1. ABOUT THIS GUIDE

This guide is intended for users with varying levels of knowledge and experience of the Domotz Pro system:

- Custom integrators (Audio/Video, Home Automation, Security Systems, Digital Signage, etc)
- IT Managed Services Providers
- IT Technical Support Staff
- Enterprise IT Management

Basic knowledge of computer networks and systems is required to fully understand the concepts and guidelines explained in this guide. Familiarity with the concepts of a MAC address, IP address, Remote connectivity, Network Devices (including but not limited to PoE Switches) and Power Distribution Units is expected.

The information in this document is subject to change without notice and should not be construed as a commitment by Domotz Inc. Domotz Inc. assumes no responsibility for any errors that may appear in this document.
2. INTRODUCING THE DOMOTZ PRO SYSTEM

Domotz Pro is a network monitoring and remote technical support system that gives its users full control over their networks. Domotz detects and monitors IP devices on the network, where the Agent is installed on, regardless of its brand or manufacturer, giving remote access to devices, network health analysis tools and the ability to get notified in the event of devices’ connectivity changes.

Such features let professionals detect and troubleshoot problems that may arise on a customer’s site remotely and without the need to go on site.

2.1. Account billing type

There are two different account billing types in Domotz Pro: Credits type and Subscription type.

The Credit billing system is based on purchasing Domotz credits and then using them for activation or extending the Domotz Agents.

In case of Subscriptions billing type, Domotz will bill automatically every month, using a valid credit card, based on the number of installed Domotz Agents.

To understand which account billing type is associated with your Domotz Pro account, please, log in to portal.domotz.com/portal/account. If in that page you find the payment method section (like shown in the picture below), it means that your account has the Subscription billing type. If the payment method section is not present, it means that your account is using the Domotz Credits.

Please, be careful while reading the following guide, because it contains information for both account billing types.

![Payment Method Image]

Above: Subscription billing type.
2.2. Key Features

**Automated Network Discovery and Monitoring:** Domotz discovers and monitors all IP connected devices regardless of brand or manufacturer. Standard monitoring is restricted to subnets not exceeding /22. Multiple VLANs are supported with specific configuration. For Advanced Plan subscribers, external Private Layer 3 subnets (max /24 subnet mask) and external Public IP/Hostname are allowed.

**Professional Dashboard:** A user friendly dashboard allows quick viewing and navigation between multiple Agents and customer sites.

**Remote Device Access:** App and WebApp embedded remote connectivity to devices that support HTTP, HTTPS, RDP, SSH or Telnet connections – without the need to establish a VPN. Remote connectivity to virtually any proprietary/common TCP Protocol (allowing the remote client/server connectivity to virtually any system).

**Automatic Network mapping:** Domotz automatically discovers devices connected to the individual ports of a managed network switch with details such as type of device, hardware manufacturer, model, IP address and others.

**Network Interfaces Traffic and Errors:** Monitor data traffic, packet losts and errors for individual network interfaces of SNMP enabled devices. Historical values available for each Network Switch port.

**Wi-Fi Access Point Monitoring:** Enhanced monitoring of supported Wi-Fi access point and connected clients, with details about signal strength and noise level of APs for every channel.

**SNMP and TCP Service Monitoring:** Monitor any SNMP v2 OID values or availability of TCP Service on any port. Configure thresholds for alerting on those items.

**Network and Device Alerts:** Domotz users can get an unlimited number of alerts by email or mobile push notification about various events happening within the monitored network. Alerts can be configured on a per account basis.

**Remote power management:** Domotz provides the ability to turn devices on and off using the web or mobile app via PoE (Power over Ethernet), PDU (Power Distribution Units) or smart plugs that Domotz currently supports. Soft-Reboot capability supported. Reboot capability via Web Remote Connection available.

**Team management and Collaboration:** A Team Master can invite Team Members to oversee monitored networks and provide remote tech support or access to the Agent’s devices. The Team Master can also share access to specific Agent to other Domotz Pro users.

**Network Diagnostics:** Domotz Pro users can perform speed tests, check network health or device connectivity, and perform bandwidth analysis to detect possible bottlenecks or packet loss.

**Reports and Logging:** Domotz Pro users can generate monthly and snapshot reports of activities on the specific network, which can be provided to the network owner.

**Manufacturer Support:** Domotz Pro users can launch troubleshooting sessions with partner Manufacturer support teams (e.g. Luxul, NuVo, etc).

**IoT Integration:** Domotz Pro users can leverage deeper integrations with partner Manufacturers.

**Customer Facing App:** Domotz Pro users can offer their customers a customized App to access and control their network from Remote. Schedule Internet Access at device and members level is available through this app.
2.3. The Agent

To monitor and manage a network, Domotz needs a device running on the network 24/7. We call these "Domotz Agents". You can install a software Agent on hardware you may already own or you can purchase turnkey hardware.

Option A: Install Software
The Domotz Portal contains all the links to install software on several different hardware platforms, including Raspberry Pi, Synology, QNAP, ReadyNAS, any Linux Debian-like server or Ubuntu Core platforms. In these cases however, we cannot guarantee availability or support of every feature. Log In to portal.domotz.com to download packages or link to installers.

Option B: Purchase Turnkey Hardware
For a simple, turnkey experience, you can purchase Powered by Domotz from one of our valued partners. Visit the Purchase/Install Agent page for info on where to buy turnkey hardware. They supports complete automatic software updates and ensures smooth running and support of all of Domotz’ functionalities.

2.4. The Application

Domotz has developed Web, iOS and Android applications to give its users flexibility and the best user experience when managing a network. The Web application is the main user interface and communicates data with the Domotz Agent.

Domotz mobile applications are designed so that users are able to provide remote tech support on the go. The Android and iOS applications can be downloaded from Google Play and App Store respectively.

If you have only one Domotz Agent installed that Agent will be the default view in the app when you log in to your account. If you have multiple Agents simply tap on the drawer menu button to access additional Agents. Tap on the Agent you want to access and you will be redirected to that Agent’s page. You can also use the map on the Pro Dashboard to easily navigate between your installations.

Full description of Domotz features can be found in Section 4. DOMOTZ APPLICATION REFERENCE

2.5. The User Portal

The Domotz Portal is the main source of account management information. From the Portal, users can find available information about an Agent’s name, version, status, expiration date, extend the expiration date, purchase additional credits, change subscription plans, change password to the Domotz account, manage team members, manage company configuration and branding, change global settings, enable Two-Factor Authentication and access to the community, knowledge base, blog and more.

From the Portal users can also get the Domotz Agent installation instructions for any of our supported hardware. For more details please refer to Section 5. USER PORTAL AND ADMINISTRATIVE FEATURES
3. INSTALLING AND STARTING THE DOMOTZ AGENT
3.1. Installing a Domotz Box
Make sure you have an account:

- You can create an account at: https://portal.domotz.com/login. If you don’t know your username, check with the person that manages your company’s Domotz account. You will need to be listed as a member of your company’s team. New team members can be added in the portal at: https://portal.domotz.com/

Check your billing info:

Please refer to @2.1. Account billing type to understand which account billing type you have.

- If you have a Credits account you can verify your available credits by logging in to https://portal.domotz.com/ with your Domotz account credentials. If you need more credits, check with your team leader. Send an email to support@domotz.com if you need any help with this. You will be able to activate a Domotz Agent without any credits but you will need to add credits within 24 hours in order to be able to continue monitoring the Agent.

If you have available credits, when the Domotz Agent is activated 12 credits will automatically be allocated to the Agent giving it a 12-month expiration. This can then be changed later should you wish (see section @4.1. The Multisite Dashboard for more details.)

- If you have a Subscription account please verify your payment information by logging in to https://portal.domotz.com/portal/account with your Domotz account credentials. The payment, which depends on the chosen Subscription plan, will be made automatically at the beginning of every new month.

Make sure you have the mobile app:

- You’ll need a Domotz app for the installation process. Download the Domotz Android or iPhone app.

Activating your Domotz Box:

1) Connect the Domotz Box to the network you want to monitor, by plugging it in to the network (router or a network switch) using the network cable provided. Plug the box into a power source and make sure it’s ON.

2) Wait 5 minutes while the Box is automatically provisioned with the latest software. Please do not disconnect the Box during this phase.

3) Connect your mobile phone to the same network as the Box. Open your app and press “Find new Agent” from the left side hamburger menu. Once the Domotz Agent is found, you’ll be prompted to tap the “Configure” button.*

4) You’ll be prompted to Login. Insert your Domotz Pro account credentials and press “Login” and name your Agent/Site to activate your agent.

The manual part of the configuration is done. The Domotz Agent will proceed with scanning the network and detecting all the devices. This can take anywhere from a few up to 10 minutes, depending on how many devices there are on the network.

*Alternative Local Set-Up: If you encounter any issues with step 3 of the instructions, you can also configure your Domotz Box by searching for the IP address of the Domotz Box on your local network. Once you have the IP you can use any browser to go to http://<ip address>:3000 . Afterwards, continue on to step 4.
3.2. Installing on Other Supported Platforms

Domotz Agent is available, for free, on a number of platforms, such as:

- Windows PC/Server
- Ubuntu 16.04 or higher
- QNAP NAS
- Synology NAS
- ReadyNAS
- Raspberry PI for self-installation
- Virtual Machine / Virtual Server

Note: Installing the Agent on platforms other than the Domotz Box is not recommended for professional monitoring because OS changes in third-party platforms may introduce incompatibilities. In addition, we may not be able to provide technical support and advice related to those platforms. Note that not all features are available on third-party hardware. (special configurations, Violet device blocking, etc.)

⚠️ The Domotz Agent complete auto-update feature is only available on Domotz Box
3.2.1. Domotz Agent Installation on QNAP

To install the Domotz Agent on your QNAP:

- Visit the App Center on your QNAP NAS.
- Search for the Domotz app in the Home Automation Section.
- Once you find the Domotz application click “Install”. Once the installation is completed click “Open”

Below are some screenshots outlining the steps in the process.
3.2.1.1. QNAP first time set-up

The next step is to configure your Domotz Agent.

By clicking Open on the first time you will be brought to the Domotz Agent activation page.

If you already have a Domotz account, you can login straight away. Otherwise you can create a domotz account signing up from here (please make sure you specify the right Country):

Once logged in you can finally activate your agent, with the following steps:

1. Assign a name to the Agent
2. Specify whether you run the agent at home or office
3. Press the “Activate your agent” button
Once this has done, the Domotz Agent will proceed scanning your network for devices. This will take anything from a few minutes up to 15 minutes depending on how many devices you have on your network.

At this point you can download the mobile app (if you do not have already) and open it.

PLEASE NOTE:

By pressing “Done” you will enter the local Domotz Agent Web UI. This is not the main Domotz app, that is accessibile from mobile apps and our website. The local Agent Web UI is only meant to provide a small subset of the Domotz features (Agent info, Network Info, Route Analysis, Speed Test).
3.2.2. Domotz Agent Installation on Synology

To install the Domotz Agent on your Synology:

1. Visit the App Center on your Synology NAS.
2. Search for the Domotz app.
3. Once you find the Domotz application click “Install”. Once the installation is completed click “Open”

Below are some screenshots outlining the steps in the process.
3.2.2.1. Synology first time set-up

The next step is to configure your Domotz Agent.

By clicking Open on for the first time you will be brought to to the Domotz Agent activation page.

NOTE: If you can't see the Domotz Hub app don't worry. If the Domotz Package is in Running mode, please connect to port 3000 of your NAS with a web browser, like this: <NAS_IP_ADDRESS>:3000 and you'll be inside the Domotz Agent login page. Another way to install the Agent would be to download the Domotz Pro mobile App on your phone and follow the steps to Add a New Agent: the App will find the Domotz Agent running inside the NAS automatically.

@4.1.1. Hamburger/sidebar menu

If you already have a Domotz account, you can login straight away. Otherwise you can create a domotz account signing up from here (please make sure you specify the right Country):

Once logged in you can finally activate your agent, with the following steps:

1. Assign a name to the Agent
2. Specify whether you run the agent at home or office
3. Press the “Activate your agent” button
Once this has done, the Domotz Agent will proceed to scanning your network for devices. This will take anything from a few minutes up to 15 minutes depending on how many devices you have on your network.

At this point you can download the mobile app (if you do not have already) and open it.

By pressing “Done” you can enter the local Domotz Agent Web UI
3.2.3. Domotz Agent Installation on RASPBERRY PI

3.2.3.1. Getting started

This section contains a few tips and tricks on how to get started with the Domotz Agent on your Raspberry Pi. We’ll go through what you need to get going with a brand new Raspberry Pi, so if you already have Raspbian installed, you can skip straight to section @3.2.3.3. Installing the Domotz Agent . The Agent is compatible with all Raspberry Pi platforms to date, as of February 2016.

If you bought a Raspberry Pi or pre-configured memory card from Domotz, please proceed to section @3.2.3.4. First time setup , after connecting your Raspberry Pi to a power adapter and your network.

Note that your Raspberry Pi needs to have a network interface of some kind, or the Domotz Agent won’t be able to detect the devices on your network.
3.2.3.2. Installing Raspbian

Installing the Domotz agent on your Raspberry Pi is a lot more involved than installing it on a NAS, due to the fact that the Raspberry Pi needs to have an OS installed on it. First, there are some prerequisites and we’ll take you through everything you need here if you’re starting from scratch.

In addition to your Raspberry Pi board you’ll need a micro SD card onto which you need to install an operating system. We’d recommend getting a Class 10 or faster memory card, as it’ll make the install quicker. Another option is to buy a ready made micro SD card from the Raspberry Pi foundation. If you bought one of these, then you can skip to section 3.2.3.3. Installing the Domotz Agent.

You’ll also need either a USB cable or a USB power adapter so you can power your Raspberry Pi, and ideally a screen of some kind with HDMI input, an HDMI cable, a mouse, a keyboard and a network cable.

Once you have the above things, let’s get the operating system installed. We’d recommend using NOOBS if you’re not familiar with Linux and you can download it from the Raspberry Pi foundation by going here – https://www.raspberrypi.org/downloads/ Click on NOOBS and download the “Offline and network install”.

The following guide explains how copy the files onto your micro SD card and how to install Raspbian – https://www.raspberrypi.org/help/noobs-setup/. This is when that monitor or TV comes into play, as once you’ve prepared the micro SD card according to the instructions, you need to plug your Raspberry Pi into the monitor and connect a keyboard and a mouse to it. After a few seconds, you should see a screen that will ask you to install the OS, simply click on Raspbian followed by Install and the OS should be installed.

Once the installation is done and your Raspberry Pi has rebooted, you’ll see a setup screen. You can configure some options here and we’d recommend enabling to boot into the graphical user interface. Once you’re done, simply select Finish to boot into the Raspbian desktop environment. Now you need to connect your Raspberry Pi to your network via a network cable, so we can continue with installing the Domotz Agent.

Note that if you don’t make any changes in the setup menu, you can start the graphical user interface by typing “startx” and hitting enter.
3.2.3.3. Installing the Domotz Agent

You’re now at the point where you need to download and install the Domotz Agent on your Raspberry Pi.

1. Make sure your Raspberry Pi is connected to the internet. We recommend to use a network cable and connect your Raspberry Pi directly to your router.

2. Download the latest Domotz Agent for Raspberry Pi

If you use the built-in web browser in Raspbian, go to the Domotz Community to download the latest Domotz Agent. The file should automatically end up in the /usr/home/Downloads

   If you have a headless setup (no screen, keyboard or mouse connected), you can login to your Raspberry Pi via SSH using a terminal software such as PuTTY or Tera Term in Windows, or the built-in options in OS X or Linux. The default username is pi and the password is raspberry. Then simply type the following commands to start the download:
   
   cd Downloads
   wget <file-path-as-specified-on-the-domotz-portal>

3. Install the Agent

Click on Menu, Accessories, Terminal. A command line window with some green and blue text should appear on the screen. In case of headless installation, just login to your Raspberry Pi via a terminal. Go to the download directory (if you’re not already there) by typing "cd Downloads" and hitting enter.

Type the following command to install the Domotz Agent. Note that in place of <package name> you need to type the name of the file you downloaded. As Raspbian is a Linux-based OS, you can simply type the first couple of letters of the file name and then hit the tab key on your keyboard and the rest of the text will be automatically filled in for you.

   sudo dpkg -i <package name>

   Note: To list files in Linux, type "ls" and hit enter and you’ll see the files in the current directory.

The installer for the Domotz Agent should now be running. The installation will take anything between five and 15 minutes, as the installer is downloading parts of the software and installing it onto your memory card.

Once the installation has finished, the Agent will be automatically started and you’ll see a link that you can either double click to open in a browser, or copy and paste into your browser to continue the setup.

   If you want to check that everything is working properly from the command line, you can run sudo /etc/init.d/domotz status to get a status message

   If you want to uninstall your Domotz Agent, simply type sudo dpkg --purge domotz and hit enter in the terminal.
3.2.3.4. First time setup

The next step is to configure your Domotz Agent. To do so, make sure you’ve downloaded an installed the Domotz App on your mobile device. Then simply tap on the drawer menu button and tap on “Find New Agents” towards the bottom of the menu. This will automatically detect any new Domotz Agents on your network, as long as your mobile device is connected to the same network as your Domotz Agent. You can then proceed to configuring your Domotz Agent following the steps below on your mobile device without having to know the IP address of your Domotz Agent.

Alternatively, you can type in the IP address and port shown in the Domotz App in a web browser on your PC. For example, if the IP address was 192.168.1.39 you type 192.168.1.39:3000 and then hit enter. You should now see the Domotz Agent webpage.

At this point, you’ll be asked to create an account if you don’t already have one. Please follow the on-screen instructions.

If you’re running any other web service on your Raspberry Pi that uses port 3000, the Domotz Agent will automatically use the next available port, i.e. 3001.
SIGN UP

Email
__________________________
@domotz.com

Password
************

Repeat Password
************

Next >>

By proceeding to create your account and use Domotz, you are agreeing to our Terms of Service and Privacy Policy. If you do not agree, you cannot use Domotz.

<< Back to Login
Once you've created your account, the Domotz Agent will proceed to scanning your network for devices. This will take anything from a few minutes up to 15 minutes depending on how many devices you have on your network.
DISCOVERING

To discover all devices on an average network it will take up to 15 minutes.

We use a continuous discovery procedure, you can start using Domotz as soon as you downloading our app.

iOS App Store

Google Play Store
This also means that it’ll take some time before all of your devices appears in the Domotz App on your smartphone or tablet. Once the scan has finished, click/tap Done to continue to the Domotz Agent web UI.

Note that the setup of the Domotz Agent will fail if the time and date isn’t set correctly on your Raspberry Pi. To fix this, simply update the time and date on your Raspberry Pi and you’ll be able to proceed with the setup.
4. DOMOTZ APPLICATION REFERENCE

4.1. The Multisite Dashboard

The multisite dashboard is designed with simplicity in mind. It contains a map and a list of all the Agents associated to the account. On this page you can quickly sort, filter and visualize multiple sites and go to the Agent you wish to interact with.

The location of an Agent on the map is based on the address provided in the Customer Management tile (see section @4.8. Customer Management). If that address is not provided, the system uses the Agent coordinates automatically detected via ip-geolocation, which might not be very accurate.
4.1.1. Hamburger/sidebar menu

The menu allows you to see basic information regarding your Domotz account:
• Available Credits – Shows how many credits are in your account (Not present if you are a new user with Subscriptions)

• Account Alerts - You are able to turn off all alerts for your account so you will no longer receive push alerts or emails for any Domotz Agents that you are monitoring.

• Add New Agent – To add new Agents present in the network to your account

• Logout of your Domotz Account

Other sections are explained in more detail below:

• **My Agents** – List of Agents you are currently monitoring:
- **Collaborations** – Number of collaboration requests that have not been accepted yet:
- **Expired** – Shows all Domotz Agents installed from this account that are expired:
My Domotz Eyes configured – Details on the Agents having Eyes configured as well as the devices being monitored with the mean of Eyes:
Domotz Eyes add additional capabilities to your agents such as TCP and SNMP service monitoring.

*Eyes Consumption*

7/500

**Agents with Domotz Eyes consumption**

- **Demo London Office**
  - 5 Domotz Eyes

- **Demo Lab**
  - 2 Domotz Eyes
Domotz Eyes Settings

Define the updating time and the amount of Domotz Eyes for *Don’t touch me!*

Domotz Eyes sampling interval

Set the frequency of the calls sent in order to retrieve fresh data every:

- 30 mins
- 15 mins
- 10 mins
- 5 mins
- 2 mins

Total amount of the Domotz Eyes

The number of Domotz Eyes you can use will decrease (as you increase the monitoring frequency)

Domotz Eyes Consumption: 18/750
Upgrade

Devices with Domotz Eyes Consumption

The following devices have Domotz Eyes on them:

- **Lexmark DocuPrint CP115w 3**

  *1 month*  
  Set a location counter...  
  Domotz Eyes
4.2. The Agent Dashboard
The Agent site dashboard currently contains tiles for quick access and some basic information under each one.

**Important devices:**

- Shows the status of the important devices and highlights if any of them is offline.
- Selecting this tile takes you to a detailed list of all your important devices as well as all features explained in sections @4.3. Device List and @4.4. Device Details

**Devices:**

- Shows the total number of devices and the number of devices that are online
- Selecting this tile takes you a page containing a list of all the devices (or just the online ones if clicking on online) on your network as well as all features explained in sections @4.3. Device List and @4.4. Device Details

**Network:**

- Shows the results of the last speed test performed showing upload and download rate.
- Selecting this tile takes you to all network related tools explained in section @4.5. Network

**Alerts:**

- Shows the number of standard or custom alerts that have been configured.
- Selecting this tile takes you to the Alert Manager described in section @4.6. Alert Manager

**Collaboration (only available to the license owner / team master):**

- Shows the number of people, outside your team, that have been granted or have a pending permission to access your Agent.
- Selecting this tile takes you to the collaboration page described in section @4.7. Collaboration*

**ZigBee (BETA Only available to users that have a Control4 controller):**

- Provides monitoring details for Control4 devices connected to your network via ZigBee enabled protocol (Please note we do not have any specific agreements with Control4 or any 3rd party manufacturers or providers for this monitoring and it is provided on an as-is basis).
- Selecting this tile takes you to the ZigBee page described in section @4.12.2. Zigbee Monitoring

**Cresnet (Only available to users that have a supported Cresnet controller):**

- Provides monitoring details for devices connected to your network via the Cresnet Hubs.
- Selecting this tile takes you to the Cresnet page described in section @4.12.3. Cresnet™ Monitoring
**Customer Management:**

- Shows the site details of the customer to whom this Agent belongs. More details can be found in section @4.8. Customer Management

- Includes Client App tab to allow the user to activate and manage the Violet App. Described in separate document “Violet Digital Support Customer Facing App”

**Reports & Logging:**

- Displays last remote connections made to devices, power activities on devices, Notes added, and when Agent alerts are disabled/enabled.

- Allows you to generate a report covering the previous 30 days of activity on the Domotz Agent or the snapshot with all the devices discovered by the Domotz Agent.

- More details can be found in section @4.12. Integrations

**Manufacturer Support (Will only be available to users with partner Manufacturer devices):**

- Allows you to share your Agent access with the various hardware manufacturers that offer partner support with Domotz (e.g. Luxul, NuVo, etc). More details can be found in section @4.10. Manufacturer Support

**Security (BETA):**

- Provides proactive scanning for TCP Ports, identifying the open ports and sending alerts in case of detected issues.

**D-Tools (when enabled at account level):**

- Allows user to import data from D-Tools projects directly into Domotz Pro using an API-Key provided by D-Tools.
4.3. Device List

The device list is the typical entry point you access from the Agent Dashboard, when tapping on "Devices" or "Important Devices" tiles. Both tiles will bring you to different views of the device list page.
<table>
<thead>
<tr>
<th>Location</th>
<th>Device Description</th>
<th>Manufacturer</th>
<th>Location Details</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud</td>
<td>Ama Website</td>
<td>AWS</td>
<td>Cloud</td>
<td>13.32.255.84</td>
</tr>
<tr>
<td>Entrance</td>
<td>Kevo Plus Bridge</td>
<td>Unikey</td>
<td>Entrance</td>
<td>First Floor</td>
</tr>
<tr>
<td></td>
<td>LILIN Front Porch</td>
<td>Merit</td>
<td>Entrance</td>
<td>Ground Floor</td>
</tr>
<tr>
<td>Front Garden</td>
<td>Ring Pro Doorbell</td>
<td>Universal</td>
<td>Front Garden</td>
<td>Ground Floor</td>
</tr>
<tr>
<td></td>
<td>Access Point</td>
<td>Advanced Monitoring</td>
<td>Ruckus</td>
<td>Front Garden</td>
</tr>
<tr>
<td></td>
<td>Monoprice Camera - Garden</td>
<td>Hangzhou</td>
<td>Front Garden</td>
<td>Ground Floor</td>
</tr>
<tr>
<td>Kitchen</td>
<td>Alexa</td>
<td>Amazon</td>
<td>Kitchen</td>
<td>First Floor</td>
</tr>
</tbody>
</table>
### 4.3.1. Device List Elements

Each device in the device list has a more detailed page associated to it. In order to access its page, you simply need to tap on the device you wish to be redirected to.

The Device List provides basic information, such as:

- The **friendly name** (if set) or default names, or MAC address (automatically discovered on Layer 2 subnets)
- The **location and zone** (if set)
- The **type Icon** (either automatically or manually assigned)
- The **manufacturer**
- The **IP address**
- The green up arrow or the red down arrow, on the left of the device icon, indicates when the device joined or left the network most recently.
- The green and red "circle" arrows with a number between them shows how many times the device has connected and disconnected to/from the network in the past 24h. This number is refreshed once per hour.
- The **Round Trip Delay**

* = Only available for Premium Plan and on the Web

- The plug symbol, indicates that the device has been configured as plugged-in into a PDU or smart plug.

- The “bolt” symbol indicates that the device has been automatically recognized to be connected to a PoE capable switch port.
• The star symbol indicates that the device is on the “favourites” list

• The “port” symbol indicates that the device is connected to the network via LAN cable (if this detail is available)

• The “Wi-Fi” symbol indicates that the device is connected to the network through a supported Wi-Fi access point and provides a visual indication of the Wi-Fi signal level (Green-Yellow-Red color code)

• The "Lock" symbol might indicates that the device offer additional capabilities through Domotz but credentials are required to unblock these capabilities
• Where available the Manufacturer’s symbol will be displayed next to the device name

• The Round Trip Delay is displayed like below. The value represents the last round trip delay from the device to the Domotz Agent. *Only available on the Web interface of Domtoz Pro.

<table>
<thead>
<tr>
<th>Az Berry Reloaded</th>
<th>Latest Ping RTD - in range</th>
<th>Historical Ping Range</th>
<th>Raspberry IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 months</td>
<td>&lt;1ms</td>
<td>&lt;1ms - 2ms</td>
<td>192.168.5.55</td>
</tr>
</tbody>
</table>
4.3.2. Quick Filters

The top menu bar, highlighted in red below, shows a number of filtering options allowing you to quickly access lists of devices sharing some characteristics.
4.3.3. Categories

Tapping on the Categories option allows you to view different sets of devices:

- **All** = All devices are displayed

- **Favorites** = Only favorite devices will be displayed. In section 4.4.1.4 we explain how to set up a device as favorite. Favorites are local to the Mobile App or Web Browser.

- **Important or Indifferent** = These are devices that may or may not have an impact if one of them would go offline. In section 4.4.1.3 we explain how to set up Important/Indifferent devices

- **Plugged-in** = These are devices that are connected to a supported power switch and can, as such, be turned on or off remotely. In section 4.4.1.4 we explain how to configure recognized IP Power Switches

4.3.4. Online/Offline

Tapping on Online (or Offline) allows you to show only those devices which are currently Online (or Offline) within the selected Category

4.3.5. Searching

Type in a device name, location, vendor, etc. to find the device you are looking for.
4.3.6. Sorting and Grouping

Sort by allows you to sort your devices by IP Address, Name, Status change and Status count. You can select to sort from lowest to highest value, or highest to lowest.

Group by allows you to group your device by Make, Type, Category, Location, Zone or you can select No Group if you don’t want to group your devices.
4.3.7. Multiple Select

This allows you to select multiple devices and edit the properties by clicking on the Pick an Action button. The following properties may then be edited for all selected devices:
Edit Properties for 1 Device

Mark as Important

Set Standard Alert

Location:
  Edit

Zone:
  Edit

Device Type:
  Edit

[Cancel] [Apply]
4.3.8. Manage Devices or Subnets

Within the devices list, the user is able to add non-IP-connected devices ("Dummy Device" not connected in anyway to the network) that can be connected to a PDU or smart outlet to enable simple, easy power management.

Furthermore the user is able to configure the extended monitoring features including External hostname / IP and Private Subnet Scan.
<table>
<thead>
<tr>
<th>MAC Address</th>
<th>Device Name</th>
<th>Location</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>16:62:71:1C:B9:CE</td>
<td>Unknown</td>
<td>Set a location or zone</td>
<td>192.168.5.245</td>
</tr>
<tr>
<td>82:AA:E3:6A:A7:E4</td>
<td>Unknown</td>
<td>Set a location or zone</td>
<td>192.168.5.247</td>
</tr>
<tr>
<td>08:00:27:94:E0:A6</td>
<td>PCS</td>
<td>Set a location or zone</td>
<td>192.168.5.250</td>
</tr>
<tr>
<td></td>
<td>PROCURVE J9029A</td>
<td>Machine Room</td>
<td>192.168.5.250</td>
</tr>
<tr>
<td>00:D0:00:70:F4:57</td>
<td>FERRAN</td>
<td>Set a location or zone</td>
<td>192.168.5.254</td>
</tr>
<tr>
<td></td>
<td>MediaAccess DG</td>
<td>Set a location or zone</td>
<td>192.168.5.254</td>
</tr>
<tr>
<td>04:13:4E:57:0E:6A</td>
<td>Luxul</td>
<td></td>
<td>192.168.5.254</td>
</tr>
</tbody>
</table>
By clicking on the "Manage Devices or Subnets" button, the user can chose one of the following options:

- Add a Dummy Device
- Add an External Hostname/IP Device*
- Configure an External Private Subnet to be scan*
- Information on how to configure VLAN support for Domotz Box
- Device blacklist (the ability to not monitor the particular device anymore)
- Device Auto Discovery (the ability to turn off Device Auto Discovery)
Which kind of device would you like to add to your Agent?

Once you have added it you will find it into your devices list

- Add a Dummy Device
- Add Single External Hostname/IP
- Configure a Private Subnet Scan
- Configure a VLAN

Device Discovery Settings

- Device Blacklist: 0
- Device Auto Discovery: Active

Device Ping RTD Settings

- Device RTD: Active
4.3.8.1. Add a dummy device (non-IP connected device)

This feature allows to add a non-IP-connected device to a PDU or smart outlet to enable easy power management.
Some information are required to be added to the device:

- **Name** (mandatory)
- **Type** (mandatory, defaults to Generic)
- **Location** (optional)
- **Zone** (optional)

The device won’t be monitored and the device detail view will only show the Info tab.
4.3.8.2. Add an external hostname/IP*

External Hostname/IP monitoring allows to monitor virtual devices anywhere on the web, such as:

- A website
- An off-site server
- An external TCP service such as VoIP, FTP, etc.

A maximum of 20 External IP device can be added.

A valid IP or Hostname must be assigned to the device (mandatory), while Type and Name are optional.
Once added, the external Hostname/IP is monitored like any other device (ping every 30 seconds).

* = Available on Advanced and Premium Plans only
4.3.8.3. **Configure an External Private Subnet Scan**

With Private Subnet Scan it is possible to monitor up to 8 different Layer 3 subnets of a VPN-connected LAN or other connected/routed subnets.

With Private Subnet Scan, you can monitor:

- **Modems and/or routers on different subnets**

- **Networks and network devices routed on different subnets**

- **Multiple sites or buildings connected via VPN**

The user must be able to set additional subnet to be monitored
Private Subnet

Manage your Private Subnets

Subnets consumption 1/3 Add

Configured Subnets

Add a Private Subnet

Subnet 1
192.168.6.0/24

Edit
For each subnet the user must specify:

- Subnet name
- Network address (starting IP address of the subnet)
- Subnet mask

Device monitoring includes:

- Network Status
- Tcp services available
- Remote connection

Due to the limitation of Layer 3 information (MAC addresses are not propagated on top of this Layer), static IPs are recommended for devices to be monitored through this feature.

* = Available on Advanced and Premium Plans only

4.3.8.4. Configure a VLAN

When clicking this button, the user is provided with information on how to configure a VLAN.

4.3.8.5. Device Blacklist

In this section you'll be able to blacklist any device that you don't want Domotz Pro to monitor. You won't see them in the devices list and you won't be alerted if any changes on their status.

4.3.8.6. Device Auto Discovery

By suspending Auto Discovery, only previously discovered IPs will be monitored. Domotz Pro will not be able to detect any IP changes or new devices.

4.3.8.7. Device Ping RTD Settings*

Here you can disable the automatic RTD pings from the devices to the Domotz Agent.

* = Only available for Premium Plan

Device Ping RTD Settings

[Toggle switch for Device RTD]
4.4. **Device Details**

Once you tap on a device you enter the Device Details screen. This is the page where all the information and operations for a device are available.

Starting at the top, we have three circles with key information:

- **Status** – shows if the device is online or offline

- **IP Address** – shows the IP address of the device

- **Changes** – shows how many status changes the device has had in the past 24h, i.e. how many times it’s gone offline/online over the past 24h.
There are five default tab screens available, **Info, Connect, Alerts, History and Eyes** and some other tab screens which vary depending on the type of device (for instance **Config**, for IP-based PDUs, smart plugs or supported Home Controllers, **Interfaces** for SNMP-enabled Network Interface traffic and mappings and other device-specific tabs).
4.4.1. Info

The info view of a device allows you to do a lot of different things, from getting basic details about the device, to editing the device name and location, adding a note, selecting the type of device it is, etc. We’re going to cover most of the options in detail in this section and explain the functionality of every option.
4.4.1.1. Type

To change the device type, simply tap anywhere inside the Type box. A new screen will appear with options for several different devices:
## Device Types

**Common Types**

<table>
<thead>
<tr>
<th>Home Automation</th>
<th>Notebook</th>
<th>Server</th>
<th>Network Equipment</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAS</td>
<td>Printer &amp; Fax</td>
<td>Mobile</td>
<td>Tablet</td>
</tr>
<tr>
<td>VoIP</td>
<td>TV</td>
<td>Audio &amp; Video</td>
<td>Camera</td>
</tr>
<tr>
<td>Media Player</td>
<td>Desktop</td>
<td>Wi-Fi</td>
<td></td>
</tr>
</tbody>
</table>

## All Types by Category

### Audio & Video

<table>
<thead>
<tr>
<th>Audio &amp; Video</th>
<th>Audio Player</th>
<th>AV Receiver</th>
<th>Cable Box</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
On top most **Common Types** will be presented, scrolling down all types are shown grouped by Category (Audio&Video, Home&Office, Network, Smart Home, Mobile, Server, Engineering).

To select the type you want to assign to your device, simply tap on one of the available types.
4.4.1.2. Name, Location, Zone

To change the name of your device, simply tap anywhere in the Name box and you’ll get a field to enter the name of the device. The procedure is the same for entering the Location or Zone information.
Choose a room

- Kitchen
- Living Room
- Machine Room
- Master Bedroom
- Meeting Room
- Nas Stack
- Office
- Open Space
- Sala Server

Services SSH,
<table>
<thead>
<tr>
<th>Zone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alessio</td>
</tr>
<tr>
<td>Basement</td>
</tr>
<tr>
<td>Brent Desk</td>
</tr>
<tr>
<td>First Floor</td>
</tr>
<tr>
<td>Ground Floor</td>
</tr>
<tr>
<td>Iacopo</td>
</tr>
<tr>
<td>Main Desk</td>
</tr>
<tr>
<td>Rack Desk</td>
</tr>
<tr>
<td>Remote Corner</td>
</tr>
<tr>
<td>Second Floor</td>
</tr>
<tr>
<td>Tavolo dei Giochi</td>
</tr>
<tr>
<td>Tv Desk</td>
</tr>
</tbody>
</table>
**Location** is the room/site where the device is located and **Zone** is the area within the location (Rack, Floor #, etc.). These are all free text fields that also maintain a list of possible values so you don’t have to insert the same information multiple times.
4.4.1.3. Important/Different

The Important/Indifferent option allows you to filter devices based on if they’re important or not for your company.

For example, your NAS would potentially be a device that you would like to be sure is always online and therefore you could mark it to be Important, then by tapping on the categories button in the main menu in the Domotz app, you can easily filter for important devices only.

Important/Indifferent this is a key concept within Domotz. Since all features of Domotz are available for each device in the home, this is a way for professional installers and service providers can use to identify devices they want to monitor.
It's very easy to configure the Important/Indifferent status of a device. Simply tap on either word to change the device from important to indifferent. In this example, the device is set to Important.

For some device types (e.g. Network Equipment) the device is marked as Important by default. This capability and its behavior can be controlled and configured from the Portal, under the Account □ Settings section.
4.4.1.4. Add To Favorites

You can add devices to your favorites list in order to have quick access if you want to be able to check in on them more often than the rest of your devices. To add a favorite, simply tap on the star in the Add to Favorites box and it'll change from grey to yellow to indicate you made this device a favorite.

Favorite is an information local to the user app. You may set different Favorites for the web app and others for the mobile app.
4.4.1.5. **Delete Device**

This option allows you to delete a device as the name suggests. You would use this option to remove a device that isn't likely to re-appear on the network for whatever reason. In the screenshot below, we have a device that went offline 10 days ago and it should potentially be a prime candidate to be removed from your list of devices.
The delete of an offline device is a logical remove of the device from the view. If it reconnects to the network, it'll appear again in the list of devices. This allows the user to be always fully informed of the real status of the network and any connected device. It is possible to remove ALL the offline devices in once, from the Offline tab □ "Remove all offline devices” button.

You can also remove an online device. In this case all device data will be deleted and the device will reappear as new at the next scan.
Also dummy devices and external Hostames/IPs can be deleted in the same way.
4.4.1.6. Customizable Offline

This allows you to determine how long a device must be unresponsive before being considered offline. Domotz checks for the status of all devices every 30 seconds and by default reports the device as offline if it has not responded for 2 minutes (10 minutes for mobile devices). For some devices this may be too frequent. If you would like to change this behaviour you can increase this up to a maximum of 24 hours. Details on how to do this are in the screenshots below:
Device Status Settings

Device Status is checked every 30 secs by default.

Use custom time window

Consider a device offline when it disappears from network for longer than:

Hours: 0
Minutes: 2

[Cancel] [Apply]
Device Status Settings

Device Status is checked every 30 secs by default.

Use custom time window

Consider a device offline when it disappears from network for longer than:

Hours: 0
Minutes: 2

Cancel  Apply
Once you have changed the setting the Status line will now reflect the new frequency. Please note that there are 3 possible **Status messages**:

- **Online**

- **Online — Unreachable**: the device has not responded at the last status check but has not yet reached the new customized offline threshold. E.g. for the first 10 minutes a mobile device with Custom Offline thresholds set (10 minutes) disappears from the network.

- **Offline**

  Mobile devices by default will use a custom time window of 10 minutes to avoid frequent online/offline messages from being sent. This can be edited just like any other device.
4.4.1.7. Power on/off, power re-cycle

& PoE Network switch mapping

In case a device is connected to a PDU, a smart plug or a PoE network switch, additional elements are shown in the Info section. Power control to on/off or just re-cycle the device are directly available at this level:
Name
Lexmark

Type
Printer & Fax

Location
Open Space

Zone
Remote Corner

Indifferent

Important
Add to Favorites
Delete Device

Digital loggers
Outlet 6

19
catalyst37xxStack

100 Mb/s ≈ 6.2 Kb/s ≈ 176.0 Kb/s
4.4.1.8. Native Reboot buttons for supported devices

For certain supported devices we also include a Reboot Now button which makes use of the native reboot software commands to the device itself. This button will be visible below the Status section as in the image below. For a complete list of supported devices, refer to the Community forum pages at http://community.domotz.com
MacBookProRossali

Name
MacBookProRossali

Type
Notebook
Location
Choose a room
Zone
Add a zone

Indifferent
Add to Favorites
Delete Device

Status (30 sec check)
ONLINE

Last Status Change
7 hours ago

Status Changes 24h
2x

Reboot Device

Reboot Now

Services
Unknown

Make
Apple, Inc.
4.4.1.9. SNMP V2 Community strings

Many features of Domotz are based on SNMP v2. In order to work, Domotz needs the communities for Read and Read/Write specified in this section to reflect the current settings of the device you are monitoring.

Default values (public for Read and private for Read/Write) are pre-configured for all devices.

Changing the values triggers the rediscovery of features based on SNMP values (e.g. Network Interfaces, OID based EYE, etc). From this section it is also possible to override community strings for all the devices.
4.4.1.10. Other details and Wake On LAN Management
Belen (GNUberry)

**Online Status**

**IP Address**

**Changes**

**Last Status Change**
20 days ago

**Status Changes 24h**
0x

**Services**
SSH, Unknown

**Make**
Raspberry Pi Foundation

**Model**

**IP Address**
192.168.5.67

**DHCP Name**
domotzbox

**MAC Address**
B8:27:EB:B0:38:1C

**First Seen**
2017 Jan 24 - 08:37 AM (CET)

**Wake On LAN**

**Enable Auto-WOL**

**SNMP V2 Communities**
At the bottom of the **Device Details**, Domotz provides the support for Wake On LAN as well as other details.

- **Wake On LAN button**: sends immediately a Wake On Lan command to the device (only available if the device is offline) (*)

- **Enable Auto-WOL toggle**: enable Automated Wake on LAN. A WOL command is automatically sent if the device goes offline

- **Note**: Free text field for entering notes regarding the device

- **Names**: several protocols are supported to automatically retrieve names from devices (Domain Names, SNMP names, Bonjour/Avahi names, UpNp names, etc)

- **Model**: where applicable, the device model is automatically discovered by the system. User can override this with his information

- **Description**: SNMP description is automatically retrieved by Domotz on SNMP v2 enabled devices

- **Services**: Domotz discovers automatically some TCP services available on the device for Remote Connection

(*) Wake on Lan command has effect only if the device is actually supporting Wake On Lan
4.4.1.11. Response Time Delay*

From the device info window you can see the last RTD value for the device, and the historical values. A new RTD value is presented every 30 minutes. If you want to disable the automatic ping requests from the devices to the Agent you can do it from the Manage Devices or Subnets (see @4.3.8.7. Device Ping RTD Settings*).

Clicking on the historical graph icon you'll see the history of values and the possibility to perform a ping command from the device to the Domotz Agent.
Ping Round Trip Delay (RTD) and Packet Loss

Show

- Worst RTD
- Median RTD
- Best RTD
- Packet Loss

Chart showing ping round trip delay and packet loss over time.
You also have the possibility to set an alert on the latest RDT value

<table>
<thead>
<tr>
<th>Alerts on Connection Performance</th>
<th>Mobile</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ping RTD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ping Delay trigger thresholds</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Median Latency</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ms</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>Packet Loss</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%</td>
<td>15</td>
<td></td>
</tr>
</tbody>
</table>
4.4.2. Connect

The Connect option allows you to connect to a device, with a single click.

The currently supported options include:

- Embedded Remote Connection for Web Services (HTTP, HTTPS), Remote Desktop (RDP), and Console Access (Telnet, SSH)

- Generic TCP Tunnel for remotely connect to virtually any single device through the mean of any TCP proprietary protocol. For example, this can be used to remotely program an Home Automation system like Crestron, Lutron, Savant, Control4, etc, or to access VNC Servers, or SSH via proprietary terminal client, FTP server, Apple Airport, and many others.

**Security Note:** When clicking the Remote Connection (either HTTP or HTTPS, SSH or Telnet, or RDP), we establish a secure channel (Encrypted Overlay Network) between your home network and our cloud and an HTTPS channel between the App (either Mobile App or WebApp). Therefore the entire communication from the App to the Agent is encrypted (and nobody can sniff the content of it). Of course, the communication between the Agent and the end-device (e.g. a WebCam), if it is over a non-secure channel (e.g. http), is not encrypted, but that is only internal to the local network (We assume you trust your network, otherwise you wouldn’t have non-encrypted services).

Moreover, if you look at the URL when opening a Remote Connection through the WebApp, and you copy and paste that URL on a different PC/Client, you won’t be able to reach the end-device. This has been designed in order to allow people to use the Domotz App even in a non-secure location: e.g., if you are in an Internet Cafe’, over a non-secure WiFi, anybody with a little bit of IT skills can identify the URL you are connecting to (even if it is over HTTPS). But with only that URL, the hacker can’t reach your home device.

Finally, the Domotz solution for the Remote Connectivity guarantees an additional level of security, given that all the supported protocols are encrypted when the data is exposed on the public network. Therefore, even the data for the Telnet and Http Remote Connection (which, by default, are not encrypted), with the Domotz solution, they are secured on the public network by this encrypted channel.

For full Domotz Security details, please see the Domotz Security document.
4.4.2.1. Automatically discovered services

The Domotz Agent automatically identifies whether a device is running any of the supported services (by checking on the most typical ports) and makes them available as clickable items as shown in the screenshot below.
Available Connections

- **Console Access**
  - SSH via port: 22

- **Web Portal**
  - HTTP via port: 80

- **Web Portal**
  - HTTPS via port: 443

- **Web Portal**
  - HTTP via port: 8080

Create a custom connection

Open a TCP tunnel
4.4.2.2. Create/Remove Custom Connections

The automated discovery only checks services on standard or typical ports. It is possible that on some devices, these services are installed on different ports. In this case, if you know the port, you can create up to 8 custom connections for each device by using the Create Custom Connection button. Custom connections feature a red "x" button allowing you to remove the connection.
Available Connections

- **Console Access**
  - SSH via port: 22
  - Connect

- **Web Portal**
  - HTTP via port: 80
  - Connect

- **Web Portal**
  - HTTPS via port: 443
  - Connect

- **Web Portal**
  - HTTP via port: 8080
  - Connect

Create a custom connection
Open a TCP tunnel
Create Custom Connection

- RDP
- HTTP
- HTTPS
- Telnet
- SSH

Connect via port:

22

Buttons:
- Cancel
- Connect
Console Access SSH
via port: 300

Do you want to remove this custom connection?

Yes, Remove

Cancel
4.4.2.3. Open a TCP Tunnel

By specifying a port to be used, it is possible to create a generic TCP Tunnel and open a port for a 3rd party software connectivity to the device.
Open a TCP Tunnel

By creating a TCP Tunnel, you will open a port for 3rd Party software connectivity to this device.

Please specify the port to be used.

Connect via port:

[Buttons]
- Cancel
- Connect
Once the TCP Tunnel is created and in place, you can use the endpoint Host and Port of the tunnel into your local 3rd party software to remotely connect to the end device.

For security reason the Tunnel will be terminated in 1 hour since the creation. However, the connection can be closed at any time ("Close connection" button) and the configuration removed (click on the "X" on the TCP direct connection icon).
4.4.3. Alerts

In the Alerts section of a device you can easily configure alerts for that device. There are three alert options for a device: Standard, Custom and No Alerts. By default, all devices are set to No Alerts.
No Alerts will be sent for this device
4.4.3.1. Standard vs Custom Alerts

Standard Alerts are particularly useful if you want to reuse the same set of alerts on a number of devices. In this case, you can select Standard, to have them applied to the device.

Tap the Edit Standard Profile button in order to enter the Alert Configurator to visualise or modify your standard alerts.

⚠️ If you change the Standard Alerts, all devices configured with Standard Alerts will be affected.

If, instead of applying your typical set of alerts you want to apply a very specific set of alerts for that device, select Custom, and the Alert Configurator will appear. Please refer to section @4.6.3.1. Standard and Custom Alert Configurator for more details about the Alert Configurator.

4.4.3.2. Type of alerts

A device Alert is triggered by an event of connectivity of the device and generates a notification. SNMP and TCP Service Monitoring Alerts are discussed later in this document.

Possible Events currently supported:

- **HB LOST**: triggered as soon as the device loses an IP heartbeat (a heartbeat check consists of 5 “pings” sent every 30 seconds)

- **DOWN**: triggered as soon as the device has been down for Custom Offline thresholds (default is 2 minutes, which is 4 consecutive heartbeats lost)

- **UP**: triggered as soon as the device is back online

Available Notification channels:

- **EMAIL**: email sent to your account when the selected event has happened

- **MOBILE**: This is a mobile app push notification (not an SMS)

HB LOST is triggered as soon a device loses connectivity heartbeat. This is more accurate than DOWN, but can generate a lot of false positives. There are devices (some smart TVs for instance) that often miss a heartbeat even though they are fully working. In those cases, HB LOST could generate a lot of unnecessary emails. We recommend to use DOWN in those cases, and limit the usage of HB LOST only to the cases where it can add real value to your work/troubleshooting activity.
4.4.3.3. **Advanced Alerts**

Advanced Alerts feature enables additional alerting options on your network devices and status. Be notified when your network performance decays or when one of your devices IP Address changes.

* = Available on Advanced Plan and Premium Plan only
### Agent Alerts
Alerts are enabled

<table>
<thead>
<tr>
<th>Network Event</th>
<th>Mobile</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Lost/Recovered</td>
<td></td>
<td></td>
</tr>
<tr>
<td>New Device Discovery</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security issues</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Performance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Performance</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

**Network Performance trigger thresholds**

<table>
<thead>
<tr>
<th></th>
<th>Download</th>
<th>Upload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mb/s</td>
<td>57</td>
<td>23</td>
</tr>
</tbody>
</table>
4.4.4. Config

This tab screen is displayed for those device having special settings supported by Domotz. In particular, in this section you can find the place to configure and operate supported Power Distribution Units (PDUs) and IP-controlled power outlets (smart plugs).
4.4.4.1. Smart Plugs & PDUs

For a current list of supported PDUs and smart plugs, visit our Communities page at: http://community.domotz.com. You can also contact support@domotz.com if you have any questions or requests to support new devices.

If a smart plug or PDU is supported by Domotz, the Config section is automatically displayed with an entry for each port of the device.
<table>
<thead>
<tr>
<th>Plug</th>
<th>Name</th>
<th>Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>+</td>
<td>lamp</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Smart Tv</td>
<td></td>
</tr>
<tr>
<td>+</td>
<td>Add a custom name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>BSkyB</td>
<td></td>
</tr>
<tr>
<td>-</td>
<td>Nest Smoke Sensor</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lamp</td>
<td></td>
</tr>
<tr>
<td>+</td>
<td>Add a custom name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fan</td>
<td></td>
</tr>
<tr>
<td>-</td>
<td>Outlet 5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Add Devices</td>
<td></td>
</tr>
</tbody>
</table>
Here you have basic on/off control of the switch as well as a power-cycle button (if natively supported by the PDU itself). You’ll be prompted to confirm that you want to change the power state of the switch each time.

Domotz has an extremely useful feature where you can “Connect a Device/Connect additional devices” to the plug. What this does is that it creates a symbolic link between the outlet and the devices you selected, so you can easily keep track of what is plugged in where.

To “Connect a Device/Connect additional devices” simply start by tapping on the symbol to the right of the devices name.

You should see a screen similar to the one below. Tap on the plug symbol in front of the device that is plugged in to the smart plug to create the connected device.
Connect a Device

- portal.domotz.com
- catalyst37xxStack
- B8:27:EB:D3:64:4A
- A4:13:4E:65:60:70
- Sala Server
- Garage
- domotzbox-raspbian-b827eb4...
When the devices have been linked, you will be able to switch them on/off not only from the smart plug or PDU Config tab, but also from the linked device page. In the picture below you can see a QNAP NAS connected to a Digital Loggers PDU power switch. The on/off and reboot buttons also appear in the Info section of the QNAP NAS.
Please always make sure that the associated device of a PDU you have set up within Domotz matches the real wired configuration.
4.4.1.1. Username and password

Our implementation of smart plugs and PDUs typically use the default username and password of the supported devices. This is normally tested by our Agent at discovery time. If default user and password are used, you are not asked to provide credentials. If default credentials do not work, you will see the Config section of that device locked.
The section can be unlocked by entering the correct device access credentials.
4.4.5. Eyes

Domotz Eyes allow you to monitor services and other details on your network devices. Currently this includes:

- TCP Services

- SNMPv2 Sensors (via OID)

Other monitoring services may be added in the future.
4.4.5.1. Configuring a Domotz Eye

You will now see a new tab labelled Eyes. This is where you will configure the various TCP services or SNMP sensors. Please note that you can configure a maximum of 20 TCP services per device and unlimited SNMP sensors. The only limitation will depend on the plan you have subscribed to (see 5.2.2. Lite vs. Advanced vs. Premium).

Initial Domotz Eyes Configuration screen:
4.4.5.2. How to add a TCP Service to be monitored
To Add a new TCP service to monitor, enter the name of the service or TCP port number associated with it and the search box will return all available services that match the text entered:
<table>
<thead>
<tr>
<th>Port</th>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>180</td>
<td>ris</td>
<td>Intergraph</td>
</tr>
<tr>
<td>280</td>
<td>http-mgmt</td>
<td></td>
</tr>
<tr>
<td>380</td>
<td>is99s</td>
<td>TIA/EIA/IS-99 modem server</td>
</tr>
<tr>
<td>480</td>
<td>loadsrv</td>
<td></td>
</tr>
<tr>
<td>580</td>
<td>Port - 580</td>
<td></td>
</tr>
<tr>
<td>680</td>
<td>Port - 680</td>
<td></td>
</tr>
<tr>
<td>780</td>
<td>wpgs</td>
<td></td>
</tr>
<tr>
<td>800</td>
<td>m dbs_daemon</td>
<td></td>
</tr>
<tr>
<td>801</td>
<td>device</td>
<td></td>
</tr>
</tbody>
</table>
Once the TCP service is added, the Domotz Agent will start monitoring that service. The port will be marked as available (green) if the Service is available on that port or unavailable (red) if not:

![Domotz Eyes](image)

**Domotz Eyes**

Use Domotz Eyes to monitor services and data.

**TCP Services**

- **http**
  - World Wide Web HTTP
  - Port: 80

- **gopher**
  - Port: 70

On every single TCP service monitored, the user can set a "Custom" alert (from the Alerts tab) to be informed when the service change status (from available to unavailable and vice-versa):
## Alerts

<table>
<thead>
<tr>
<th>Device Event</th>
<th>Mobile</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Goes Up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device Goes Down</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Heart Beat Lost</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Change</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### TCP Services

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Mobile</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>70</td>
<td>gopher</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>80</td>
<td>http</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>

World Wide Web HTTP
4.4.5.3. How to configure an SNMP Sensor
4.4.5.3.1. **Determine OID**

It is very helpful to use an MIB Browser iReader like the following: [http://ireasoning.com/mibbrowser.shtml](http://ireasoning.com/mibbrowser.shtml) – free version for end users). Using this tool it is possible to navigate the OID tree for devices that support SNMP to find the OID sensor that you want to monitor.

![MIB Browser](image)

It is important to configure your MIB tool for SNMP version 2c

The following is an example of a Sensor that will allow you to monitor the level of black ink level of my printer. In order to do this you will need to find some information in order to find the data you are looking for:

- Index number for Black cartridge
- Maximum level for the black ink cartridge (to compare to current level in order to determine percentage consumed).
- Current level of black ink cartridge

In order to do this, you will do the following:

1. You identify the reference index for the black cartridge (in this case the index is 4):
   Using this index, I can get other details for OIDs that are related to this cartridge, i.e. the Maximum level and actual level of the toner in that cartridge which I can then monitor and use to define my alerts.
2. From the OID of the SuppliesMaxCapacity (in my case 1.3.6.1.2.1.43.11.1.1.8.1.4): you get 2500. This is the MAX value of the black toner that is supported by my printer. I will need this later to set up the alert.

3. Then you can get the the OID of the SuppliesLevel (the OID for the Black cartridge in the example is 1.3.6.1.2.1.43.11.1.1.9.1.4)
This OID is what you will add to Domotz and will begin to monitor from the Eye tab of the device (1.3.6.1.2.1.43.11.1.1.9.1.4)
You can refer to the manufacturer’s documentation to determine the correct OID and expected values.
4.4.5.3.2. Configure SNMP Sensor in Domotz

(using OID suggestions)

In the Device Details screen go to the Eye tab and click on 'Add an SNMP Sensor'. If Domotz has the selected device's OID information present in its database, you'll find a list of suggested OID when adding a new SNMP sensor as below. You can click on the '+ ' icon next to a specific OID to add that SNMP sensor to the device.
Add an SNMP Sensor

Insert OID

Suggested OID for this device

Black Toner - Maximum level
1.3.6.1.2.1.43.11.1.1.8.1.1

Cyan Toner - Maximum level
1.3.6.1.2.1.43.11.1.1.8.1.2

Magenta Toner - Maximum level
1.3.6.1.2.1.43.11.1.1.8.1.3

Yellow Toner - Maximum level
1.3.6.1.2.1.43.11.1.1.8.1.4

Black Toner - Current level
1.3.6.1.2.1.43.11.1.1.9.1.1
In the Device Details screen go to the Eye tab and click on ‘Add an SNMP Sensor’. If the Suggested OID list is empty or you simply want to add a custom OID you can click on ‘Insert OID’ and you'll be prompted with the following popup:

(Cthrough discovered OID)

In the Device Details screen go to the Eye tab and click on ‘Add an SNMP Sensor’. If the Suggested OID list is empty or you simply want to add a custom OID you can click on ‘Insert OID’ and you'll be prompted with the following popup:
Add an SNMP Sensor

Insert OID

Configure SNMP Sensor

Sensor Name
Black Toner Level

Consumable

OID
1.3.6.1.2.1.43.11.1.1.9.1.4

OUTPUT TYPE

- String
- Numeric

Cancel Add
From this screen, you will need to add:

- Sensor Name

- Assign to category (for sorting purposes):

  **Sensor Category**

  Select a category:

  - [ ] CPU
  - [ ] Consumable
  - [ ] Disk Space
  - [ ] Memory
  - [ ] Network Traffic
  - [ ] Temperature
  - [ ] Other

- Insert OID

- Define output type of Sensor (String or Numeric)
Domotz will confirm that the OID is in the correct format but cannot check that the value entered is valid.

The type of value the OID will return must match the manufacturer documentation and is important for the types of Alerts you then wish to create based on this Sensor (see Setting @4.4.3. Alerts).

Once you have configured your Sensors you will see them listed with the value that the device is returning for that OID. By clicking on the arrows on the far right you can show/hide details of the individual Sensors.
### SNMP Sensors

**black**

<table>
<thead>
<tr>
<th>OID</th>
<th>1.3.6.1.2.1.43.11.1.1.9.1.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output Type</td>
<td>Numeric</td>
</tr>
<tr>
<td>Last checked</td>
<td>2018 Aug 01 - 02:47 PM (CEST)</td>
</tr>
</tbody>
</table>

**Drawer**

| 4 |
SNMP Sensors Name, Category and Type fields may be edited (clicking on pencil icon), but the OID cannot be changed.

If SNMP data of the selected device are present in the system, the user is prompted with a window suggesting available OIDs configurable for that specific device.

The user can accept the suggestion or edit it, modifying the proposed values.

If any of the suggestions suits the user needs, he can proceed inserting his own sensors, through the procedure described above.
4.4.6. Interfaces

For SNMP enabled devices with Network Interfaces, Domotz is able to display the status and traffic information of their interfaces. Traffic information is collected and stored, so that the user can see the historical data and monitor the interfaces.
4.4.6.1. Automatic Port Mapping

For many managed switches, Domotz is able to automatically detect and associate the devices with the port to which they’re connected.

Individual information for each port of the switch is displayed such as max throughput, current upload and download rate.

For a complete list of supported devices, refer to the Community forum pages at http://community.domotz.com.

4.4.6.2. Power over Ethernet (PoE)

If a Managed Network Switch has PoE capabilities, additional data will be displayed under the Interfaces tab:

- **PoE Power Consumption and Budget information** – this is a graphical representation of the power consumption in watts and percentages (out of the total budget) of the aggregated data from the PoE ports

![PoE Power Consumption and Budget](image)

*PoE Port Toggle Button* – for PoE ports there is also the option to toggle their state on/off as shown in the image below. Power consumption (in watts) is also displayed (if applicable) for the individual port.

![PoE Port Toggle Button](image)

PoE management and Automatic Port Mapping requires SNMP enabled with the community settings configured correctly in the Info section of the Device Details.
4.4.6.2.1. **Diagnostic and Port Details Window**

For every single switch interface port there is additional information which can be accessed by selecting the port name or icons on the left of the SNMP information list.

A tap on a port name or icon or graph icon from the Interfaces list will open a more detailed information window regarding that port shown as a list of devices that are mapped to it.

**Tab “Diagnostic”**

The chart provides information related to:

- Bandwidth usage: inbound and outbound directions
- Errors: inbound and outbound
- Discarded packets: inbound and outbound

You can chose among three different time frames (1 day, 7 days, 1 month – that is the defaulted value).
Lexmark

Show

☑ Bandwidth ☐ Errors ☐ Discarded

Inbound — Outbound

1.2 Mb/s

LAST SAMPLED VALUES:

0.16  0.01
Tab "Info"

The port details window is a visual representation of the individual port the following information:
eth0
Operation Status Up

01

Consumption undefinedW (undefined%)
- port maximum throughput
- port upload and download bandwidth consumption
- PoE power consumption (if any)

Additional information are provided in this visualization:

- *Last Seen Status*: shown only if the device is down. It would also indicate the time that has passed since the mapped device was last online

**Administration Status Down**

**Last Device Seen**

(5 hours ago)

- *Port Statuses:*
On both tabs mapped device(s) are listed – device(s) have been automatically mapped to this port and have the following information:

- Associated Name of the device (as shown in the Devices List)
- IP Address of the device

CAM FRONT GARDEN
192.168.100.84
4.4.7. History

The History tab displays how many times your device has connected to- and disconnected from the network and at what time(s) it occurred.

Domotz performs a connectivity check (heartbeat) and reports in this section when changes in connectivity have occurred.

Some devices (e.g. mobile) can lose connectivity quite often during normal operation, so such details may not be relevant.

For many other devices, History offers a useful snapshot of the recent history of the device. It can help to visualize a behavior that you may not otherwise notice, and tell you if further investigation is needed.
Device Went Up
2018 Jul 12 11:48 AM (CEST)

Device Went Down
2018 Jul 12 11:45 AM (CEST)

Device Went Up
2018 Jun 28 11:59 AM (CEST)

Device Went Down
2018 Jun 28 11:42 AM (CEST)

Device Went Up
2018 Jun 28 11:27 AM (CEST)

Device Went Down
2018 Jun 28 11:22 AM (CEST)

Device Went Up
2018 May 28 10:51 AM (CEST)
Device Went Down
2018 May 28 10:48 AM (CEST)
4.4.8. Security Camera*

The Security Camera Features is not available in the Lite Plan.

* = Available on Advanced Plan only
4.5. Network

The network section includes a number of tools that help analyse the network to which the Agent is connected.
4.5.1. Info

The Info tab displays handy information such as the public (Internet-facing) IP address, network gateway, DNS and DHCP server.

<table>
<thead>
<tr>
<th>Public IP Address</th>
<th>79.59.208.185</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Name</td>
<td>host185-208-static.59-79-b.business.telecomitalia.it</td>
</tr>
<tr>
<td>Provider</td>
<td>TELECOM-ADSL-POOL</td>
</tr>
<tr>
<td></td>
<td>NAS DHCP Pool Padova</td>
</tr>
<tr>
<td></td>
<td>79.59.128.0 - 79.59.255.255</td>
</tr>
<tr>
<td>Gateway</td>
<td>192.168.5.1</td>
</tr>
<tr>
<td>DNS</td>
<td>8.8.8.8</td>
</tr>
<tr>
<td>DHCP</td>
<td></td>
</tr>
<tr>
<td>Interface</td>
<td>192.168.144.0 (ext248)</td>
</tr>
<tr>
<td></td>
<td>52.30.7.143 (ext2042287)</td>
</tr>
<tr>
<td></td>
<td>192.168.5.10 (eth0)</td>
</tr>
</tbody>
</table>
4.5.2. Route

The Route Analysis allows you to send test packets to any Internet public server and measure packet loss in percentage, as well as round-trip delays.

This can be useful to understand where bottlenecks and issues reside in communicating with an external (or internal) target. For example, you can simply type in a website name or an IP address to start the analysis, then select if you want to send 10, 20 or 50 packets. We recommend starting with 10 packets. Once you've selected your options, simply select Start to begin the test.
Select a service:

Spotify

Packets number

10  20  50

This test will last approximately 10 seconds.

Start
Network Health Analysis

Loss%  Avg
---  ---
0.0  16.3ms  Router

Loss%  Avg
---  ---
0.0  0.4ms  ISP

Loss%  Avg
---  ---
0.0  27.8ms  Target

Sent 10 packets to

```
Start: Wed Aug 1 15:49:05 2018
HOST: deb01

<table>
<thead>
<tr>
<th>#</th>
<th>IP Address</th>
<th>Loss%</th>
<th>Sent</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>192.168.5.1</td>
<td>0.0%</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>192.168.15.2</td>
<td>0.0%</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>79.59.208.190</td>
<td>0.0%</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>???</td>
<td>100.0</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>172.18.33.112</td>
<td>0.0%</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>172.18.34.22</td>
<td>0.0%</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>172.19.241.137</td>
<td>0.0%</td>
<td>1</td>
</tr>
<tr>
<td>8</td>
<td>195.22.192.178</td>
<td>0.0%</td>
<td>1</td>
</tr>
<tr>
<td>9</td>
<td>72.14.216.154</td>
<td>0.0%</td>
<td>1</td>
</tr>
<tr>
<td>10</td>
<td>???</td>
<td>100.0</td>
<td>1</td>
</tr>
<tr>
<td>11</td>
<td>108.177.3.76</td>
<td>0.0%</td>
<td>1</td>
</tr>
<tr>
<td>12</td>
<td>108.170.245.72</td>
<td>0.0%</td>
<td>1</td>
</tr>
</tbody>
</table>
```
You’ll see a graphical representation of the route, then once the test is finished, you’ll see how long it took and if there were any obvious issues within your LAN (before the Router), between the Router and the ISP cabinet or between ISP and the selected target.

You can select “See raw data” to get a full breakdown of the entire route. To start a new test, simply select Done and you’ll return to a screen where you can enter a new URL or IP address.

*This feature is based on MTR, a program that combines the functionality of traceroute and ping. It’s licenced under the terms of GNU General Public License Version 2 ([http://www.gnu.org/licenses/gpl-2.0.html](http://www.gnu.org/licenses/gpl-2.0.html)).*
4.5.3. Speed Test

Domotz automatically executes a speed test between the Agent and the nearest test server every 6 hours. The following features are visible in this tab:

- Searchable graph, allowing you to zoom, search and filter the history of the speed tests results

- Statistics are shown in the lower-left hand corner of the screen

- You can disable the automatic speed test using the toggle button below the graph

- It is also possible to run the test manually at any time by selecting the Test Now button

The speed tests are based on test Servers spread around the globe.
Network Health Analysis

Show

- Download
- Upload
- Ping

LAST SPEED TEST:
7 hours ago

Download: 74.2
Upload: 20.9
LAST SPEED TEST:
7 hours ago

\[ \begin{array}{ll}
\text{Download \cdot Mb/s} & 74.2 \\
\text{Upload \cdot Mb/s} & 20.9 \\
\end{array} \]

AVERAGE OF:
1 MONTH

\[ \begin{array}{lll}
\text{Download \cdot Mb/s} & 73.5 & \text{Upload \cdot Mb/s} & 21.3 & \text{Ping \cdot ms} & 17.0 \\
\end{array} \]

OPTIONS

Automatic Speed Test
Enabled
4.5.4. Downtime

The Downtime tab displays a log of the Agent's connection status changes. Typically, this indicates when the internet connection is available (Up) or not (Down). Note that what is actually tested is the connection between the Domotz Agent and the Domotz Cloud. If you disconnect the Domotz Agent then reconnect it, you should see a pair of “Connection Down” and “Connection Up” events.

The network connection is measured from two points of view (see next section for further details):

- From the Agent point of view: every minute the Agent tries to ping outside the network. The downtime is reported as soon as the Agent is available to send the message back to the cloud.

- From the Cloud point of view: every minute the Agent sends a Heartbeat to the Domotz Cloud. If the Heartbeat is not received for few minutes, the Cloud generates a trigger (Alert marked with a “bell” in the next picture), which if enabled generate a notification (either via email or push notification).
4.6. Alert Manager

The Alert Manager allows users to quickly visualise and configure the alerts you have set up across the monitored network.

alerts are managed at user level (with a few exceptions). Each team member can set up his/her own set of alerts on the same Agent!
4.6.1. **Network Alerts**

This tab allows you to:

- Disable/Enable all alerts for Network Events such as Connection Lost/Recovered

- New Device Discovery Alerts

- Security issues Alerts

- Alert setting for Network Performance trigger thresholdes
If you ‘Mute’ the alerts for this agent, the Multi-Site dashboard will display an icon next to the Agent name indicating that alerts are disabled (see Fulham and Kytes agents below):

<table>
<thead>
<tr>
<th>Network Event</th>
<th>Mobile</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Lost/Recovered</td>
<td></td>
<td></td>
</tr>
<tr>
<td>New Device Discovery</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security issues</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Performance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Performance</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Network Performance trigger thresholds**

- **Download**: 58.8 Mb/s
- **Upload**: 17.1 Mb/s
If an Agent connection is lost, this can be for two reasons:

- The network’s Internet connectivity was lost

- The Domotz Agent itself has been disconnected from accessing internet
4.6.2. Explanation of Network Connection and Agent Status Management

This section offers some background on how Domotz populates the Network Health Analysis --> Downtime tab versus how Domotz triggers the "Agent Connection Lost" alert.

The two features (Downtime tab and Agent Connection Lost alert) are similar in idea, but technically speaking they have been implemented in a very different way. This is important, because it is a good way to guarantee that both are working correctly, or to identify if there is a misalignment in one of the two mechanisms.

Basically, every Domotz Agent sends a packet (or train) of 4 'pings' to "echo.domotz.com" once each minute. It also sends a "heartbeat" to the Domotz Cloud to determine whether the agent is still alive.

Agent Perspective: Missing Ping --> triggers an entry in the Downtime Tab

If the Domotz Cloud does not receive at least one of the pings in the packet, e.g. the DNS is failing, there is no internet connection, the network cable is detached from the Domotz Agent, or the Domotz ping server at echo.domotz.com is not available, the Domotz Agent tracks the time that the first ping was lost.

Two minutes after the Domotz Cloud starts receiving replies to ping messages again, the Agent notifies Domotz Cloud that the connection is UP again and that there was a Downtime of X minutes (starting from the first ping lost). This populates the Downtime Tab. The two-minute delay ensures that the connection has become stable again before recording the data.

What happens if the Domotz Agent is turned off (remove the power cable from the Domotz Agent)?

In this case, the Agent does not send any ping (of course) and cannot be aware if there is connectivity or not. Therefore, there will be no entry in the Downtime Tab, for the whole period the Domotz Agent is off.

However, the Domotz Cloud is still aware that something is going on. See next:

Cloud Perspective: Missing Heartbeat --> triggers the alert (if configured in the Alert management - Agent Connection Lost)

After Five(5) minutes have passed since the Domotz Cloud received the last Heartbeat from an Agent, the backend declares that Agent to be OFFLINE.

If the Agent Connection Lost Alert is configured, you will receive an email from our backend stating that the we haven’t received any information from that Agent in the last five minutes.

Once the Agent starts sending heartbeats again, you will receive an email from our backend stating that the connection to the Agent was recovered.

This last mechanism works both if you disconnect the power cable or the network cable from the Domotz Agent, because it's triggered by the Domotz Cloud.
### 4.6.3. Device Alerts

In this section you can set alerts for any device on your network. On the left is the device name or MAC address. There are three main options for each device:

<table>
<thead>
<tr>
<th>Device</th>
<th>Option 1</th>
<th>Option 2</th>
<th>Option 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Qnap</td>
<td>+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digital loggers</td>
<td>+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nas Synology</td>
<td>+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PROCURVE J902...</td>
<td>+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sasha G (Domotz ...)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
• Custom – Device specific customized alerts

• Standard – the alert type that can be reused for more than one device

• No – Indicates that there is no alert associated to this device

The buttons related to individual devices turn green or red depending on if they have been selected (Green for Custom and Standard, Red for No Alerts). The alerts are configured by tapping on either the standard gearbox icon or + button for the device you want to set up the alert to. This takes you to the Alert Configurator page.
4.6.3.1. Standard and Custom Alert Configurator

This page is used to set up events and medium for different alerts.

The Alert Configurator is also accessible from the individual device alert page (see section @4.4.3. Alerts )

<table>
<thead>
<tr>
<th>Device Event</th>
<th>Mobile</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Goes Up</td>
<td>✔️</td>
<td>📡</td>
</tr>
<tr>
<td>Device Goes Down</td>
<td>🗯️</td>
<td>✔️</td>
</tr>
<tr>
<td>Heart Beat Lost</td>
<td>🗯️</td>
<td>📡</td>
</tr>
<tr>
<td>IP Change</td>
<td>🗯️</td>
<td>📡</td>
</tr>
</tbody>
</table>
Configured standard alerts will be consistent among all devices using these Alerts whereas the Custom Alerts are unique to the device for which they have been configured. You can choose whether to receive mobile app push notifications, emails to the account associated with Domotz Pro, or both.

<table>
<thead>
<tr>
<th>Device Event</th>
<th>Mobile</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Goes Up</td>
<td>✅</td>
<td></td>
</tr>
<tr>
<td>Device Goes Down</td>
<td>✅</td>
<td></td>
</tr>
<tr>
<td>Heart Beat Lost</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Change</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**TCP Services**

- No Service monitored for this device

Manage TCP services

**SNMP Sensors**

- No alerts on SNMP for this device

Configure an SNMP alert
4.6.3.2. Setting an Event on a TCP Service

The Custom Alerts tab allows you to configure Events for TCP Services as well as for SNMP Sensors. You can configure a maximum of 20 TCP services per device.
# Alerts

<table>
<thead>
<tr>
<th>Device Event</th>
<th>Mobile</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Goes Up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device Goes Down</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Heart Beat Lost</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Change</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## TCP Services

- No Service monitored for this device

Manage TCP services

## SNMP Sensors

<table>
<thead>
<tr>
<th>Mobile</th>
<th>Email</th>
</tr>
</thead>
</table>
Select the service you wish to monitor by tapping on the + button next to it. You will then see it appear in the Events configured for that device. You can then select to receive notifications via mobile push notification or email. To remove monitoring of the service, click on the red X next to the port number.
## Lexmark

### Online Status
- **IP Addr.:** 192.168.0.100
- **Changes:** 0 times

### Alerts

<table>
<thead>
<tr>
<th>Device Event</th>
<th>Mobile</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Goes Up</td>
<td>![Icon]</td>
<td>![Icon]</td>
</tr>
<tr>
<td>Device Goes Down</td>
<td>![Icon]</td>
<td>![Icon]</td>
</tr>
<tr>
<td>Heart Beat Lost</td>
<td>![Icon]</td>
<td>![Icon]</td>
</tr>
<tr>
<td>IP Change</td>
<td>![Icon]</td>
<td>![Icon]</td>
</tr>
</tbody>
</table>

### TCP Services

<table>
<thead>
<tr>
<th>Service</th>
<th>Mobile</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>70 • gopher</td>
<td>![Icon]</td>
<td>![Icon]</td>
</tr>
<tr>
<td>80 • http</td>
<td>![Icon]</td>
<td>![Icon]</td>
</tr>
</tbody>
</table>

**World Wide Web HTTP**
Above: An example of TCP email alert.
4.6.3.3. Setting an Event on a SNMP Sensor

To set an Event for an SNMP Sensor you should click on the "Configure an SNMP alert" button and you will get the following popup with a list of currently configured Sensors or the possibility to create a new sensor (will take you to the SNMP Configuration screen previously described):

![Choose a Sensor](image)

By selecting the Sensor you will be able to configure up to 3 Events per sensor. The type of alert will depend on whether the Sensor is a String or Numeric value.

**String:**
Alert Configuration

Battery Empty

Alert Behaviour
Send an alert if the String:

- contains empty
- is equal to
- does not contain
- is different from

Communication Channel
How do you want to be notified?

Mobile
Email

Add Alert

Numeric:
You will then see the configured Alerts appear in your list of Custom Alerts configured for your account:
<table>
<thead>
<tr>
<th>Alert Type</th>
<th>Mobile</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Goes Up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device Goes Down</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Heart Beat Lost</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Change</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP Services</td>
<td></td>
<td></td>
</tr>
<tr>
<td>70 · gopher</td>
<td></td>
<td></td>
</tr>
<tr>
<td>80 · http</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SNMP Sensors</td>
<td></td>
<td></td>
</tr>
<tr>
<td>black finished</td>
<td></td>
<td></td>
</tr>
<tr>
<td>black</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>is less than &quot;50&quot;</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
You can remove the Event by clicking on the red X or set the alert to be received via email or mobile push.

Events cannot be edited. The Event formula will be shown below the alert name in the Alerts tab but you can only delete an Event. If you want to change the formula a new Custom Event will need to be created.

Events are tied to the Agent and not the user, so if you add/remove an Events this will affect anyone who is monitoring this Agent as well. i.e. If you delete an SNMP Sensor Event, another user who was receiving alert messages for this Sensor will no longer receive them.

Above: SNMP email alert example
4.7. Collaboration*

This feature is only available to the Team Master and delegated Team Members

With the Collaboration feature the Agent owner (and any delegated Team Member) can grant network access to a trusted person, as long as this person has a Domotz account (each Agent can be shared with max 2 people). This should be used to share Agents outside of your organization. You can also create a Team of colleagues from the Domotz Portal (see @5.1. Team Management).

* = Available on Advanced and Premium Plans only
4.7.1. Invite a Guest

To give a trusted third party access to your Agent/network, simply tap on the Collaboration tile in the Agent Dashboard and you’ll see the following screen.
Agent Collaboration

Share your Domotz Pro Agent with people you trust.

Support Teams

---

Collaborators

Invite a Collaborator

You do not have any collaborator for this Agent.
Tap on Invite a Collaborator:
Invite a Domotz User you trust to access your Agent:

Domotz User Email Address

Invite

Cancel
Now simply fill in the persons email address (used as a Domotz Account) and tap on Send. You can only invite existing Domotz Account users.

You’ll see a Pending notification until the other person has accepted the invite.
Agent Collaboration

Share your Domotz Pro Agent with people you trust.

Support Teams

Domotz

Collaborators

Invite a Collaborator

Pending
The person you've invited will receive an email informing them that you've shared access to your Domotz Agent and they'll receive a notification in their app that they've been invited to access your Domotz Agent. Your Domotz Agent will show up in their app under Guest Agents and they can select it from the list of Agents and can access it just like any other Domotz Agent.

When the guests accept the invitation, his status will change from Pending to Accepted.
Agent Collaboration

Share your Domotz Pro Agent with people you trust.

Support Teams

domotz

Collaborators

Invite a Collaborator

Accepted

Accepted
4.7.2. Remove a Guest

To revoke access, simply tap on the small red X by the persons email address and you'll be asked if you want to remove the guest from your Agent.
Agent Collaboration

Share your Domotz Pro Agent with people you trust.

Do you want to remove this guest from your agent?

Yes, Remove

Cancel
Simply tap "Yes, Remove" and the person will have their access to your Agent revoked. An email will be automatically sent to inform the person that they can no longer access your Agent.
4.7.3. I am a Guest

If I am a guest of somebody else's Agent (I was invited and accepted), I can monitor that Agent just like any other Agent. In this case the Collaboration section will simply display the owner’s account, the Agent Name, and button to leave the collaboration.
The "Leave Agent" function is permanent and you will be unable to access the Agent any longer. The owner will need to invite you again to restart the collaboration.
4.8. Customer Management

Contains key details about the customer site. This will be used as reference contact information for the location where the Agent is set.
The physical address specified here will be used in the Multisite Dashboard (see section @4.1. The Multisite Dashboard).

⚠️ The Email address is required to enable the Violet Digital Support Client App. The Email address must be different from any email used to create Domotz Pro user accounts.

This section also contains a Note field. This can be used to keep track of some notes strictly related to the specific Agent/Network.
4.8.1. Client App

This is where you will enable the Violet Digital Support Client App for your customers and manage which devices you will allow them to see and which devices they can turn on/off or Internet block from Violet.

In the images below you will see the various phases of enabling the customer for Violet Digital Support:

1 – If an email address has not been added

2 – If the email address is available but the customer is not enabled for Violet

3 – The message screen you get, letting you know that the customer will receive an email to activate their account for Violet
Violet - Digital Support App
Violet access is disabled. Enable it for olga.nevzora.93@gmail.com

Important

Client app
Do you want to Disable the Client App for mail.com?

Ok, Disable
Cancel

Network Equipment

Visible  Power Control  Blockable
You can configure the visible, power controllable and blockable devices before inviting your customer into the Violed Digital Support App.

⚠️ Blocking feature is only available through Violet when the Domotz Agent is configured on a Domotz Box or on a Luxul Router. Devices discovered on the tagged VLANs configured on the Domotz Box cannot be blocked through Violet Digital Support App due to technical limitation to the implementation of the pausing functionality.
4.9. Reports and Logging

In the Reports and Logging Tile there are three screens that give you important information regarding the Agent. First is the Logging tab that will show you the last user events on the platform which include:

- Remote connections created to devices on the platform (See section @3.2. Installing on Other Supported Platforms )

- Enable/Disable of Agent alerts (see Alert Manager section @4.6. Alert Manager )

- Power actions on devices (through PDU, PoE or Software Reboot, Ruckus, Sonos and other supported devices reboots)

- Manually inserted Notes (Notes are added by clicking on the Add a Note button)

You can also generate pdf reports that cover activity from the past 30 days. This report will be sent to the email address associated with your Domotz account. You can also add up to 4 additional email addresses to the recipient list. Reports can be generated at any time and there are no limits on how many reports you generate.

You also have the option to export a list of all devices recognized on your network. This list is sent in an excel format.
Wednesday
1 August 2018

tz.com
08/01/2018 - 04:04 PM
Agent Alerts have been enabled

Agent Alerts have been disabled

Agent Alerts have been disabled

Tuesday
31 July 2018

itz.com
07/31/2018 - 03:59 PM

x64
Console Access SSH via port: 22
Reports & Logging

Logging  Monthly  Devices

Monthly Report
Last 30 days

Add an additional recipient

deemo-us@domotz.com

anyaddress@domotz.com

Send now ➡️
Device List

Export list of all devices on my network

Send via email: 

brent@domotz.com
4.10. Manufacturer Support

In collaboration with hardware manufacturers, Domotz has introduced the possibility to grant access to your Domotz Agent directly to a partnered manufacturer's support team via the Manufacturer Support Tile. This tile is only available if you have devices on your platform that are supported by our partner manufacturers.
The first screen will contain a list of partner manufacturers that are available to support your devices. The second is the message that you will receive when you enable the access. Please note that this access will expire 3 hours after it is granted so you should contact the Manufacturer’s support team before activating it.
5. USER PORTAL AND ADMINISTRATIVE FEATURES

The Domotz portal gives users all the available information and administrative features related to the account, associated Agents, licences and teams.

The following sections are available:

- **Web App**: opens the Domotz web application.

- **Team**: used for team management (visible to Team Masters only)

- **Subscriptions**: List of Agents installed and details about credits and subscription plans

- **Domotz Software**: use this section if you want to download versions of Domotz for your NAS or your Raspberry Pi and quick links to the mobile app stores

- **Account**: insert your account details here (for example billing info, company details, etc.)

- **Password**: link for changing account password

5.1. Team Management

Domotz Pro is designed to allow members of the same organization to access, in a controlled way, the same pool of Agents. The owner of the Domotz Pro account (Team Master) can create team members.
5.1.1. Team Master

A Team master is responsible for the administration of multiple networks. He can:

- Use all features of domotz
- Buy and extend licences
- Create and remove team members
- Share an Agent with people external to the team (see section 4.7. Collaboration*)

5.1.2. Team Members

A Team member can access any Agent set up by the Team (either Team Master or other Team Members).

He can:

- Access all features of an Agent, exactly like his Team Master
- Set-up his own set of alerts

A Team Member:

- Cannot buy or extend licences
- Cannot create or remove other team members
- Cannot share an Agent with people external to the team
- Cannot view or change Account Info

5.1.3. Field Operators

This is a special type of Team member. They have the same capabilities as normal Team Members, but only permissioned on certain agents assigned by the Team Master.

Field Operators can also configure new Agents, and by default, they will have access to these configured Agents.
5.1.4. Configuring Team Members

Team Masters (only) will have a Team section available in the user portal as shown in the screenshot below.

You can add a new Team Member or Field Operator by clicking on the Add member button. The email address specified will receive an email with a link to finalize the Domotz account providing a new password. If you don't see the incoming email please check your spam folder, or delete the member and create it again.

PLEASE NOTE: the email that you specify as Team Member or Field Operator can't be an already existing Domotz Account.

5.2. Subscription plans

In the latest version of Domotz Pro, the concept Subscription Plans (Standard/Advanced) have been introduced to give the customer more flexibility for their annual licenses as well as the possibility to add those premium features that they are interested in.
5.2.1. Your Agents

In this view you see a list of your current Agents including Version, Status and Expiration dates.

In case you use Domotz Credits billing type (see @2.1. Account billing type ), you can also see how many credits you have available and can purchase more credits and extend Agent expiration date by clicking on Extend.
### 5.2.1.1. Credits History*

*Only for users with Credits Account type (see [2.1. Account billing type](#))

Credits History will give you the complete history of credits purchased/used on your account:

![Credit History Table](image)

<table>
<thead>
<tr>
<th>Date</th>
<th>Action</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016 Feb 19</td>
<td>DemoZ Edmund Activation 'Violet' for agent 'Demo London Office'</td>
<td>0</td>
</tr>
<tr>
<td>2016 Feb 19</td>
<td>DemoZ Edmund Activation 'Extended Remote Connection' for agent 'Demo Lab'</td>
<td>-12</td>
</tr>
<tr>
<td>2016 Feb 19</td>
<td>DemoZ Edmund Activation 'Extended Remote Connection' for agent 'DemoZ London G...</td>
<td>0</td>
</tr>
<tr>
<td>2016 Feb 19</td>
<td>DemoZ Edmund Activation 'Extended Remote Connection' for agent 'DemoZ London G...</td>
<td>0</td>
</tr>
<tr>
<td>2016 Feb 19</td>
<td>Extended agent 'Demo Lab' expiration (and its elements) by 365 days</td>
<td>-12</td>
</tr>
<tr>
<td>2016 Feb 19</td>
<td>Operation Cost (reduced agent expiration)</td>
<td>-1</td>
</tr>
<tr>
<td>2016 Feb 19</td>
<td>Reduced agent 'Demo Lab' expiration by 365 days</td>
<td>46</td>
</tr>
<tr>
<td>2016 Feb 19</td>
<td>Extended agent 'Demo Lab' expiration (and its elements) by 365 days</td>
<td>-12</td>
</tr>
<tr>
<td>2016 Feb 19</td>
<td>DemoZ Edmund Activation 'Extended Remote Connection' for agent 'DemoZ London Office'</td>
<td>0</td>
</tr>
<tr>
<td>2016 Jan 12</td>
<td>Redeemed voucher code KAJL-HILJ-7KS</td>
<td>10</td>
</tr>
<tr>
<td>2016 Dec 11</td>
<td>Extended agent 'Demo Lab' expiration (and its elements) by 365 days</td>
<td>-12</td>
</tr>
</tbody>
</table>
5.2.2. Lite vs. Advanced vs. Premium

All the basic features (e.g. device status monitoring, network monitoring, alerting, remote connections) are included in the Lite plan and available for all the configured agents.

Some additional features (e.g. Extended Monitoring, Security Camera Integration etc) are optional and included in superior plans as follows. Domotz users can now upgrade to superior plans, in order to have more features.
The differences between plans are connected with:

- The **Lite Plan includes up to 300MB/month** of traffic while connected to a remote device using a custom **remote connection** (HTTP, HTTPS, SSH, Telnet, RDP). If you need more bandwidth per month, you have to upgrade to a larger plan. The **Advanced Plan includes up to 1GB/month** of traffic during remote connections. The **Premium Plan includes up to 10GB/month** of traffic during remote connections.

- The **Domotz Eyes** feature (for monitoring TCP Services, SNMP OID sensors) is not included in the Lite Plan. The **Advanced Plan** enables up to **100 Domotz Eyes** and a maximum frequency of **2 samples per hour**, to use for each Agent. Each TCP service or SNMP sensor counts as 1 Domotz Eye towards your plan. You can increase this amount depending on the number of SNMP sensors or TCP services you want to monitor, by upgrading to the **Premium Plan (1500 Domotz Eyes and a maximum frequency of 30 samples per hour)**.

- The **Wi-Fi Access Point Monitoring** is not available in the Lite Plan. With Wi-Fi Access Point Monitoring, you get simple, hassle-free monitoring of Ruckus Wi-Fi access points and connected clients. Additional manufacturers' products will be added in the future. Check @4.11.5 for details.

- With **Security Camera feature**, any Camera that is compliant with the ONVIF standard will be integrated in the monitoring system. It allows you to check Camera configuration and operation status, test Video output through Snapshots and Streaming integrated capability, or restart it when it becomes necessary.

- **Advanced Alerts** feature enables additional alerting options on your network devices and status. Be notified when your network performance decays or when one of your devices IP Address changes.

- With **Extended Monitoring**, you can monitor up to 5 devices or services anywhere on the web (website, off-site server, etc.), and up to 8 subnets on Layer 3, with a max of /24 network mask (modems, routers, VPN-connected networks, etc.). The feature is available only with the Advanced Plan.

- The **Public API** feature gives you access to our public APIs in order to create your own software taking advantages of the info retrieved from your Domotz Agent (list of devices, status, network health etc...). 500 calls per day with the Advanced Plan and 5,000 calls per day with the Premium Plan. The feature is not available on the Lite Plan.

### 5.2.3. Agent Management

In this section, you will be able to manage your agents:

- Activation status
- Agent Version
- Extend expiration
- Shorten expiration
- Rename Agents
5.2.3.1. Extend Agent

If you use subscription billing type (see @2.1. Account billing type ), Domotz will bill automatically every month, using a valid credit card, based on the number of installed Domotz Agents.

In case you use Credits billing type (see @2.1. Account billing type ) you can decide how long to extend your expiration date up to a maximum of 36 months. The credits required will be deducted from the total number of available credits. When an option is selected you will see the new calculated expiration date.
5.2.3.2. Redeem Credits*

*Only for users with Credits Account type (see 2.1. Account billing type)

You can also decide to shorten the expiration date and return the unused credits back to your account. This is done by clicking on the Shorten expiration date link in the Edit screen for the Agent. This will remove all credits and the new expiration date will be when the current credit is scheduled to expire.

There is an operational charge of 1 credit to perform this operation
5.2.3.3. Edit Agent

In this section there are additional information about the selected Agent such as activation date, package version, local IP address, MAC address of the physical device binded to the Agent. Agent's name can be changed from this section.

5.2.3.4. Delete Agent

From the Edit section you can also delete the Agent from your list. Delete Agent will remove all the data related to an Agent. It can be useful if you want to move a box from a location to another, to get rid of previous data. Please be advised that:

- A delete operation is only possible when the Agent is disconnected.
- A delete operation will permanently remove all data related to an Agent.

In order to activate a new agent after a delete you need to follow the steps for starting the Agent for the first time indicated in section 3. INSTALLING AND STARTING THE DOMOTZ AGENT.
5.2.3.5. Clean up Agent Data

From the Edit section you can also Clean up the Agent data. All the configuration made inside the Agent, together with the scanned info will be deleted. The Agent name and subscription status will remain as it is.

---

5.3. Get Domotz Hardware

If you’d like to install the Domotz Agent on a NAS, Raspberry Pi or Linux Debian, there is a link to the Domotz Software page inside portal.domotz.com.

If you’d like to buy a Domotz box you can rely on our distribution partners; you can find the updated list here.

5.4. Account Management

This is the section that you will use to change/update your Account details as well as defining the default behavior for all the Agents (e.g. policy for automatic assignment of devices as ‘Important’) and related Alerts.

Furthermore, in this section
5.4.1. Account Info

In this section, you can configure your billing account details (invoice address, type of account, name, country, etc).

In case you use Subscription billing type (see 2.1. Account billing type), you must also fill your payment method information.
5.4.1.1. Invoice information*

*Only for Subscription Account billing type (check @2.1. Account billing type).

Once you’ve specified payment method, you will be able to control the Invoices information. It includes Invoices History with their dates and payments values. You can easily download any Invoice in PDF.

There you can also find Estimated Upcoming Invoice information about the next payment. If you click on ?, you will see its details with Subtotal, date and the Plan you use.
5.4.2. Branding

This tab allows you to configure your contact info and upload a company logo for display in the Violet customer app and in reports generated.
5.4.3. Settings

This tab allows you to configure the default behavior of the Domotz agents (this settings will be applied to all your agents).
5.4.3.1. Daily Alert Digest

This section allows you to configure the Alert Digest feature, which will collect notifications and alerts and send them in an email. **Daily Alert Digests** can be configured one of two ways:

- **One time per Day**: All email alerts currently sent in real-time, will be sent in a summary email once a day.

- **Time Window**: All notifications and alerts retrieved during the configured time are collected and sent at the end of the time window.
DOMOTZ DAILY ALERT DIGEST

Enabling this setting Domotz will collect notifications and alerts, currently sent in real-time, and send them in a summary email.

The time will reflect your current timezone: Europe/Rome

**Behaviour**

**Disabled**
Send all triggered events in real-time via email

**One Time per Day**
It collects all the notifications and alerts retrieved during the previous 24 hours and it sends them at a specified time of the day.

Send me the Alert Digest everyday at:

- Hours: 8
- Minutes: 30
- AM/PM: PM

**Time Window**
It collects all the notifications and alerts retrieved during the configured time and sends them at the end time window.

- **Start collecting email alerts**
  - Hours: 7
  - Minutes: 30
  - AM/PM: PM

- **Send collected email alerts**
  - Hours: 8
  - Minutes: 30
  - AM/PM: PM

[Buttons: Cancel, Save]
5.4.3.2. Important Device Classification

The following account-wide options are available and will apply to all account Agents:

- **Disabled**: Installer must manually assign devices as Important or not. By default all devices will be assigned ‘Indifferent’

- **Always use Domotz Classification**: Domotz will always assign network newly discovered devices like routers, switches, etc., as Important Devices based on their discovery

- **Use Domotz classification once**: Domotz will assign newly discovered devices as Important Devices only during initial discovery. Devices that are discovered later will not be automatically assigned as Important.

**AUTOMATIC IMPORTANT DEVICES CLASSIFICATION**

Automatic Important Devices classification allow you to decide how the device will be marked as important.

**Behaviour**

**Disabled**
You have to mark important devices manually

**Always use Domotz classification**
Always let Domotz decide which devices are important

**Use Domotz classification once**
Domotz will classify important devices at the first scan only

[Buttons: Cancel, Save]
5.4.3.3. D-Tools

Save time and effort by importing your D-Tools project for fast setup and configuration of the Domotz Agent.

The D-Tools tile will appear in your Agents dashboard after Domotz Pro app restart.

**D-TOOLS**

Save time and effort by importing your D-Tools project for fast setup and configuration of the Domotz Agent.

The D-Tools tile will appear in your Agents dashboard after Domotz Pro app restart.

**Behaviour**

**Disabled**

D-Tools integration not active

**Enabled**

Save time and effort by importing your D-Tools project
5.4.4. Two-Factor Authentication

This tab allows you to configure Two-Factor Authentication to add more security to your Domotz account.

Protect your account with Two-Factor Authentication

This feature will add more security authenticating your Domotz Services.

Two-Factor Authentication

Will be applied to your account

When enabling the 2FA – via toggle button – the user is requested to enter his password and confirm.

TWO-FACTOR AUTHENTICATION

To activate it, please enter your Domotz account password

Enter your Password

[Cancel] [Next]
After this step, the 2FA token (QR Code) is generated and needs to be saved and used inside an external application like Google Authenticator or Microsoft Authenticator to generate fresh Domotz login codes.
While acknowledging the token saving, the user can chose to flag the option “Remember me”, which allows to trust the device and skip the authentication.

Two-Factor Authentication Token

Please save this token and use it inside an external application like Google Authenticator or Microsoft Authenticator to generate fresh Domotz login codes.

I've securely saved the token

Continue
At the 2FA activation process completion, the page displays:

- The list of Trusted devices (all devices that do not require the two-step authentication at login moment, if the "Remember me" option has been selected). By clicking the bin icon, the user can remove one device from the list.

- The code being used

- The button to renew the security token (the previous token will be disabled and the user will be prompted to insert a new code).
The user can disable the 2FA at any time (by using the toggle button and inserting his password).

The Team Masters can check whether or not, his team members have configured the 2FA for their accounts, in the Team section available in the user portal.
5.4.5. Domotz PRO Public API*

The Domotz Pro Public API (RESTful) provides developers with an easy and comprehensive way to integrate third party applications.

An application programming interface key (API Key) is the code required in your own application to execute RESTful API calls against the Domotz Cloud, allowing you to retrieve and manage your own account and your Domotz Agents.

You will need at least one API Key to access to your data through the Domotz Pro Public API.

To create API Key you need to visit the Portal, under Account section select the API Key tab: click on create a API Key, fill the password of your account to unlock the service, give a name to a new API Key.
Now new API key is created! You can see its code and Endpoint.

⚠️ Don't forget to copy the API Key code and save it in a safe place, clicking on Copy. Please, note that after closing the popup you will not be able to do see the key anymore.
You will see the created API key and control the number of calls made during the last 24 hours. The total number of API calls which can be executed in 24 hours is a function of the number of configured Agents on the Advanced plan (or higher). For more details, visit the Portal under Account and API Key section.

You can create multiple API keys if you need to.

The API Key can be used to retrieve general information about all the configured Agents. However, details of the Agents, list of devices and other Agent related information are only available through the Public API on Agents configured on an Advanced plan (or higher).

Please refer to the Domotz PRO Public API documentation for additional information on their usage: https://portal.domotz.com/developers/
5.4.6. Utility Integration

Within this section, it is possible to enable the D-Tools integration to import D-Tools project for fast setup and configuration of the Domotz Agent.

As soon as D-Tools is activated, the D-Tools tile will appear in the Agents dashboard.
6. APPENDIX A - DOMOTZ AGENT LOCAL SETTINGS

The Domotz Agent has a built-in http service running on port 3000. You access the built-in service by visiting \texttt{http://<ipaddress>:3000} in your browser. This will allow you to see details and access various functions including:

- **Agent Info** – Details about the Agent configured on the device

- **Network Info** – Details and network configuration (see below)

- **Route Analysis** – Allows you to run the same Route Analysis test that is available in the Agent

- **Speed Test** – Allows you to run the same speed test that is available in the Agent

- **Web App** – Opens the Domotz Pro Web App

6.1. Resuming an Agent after changing Agent hardware

PLEASE, CONTACT DOMOTZ SUPPORT BEFORE YOU CHANGE THE HARDWARE

If you ever need to change the hardware that your Agent is running on and don’t want to lose your configuration you should contact Domotz Support at support@domotz.com who will give you instructions. Once these instructions have been followed you will be able to connect to the http portal and you will see a button to ‘Resume Agent’. This will allow you to move your current configuration over to the new hardware without losing it.

Note: It is very important that you do not delete the Agent from the Domotz Web Portal before moving to the new hardware or you will lose all your details.

6.2. VLAN and Network Interface Configuration

(available only on Domotz Hardware)

These details are meant for users who have multiple VLANs or want to configure the Domotz Hardware on a Static IP and are already aware of related configuration and procedures. For further details and step-by-step guides on how to configure VLANs on switches and Domotz Agents, the user should refer to detailed guides (for example, please refer to: \texttt{http://www.sbprojects.com/projects/raspberrypi/vlan.php}).

In order to allow Domotz to discover and monitor devices on two or more VLANs, the user should configure both the switch and the Domotz Agent for multiple VLANs:
6.2.1. **Switch Configuration**

The interface port of the switch which will be used to connect the Domotz Box/Pi, should be configured:

- in Access mode / Untagged for the main interface used by the Domotz Box/Pi to communicate with the gateway (e.g. eth0).
- in Trunk 802.1q mode / Tagged for the additional VLANs to be monitored (e.g. the eth0.10 used for lan 10)
- Please refer to your specific switch/model guide on how to configure Trunk 802.1q and Access mode (Untagged/Tagged) for the port.
6.2.2. Domotz Agent Configuration

You can find all the necessary information for configuring the Domotz Box to monitor multiple VLANs or to configure the Domotz Box with a Static IP in the Network Info section of the http portal.

Network Info:

When you press the Edit button you will see:

Switching the DHCP toggle to Off you will be allowed to specify Static IP and non-DHCP based subnet mask, Gateway and DNS servers.

When pressing the VLAN Config button you will see the following screen which will assist you in this configuration.
For every VLAN that you want to add, you need to specify:

- the Identification number of the additional VLAN
- the Static IP address of the Network Interface of the Domotz Box on the additional VLAN
- the subnet mask on the additional VLAN

Make sure that the IP Address on the additional VLAN is not in use, and it is not the */.*.*.0 of that subnet (e.g. do NOT use IP addresses like 172.16.10.0).

⚠️ Devices discovered on the tagged VLANs cannot be blocked/paused through Violet - Customer Facing App (Violet Digital Support Client App) due to technical limitation to the implementation of the pausing functionality. Domotz recommends configuring the Domotz Box on the same subnet as primary interface where devices which might be blocked through Violet Digital Support Client App are expected to be.
7. APPENDIX B - ACCESSING THE DOMOTZ AGENT

Normally, we do not give users the root password for accessing Domotz Agents.

This is to ensure that the domotz agent behaviour is not altered. Normally, root access is not needed unless you need to make non-standard configuration changes suggested by Domotz Support and following their instructions.

For security reasons, the password is different for each Agent. If, for any reason, you need to access a Domotz Agent, you should request the password details from our support team by specifying the MAC address of the Agent.

Please, be aware that if any changes are made to the Domotz Agent configuration, we cannot guarantee future support on the Domotz Agent’s functionality.