpl/eL5e9BpQLOK8GAM6fwPbghkvL4M a59j3oNS/w0vghuRpgf21W/LQKRTLOuZELNuUhd5BVm8R80R6NsG0URgan+G0FQ8abb09119j3N7jBQ9tTaf91+g3VwbxI8 MF0tunM50Kj9Bmg03b0pFTm83LJEE0oGfP+cS1Y5R0ywwg8p8g==

Integrations is where you can manage **SMTP**, **SNMP**, and **SYSLOG** information.

The screenshot shows the 'INTEGRATION TYPES' sidebar on the left with 'SNMP' selected. The main area is titled 'INTEGRATIONS' and includes a '+ New' button. Below this, there's a section 'NO INTEGRATION SELECTED' with a form for creating a new integration. The form fields are: 'Integration Description' (text input), 'Host Address' (text input), and 'SNMP version' (dropdown menu with 'Select SNMP Version' as the current selection). At the bottom right of the form are 'Save' and 'Delete' buttons.

Users is where you can add, and manage, the level of access you want to assign to specific users. You can also set what kind of notifications the user should receive. This is where you will want to disable email temporarily if doing an update or upgrade.

The screenshot shows the 'USERS LIST' sidebar on the left with a '+ New' button. The main area displays a list of users: admin, arie, epacke, ayelet, ran, jonta, tomas, shoukyd, john, chris, ilz, ulrica, daniel, and a 'New User' button at the bottom. To the right, there's a form for adding a new user. The form fields are: 'testing1' (text input), 'Test' (text input), 'User' (text input), '*****' (password input), and 'test@test.com' (email input). Below these fields is a checkbox 'Receive email alerts' which is checked. Underneath is a section 'Select severities levels to get alerts for.' with four tabs: 'Critical' (highlighted in grey), 'Error' (white), 'Warning' (white), and 'Info' (white). At the bottom right of the form are 'Save' and 'Cancel' buttons.

Icons that are **highlighted grey** are selected for notification, the white tabs are deselected from notification.

6.1: Centralized Authentication

By default, Indeni stores authentication information in its local database. However, you can now also use an external **LDAP** (*Lightweight Directory Access Protocol*) repository to access Indeni.

Please Note: This feature is available in version 6.2+, and only supports Microsoft Active Directory.

LDAP Setup

Configure the connection settings by navigating to the **Settings Icon**, selecting **Authentication** and clicking on **CA** (*Centralized Authentication*), then input the necessary settings to connect to your LDAP directory.

The screenshot displays the Indeni web interface for LDAP configuration. The top navigation bar includes links for About, License, Integrations, Authentication (active), Users & Groups, and Application. The left sidebar contains icons for a bell, search, list, settings, and user profile. The main content area is divided into two sections: Step 1 and Step 2.

Step 1: Centralize Authentication

Configure Centralized Authentication and group mapping for centralized user account administration

Service endpoint *

ldap://18.204.91.193:389

Full url include port. For example: ldap://192.168.0.10:389

User name *

testuser1@ad.indeni.com

Password *

Base DN *

DC=ad,DC=indeni,DC=com

Please use Base DN for users and groups authentication

VERIFIED

Step 2

group

Limit results: 50

- + Group Policy Creator Owners
- + group1
- + group10
- + group2
- + group3
- + group4
- + group5
- + group6
- + group7
- + group8
- + group9
- + Windows Authorization Access Group

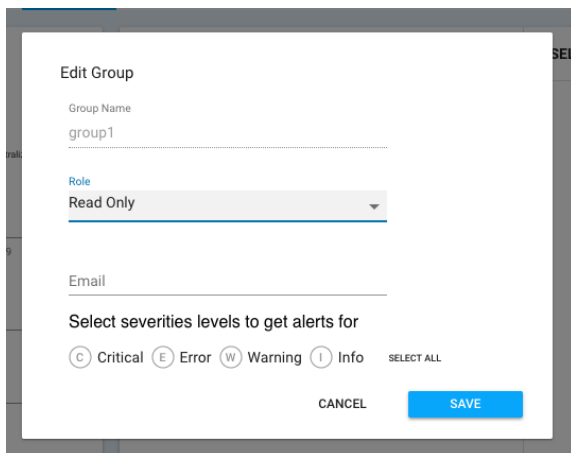
STEP 1. Enter the LDAP Endpoint, Username and Password, and the Base DN. The LDAP user should be in the user@domain.com format. We support endpoint domain names, and LDAPS over port 636.

You will need to test and **verify** the details before you can move on. Depending on how many groups there are in the organization this can take up to 5 minutes.

Please Note: The Base DN details should auto-populate based on the @domain of the username.

STEP 2. It is recommended that you search for the group you want to add. You can filter change the results by 50, 100, or 200 groups. Click on the plus sign to add the group.

STEP 3. Before the group is added you will need to assign a Role, and email preferences that will be assigned to all the users within the group. Individual role types and email notification preferences can be set once they login. You can also set a group distribution email while editing the LDAP group.



The screenshot shows a modal window titled "Edit Group". It contains the following elements:

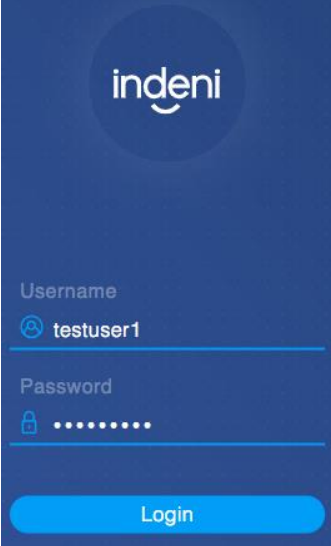
- Group Name:** A text input field containing "group1".
- Role:** A dropdown menu currently showing "Read Only".
- Email:** A text input field.
- Select severities levels to get alerts for:** A section with four radio buttons: "Critical", "Error", "Warning", and "Info". None are selected. To the right of these buttons is a link that says "SELECT ALL".
- Buttons:** "CANCEL" and "SAVE" buttons at the bottom right.

Please Note: Notification for severity levels are not selected by default and are not highlighted. Once selected, they will highlight to the color that represents their severity type.

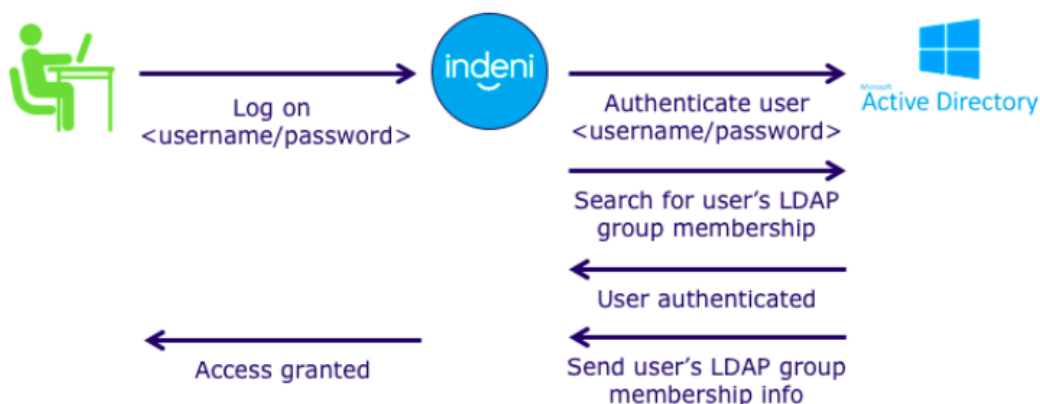
The group is saved to the WebUI, and LDAP users assigned to the group can login to Indeni with their LDAP username, without the @domain details.

User Login

Any time a user attempts to login to Indeni, *if a LDAP server is configured*, the username and password will be forwarded to the specified LDAP directory server to determine if the credentials are correct. Indeni **does not** store the LDAP usernames and passwords locally. Indeni determines what LDAP groups the user belongs to with a simple search and then verifies that the user belongs to one of the selected LDAP groups. If the user does not belong to any one of the selected LDAP groups, Indeni will fail the authentication.

A screenshot of the Indeni login interface. It features a dark blue background with the 'indeni' logo at the top. Below the logo, there are two input fields: 'Username' with a blue icon and the text 'testuser1', and 'Password' with a blue icon and a series of dots. A blue 'Login' button is positioned at the bottom right of the form.

The diagram below summarizes the authentication process.



Authentication Fallback

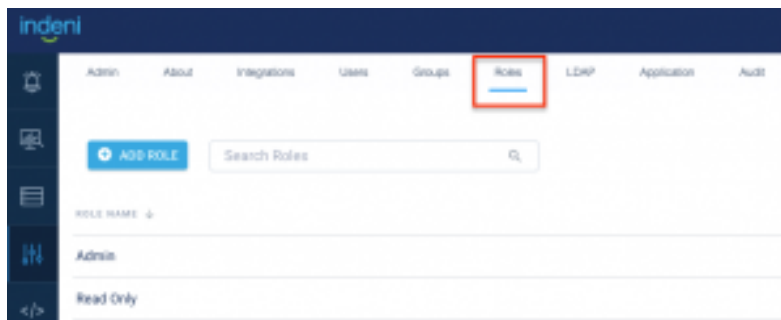
If the LDAP directory does not successfully authenticate the username and password forwarded, Indeni will fall back to the local username and password. If the username and password credential do not exist in the local user store, Indeni will fail the authentication.

6.2: Role Based Access Control

Release Version 6.5.3 onwards

Role-Based Access Control (RBAC) helps you manage who has access to Indeni resources and what operations they can do with those resources. Indeni supports two user privileges; **Administrator** and **Read-Only**. The **Administrator** role can control all aspects of the system, including assigning different roles with different privileges to users. The **Read-Only** role provides an access control category which permits a user to log into Indeni with restricted functions. Typically, a Read-Only role is assigned to an operator.

Indeni maintains at least one local administrator account and will **not** allow users to delete it. Please [contact Indeni Support](#) if you need assistance resetting the local administrator account.



Selecting Permissions for Specific Actions

Each non-admin role can be configured with a custom set of actions and screens. Selecting a permission enables it, allowing the user to access the relevant function.

ACTION NAME	PERMISSIONS				
Issues	All	Archive	Unarchive	Issue administration	
Rules	All	Show	New/Edit	Delete	Disabled
Analysis and reports	All	Show	New/Edit	Delete	

Show Button

The Show button is unique in the sense that it is the only button which does not exert control over a specific UI function. Instead, the Show button allows access to the page from which the relevant UI functions can be carried out.

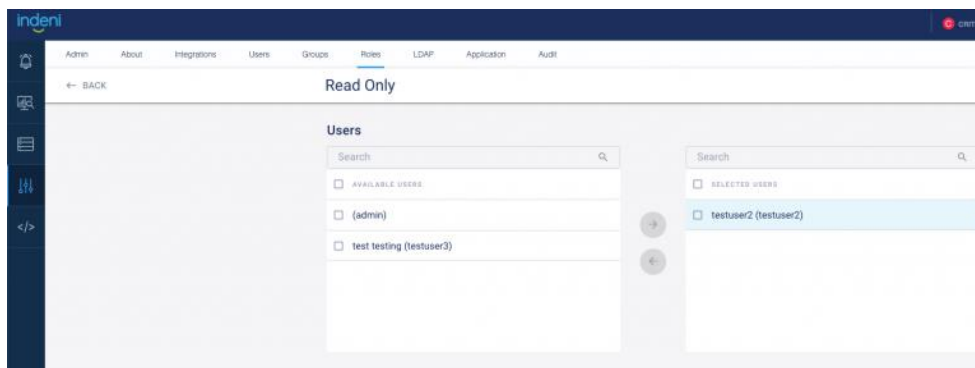
Note: The Show button is automatically selected whenever any permission for a specific action is selected. The Show button cannot be de-selected if even a single permission was selected for the Action in question – see screenshot below

ACTION NAME	PERMISSIONS				
Issues	All	Archive	Unarchive	Issue administration	
Rules	All	Show	New/Edit	Delete	Disabled
Select 'Show' to enable access					

Configuring User Level Privileges

Please Note: Only Administrator Level Users can change permission levels and assign roles to Users.

To configure RBAC for an individual **local user**, navigate to the **Settings Section**, select **Roles**, then select the user you want to assign a user privilege to. In this example, the user 'foo' is assigned **Read Only** privilege.



Configuring User Privileges at Group level

An Administrator can also assign roles to groups. For example, if there are 100 users within an Indeni user group, assigning roles to a group will simplify the user management.

You can configure RBAC for a group by scrolling down to the **Groups Section**, and assign the relevant groups to the specified role.

Operational Privileges

The table below summarizes the RBAC privileges the two user types we will have:

	Functions	Administrator	Read-Only
Issues	View summary, Current, Archived issues & Indeni Rules (Including Adding Notes to Current Issues)	✓	✓
	Archive and Unarchive Issues	✓	✓
	Issue Administration (e.g. Change Thresholds, Disable Rules)	✓	
Analysis	Create Analysis Charts	✓	✓
Devices	Issue Administration (e.g. Change Thresholds, Disable Rules)	✓	
	Device Administration - Suspend & Resume	✓	✓
	View Device Information & Run Report	✓	✓
	Backup Administration (Create, Update and Delete Backup List)	✓	
	View Backup Jobs and Retrieve Backup Files	✓	✓
Settings	Create Analysis Charts	✓	✓
	System Administration (Including Upgrades)	✓	
	Integrations	✓	
	User Administration	✓	
InDE	View Automation Scripts	✓	✓
Other	Send Support Tickets through the User Interface	✓	✓

Read-Only Privileges

Users with Read-Only access **cannot** perform any UI functions and cannot access configuration screens. The following functions cannot be accessed by users with **Read-Only Roles**:

1. **Analysis and reports**
 - Viewing existing reports or creating new ones
2. **Credential Management**
 - Viewing, creating or editing credential sets
3. **Devices:**
 - Adding or removing devices
 - Creating, removing or modifying labels
4. **Issue administration:**
 - Configuring the issue settings (*e.g. severity, thresholds*).
5. **Rules:**
 - Creating or deleting rules
 - Disabling rules
6. **Backups**
 - Creating, deleting or editing backup jobs
7. **About**
 - Updating system version
8. **Integrations**
 - Creating, editing or deleting integrations
9. **Authentication**
 - Creating, editing or deleting authentications
10. **Users**
 - Creating, editing or removing users
11. **Application Settings**
 - Edit application settings

Version Migration

When you migrate from a previous version of Indeni, existing users will remain as administrative users. Indeni will not try to “guess” which users should maintain administrative privileges and which users should have read-only access. The administrator is expected to reset the appropriate privileges.

6.3: Configuring a Proxy Server to access Indeni Insight

From 2019, [Indeni Insight](#) is mandatory in every Indeni installation. Indeni Insight is a cloud-based service that verifies Indeni best practices are in place and notifies you of urgent vulnerabilities. Indeni Insight sends non-confidential data from your Indeni instance to our cloud database.

First time Installation

If you are installing Indeni for the first time, your indeni instance will automatically test the connectivity to Indeni Insight. If the connectivity to Indeni Insight is not working, the system will prompt the administrator to check the internet connection and configure the proxy server in your environment.

First time Upgrade

After upgrade to the indeni insight mandatory release, the administrator will be reminded of the change upon login for the first time. The system will automatically test the connectivity to Indeni Insight in the cloud. If the connection was working, no further action would be needed. If the connection was not working, you would be prompted to check the internet connectivity and configure the proxy server setting.

Please Note: In GA 6.5.1 and up, Indeni Insight can be configured via the UI.

Configuring connectivity to Indeni Insight

If Indeni is having trouble connecting to the internet, it is possible that it has been set to use a proxy server. Please note that Indeni Insight requires access to “service.indeni-ops.com” over ports 80 (HTTP) and 443 (HTTPS).

To configure a proxy, open the **Settings** tab from the left, select the **Admin** option, then the **Proxy Settings** option to open the proxy settings configuration wizard. Enter the URL or IP address of the proxy server as follows:

`https://<proxy_server>:<port>`

If the proxy server requires authentication, enter as follows:

`https://<username>:<password>@<proxy_server>:<port>`

For example

`https://admin:mysecret@10.10.10.11:8080`

Click on the blue Set Proxy button to save the configuration.

Once you have configured a proxy, Indeni will automatically test the connection to Indeni Insight to ensure that it works as expected.

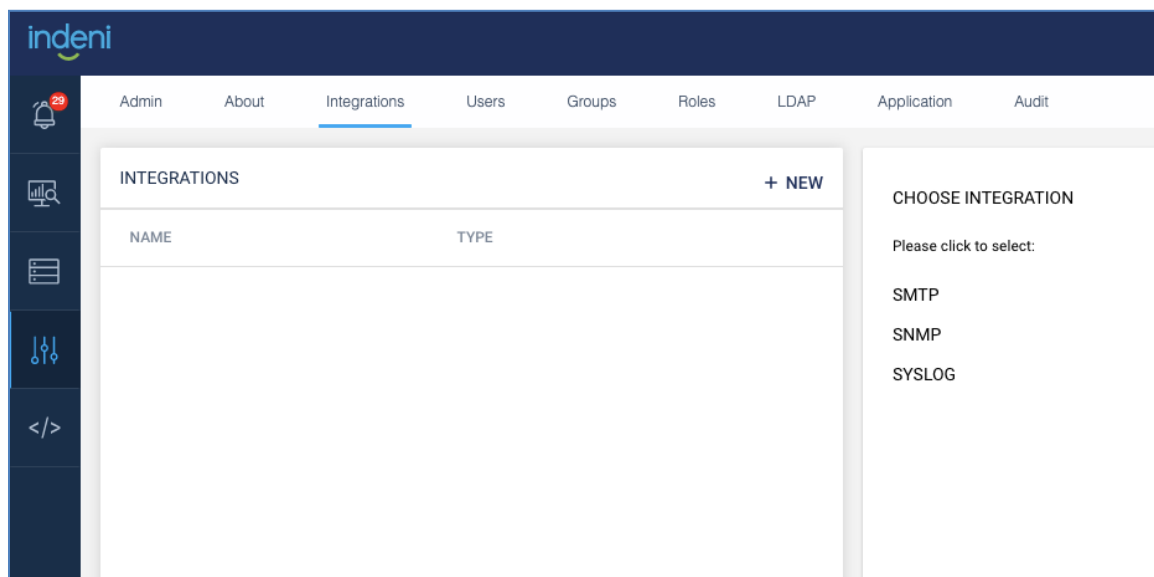
Please Note: In GA 6.5.1 and up, Indeni automatically checks the connectivity to Indeni Insight. Indeni will remind the administrator once a week if the connection to the cloud is not working. It is not possible to disable Indeni Insight.

6.4: SNMP Integration

SNMP integration enables the Indeni server to function as a SNMP trap forwarder. All alerts generated by Indeni will be forwarded to the configured host as SNMP traps. The configured host is usually a network management tool or SNMP manager. In this example, we will demonstrate the integration with SolarWinds Network Performance Monitor (NPM).

Configure SNMP

STEP 1. Click on **Integrations** tab and click **+ NEW**, select **SNMP**



STEP 2. Select SNMPv2 option. Only SNMP v2 is currently supported. Enter the IP address of the SNMP trap receiver in the Host address field. In this example, we have setup a SolarWinds server at 10.11.80.31. Next, enter the community string. This is the community string for the Indeni server. You can use any string you prefer.

We recommend “indeni” as the community string, since this field can be used on the SolarWinds to filter incoming traps.

Finally, click **SAVE** to save the settings.

EDIT INTEGRATION: SNMP

Integration Name *
SNMP

SNMP version *
SNMPv2

Host address *
10.11.80.31

Community String *
indeni

CANCEL SAVE

STEP 3. Rules with critical or error severity level have the SNMP trap forwarding enabled by default. If you want Indeni to generate traps for issues that have info or warning severity, you can enable it under **Indeni Rules** page. Create a new configuration for the specific rule you wish to enable SNMP trap.

Summary Current Archived Indeni Rules

RULES LIST

ntp

Changed

NTP servers used do not match across cluster members

Unchanged

No NTP servers configured

NTP server(s) are not configured

NTP servers configured do not match requirement

NTP sync failure(s)

Overview Configurations Disabled

CONFIGURATION New

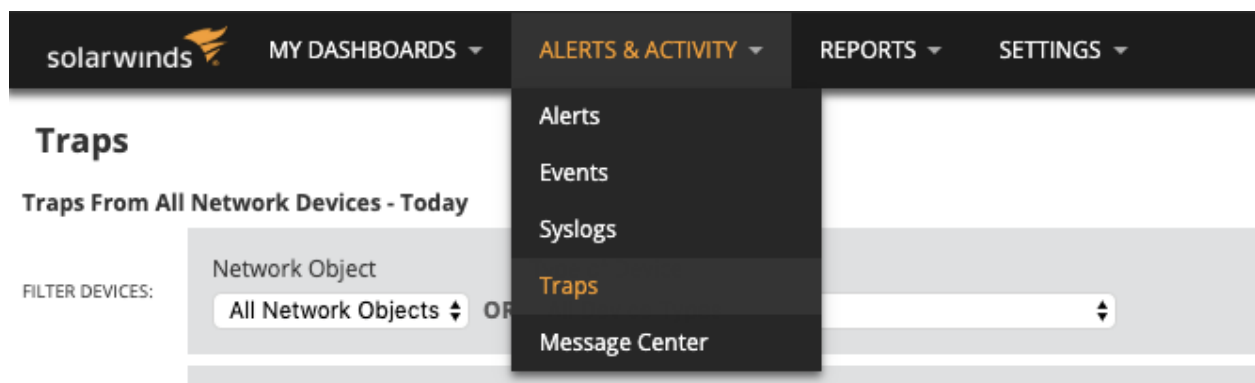
Global Configuration

New Configuration

STEP 4. Make sure SNMP box is checked. This will enable SNMP trap forwarding for this issue. Click **Save** to save the changes.

The screenshot shows the 'CONFIGURATION VALUES' form. At the top, there's a 'Name' field with 'New Configuration' entered. Below this are two tabs: 'Labels' and 'Devices'. The 'Labels' tab is active, showing a search bar and a list of labels: 'system-fortinet', 'system-Canonical', 'PAN', and 'system-f5'. To the right, the 'Selected devices & Labels' section shows a search bar and a list with 'system-all'. Below these sections are 'Actions' with checkboxes for 'SYSLOG' (checked), 'SNMP' (checked), and 'EMAIL' (unchecked). There's a 'Custom Instructions' text area. At the bottom, a 'Severity' dropdown is set to 'Warn'. 'Delete' and 'Save' buttons are at the bottom right.

STEP 5. Verify alerts from Indeni are coming in as traps. Navigate to **Traps** page on SolarWinds. Go to **ALERTS & ACTIVITY** → **Traps**.



STEP 6. Enter Indeni server IP address as the Source IP Address. This will filter out all incoming traps except the ones that were sent from the given IP. You might need to wait for new alerts to be generated in order to see new traps showing up.

The screenshot shows the 'Traps' section in SolarWinds. It includes filters for 'Network Object' (All Network Objects), 'Type of Device' (All Device Types), 'Trap Type' (All Trap Types), 'Source IP Address' (10.11.80.21), and 'Community String' (All Community). The 'Time Period' is set to 'Today' and the 'Number of displayed traps' is 250. Below the filters, there is a table of traps with columns: TIME OF TRAP, IP ADDRESS, HOSTNAME, COMMUNITY, TRAP TYPE, and TRAP DETAILS. Two traps are visible, both from 10.11.80.21, with details including IndeniAlertStatus, IndeniAlertURL, and IndeniAlertCategory.

STEP 7. If the trap details are showing the raw OIDs instead of the resolved names, you will need to update the MIB database used by the SolarWinds to the latest version. Follow this SolarWinds [Guide](#) to update your MIB database.

Trap Types and Fields

The following table lists currently supported trap types.

Trap Type	Trigger Condition
indeniNewAlertTrap	This trap is sent when a new issue is detected by Indeni.
indeniAlertStatusUpdateTrap	A status update trap is sent only when the status of an issue is changed to resolved. When an issue enters cool down state, Indeni does not send status update trap for it.

Each trap might use different OID fields. The follow table demonstrates the fields that might be used by the traps.

Trap Field	Detail
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 and the remediation text
indeniDeviceName	The name of the device the alert pertains to
indeniDeviceIp	The IP address of the device
indeniAlertCategory	The category the alert belongs to
indeniAlertBaseIdentifier	The type of alert
indeniAlertStatus	The alert status, could be unresolved or resolved.
indeniAlertAffectedObject	The alert items. An alert might contain multiple items.

Part 7: Security

Security and System

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's Failsafe Mechanism

Some critical devices could be sensitive to too much data collection, which can lead to performance problems. Although every effort has been made to minimize the device resource usage, the fail-safe mechanism is designed to provide additional protection and to prevent overwhelming a device under abnormal conditions.

As part of Indeni's data collection capabilities, Indeni will regularly track the CPU and memory utilization to identify if the device is being stressed at the monitored interval. We leverage this information to inform Indeni's task scheduling mechanism to avoid overwhelming a device. When Indeni detects that the device CPU becomes too busy, or memory becomes an issue, Indeni will significantly throttle data collection and temporarily suspend data collection until it resumes normal conditions. Indeni will continue to collect CPU and memory metrics periodically in order to resume data collection.

Indeni relies on a key-value pair in its JSON-based Knowledge scripts. A full example can be found [here](#).

```
#!/ META
name: panos-show-system-resources
description: fetch resource utilization
type: monitoring
monitoring_interval: 1 minute
includes_resource_data: true
```

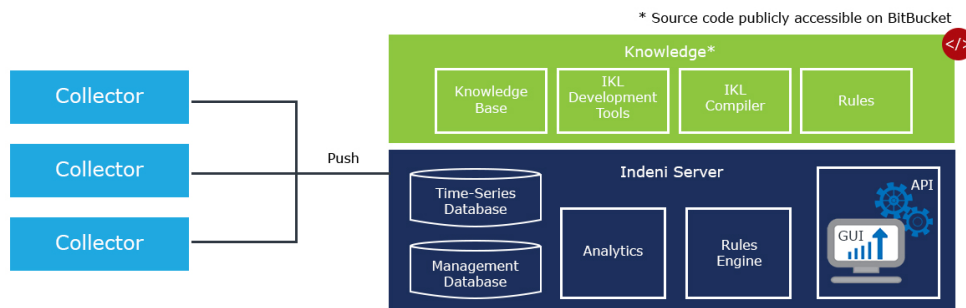
This is used by our Collector service, which schedules each of our scripts and executes them. When the value ***includes_resource_data*** is set to ***true***, it informs the Collector that the script should be executed even when the analyzed device has reached critical thresholds for CPU and Memory. For scripts that should be disabled under high stress, the key-value pair is simply non-existent. That is because the Collector service determines that the key *includes_resource_data* is set to *false* by default.

During clearly identified high stress intervals, Indeni will simply observe the CPU and memory. This allows us to analyze fundamental system resources such as CPU and Memory in order to identify when it is safe and healthy to execute the rest of the scripts again.

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.

Application Architecture



When you install the Indeni application, on a physical machine, as a virtual machine in your private cloud or as a virtual instance in a public cloud environment, you are installing multiple components:

- Indeni base operating system – Ubuntu, a Debian-based Linux operating system maintained by Canonical. This operating system was selected for its stability, reliability, and security. For example, it is the dominant operating system in some of the world’s largest data centers, as well as the Amazon Web Services public cloud.
- Indeni server application – a Java-based application which receives the data collected from devices by the collector (see below), stores it, analyzes it for issue and report generation and makes it available for users. The server application is also responsible for enforcing permissions on data access and modification. The server application exposes an Application Programming Interface (API) which provides access to the data stored by the server.
- Indeni collector application – a Java-based application which connects to the network and security devices, logs in using the credentials it receives from the server and retrieves data 24/7. The collector is a lightweight application designed to be deployed in multiple locations, separate from the server or on the same machine.
- Indeni Postgres database – All configuration data used by Indeni is stored in this database. It includes the list of devices to connect to, their credentials, the issues that were generated, rule configuration, etc. This database does not contain the actual data collected from devices.
- Indeni in-memory metric database – Data collected by the collector is parsed into metrics, which are then sent to the server. The server has several in-memory

databases used to store these metrics, analyze them for issue generation and make them accessible for reporting.

Credential Management

The Indeni collector component collects data from devices across your environment. To do so, it is required to log into these devices, often times using administrator privileges. These privileges are required in order to allow Indeni to retrieve all the data the user needs. Specific commands, such as licensing information, can be outside of the reach of non-administrator users on these devices.

To achieve this, the Indeni application must store the access credentials in a way that allows the application to use them. The credentials are encrypted for storage and decrypted on the fly when needed by the application. Hashing is not an option, as it's only one way and would not allow the Indeni application to retrieve the credentials for use.

Technical details regarding credential storage:

- The credentials are stored in the Postgres database in a table called "credential". You can view the contents of this table by SSHing into the Indeni system's console and running:

```
psql indeni -c "select * from credential;"
```

- The password element of the credentials is encrypted using a symmetric algorithm and key. The algorithm is AES (identified in Java as "AES/CBC/PKCS5Padding") with a 128-bit key. We have chosen AES128 as it's considered highly secure and difficult to brute force (see [this article](#)).

Furthermore, following security best practices, each encrypted section uses a [salt](#). This means that if the same password is encrypted twice, it will result in two different ciphers.

- The key used by the AES encryption is internal to the application.

When accessing credential set information through the server API (for example, for display in the Indeni web user interface), the passwords are masked. You can see this by running the following command when SSHing into the Indeni system's console (you may need to replace the default password "admin123!" referred to in this command to the one you have set:

```
curl -k "https://192.168.197.15/api/v1/credential_sets" -u 'admin:admin123!'
```

As you can see in the output, passwords are masked using the text

```
"***** Hidden Password *****".
```

Credentials that are entered through the user interface are immediately encrypted and saved to the Postgres database.

Your Responsibility in Securing Your Data

While the Indeni server component handles the security of access to all of the data – configurations and metrics collected – it is important that the server itself is secured by you. The following must be adhered to:

- Change the default passwords for the following two users. A better option would be to remove both users, assuming you have created other users with the same privilege level in their place:
In the web user interface – change the password for the user "admin";
In the machine's console (accessible via SSH) – change the password for the user "indeni".
- Control who has access to the Indeni server's hard drive. For a physical machine, this means controlling physical access. For virtual machines, this means controlling access to the hard drive files.

- If you are using the OVA or image files provided by Indeni, then the operating system is already hardened. If not, you should consult with your information security team on how to harden the operating system which you have installed the Indeni server and collector applications on.
- Do not run any other applications on the server(s) on which you have installed the Indeni components. Other applications may have vulnerabilities which may provide an unauthorized individual access to the data stored on the machine by the Indeni application.
- Limit network access to the machine(s) the Indeni application components are installed on, to ensure only those individuals that should have access will be able to access the application.
- If you have deployed the collector component on a separate machine from the server component, you should ensure there is a firewall protecting the server and allowing only the collector to reach it on TCP port 9009.
- If you are accessing the Indeni server's API (also on port 9009) you should follow similar guidance to the previous bullet point and ensure only hosts that should be allowed may access the server on this port.
- When the Indeni support team reaches out to you regarding a vulnerability that was found in either the operating system or one of the components installed, apply the patch or workaround as soon as possible.

Compliance

The Indeni collector application does not collect any packet data from the devices it is connected to. This means that none of the traffic flowing through your network is accessed by the Indeni application in any way. No personally identifiable information is collected or stored at any point by the Indeni system, with the exception of the

information stored within Indeni pertaining to the users accessing the application.

For all compliance purposes, please follow the instructions in the section titled [“Your Responsibility in Securing Your Data”](#).

Transport Security

Data sent between your workstation and the Indeni server is always encrypted.

When you are accessing the machine’s console over SSH the SSH client/server will take care of the encryption. Should your SSH client issue you that the host key has changed on the Indeni server, please halt all communications with the server and determine if a re-install took place.

When you are accessing the machine’s web user interface over HTTPS, the data is encrypted using the protocols agreed to between your browser and the web server included with the Indeni server application. It is recommended to install an HTTPS server certificate on the Indeni server so that you can ensure you are truly connecting to it and the connection has not been hijacked.

Data sent between the Indeni server and the Indeni collector is also encrypted using HTTPS. If you have deployed both of them on the same virtual machine, the data will not leave the machine and this will add another layer of protection. If you have deployed the collector and server components on separate machines, it is best to use a firewall to ensure that only the collector is allowed to reach the server on its API port.

Data collected by the collector from the network and security devices it connects to is protected during transport by either SSH or HTTPS, depending on how Indeni is retrieving data from the given device.

Indeni Insight

Nearly every business relies on their network to engage customers, partners, and employees. As a result, IT Ops leaders need the ability to measure their network health, in addition to the productivity of their people and technologies to achieve business objectives. Indeni Insight enables senior leaders to make smarter decisions ranging from strategic decisions (what technologies should I purchase for my data center migration?) to tactical (what version of the software should we upgrade to, or what features to enable and disable) to improve operations performance.

Architecture

Once an hour, the Indeni server components collect data and posts it to a secure AWS S3 bucket owned by Indeni. The S3 bucket is PUT-ONLY for all Indeni customers, similar to how blind FTPs work. An AWS Lambda function, running under special permissions, has access to see the data posted in the S3 bucket. This function collects the data and inserts it to a MySQL database hosted in AWS as well. The S3 bucket, AWS lambda function, and MySQL database are all hosted within US-based regions of AWS.

This database contains all of the Insight data received from all of Indeni's customers. To ensure the confidentiality of our customers' information, the data is stripped of any identifying information. The working premise in the construction of the Insight database is that should the database ever be hacked, none of the information contained within it could be used to identify Indeni's customers or provide any insight into how their network is laid out.

The following is a list of all of the data collected through Insight:

- Instance unique identifier – such as 33a56092-bc25-11e7-abc4-cec278b6b50a. Uniquely identifies the Indeni server instance installed in your environment. The

Insight database does not contain any information regarding who owns this instance.

- Issue information:
 - Issue unique identifier – same format as the instance unique identifier.
 - Rule_Name – the rule in the Indeni server which generated the issue.
 - Headline – the headline of the issue – only the portion which is shared among all installations of Indeni (no environment-specific information).
 - Severity – one of CRITICAL/ERROR/WARNING/INFORMATIONAL
 - Device unique identifier – same format as the instance unique identifier.
 - The rule configuration which generated the issue – only its identifier and numeric parameters, no textual parameters.
 - Creation date/time
 - If the issue was archived, when that was.
 - If the issue was marked as resolved, when that was.
 - Note that the issue information does not include the issue's description, remediation steps, or any data which could identify a device or a user.
- Integrations information:
 - Only the types of integrations used. No information is sent pertaining to the server integrated with, credentials or anything of that nature.
- Device information:
 - Device unique identifier – same format as the instance unique identifier.
 - Device type – such as the vendor of the device, operating system running, its version, is it part of a cluster, etc.
 - Whether the device is successfully connected to Indeni, and whether there are any issues.
 - Note that the device's name and IP address are not sent via Insight.
- Rule configuration information:
 - Which rules have specific configurations and what devices/labels are they applied to.
 - For each rule, only numeric thresholds (such as CPU issue threshold) are sent

via Insight. Any other type of threshold is not sent.

- License information:
 - When a license is applied in the system, its expiration date and device count are sent to Insight. This helps ensure that users are applying their purchased licenses on time.
- User information:
 - For each user that is defined, the user unique-identifier is sent – similar format to the Instance UID.
 - For each user-defined, their email address is also sent via Insight. The email address is not stored in the Insight database, it is solely stored in the CRM system in use by Indeni.
- Indeni system information:
 - The version and build of the server component installed.
 - Performance metrics of various server and collector components (such as CPU, memory, and throughput).
- Device metrics:
 - A variety of metrics that are collected from user devices are sent via Insight. These are:
 - CPU utilization
 - Memory utilization
 - Enabled features
 - License types (without serial numbers or any license identifier)
 - Uptime of device
 - Number of concurrent connections
 - Network performance metrics (received bytes/packets, transmitted bytes/packets, dropped packets, etc.)
 - Network latency between a load balancer and its server or nodes (without identifying those nodes' IP addresses or names)
 - Network latency between a device and other devices (without identifying those devices' IP addresses or names)

- For those metrics which normally contain identifiable information (like IP addresses, or hostnames), the identifiable information is hashed via SHA1. This allows the Insight database to track the metric over time, without knowing the real device it pertains to.

Learn more by downloading the [Indeni Insight Whitepaper](#).

As an Insight user, you may request a complete dump of all data collected by Indeni as part of the Insight service. Contact support@indeni.com and make an official request for the data.

Open Source Credits

At Indeni we are using some really great open source software that helped us in building our automation platform. In order to share our love back, here is the list of open-source software that we are using.

Package name	Version
ubuntu	14.04
postgresql	9.4
accessors-smart	1.1
activation	1.1
akka-actor_2.11	2.4.17
akka-http_2.11	10.0.6
akka-http-core_2.11	10.0.6
akka-http-spray-json_2.11	10.0.6
akka-parsing_2.11	10.0.6
akka-slf4j_2.11	2.4.17
akka-stream_2.11	2.4.17
asm	5.0.3
asm-commons	5.0.2
asm-debug-all	5.0.2
asm-tree	5.0.2
aws-java-sdk-core	1.10.50
aws-java-sdk-kms	1.10.50
aws-java-sdk-s3	1.10.50
bcel	5.2
bcel-findbugs	6
bcprov-jdk15on	1.55
bcprov-jdk15on	1.55
commons-cli	1.2

commons-codec	1.1
commons-collections	3.2.1
commons-compress	1.4.1
commons-configuration	1.6
commons-dbcp2	2.1.1
commons-io	1.4
commons-lang	2.6
commons-logging	1.1.1
commons-math3	3.3
commons-pool2	2.4.2
config	1.3.0
dom4j	1.6.1
expect4j	1.2
guava	19
hamcrest-core	1.3
httpclient	4.3.6
httpcore	4.3.3
istack-commons-runtime	2.4
jackson-annotations	2.6.3
jackson-core	2.6.3
jackson-databind	2.6.3
jakarta-regexp	1.4
javassist	3.16.1-GA
jawk	1.03-SNAPSHOT
jcip-annotations	1
jetty-http	9.1.4.v20140401
jetty-io	9.1.4.v20140401
jetty-jmx	9.1.4.v20140401
jetty-jsp	9.1.4.v20140401
jetty-schemas	3.1.M0

jetty-security	9.1.4.v20140401
jetty-server	9.1.4.v20140401
jetty-servlet	9.1.4.v20140401
jetty-util	9.1.4.v20140401
jetty-webapp	9.1.4.v20140401
jetty-xml	9.1.4.v20140401
joda-convert	1.6
joda-time	2.1
json-path	2.2.0
json-smart	2.2.1
json4s-ast_2.11	3.3.0
json4s-core_2.11	3.3.0
json4s-jackson_2.11	3.3.0
json4s-native_2.11	3.3.0
json4s-scalap_2.11	3.3.0
jul-to-slf4j	1.7.21
log4j	1.2.14
logback-classic	1.1.7
logback-core	1.1.2
metrics-core	3.1.0
metrics-healthchecks	3.1.0
metrics-jvm	3.1.0
metrics-logback	3.1.0
mimepull	1.8
moultinyaml_2.11	0.2
nscala-time_2.11	2.2.0
org.eclipse.jdt.core	3.8.2.v20130121
paranamer	2.3
reactive-streams	1.0.0
reflections	0.9.9-RC1

scala-java8-compat_2.11	0.7.0
scala-library	2.11.8
scala-logging_2.11	3.1.0
scala-parser-combinators_2.11	1.0.4
scala-reflect	2.11.8
scala-xml_2.11	1.0.2
scalikejdbc_2.11	2.4.2
scalikejdbc-core_2.11	2.4.2
scalikejdbc-interpolation_2.11	2.4.2
scalikejdbc-interpolation-macro_2.11	2.4.2
scopt_2.11	3.5.0
slf4j-api	1.7.7
snakeyaml	1.16
snmp4j	2.5.0
snmp4j-agent	2.5.1
spray-json_2.11	1.3.3
sshd-core	1.3.0
ssl-config-core_2.11	0.2.1
streambuffer	1.5
woodstox-core-asl	4.1.2
xml-apis	1.0.b2
babel	6.23.0
babel-core	6.25.0
babel-loader	6.4.1
babel-plugin-transform-react-jsx	6.24.1
babel-polyfill	6.23.0
babel-preset-airbnb	2.4.0
babel-preset-es	6.24.1
babel-preset-react	6.24.1
backbone	1.3.3

backbone-validation	0.11.5
baconjs	0.7.9
bootstrap	3.3.7
chai	4.1.0
chai-as-promised	6.0.0
css-loader	0.23.1
d3	3.5.1
ejs-loader	0.2.1
enzyme	2.9.1
express	4.15.3
extract-text-webpack-plugin	1.0.1
file-loader	0.8.5
file-saver	1.3.3
gulp	3.9.1
gulp-iconfont	8.0.1
gulp-iconfont-css	2.1.0
gulp-install	0.6.0
gulp-less	3.3.2
gulp-rename	1.2.2
gulp-requirejs	0.1.3
gulp-shell	0.6.3
gulp-svg-sprite	1.3.7
gulp-uglify	1.5.4
gulp-util	3.0.8
jasmine-core	2.6.4
less-loader	2.2.3
linkifyjs	2.1.4
lodash	3.10.1
Marked	0.3.6
moment	2.18.1

<u>phantomjs</u>	2.1.7
<u>query-string</u>	4.3.4
<u>react</u>	15.6.1
<u>react-addons-test-utils</u>	15.6.0
<u>react-dom</u>	15.6.1
<u>react-test-renderer</u>	15.6.1
<u>requirejs</u>	2.3.3
<u>run-sequence</u>	1.2.2
<u>selenium-standalone</u>	6.5.0
<u>style-loader</u>	0.13.2
<u>url-loader</u>	0.5.9
<u>webpack</u>	1.15.0
<u>ws</u>	3.0.0
<u>yargs</u>	8.0.2
<u>body-parser</u>	1.17.2
<u>boom</u>	5.2.0
<u>cookie-parser</u>	1.4.3
<u>cors</u>	2.8.4
<u>debug</u>	2.6.8
<u>express</u>	4.15.3
<u>express-winston</u>	2.4.0
<u>pg</u>	6.4.1
<u>request</u>	2.81.0
<u>serve-favicon</u>	2.4.3
<u>winston</u>	2.3.1
<u>lz4-java</u>	1.4.0
<u>activedirectory</u>	^0.7.2
<u>ldapjs</u>	^1.0.1
<u>node-ssh256</u>	^0.1.1
<u>axios</u>	0.18.0

basic-auth	^2.0.0
joi	^13.1.2
jsonwebtoken	8.1.1
pg	7.4.1
pg-hstore	2.3.2
sequelize	4.33.4
memory-cache	2.83.0
request-promise	4.2.2
async	2.6.0
compression	^1.7.1
crypto-js	^3.1.9-1
helmet	^3.9.0
http-status	1.0.1
jquery	^3.2.1
ldapauth-fork	^4.0.2
node-xlsx	0.11.0
passport	^0.4.0
passport-ldapauth	^2.0.0
prop-types	^15.6.0
sinon	^4.4.6
squel	^5.12.0
hk2-api	2.4.0-b34
javax.inject	2.4.0-b34
jersey-server	2.22.2
quartz	2.2.1
xstream	1.4.9
mail	1.4.7
system-rules	1.12.0
HikariCP	2.7.1
flyway-core	4

config	1.3.0
rrd4j	2.2
trove4j	3.0.3
jaxws-rt	2.2.7
javax.ws.rs-api	2
jersey-container-servlet	2.22.2
itextpdf	5.3.0
jaxb-api	2.2.4
jsr181-api	1.0-MR1
jsr305	2.0.3
jersey-media-json-jackson	2.22.2
equalsverifier	1.7.6
jimfs	1.1
mockito-all	1.10.19
junit	4.12
scalatest_2.11	2.2.6
scalamock-scalatest-support_2.11	3.3.2
scalamock-core_2.11	3.3.2
Ansible	2.5
Docker	