



WISE-PaaS

AIoT Solutions & Marketplace

IoT Device Operation Management

English v-1.0.10



Revision History

Date	Version	Author	Reviewer	Description
2019-12-16	1.0.5	Sephiroth.Wang	Rison.Yeh	First version released Section 1, 2, 3, 4.4, 6, 7
2019-12-23	1.0.5	Alex.Shao	Sephiroth.Wang	Section 4.1, 4.2, 4.3, 4.5
2019-12-27	1.0.5	Terry.Lu	Sephiroth.Wang	Section 5.1
2020-01-08	1.0.5	Iris.Pan	Sephiroth.Wang	Section 5.2
2020-01-10	1.0.5	Wunhuei.Liou	Sephiroth.Wang	Section 5.3
2020-02-03	1.0.6	Sephiroth.Wang	Rison.Yeh	Section 6.7, 6.8, 6.9
2020-02-10	1.0.6	MingWei.Tasi	Sephiroth.Wang	Section 4.6
2020-02-12	1.0.6	Sephiroth.Wang	Rison.Yeh	Section 6.10
2020-03-11	1.0.6	Scott.Chang	Sephiroth.Wang	Section 6.3
2020-03-25	1.0.7	Sephiroth.Wang	Rison.Yeh	Add Section 6.8, and move 6.8-> 6.9, 6.9->6.10 Add Section 7.2
2020-04-01	1.0.8	Sephiroth.Wang	Rison.Yeh	Change wallpaper on first page Add new log mechanism on Section 6.6 Add Section 4.7 for device provisioning.
2020-04-06	1.0.9	Alex.Shao	Sephiroth.Wang	Section 2.1.4
2020-04-10	1.0.10	Daniel.Hung	Sephiroth.Wang	Add plugin deployment on RISC (Section 5.1.4)

Table of Contents

Revision History	1
Table of Contents	2
1. Introduction.....	6
1.1 Feature Highlights	8
1.2 DeviceOn Server Versions	12
1.2.1 WISE-PaaS/EnSaaS (Cloud)	12
1.2.2 Azure PaaS, Kubernetes (Cloud)	13
1.2.3 Standalone, VM (Cloud).....	13
1.2.4 Data Service Server for Private Cloud.....	14
1.3 DeviceOn Agent Versions	16
1.3.1 WISE-Agent (Client).....	16
1.4 Security	17
1.4.1 Role-Based Access Control (RBAC)	17
1.4.2 SSL Encryption	17
1.4.3 Security Scan.....	17
2. Getting Started	18
2.1 DeviceOn Cloud Installation.....	18
2.1.1 Subscribe to DeviceOn from WISE-PaaS/EnSaaS.....	18
2.1.2 Redeem DeviceOn AKS from WISE-PaaS Marketplace.....	19
2.1.3 Setup DeviceOn Standalone Version (On-premise)	23
2.1.4 Setup DeviceOn Standalone Version for Ubuntu Linux (On-premise)	31
2.2 DeviceOn Client Installation & Device Onboarding	33
3. DeviceOn User Interface & Functions	42

3.1	DeviceOn Server (Standalone).....	42
3.1.1	Standalone Server Control	42
3.1.2	Background Watchdog Service	46
3.2	DeviceOn WISE-Agent	46
3.2.1	WISE-Agent Connection	46
3.2.2	WISE-Agent Services.....	51
3.3	DeviceOn User Interface.....	52
3.3.1	DeviceOn Overview	54
3.3.2	Device Management	57
3.3.3	Account Management	69
3.3.4	Event Logs.....	72
3.3.5	OTA (Remote Provisioning)	74
3.3.6	System Configuration.....	86
3.3.7	Documents.....	100
4.	Hands-On LABs	101
4.1	How to Create a Real-time Action into Overview	101
4.1.1	Prerequisite.....	101
4.1.2	Step-by-Step	102
4.2	How to Remote Software Provisioning via OTA	104
4.2.1	Prerequisite.....	105
4.2.2	Step-by-Step	105
4.3	How to Set a Device Threshold and Event Notify Services	109
4.3.1	Prerequisite.....	110
4.3.2	Steps to Set Event Notification Service – Email	110
4.3.3	Steps to Set Event Notification Service – LINE	112
4.3.4	Steps to Set Event Notification Service – WeChat	115
4.3.5	Other Event Notification Services – SMS/WhatsApp.....	119

4.3.6	Steps to Set Thresholds to a Device	119
4.4	How to Visualize Device Data via Grafana Dashboard	123
4.4.1	Prerequisite.....	123
4.4.2	Step-by-Step	123
4.5	How to Enable/Disable Windows Lockdown Features	126
4.5.1	Prerequisite.....	126
4.5.2	Step-by-Step	127
4.6	How to Manage DeviceOn on AKS	128
4.6.1	Prerequisite.....	129
4.6.2	Steps to Upgrade DeviceOn.....	129
4.6.3	Step to Monitor Container Healthy and Status	129
4.6.4	Steps to Expose Database/RabbitMQ to Access.....	133
4.6.5	Steps to Deploy DeviceOn to AKS by Manual.....	134
4.7	How to Batch Provision to Your Devices.....	138
4.7.1	Prerequisite.....	139
4.7.2	Steps to Local Provisioning.....	139
4.7.1	Troubleshooting	143
5.	DeviceOn Development Guide	144
5.1	WISE-Agent Plugin Development	144
5.1.1	WISE-Agent Architecture	145
5.1.2	Prerequisite.....	146
5.1.3	Develop a Plugin on Windows Environment.....	146
5.1.4	Develop a Plugin on Linux Environment.....	151
5.2	DeviceOn UI Plugin Development.....	154
5.2.1	Prerequisite.....	154
5.2.2	Environment Setup	154
5.2.3	Develop a Sample Add-in	156

5.2.4	Develop an Add-in to Access DeviceOn API	160
5.3	Customization DeviceOn Logo, Theme and Menu.....	163
5.3.1	Prerequisite.....	163
5.3.2	Steps to Change Logo via Web UI	163
5.3.3	Steps to Change Theme via Web UI	165
5.3.4	Steps to Adjust Menu Items via Web UI	167
5.3.5	Introduce Advanced Configuration	168
5.3.6	Steps to Change Logo via Advanced Configuration	170
5.3.7	Steps to Change Theme, Color via Advanced Configuration.....	172
5.3.8	Steps to Adjust Menu Items via Advanced Configuration	173
6.	FAQ	175
6.1	Why Some of Devices Cannot Power On.....	175
6.2	Why Cannot Remote Control via KVM (Remote Desktop)	179
6.3	Why Cannot Screenshot and Always Show Device “No Login”	180
6.4	How the Device Data Flow and Debug from Edge to Cloud	186
6.5	How to Enable and Disable plugins on WISE-Agent	187
6.6	How to Enable and Adjust WISE-Agent Log Levels	188
6.7	How to Change DeviceOn Server Address (Standalone).....	191
6.8	How to Migrate/Transfer EdgeSense Database to DeviceOn (WISE-PaaS/EnSaaS)	192
6.9	How Does DeviceOn Interact with AI and Machine Learning	197
6.10	What IS WISE-PaaS Alliance, and How Does One Join.....	198
6.11	What ARE WISE-Points, and How They Used	198
7.	Reference	198
7.1	User Permission	198
7.2	Retrieve My Azure Account Information	202
7.2.1	Method 1 – Create & Get Information on Azure Portal	202
7.2.2	Method 2 – Create via Azure CLI (Command-line Tool).....	207

1. Introduction

A surge in market demand for Industrial IoT products has rapidly increased the number of connected devices that are currently deployed and managed across different locations. It is essential to effectively manage, monitor, and control thousands of connected devices while ensuring uninterrupted service. Devices must work properly and securely after they have been deployed - without requiring frequent visits from service technicians. Customers require secure access to their devices in order to detect, troubleshoot, and undertake time-critical actions.



With Advantech's WISE-PaaS/DeviceOn, users can swiftly utilize onboard devices, efficiently monitor device health status, and securely send software and firmware updates over-the-air (OTA) on-site and remotely at scale.

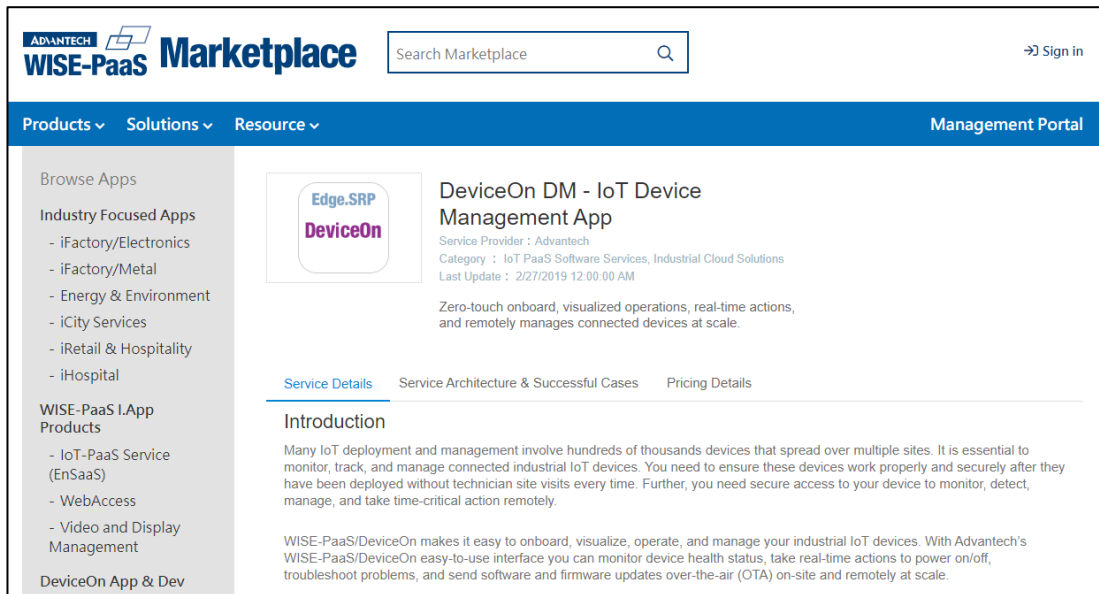
Advantech's brand-new designed IoT device operations and management App solution gives users a transformational plug-and-play experience. Beginning with onboarding devices, [WISE-](#)

[PaaS/DeviceOn](#)'s zero-touch IoT tech seamlessly registers Advantech hardware systems with identity security and field site settings. A fast and simple setup helps provide instant intelligent edge onboarding, data acquisition, and status visualization at the device operations center. Power on/off, troubleshooting, and mission-critical actions are available at the tap of a button for quick and easy access. OTA software updates itself securely by sending software patch, firmware, software, and configuration updates through batch provisioning. The App is designed to ensure maximum efficiency in IoT device operations and management.



Power up your IoT devices with this hardware and software integrated solution. Get the most out of the WISE-PaaS/DeviceOn's features with predictive device maintenance like IPC HDD lifecycle prediction, analytics-based dashboard and automated event alerts. In bringing artificial intelligence to your IoT needs, Advantech delivers improved risk management, faster daily operations, and better device performance while improving business value and intelligence through the extraction of big data.

WISE-PaaS/DeviceOn is compatible with all Advantech hardware systems and works on popular platforms and services like the WISE-PaaS public/private cloud, Microsoft Azure, VM on-premise, and Kubernetes. [Get your WISE-PaaS/DeviceOn version on the WISE-PaaS Marketplace](#) and kick-start your new and improved device operations and management experience.



1.1 Feature Highlights

- **Device Connectivity & Monitoring**

With more and more IoT devices in the field and the need for remote management and monitoring of those devices, the most important thing is how to achieve secure and fast onboarding to WISE-PaaS/DeviceOn. There are two mechanisms provided, one is **Zero-touch**, where the user does not need to configure any of their devices. Just power-on the devices and they will connect to DeviceOn automatically. However, there is the limitation that the device's network must have the ability to directly connect to the public cloud. The second mechanism is called **"One-time configuration, automated onboarding"**. Based on this mechanism, the user only sets up one device to connect to the cloud and uses this device to search and bring others to the cloud. Furthermore, this scenario supports public/private provisioning if there is no public cloud connection due to environmental limitations.

DeviceOn supports general real-time monitoring of device health that includes hard disk, CPU, memory, network load and provides various alerting mechanisms. Additional proprietary sensors such as CO2, battery monitoring or various proprietary protocols can be supported through design-in services.

- **Bulk Management & Maintenance**

For management and real-time control of a group of devices, DeviceOn offers a default overview with one-click actions, such as "One-Click Power On", "One-Click Protection", "One-Click Recovery", "One-Click Turn off backlight" and so on. Operators do not need to spend lots

of effort to setup devices one by one, but can simply “One-Click” maintain their field devices. The following actions are supported by DeviceOn:

- Power Saving
 - Power On/Off, Reboot
 - *****Backlight On/Off
- Security
 - Protection On/Off
 - System Backup/Recovery
 - ******USB Lock/Unlock
Block USB drives and removable disks (Not supported on “Administrator” user)
 - ******Keyboard Lock/Unlock
Block function key, such as “ALT”, “CTRL”, and windows key.
 - ******Touch Gesture Lock/Unlock (supported with capacitive touch panel only)
 - ******Touch Lock/Unlock
- System
 - Screenshot
 - Audio Mute/Unmute
 - *****Watchdog Enable/Disable (Default reset time is 60s)
Reboots the system if it becomes unresponsive, to avoid hanging at “BSoD” (Blue Screen of Death) or similar situations
 - ******Notification Block/Unblock
Disable windows notification from applications and other sources
 - ******UWF Enable/Disable
Helps to protect your drives by intercepting and redirecting any writes to the drive (app installation, settings changes, saved data) to a virtual overlay

Above actions prefixed with ‘*’ require the respective Advantech SUSI Driver and actions prefixed with ‘**’ require following operating systems:

- **Windows 10 Enterprise LTSC 2019 (LTSC)**
- **Windows 10 Enterprise 2016 LTSC (LTSC)**

- **Device Remote Control**

- **Device Diagnostics**

Provides remote control mechanism, such as KVM (Remote Keyboard-Video-Mouse) for real-time remote desktop access to the devices. The screenshot functionality allows to capture the device’s current screen output for potential troubleshooting. Another feature is access to Windows or Linux shells, for example in order to quickly retrieve

network status via ipconfig/ifconfig, netstat to dump socket/TCP/UDP information, without having to use the full graphical user interface.

- **OTA (Over the Air)**

OTA supports an open framework, which can easily integrate 3rd party storage, such as FTP and cloud solutions (Azure Blob, AWS S3, AliYun, Openstack Swift). It does not only support remote update and deployment, but supports automatic update from server side as well as scheduled updates that get triggered from the agent side. Scheduling helps to avoid peak network traffic times and allows implementation of download and deployment schemes that reduce potential impact to a minimum.

The framework supports upgrade package backups as well as rollback to the previous version when required.

Scripting support (shell/batch) allows to implement flexible update mechanisms.

- **Power Management**

Sets the power on/off schedule for remotely located devices; the schedule can be set on a daily, weekly, monthly, or yearly basis. Supports Agent mode enable powering on across networks.

- **Protection Management**

DeviceOn system protection is powered by McAfee, providing white list protection against unauthorized application execution, and also sending warnings of any unauthorized activities.

- **Backup & Recovery**

DeviceOn system recovery is powered by Acronis, providing hot backup and scheduled backup, and also one-click recovery.

- **Simplified Operation & Support**

In general, the utmost goal of system integrators or IoT device operation managers is meeting service level KPIs without having to spend huge efforts or daily maintenance. Once hardware fails, it results in a serious increase in operation cost. DeviceOn provides rule-based management and implements HDD failure prediction. If a managed device shows any anomaly on a specific component or sensor, DeviceOn can send alert messages through **email** or **SMS**,

or can optionally integrate with social media services such as **LINE, WeChat**. The DeviceOn overview shows overall status, upcoming schedule, top 5 potential risk devices as well as device location at a glance.

There is a summary for these feature highlights on different operation system and hardware requirement.

	DeviceOn Feature Highlight	Windows 7, 8, 10	Windows 10 LTSC, LTSB	Ubuntu 16.04 x64	Linux on RISC (Yocto)	Android on RISC
Standard Offering	Role-Based Access Control	●	●	●	●	●
	Device Zero-touch Onboarding	●	●	●	●	●
	Device & Device Group Management	●	●	●	●	●
	Device Threshold Detection (Rule-based Engine)	●	●	●	●	●
	Notification & Alert Service (Mail, SMS, LINE, WeChat)	●	●	●	●	●
	Device Realtime & Historical Data Monitoring	●	●	●	●	●
	OTA, Software, Firmware Provisioning	●	●	●	●	●
	Power Control, Terminal, Screenshot, Remote Desktop	●	●	●	◐	◐
	Backup/Recovery, Protection	●	●	●		
	Device Data with Zero-Downtime	●	●	●	●	●
	Operation Management (Batch Control & Statistical Analysis)	●	●	●	●	●
	Audio Volume Control	●	●			
Advantech Hardware Support	Hardware Watchdog Monitoring	●	●	●		
	Brightness & Backlight Control	●	●	●	●	●
	Hardware Sensor Monitoring	●	●	●	◐	◐
	BIOS Update	●	●	●		
Windows 10 Lockdown Features	USB Drive Block		●			
	Keyboard Lock & Filter		●			
	Touch Screen & Gesture Lock		●			
	Windows Notification Block		●			
	UWF Protection		●			

1.2 DeviceOn Server Versions

DeviceOn is based on a microservice design, each component is stateless and supports multiple instances for scale up. This results in heavily simplified deployment to WISE-PaaS (Cloud Foundry), Azure PaaS, standalone virtual machines or Kubernetes. Both public cloud and private cloud (on-premise) deployments are supported. This chapter provides an introduction and provides a summary of requirements for those scenarios. The container version of DeviceOn starts from version number **v-1.1.x** (WISE-PaaS/Azure Kubernetes), while the standalone version starts from **v-4.1.x**. The standalone version comprises of IoT Hub, database (PostgreSQL and MongoDB), Dashboard (Grafana), Webservices (Tomcat) and DeviceOn core applications.

1.2.1 WISE-PaaS/EnSaaS (Cloud)

The WISE-PaaS/EnSaaS version consists of three containers as listed below. In this scenario DeviceOn requires 1408 MB of RAM at least.

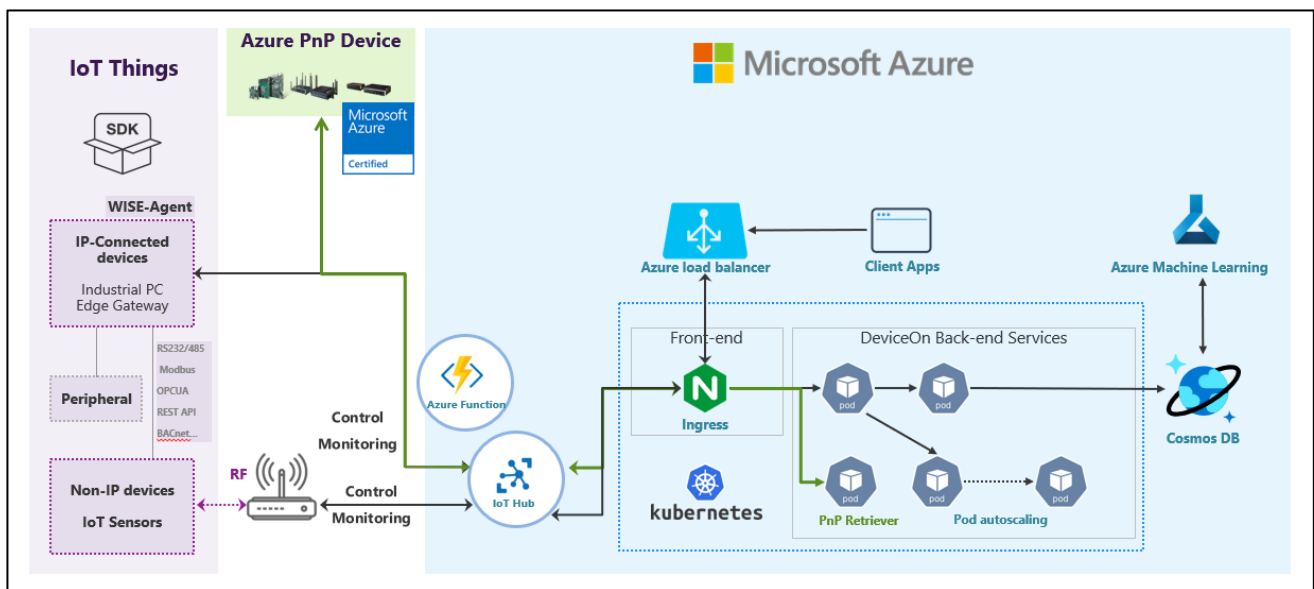
Application Name	Version	Memory Used	Purpose
deviceon-worker-1.1.x	v-1.1.x	384MB	Worker that processes device messages, status, notification, scheduling etc.
portal-deviceon-1.1.x	v-1.1.x	768MB	Provides the DeviceOn web interface for remote control and monitoring.
provisioning-worker-1.1.x	v-1.1.x	256MB	Worker that provisions devices with configuration, software, firmware etc.

≡ Organizations / AdvEIoT / DeviceOn			
Organization	AdvEIoT ▾	Space	DeviceOn ▾
Application List	Service Instance List	Route List	Usage
Name ▲	Package State	State	
○ <u>deviceon-worker-1.1.39</u>	STAGED		
○ <u>portal-deviceon-1.1.39</u>	STAGED		
○ <u>provisioning-worker-1.1.39</u>	STAGED		

1.2.2 Azure PaaS, Kubernetes (Cloud)

The Azure Kubernetes Service (AKS) makes it easy to deploy a managed Kubernetes cluster to Azure. AKS reduces the complexity and operational overhead of managing Kubernetes by offloading much of that responsibility to Azure. Azure handles critical tasks like health monitoring and maintenance for those Kubernetes services.

Deploying DeviceOn on the Azure Kubernetes Service is easy and with just a few steps, containers or nodes can be scaled up to manage thousands of devices. Moreover, DeviceOn can leverage the Azure IoT Hub and Cosmos DB for Azure native security and performance. Since the data is already stored on the Azure cloud, it is much easier to leverage the Azure ecosystem – for example using the provided data for Azure Machine Learning. DeviceOn can be deployed to Azure Kubernetes directly from the WISE-PaaS/Marketplace.



1.2.3 Standalone, VM (Cloud)

The standalone version provides all packages of the DeviceOn software in one installer package, including RabbitMQ as a message broker, MongoDB, PostgreSQL as databases, Grafana for visualization, Tomcat for web services, and a watchdog service that protects DeviceOn core components from crashing or becoming unresponsive.

This section specifies the minimum hardware requirements for DeviceOn Cloud (Standalone) and the operating systems on which DeviceOn is supported. In general, the better the hardware configuration of your computer, the better your experience with DeviceOn will be. To achieve a more satisfying experience with DeviceOn, particularly in terms of the client software, it is highly recommended that your system be substantially better than the minimum requirements specified in the following

sections. This is particularly true if running server software locally on the same system as the client software.

Attention to the following areas can make a significant improvement to your overall user experience and enjoyment of the software:

- Memory - the more RAM your computer has, the better.
- CPU speed - the faster, the better.
- Hard Drive - the larger, the better.

General Operation Systems and Recommendations:

- ✓ **Windows Server 2008 R2 64-bit** ([KB2999226 Required](#))
- ✓ **Windows Server 2012 R2 Standard 64-bit** ([KB2919442](#), [KB2919355](#), [KB2999226 Required](#))
- ✓ **Windows Server 2012 R2 Datacenter 64-bit** ([KB2999226 Required](#))
- ✓ **Windows Server 2016/2019 64-bits**

Reserve Port for DeviceOn Server Used

	Name & Description	Inbound Port
1	DeviceOn HTTP, HTTPs Web Services	80, 443 [Depends on Installation]
2	DeviceOn Dashboard (Grafana)	3000 [Depends on Installation]
3	Message Broker (RabbitMQ) MQTT, MQTTs	1883, 8883
4	Message Broker (RabbitMQ) AMQP, AMQPs	5671, 5672
5	Message Broker (RabbitMQ) Management Console	15672
6	Repeater for Remote Desktop	5501
7	Websockify for Remote Desktop	6083 ~ 6183
8	Database for MongoDB	27017
9	Database for PostgreSQL	5432

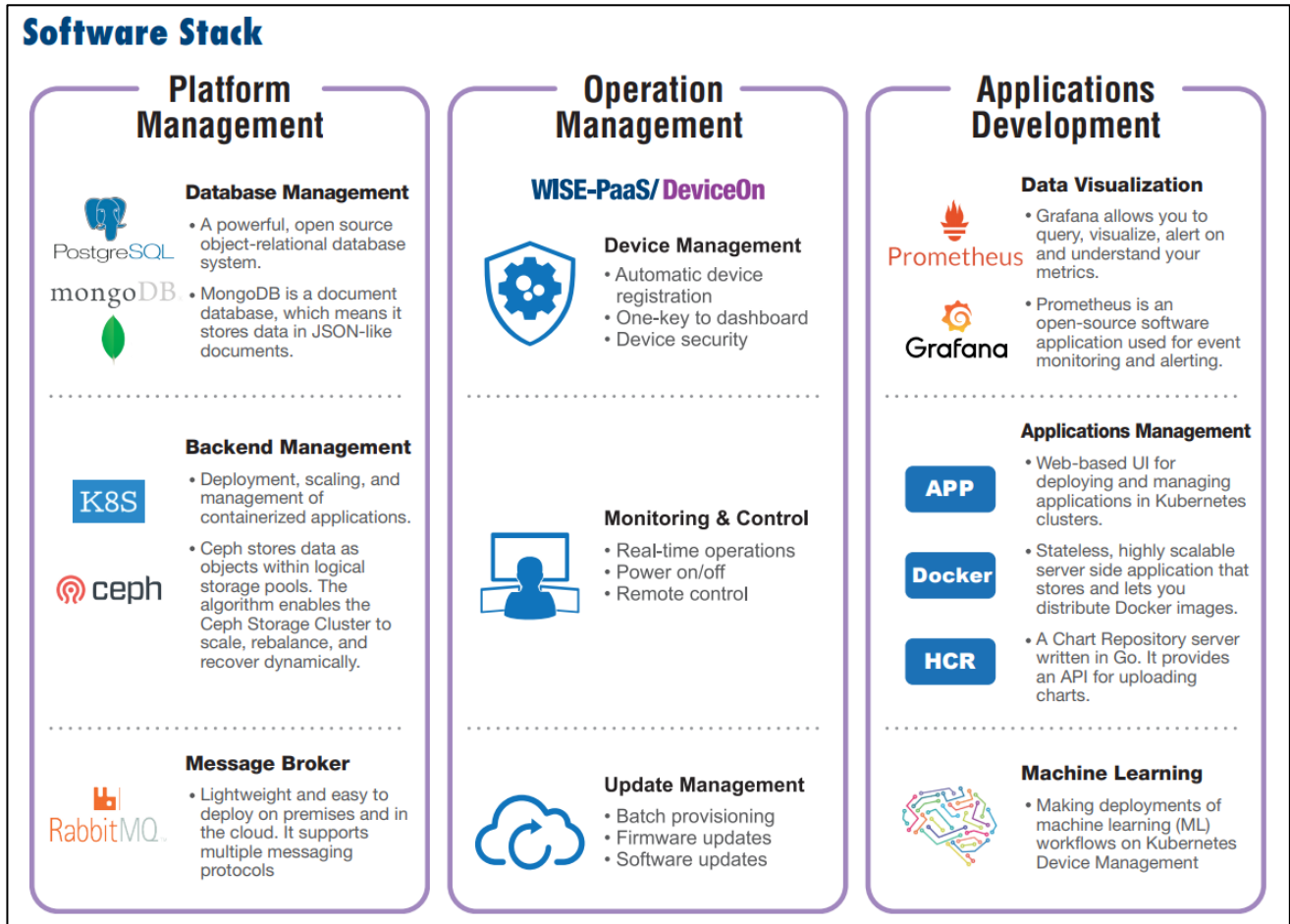
Hardware Minimum Requirements:

- ✓ **Intel® Core™ i5 2.3 GHz CPU and at least 8GB of RAM**
- ✓ **25 GB root partition for the system**
- ✓ **100 GB data storage partition (for documents and indexing)**

1.2.4 Data Service Server for Private Cloud

For accelerated IoT application deployment, Advantech offers the Data Service Server [EIS-S230](#) as a stable and reliable all-in-one solution for your back-end data service or light private cloud. It is built around an Intel Xeon or Core i7 CPU to offer best in class computing performance for data services. Moreover, EIS-S230 comes preinstalled with Kubernetes to support micro-services, as well as

complete back-end software components including RabbitMQ as IoT Hub, MongoDB and PostgreSQL as database, Grafana for data visualization and Prometheus for back-end management. EIS-S230 also provides a dynamic scale out function that allows extension of resources as necessary. It is a perfect tool to create IoT applications more easily and flexibly and to speed up time to market.



Features:

- Integrated solution (HW+SW bundle) for back-end data service and light private cloud
- Pre-configured system: Intel Xeon platform with 32GB RAM, 512GB mSATA SSD including Ubuntu Linux OS
- Open and flexible infrastructure: Kubernetes support, multiple database options, on-demand microservices
- Integrated IoT Software: Private Cloud Deployment, Platform Management, Application Integration
- Integrated Applications: WISE-PaaS/DeviceOn, Grafana, Prometheus, Kubeapps, Kubernetes Dashboard
- Sustainable Management: Condition Monitor, Load Balance, Advanced Recovery
- **WISE-PaaS/DeviceOn inside for feature-rich IoT Device Management**

1.3 DeviceOn Agent Versions

Advantech provides a device client that is used to communicate and exchange information between IoT (Internet of Things) devices and the DeviceOn cloud services, called **WISE-Agent**. WISE-Agent provides a rich set of user-friendly features that are intelligent, standardized and scalable.

- **Standardization**

The communication protocol between client and cloud is based on the industry standard MQTT protocol. The IoT sensor data format is following the IPSO Alliance definition, implemented in JSON.

- **Portability**

The whole framework is written in C language and follows the ANSI C Standard. C compilers are widely available for most platforms and allow easy porting to different architectures or operating systems.

- **Scalability**

The WISE-Agent has a modular design and provides a plugin concept that allows flexible addition of new data sources or extra functionality.

1.3.1 WISE-Agent (Client)

WISE-Agent is support on different platforms running Windows 7 (or newer) or Ubuntu 16.04 x64 (or newer). Please contact us for others architectures (e.g. RISC) or operating systems (e.g. Yocto based Linux/Android).

General Operation Systems and Recommendations:

- ✓ **Windows 7/8/10 32-bit/64-bit**
- ✓ **Ubuntu 16.04, 18.04 x64**
- ✓ CentOS 7.6 x64
- ✓ Other Linux flavours (e.g. Yocto) on x86 or RISC (on a per project basis)
- ✓ Android on RISC (on a per project basis)

Assigned Ports for Device Communication

Name & Description		Outbound Port
1	MQTT, MQTTs Message Client	1883, 8883
2	Remote Desktop VNC Client	5501

Hardware Minimum Requirements:

- ✓ **Intel® Celeron™ 1.10 GHz CPU and at least 2GB of RAM**
- ✓ **500 MB root partition for the system**
- ✓ **Advantech HW with respective SUSI driver 3.02/4.0 support is required for the HWM (Hardware Monitoring Management) feature to be available**

1.4 Security

1.4.1 Role-Based Access Control (RBAC)

DeviceOn supports three different user roles - “Root” (perpetual version only), “System Admin” and “Device Admin”. There is only one single “Root” account per system, which has the highest permission level and can create “System Admin” or “Device Admin” accounts. The intermediate user level “System Admin” can be used to create “Device Admin” accounts. “Device Admin” accounts have the lowest permission level. Please refer to Section 7.1 for details on access permission levels.

1.4.2 SSL Encryption

- **HTTPS on DeviceOn Web Server**

The principal motivations for HTTPS are authentication of the accessed website, protection of the privacy and integrity of the exchanged data while in transit. It protects against man-in-the-middle attacks. The bidirectional encryption of communications between a client and server protects against eavesdropping and tampering of the communication.

- **SSL Connection on Database (PostgreSQL, MongoDB)**

PostgreSQL and MongoDB have native support for using SSL connections to encrypt client/server communications for increased security.

- **Create Security Credentials on Database**

Databases are by default protected by secure credentials and require explicit authentication for connections. This avoids accidentally deploying platforms with unprotected access.

- **Device Connectivity via MQTT SSL**

RabbitMQ supports multiple protocols including MQTT, which the most popular IoT (Internet of Things) protocol. By default, SSL is used to encrypt all MQTT traffic for device connectivity.

- **Enforce Password Policies**

While DeviceOn allows you to set some of your own passwords, please make sure those meet the minimum complexity requirements established by your specific organization.

1.4.3 Security Scan

The DeviceOn server pass through below famous vulnerability tools to ensure security for your AIoT solutions. Furthermore, all the testing including anti-malware (**Trend Micro** and **Kaspersky**)

- **Web Application Assessment Report (Micro Focus)**

[WebInspect](#) is an automated dynamic testing tool that mimics real-world hacking techniques and attacks, and provides comprehensive dynamic analysis of complex web applications and services.

- **OpenVAS (Open Vulnerability Assessment System)**

[OpenVAS](#) is a full-featured vulnerability scanner. Its capabilities include unauthenticated testing, authenticated testing, various high level and low-level Internet and industrial protocols, performance tuning for large-scale scans and a powerful internal programming language to implement any type of vulnerability test.

The scanner is accompanied by a vulnerability tests feed with a long history and daily updates. This [Greenbone Community Feed](#) includes more than 50,000 vulnerability tests.

- **Nessus**

[Nessus](#) is the de-facto industry standard vulnerability assessment solution for security practitioners. The latest intelligence, rapid updates, an easy-to-use interface.

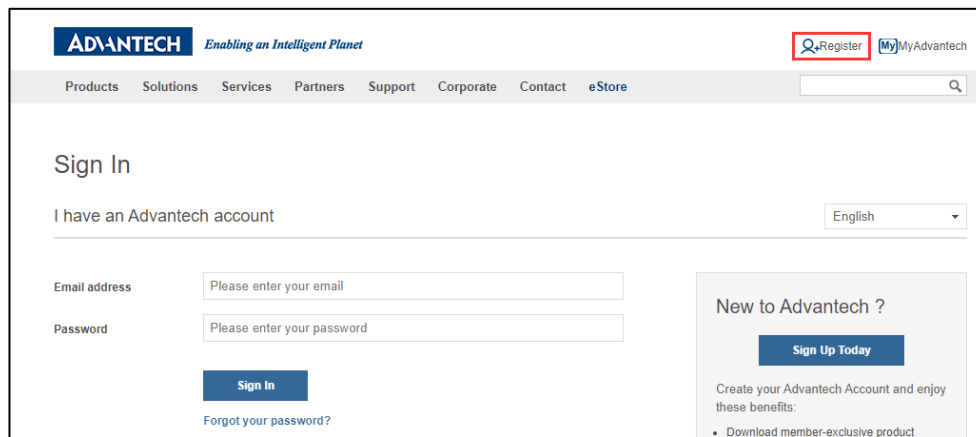
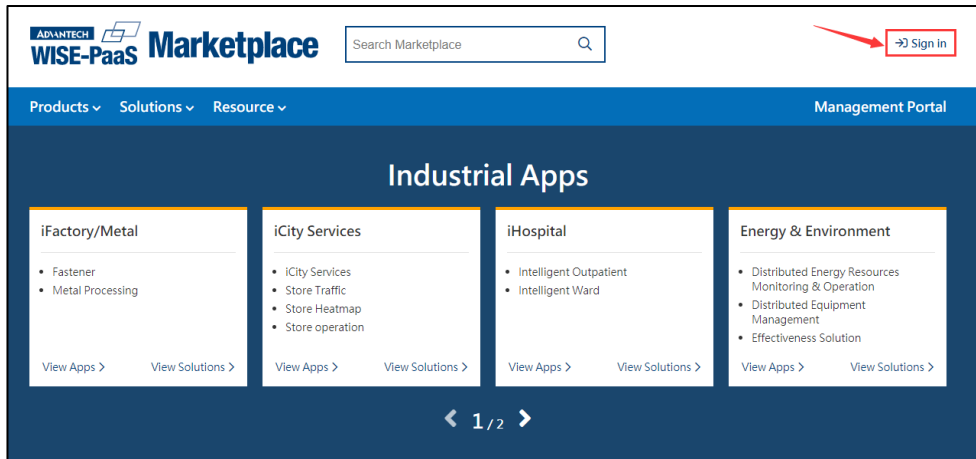
- ✓ Covers an industry-leading 47,000+ vulnerabilities
- ✓ Unlimited scans at no extra cost
- ✓ Compliant with PCI, HIPPA, GLBA, CIS, NIST, and more

2. Getting Started

2.1 DeviceOn Cloud Installation

2.1.1 Subscribe to DeviceOn from WISE-PaaS/EnSaaS

Step 1: Sign in to your MyAdvantech Account on [Marketplace or create one](#)

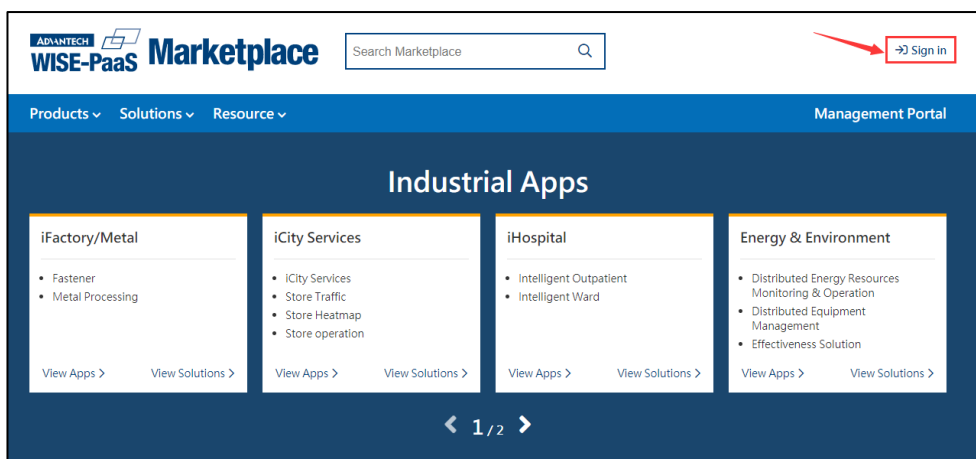


Step 2: Subscribe WISE-PaaS/DeviceOn

Step 3: Login to WISE-PaaS Management Portal

2.1.2 Redeem DeviceOn AKS from WISE-PaaS Marketplace

Step 1: Sign in to your MyAdvantech Account on [Marketplace or create one](#)



ADVANTECH *Enabling an Intelligent Planet* [Register](#) [MyAdvantech](#)

Products Solutions Services Partners Support Corporate Contact eStore

Sign In

I have an Advantech account English

Email address

Password

[Sign In](#)

[Forgot your password?](#)

New to Advantech ?

[Sign Up Today](#)

Create your Advantech Account and enjoy these benefits:

- Download member-exclusive product

Step 2: Redeem “[WISE-PaaS/DeviceOn](#) (App on Microsoft Azure)”

Edge.SRP
DeviceOn

WISE-PaaS/DeviceOn - IoT Device Management App

Service Provider : Advantech
 Category : IoT PaaS Software Services, Industrial Cloud Solutions
 Last Update : 2/27/2019 12:00:00 AM

Zero-touch onboard, visualized operations, real-time actions, and remotely manages connected devices at scale.

[Service Details](#) [Service Architecture & Successful Cases](#) [Pricing Details](#)

One-time Perpetual Licenses

DeviceOn Perpetual License (App on Microsoft Azure)	DeviceOn Perpetual License (Standalone Version)	DeviceOn Perpetual License (Data Service Server Version)
<div>55 WISE-Point</div> <div>32WSWPDOAZURA1</div> <div>Subscribe</div>	<div>55 WISE-Point</div> <div>32WSWPDOOP03A1</div> <div>Redeem</div>	<div>55 WISE-Point</div> <div>32WSWPDOOP02A1</div> <div>Redeem</div>

Select your license quantity and click “**Confirm**”.

New Purchase – Select Your License Quantity

Product Category: IoT PaaS Software Services, Industrial Cloud Solutions

DeviceOn Perpetual License (App on Microsoft Azure)
32WSWPDOAZURA1 License:

WISE-Point
50.00

10 devices

▼

+ Microsoft Azure Infrastructure Cost (monthly estimated USD\$ 194)

Please carefully check the purchase details before continue.

Confirm

Confirm your license quantity and click “**Confirm Redeem**”.

Confirm Your License Quantity

Product Category: IoT PaaS Software Services, Industrial Cloud Solutions

DeviceOn Perpetual License (App on Microsoft Azure)
32WSWPDOAZURA1 License:

WISE-Point
50.00

10 devices

▼

+ Microsoft Azure Infrastructure Cost (monthly estimated USD\$ 194)

No refund policy applied to this digital product. Please carefully check purchase details before confirming the redeem transaction.

Previous

Confirm Redeem

To deploy DeviceOn to your Azure subscription, a set of Azure account information is required. You will be prompted to enter required information on the WISE-PaaS/Marketplace when you choose “Create Deployment”. WISE-PaaS Marketplace will use the provided information to automatically deploy DeviceOn to your Azure subscription. There are two methods to retrieve those parameters for your Azure subscription, please reference Section 7.2.

Processing Your Purchase

A license key will be sent to your email shortly.

Would You Like To Deploy This App To Microsoft Azure?
Please enter your Microsoft Azure information to initiate deployment
(don't have Azure account yet? [contact us to create one](#))

Azure Subscription ID:
 a

Application (client) ID:
 b

Directory (tenant) ID:
 c

Client Secret:
 d

[How to retrieve my Azure account information?](#)

[Done. Skip Deployment](#)
[Create Deployment](#)

After deployment, you will receive a mail to get server information, including account, password and URL.

ADVANTECH

Dears,

Thank you for purchasing WISE-PaaS/ DeviceOn

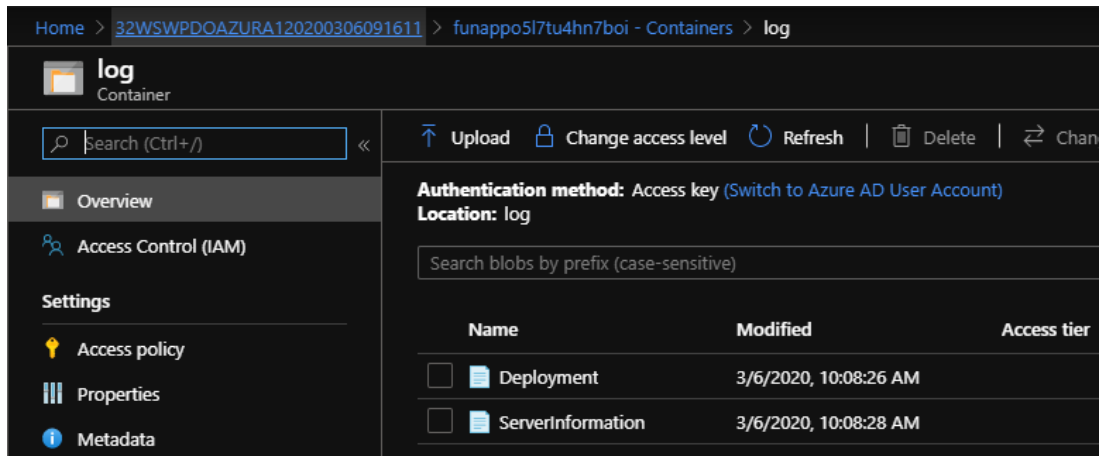
This letter informs you that the service has been deployed on Azure PaaS successfully with following access information.

● DeviceOn Portal: http://10.70.20.120	● Grafana Dashboard Portal: http://10.70.20.170
Username: root@advantech.com	Username: admin
Password: W10@w00d	Password: admin

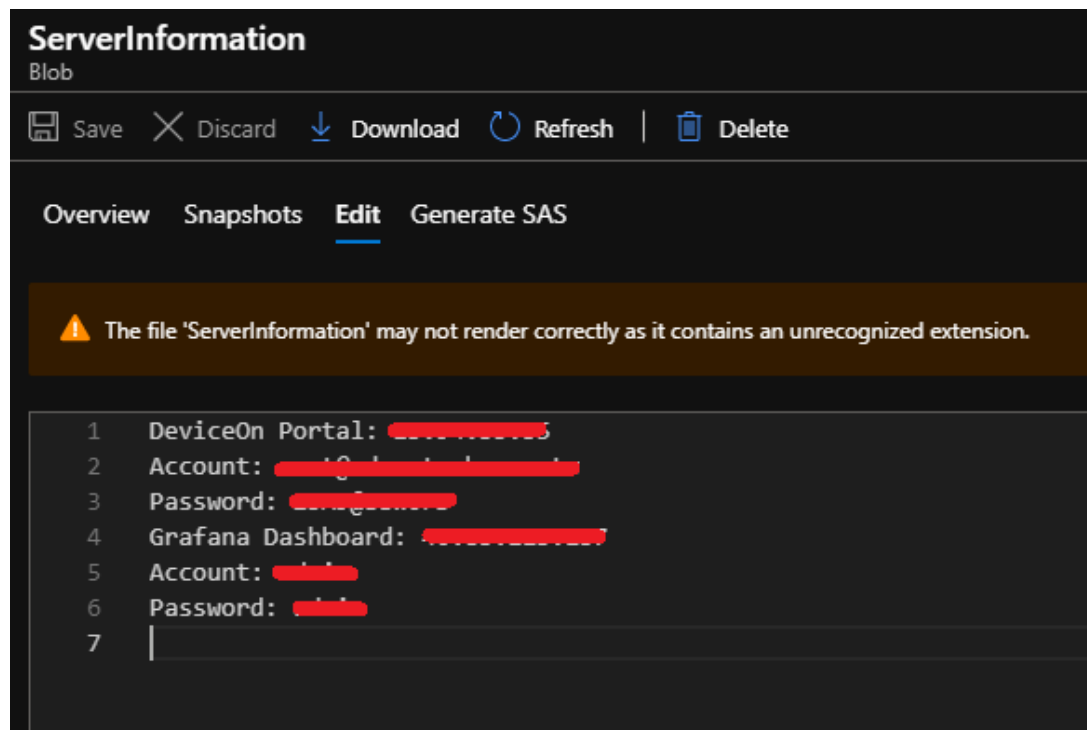
Note: Auto-activation apply to first-time purchase and deployment.
Product information and additional license purchase: <https://wise-paas.advantech.com/en-us/marketplace/detailinfo/52>

This is an automatically generated email, please do not reply.
Best regards,
Advantech WISE-PaaS Alliance

To prevent your mail blocked, we write the server information in Azure blob simultaneously.



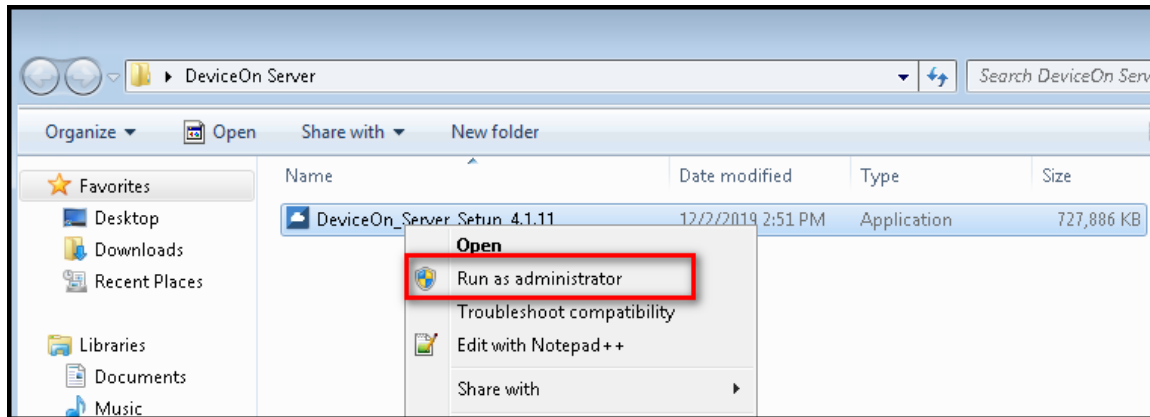
The credential and access information also on the “ServerInformation”.



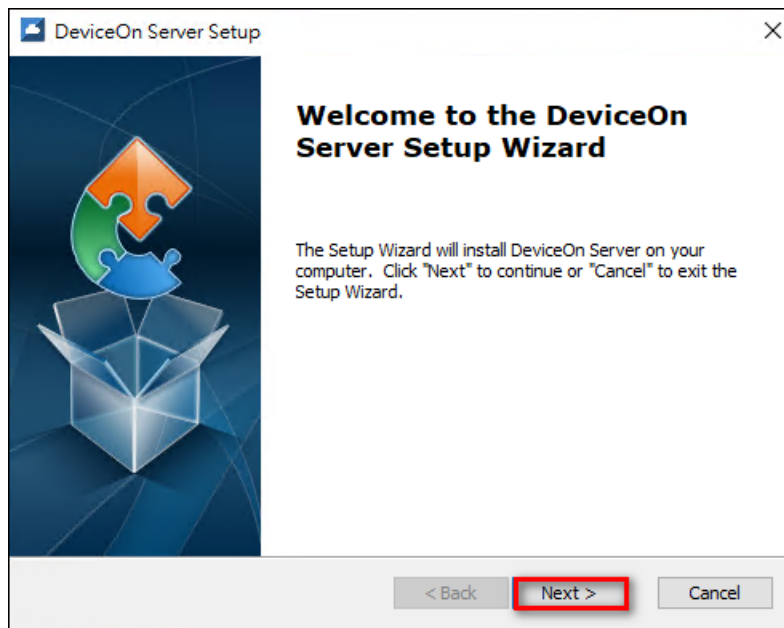
2.1.3 Setup DeviceOn Standalone Version (On-premise)

Step 1: Install the DeviceOn package on your system

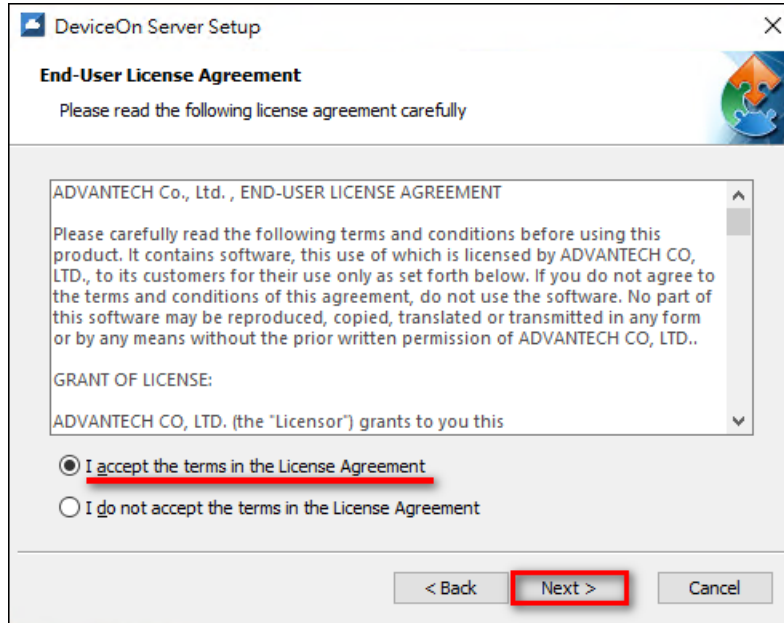
Copy the installation file (**DeviceOn_Server_Setup_4.1.x.exe**) to your target system and run it as administrator.



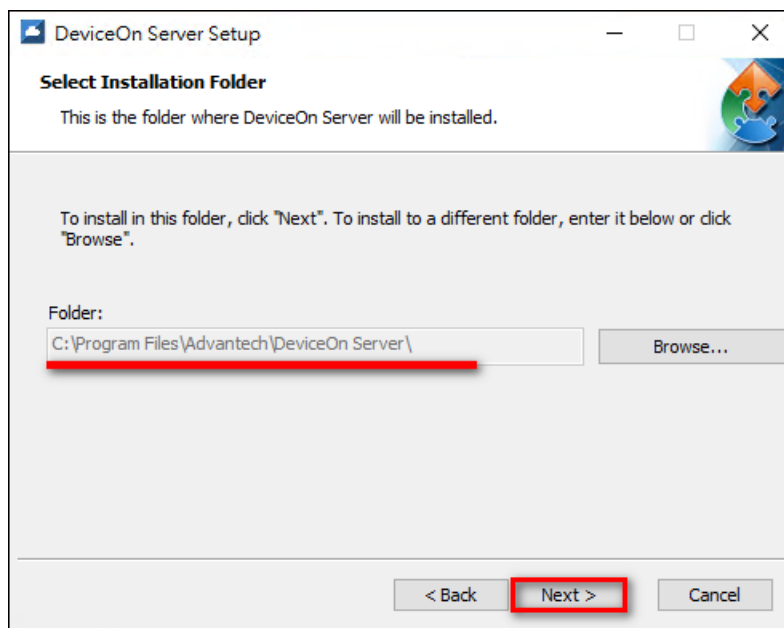
Click **“Next”** to start the installation process.



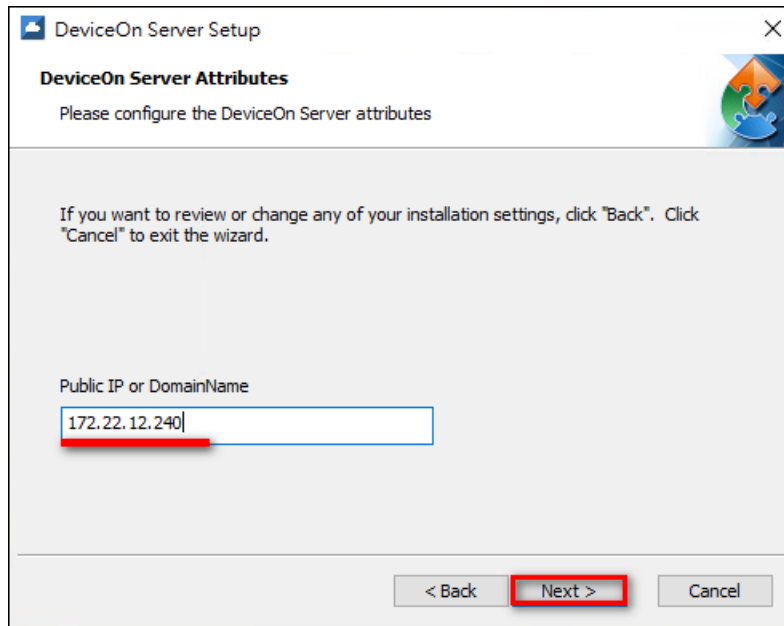
Select **“I Accept the terms in the License Agreement”** and click **“Next”**



Select the “**Installation Folder**” for DeviceOn Server and click “**Next**”



Enter “**Public IP**” or “**Domain Name**” for this physical/virtual machine and click “**Next**”. This information is required for “Edge Device” connectivity, please make sure your device is reachable under this IP or Domain Name.



Note: You can start a Windows command prompt and type “ipconfig” to retrieve your IP address(es) on this physical/virtual machine.

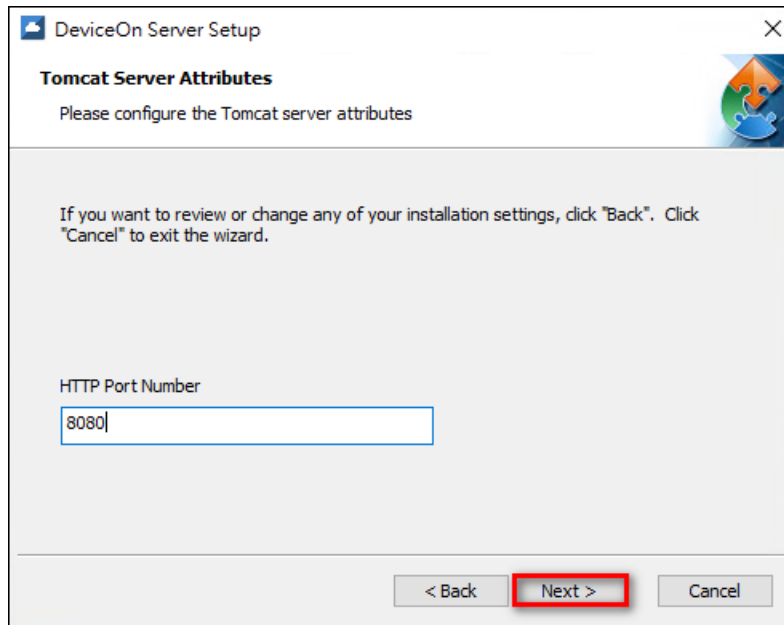
```
C:\Users\Sephiroth>ipconfig
Windows IP Configuration

Ethernet adapter 乙太網路 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
Ethernet adapter 乙太網路:

    Connection-specific DNS Suffix  . : ADVANTECH.CORP
    Link-local IPv6 Address . . . . . : fe80::194f:a776:464c:eb9b%9
    IPv4 Address. . . . . : 172.22.12.240
    Subnet Mask . . . . . : 255.255.252.0
    Default Gateway . . . . . : 172.22.15.254
                                172.22.15.130
```

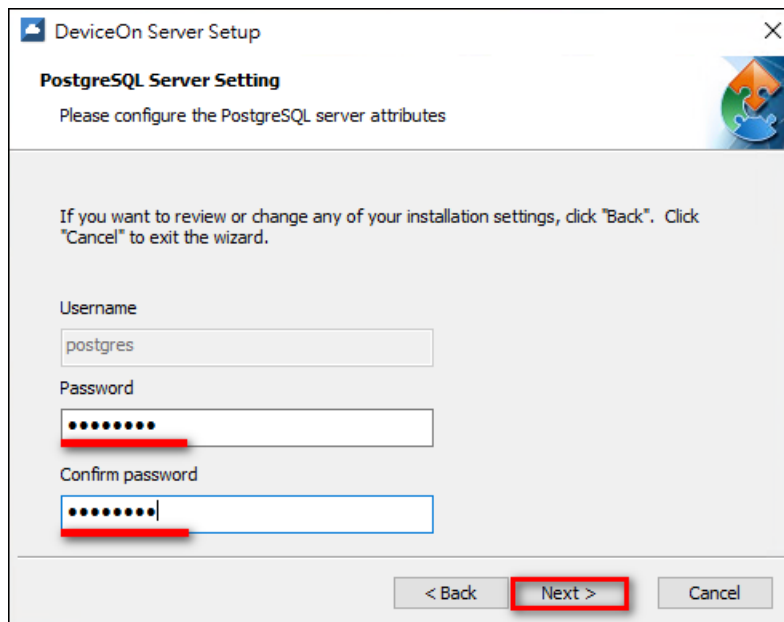
You will need to configure the HTTP port number that is used for web browser-based access the DeviceOn management portal. The default port is 8080, but you can select any other port as long as it does not conflict with any other application or service. Click “**Next**”.



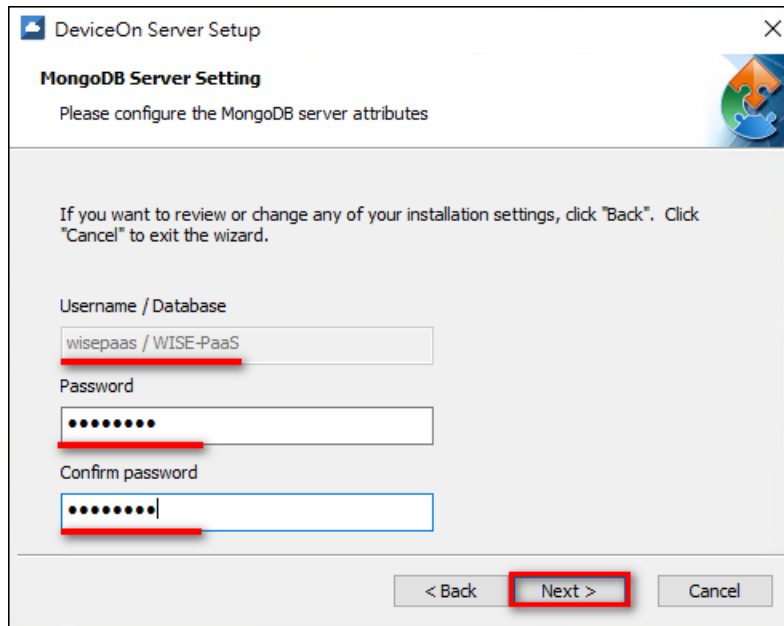
Configure the password of the relational database (PostgreSQL) that DeviceOn uses to manage account, device, permission, and relation data. The default account name is “**postgres**” and the password should follow below guideline.

Strong Password Rules:

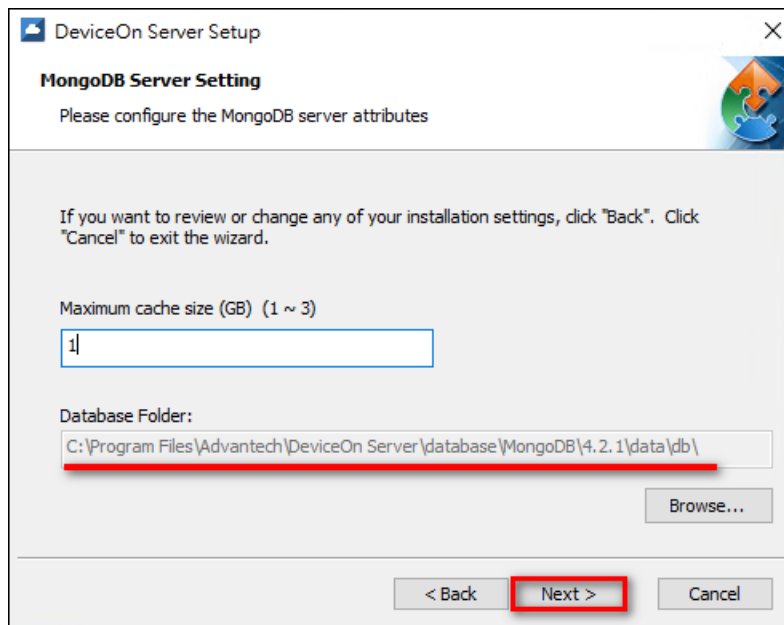
Minimum eight characters, at least one number, one lowercase letter, one uppercase letter, and one special character (Blank character, Backslash(\), Double quotes(") are prohibited)



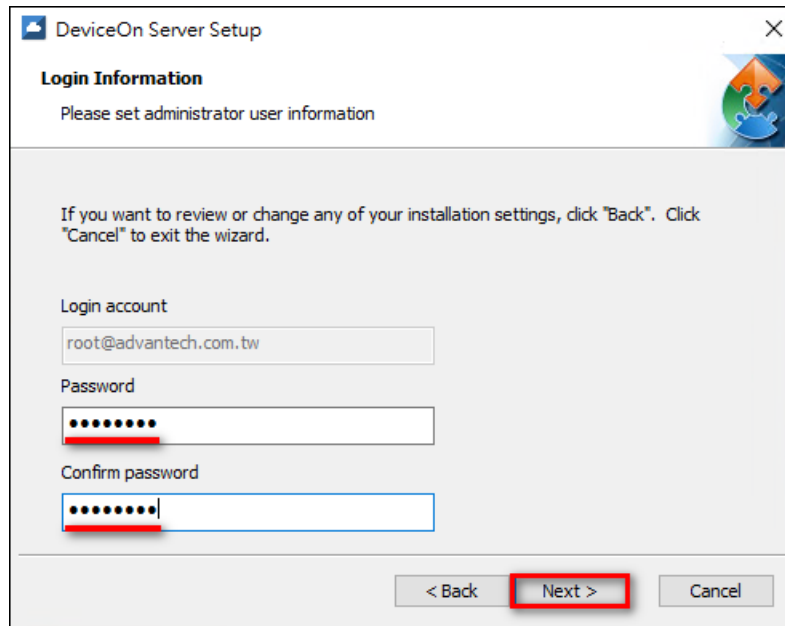
Configure the password of the NoSQL database (MongoDB) that stores device sensor data. The default account and database is “wisepaas/WISE-PaaS”. This password should also follow strong password rules as outlined above.



Select the database installation path and cache size of MongoDB and click **“Next”**. A larger cache size will result in better performance. For more information on this parameter, please refer to the [official documentation](#).

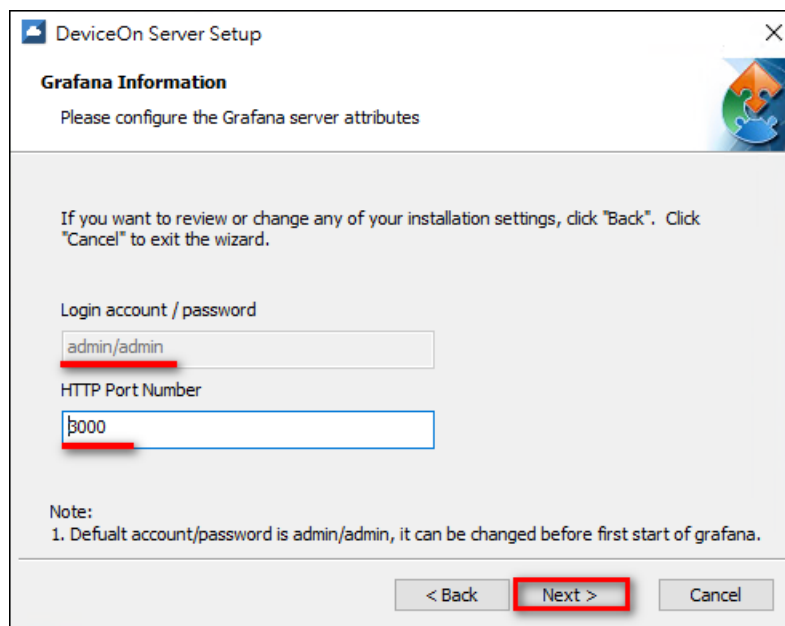


Configure the password of the root account (dummy name “root@advantech.com.tw”) and click **“Next”**. This root account has the highest permission level and is used to log in to the DeviceOn web service and create other user accounts.



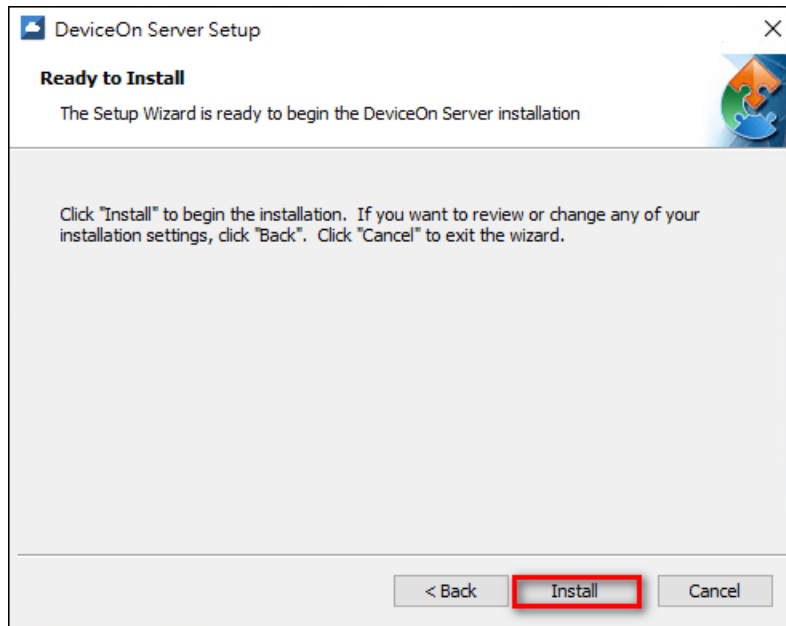
The screenshot shows the 'DeviceOn Server Setup' window with the 'Login Information' tab selected. The window title is 'DeviceOn Server Setup' with a close button (X) in the top right corner. Below the title bar, there is a puzzle piece icon. The main heading is 'Login Information' followed by the instruction 'Please set administrator user information'. A paragraph of text states: 'If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.' Below this, there are three input fields: 'Login account' with the text 'root@advantech.com.tw', 'Password' with masked characters, and 'Confirm password' with masked characters. At the bottom right, there are three buttons: '< Back', 'Next >' (highlighted with a red rectangle), and 'Cancel'.

Set up the HTTP service port for Grafana dashboard. The default user name and password is admin/admin. You will be able to modify this at the first login.

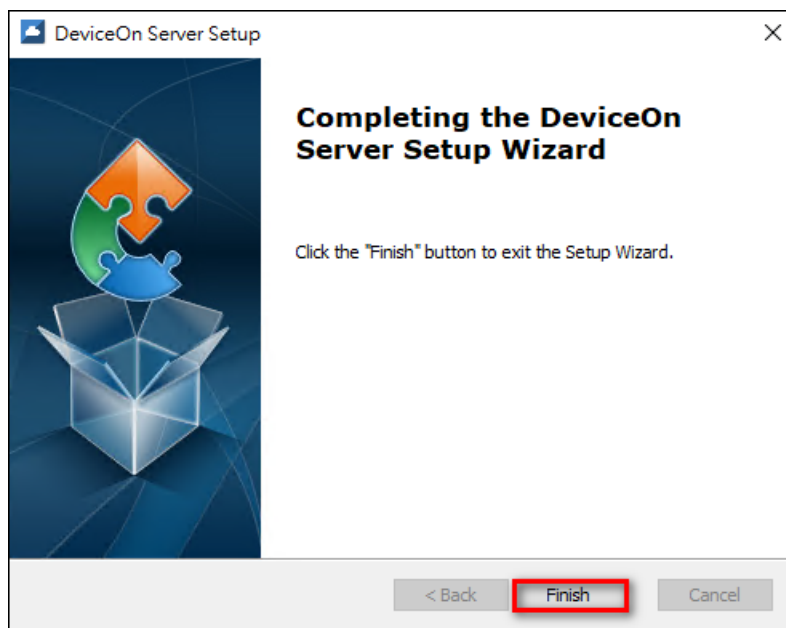


The screenshot shows the 'DeviceOn Server Setup' window with the 'Grafana Information' tab selected. The window title is 'DeviceOn Server Setup' with a close button (X) in the top right corner. Below the title bar, there is a puzzle piece icon. The main heading is 'Grafana Information' followed by the instruction 'Please configure the Grafana server attributes'. A paragraph of text states: 'If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.' Below this, there are two input fields: 'Login account / password' with the text 'admin/admin' and 'HTTP Port Number' with the text '3000'. At the bottom, there is a 'Note:' section with the text: '1. Default account/password is admin/admin, it can be changed before first start of grafana.' At the bottom right, there are three buttons: '< Back', 'Next >' (highlighted with a red rectangle), and 'Cancel'.

Click **"Install"** to begin the installation.



Click **“Finish”** to exit the program.



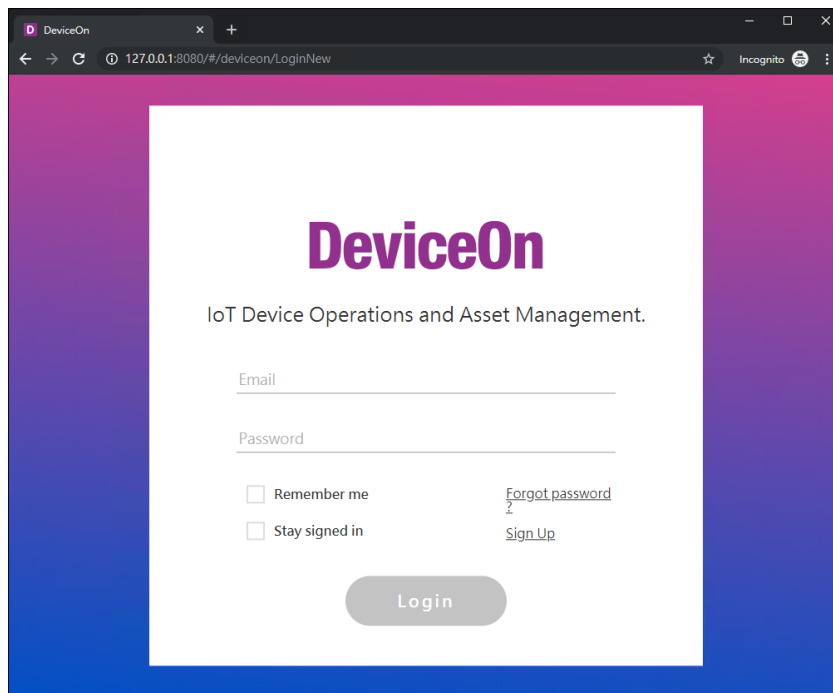
Step 2: Launch DeviceOn Web Service Shortcut on Desktop

Two shortcuts will be generated on the desktop - one is for the DeviceOn web portal and the other one is for the Grafana dashboard.



Click the **“DeviceOn Server”** shortcut in order to launch a browser and to start device operation and

management. It is recommended to use **Chrome** for the best user experience.



2.1.4 Setup DeviceOn Standalone Version for Ubuntu Linux (On-premise)

If you are interested in DeviceOn and used to Linux platform, On-Premise, we also provide an installer for Ubuntu Linux (one of the most popular Linux distribution). This section will guide you how to install DeviceOn on Ubuntu Linux.

Note here that:

- The DeviceOn Ubuntu Linux installer is named something like "**DeviceOn_Server_Ubuntu 18.04_x64_4.1.x.run**". To acquire the installer and ensure having the latest version, please contact us.
- If you are running the installer with an account other than "root", you should use "**sudo**" command to obtain higher privileges, or the installation may fail at any step.

Step 1: Open a terminal

The installer runs in CLI (Command Line Interface) mode. As such, open a terminal preferable for you.

Step 2: Copy the installer to target host

Use the way you like to copy the installer to the target host.

Step 3: Set the installer as executable

In the terminal, run "**chmod 0755 DeviceOn_Server_Ubuntu 18.04_x64_4.1.x.run**" so that the

installer as an executable file under Ubuntu Linux.

Step 4: Running the installer

Change your working directory to where the installer is and run `"/ DeviceOn_Server_Ubuntu 18.04_x64_4.1.x.run "`. You may need to run `"sudo ./ DeviceOn_Server_Ubuntu 18.04_x64_4.1.x.run "` to acquire higher privileges if you were logged in as a normal user.

Step 5: Answering some questions

Throughout installation process, it's necessary to answer some questions to complete the installation:

A. The password of user “**postgres**” to login PostgreSQL database.

→ PostgreSQL password setup.
↳ You need to input a password for super user 'postgres'

When you run into this step the question shows like above. Just input the password you would like to use to login PostgreSQL database for “**postgres**” account.

B. The password of user “**wisepaas**” to login MongoDB database.

→ MongoDB password setup.
↳ You need to input a password for user 'wisepaas' within database 'WISE-PaaS'

When you run into this step the question shows like above. Just input the password you would like to use to login MongoDB database for “**wisepaas**” account.

C. The valid IP or host name of the target host.

→ A valid IP or host name is required.
↳ The IP or host name you input here will be used by agents to acquire
↳ connection information.

When you run into this step the question shows like above. Just input the IP address of the target host. A hostname (even a FQDN) is also acceptable if you are sure that agents can connect to via the name you provide.

D. If turn MongoDB capped functionality on or not.

→ Turn 'capped' on or not.
↳ MongoDB has a feature named 'capped'. It will recycle disk size for those
↳ collections turn this functionality on.

When you run into this step the question shows like above. Just input “**yes**” or “**no**” to enable or

disable “capped” functionality. If you answer “yes”, a subsequent question followed to ask you “how much capped size, in MB, to be used? “. Just input the size, in MB, you want to use in “capped” functionality in MongoDB database.

[Capped collections](#) are fixed-size collections that support high-throughput operations that insert and retrieve documents based on insertion order. Capped collections work in a way similar to circular buffers: once a collection fills its allocated space, it makes room for new documents by overwriting the oldest documents in the collection.

E. The password of user “**root@advantech.com.tw**” to login DeviceOn portal, and the rule should follow below guideline.

Strong Password Rules:

Minimum eight characters, at least one number, one lowercase letter, one uppercase letter, and one special character (Blank character, Backslash(\), Double quotes(") are prohibited)

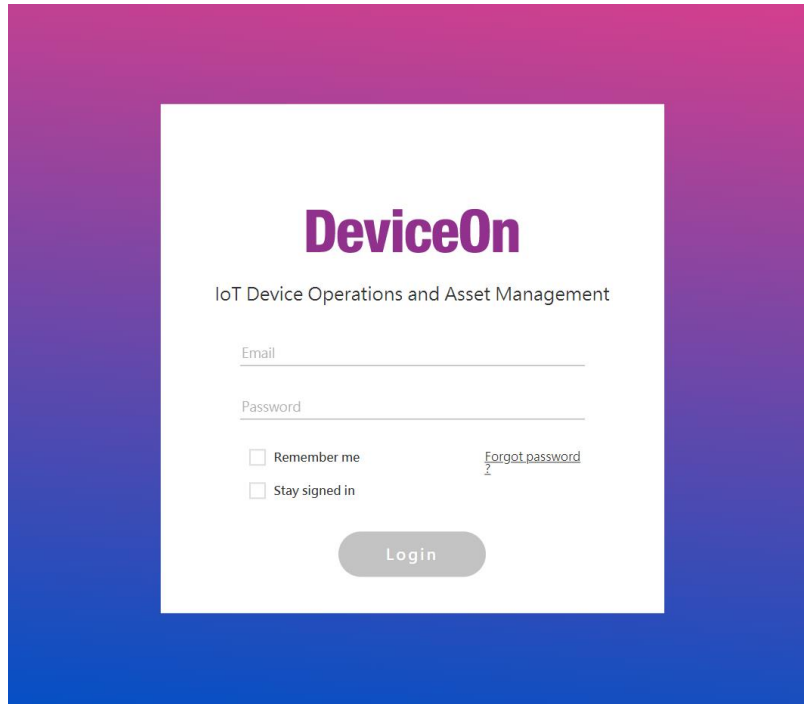
```
→ DeviceOn portal password setup.  
  ↳ You need to input a password for super user 'root' to login DeviceOn portal  
  ↳  
  ↳ NOTE THAT A VALID PASSWORD TO LOGIN PORTAL MUST CONTAIN:  
  ↳ 1) at least eight characters  
  ↳ 2) at least a number  
  ↳ 3) at least a lowercase letter  
  ↳ 4) at least an uppercase letter  
  ↳ 5) at least a special character but ' ', '\', and '\"'.
```

When you run into this step the question shows like above. Just input the password you would like to use to login DeviceOn portal for “**root@advantech.com.tw**” account.

Finally, a workable DeviceOn server should be there the target host. Open a browser and input <http://{IP-USED-IN-QUESTION-C}>, you should see the DeviceOn login page.

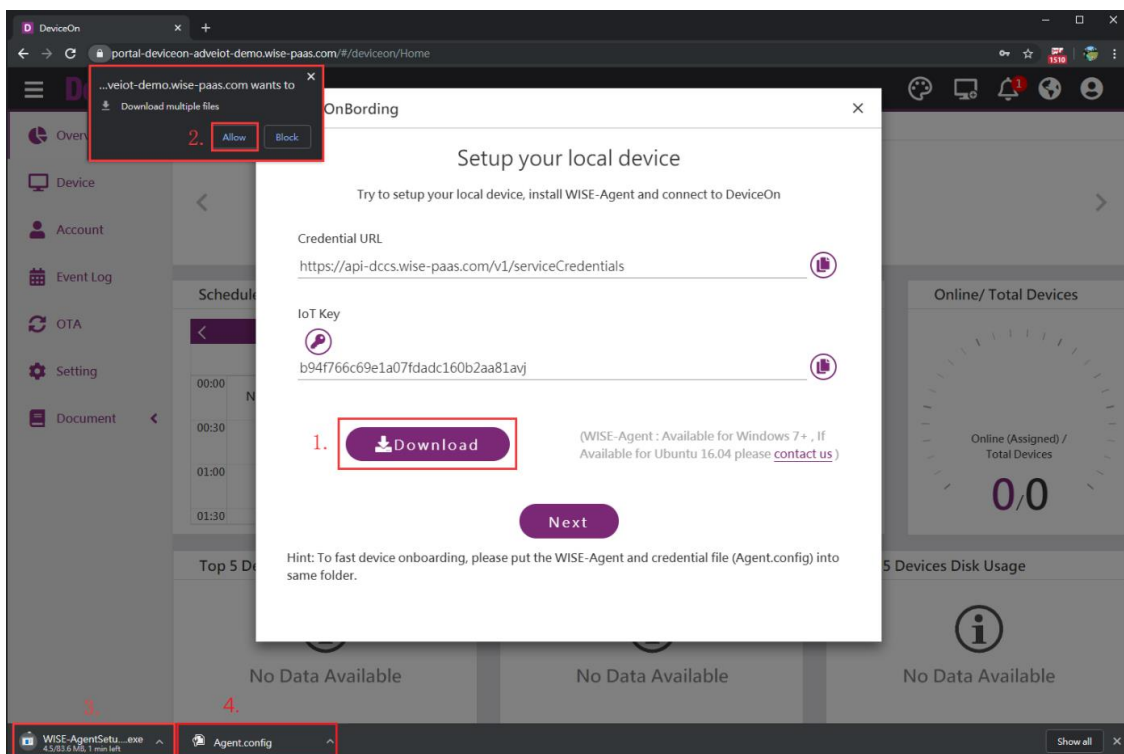
2.2 DeviceOn Client Installation & Device Onboarding

Step 1: Log in to the DeviceOn Cloud Service with Your Account and Password

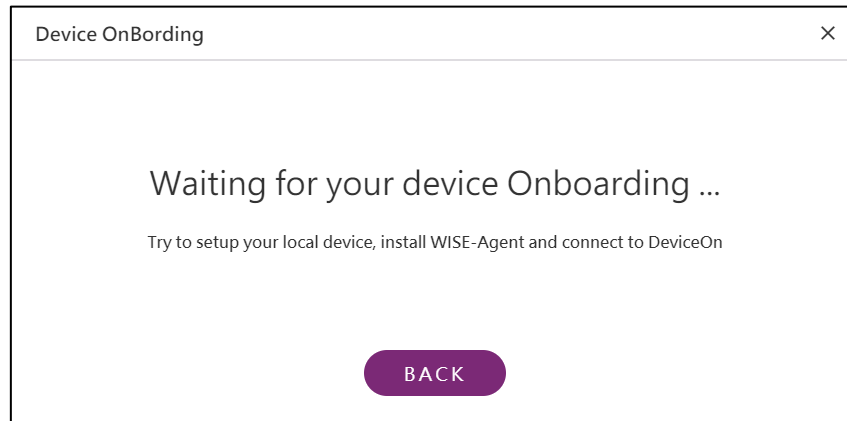


Step 2: Download WISE-Agent and Connection Configuration (Agent.config)

At the first login, the “Device Onboarding” dialog will pop up automatically. Please click “**Download**” to get the latest version of **WISE-AgentSetup.exe** and the respective connection configuration. (**Agent.config**)

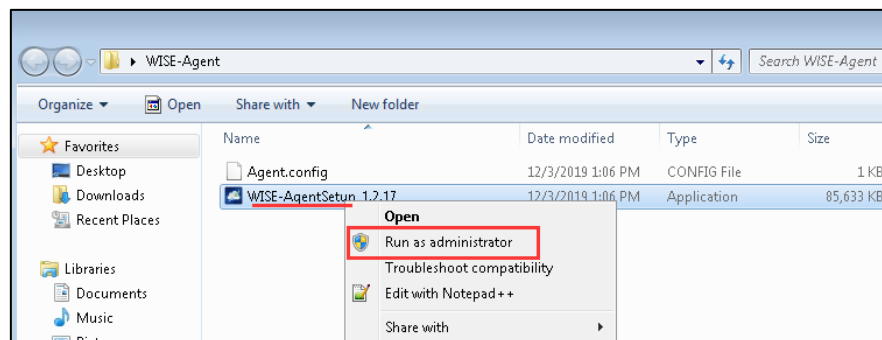


Click “**Next**” to wait for connecting devices.

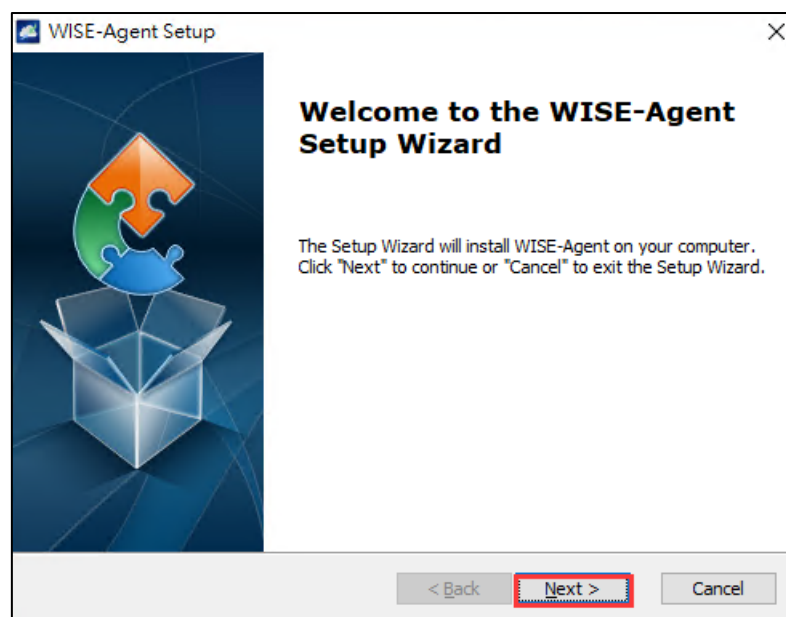


Step 3: Set up Your Local Device

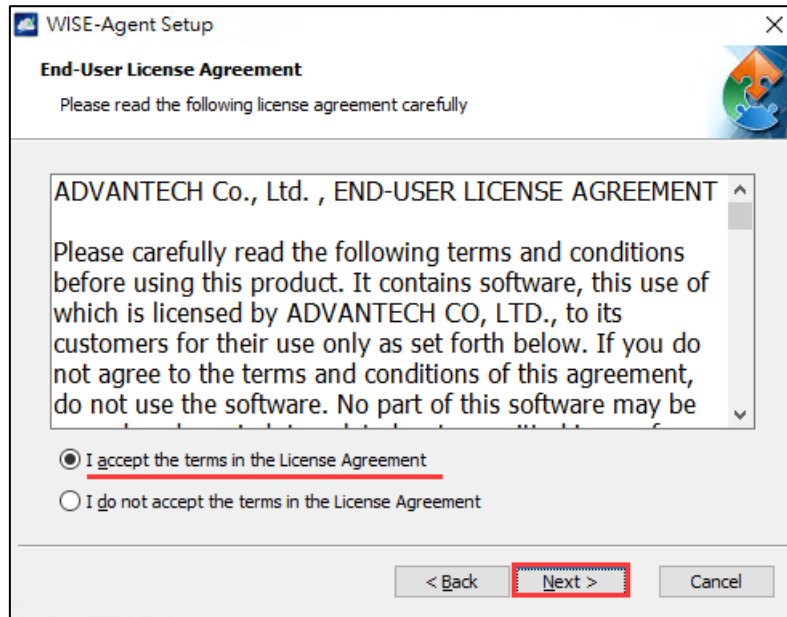
Copy those two files (**WISE-AgentSetup_1.x.x.exe** and **Agent.config**) to the target device and launch “**WISE-AgentSetup_1.x.x.exe**” as administrator.



Click “**Next**” to set up the WISE-Agent program.

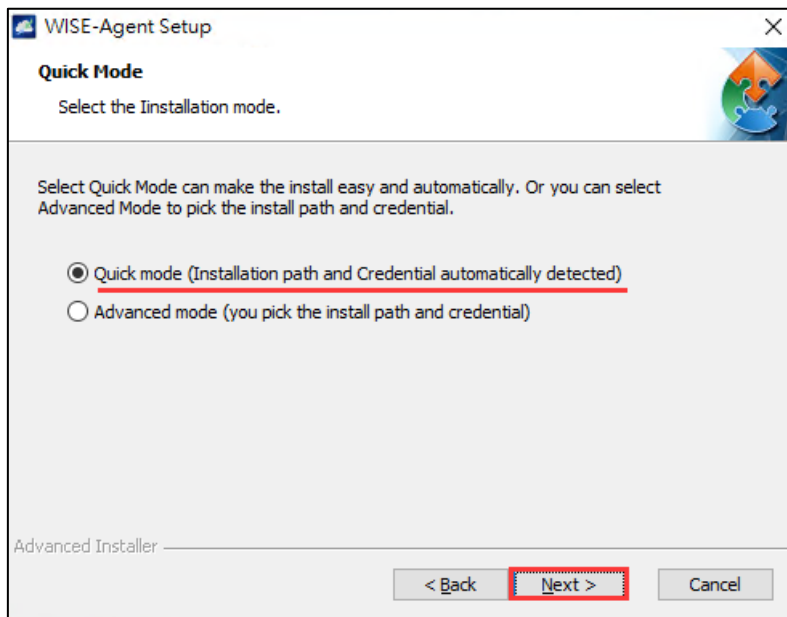


Select “**I Accept the terms in the License Agreement**” and click “**Next**”



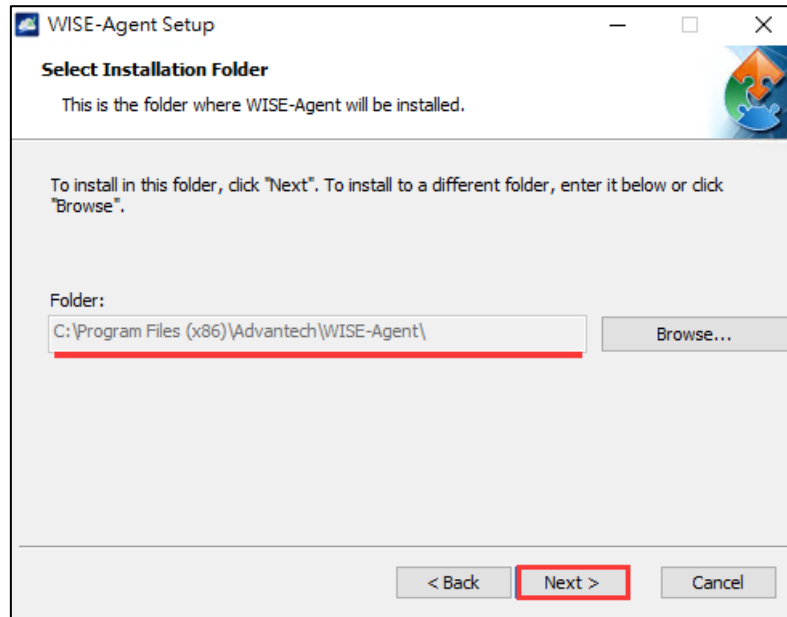
When the “**WISE-AgentSetup_1.x.x.exe**” program detects a cloud connection configuration file (**Agent.config**) in the same folder, “**Quick Mode**” as shown in this dialog will be available. For “**Quick Mode**”, the installation path is fixed to “C:\Program Files (x86)\Advantech\WISE-Agent”. If you would like to adjust the installation location, please select “**Advanced Mode**”.

Quick Mode:



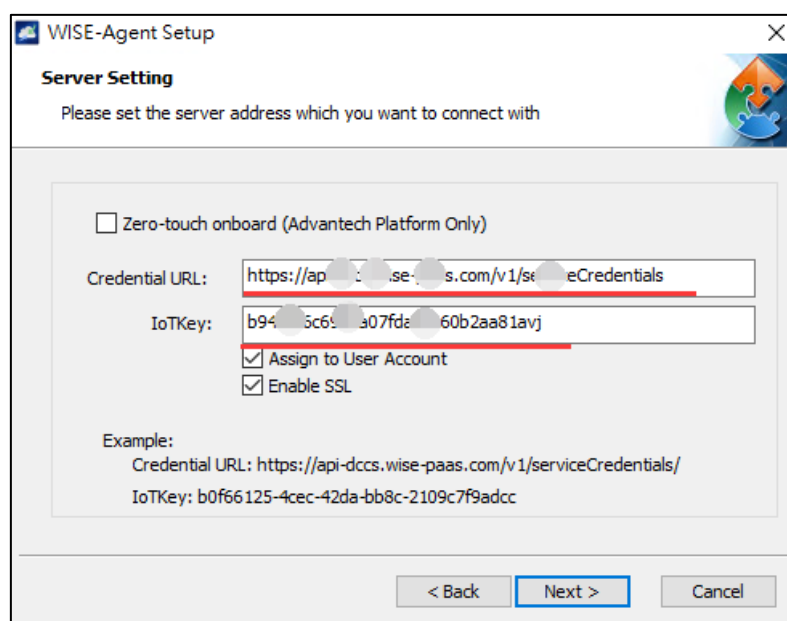
Advanced Mode:

Select the Installation folder for WISE-Agent

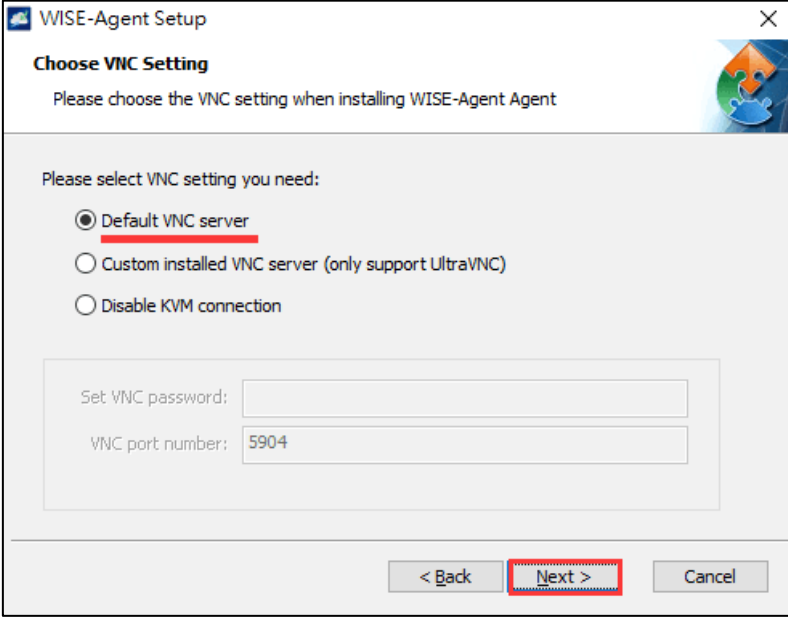


Set up the cloud connection configuration (**Credential URL & IoTKey**). This information can be retrieved from the DeviceOn web portal as shown in Step2, and click **“Next”**.

- *“Zero-touch onboarding”*: Only supported on Advantech platforms with SUSI Driver and pre-configuration on the provisioning server
- *“Assign to User Account”*: Each account has its own connection IoTKey. If checked, the device will be assigned to this account automatically.
- *“Enable SSL”*: The communication between WISE-Agent and DeviceOn Cloud is MQTT. If checked (default setting), all the messages and content are SSL encrypted (MQTT SSL port: **8883**). Otherwise, port **1883** is used for MQTT without SSL.

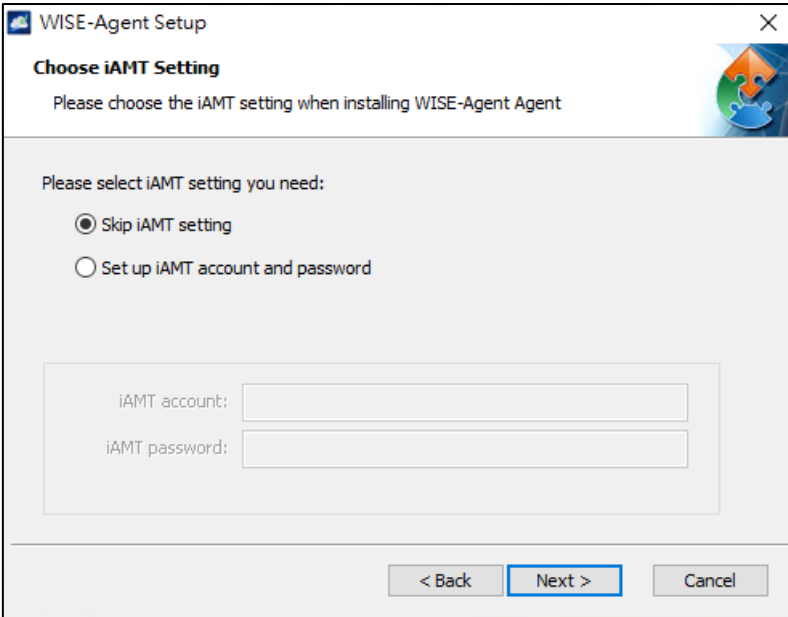


WISE-Agent supports remote desktop through built-in UltraVNC. You can manually specify the location of your own UltraVNC installation if preferred. If you do not want the remote desktop feature to be available, please select “Disable KVM Connection”.



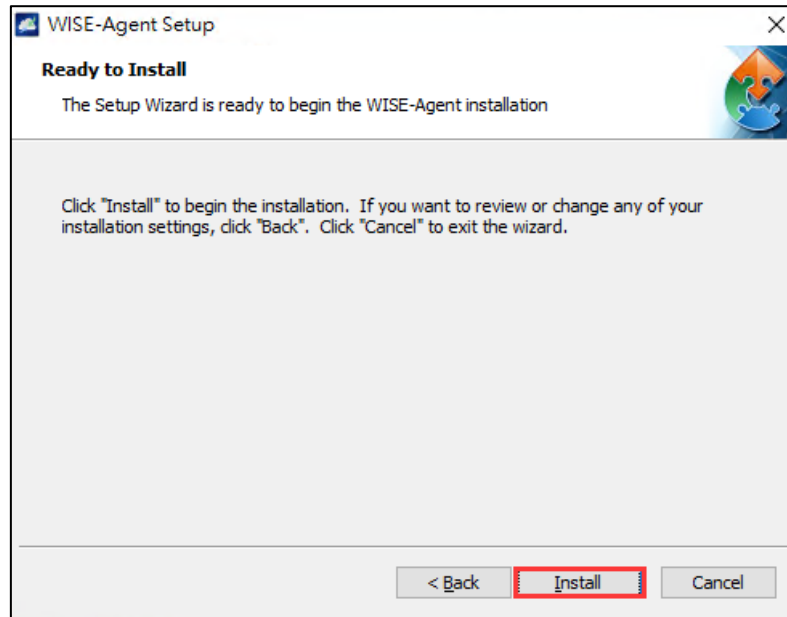
The image shows a Windows-style dialog box titled "WISE-Agent Setup" with a close button (X) in the top right corner. Below the title bar, the text "Choose VNC Setting" is displayed, followed by the instruction "Please choose the VNC setting when installing WISE-Agent Agent". A sub-instruction reads "Please select VNC setting you need:". There are three radio button options: "Default VNC server" (which is selected and has a red underline), "Custom installed VNC server (only support UltraVNC)", and "Disable KVM connection". Below these options is a section with two text input fields: "Set VNC password:" and "VNC port number:". The "VNC port number" field contains the value "5904". At the bottom of the dialog, there are three buttons: "< Back", "Next >" (which is highlighted with a red border), and "Cancel".

WISE-Agent integrates Intel AMT (Intel Active Management Technology) for remote power management (Power Up, Down, Cycle and Reset) as well as remote desktop access, even in case the operating system has crashed. However, this feature requires hardware support (Intel Core i5, i7) and the target device needs to be on the same local network as the DeviceOn server. Please pre-configure iAMT, enable it in the device’s BIOS and provide the account and password information in this dialog if you would like to enable iAMT based remote control features.

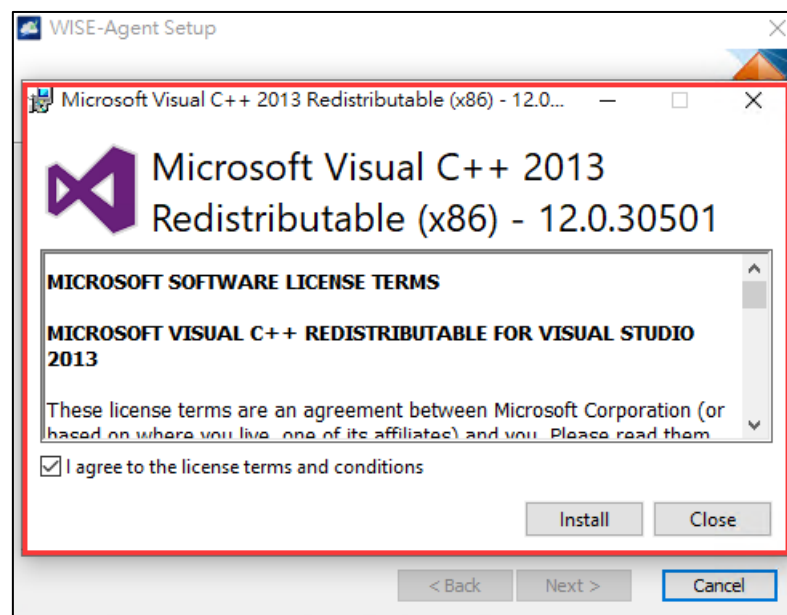


The image shows a Windows-style dialog box titled "WISE-Agent Setup" with a close button (X) in the top right corner. Below the title bar, the text "Choose iAMT Setting" is displayed, followed by the instruction "Please choose the iAMT setting when installing WISE-Agent Agent". A sub-instruction reads "Please select iAMT setting you need:". There are two radio button options: "Skip iAMT setting" (which is selected) and "Set up iAMT account and password". Below these options is a section with two text input fields: "iAMT account:" and "iAMT password:". At the bottom of the dialog, there are three buttons: "< Back", "Next >" (which is highlighted with a blue border), and "Cancel".

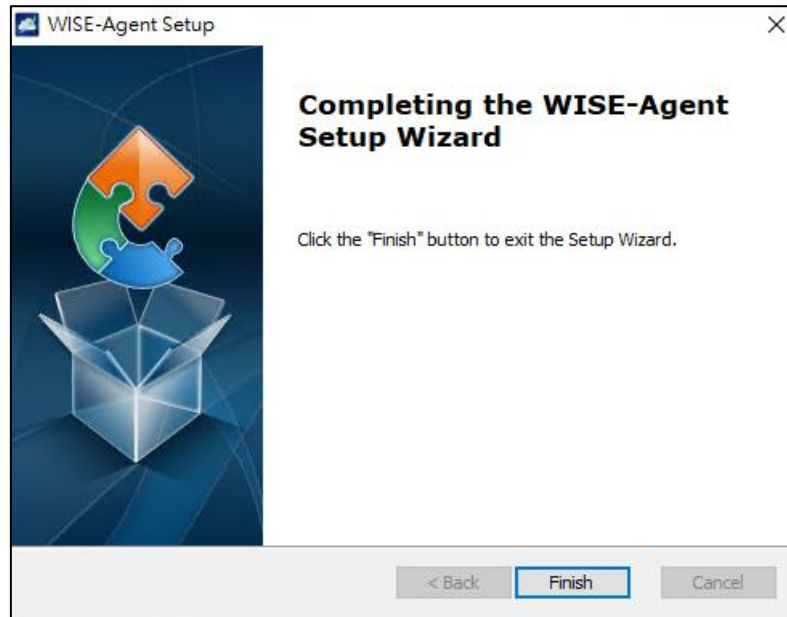
Click “**Install**” to begin the installation.



WISE-Agent requires the Microsoft Visual C++ Redistributable 2008, 2013, 2015 x86 packages, which will be downloaded from the Internet and set up during the installation process. If you are in an environment with limited or no Internet access, please download the "[Agent Dependency Package](#)" through an Internet connected device and install this package first.

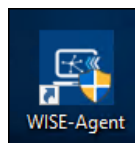


Click "**Finish**" to exit the program.

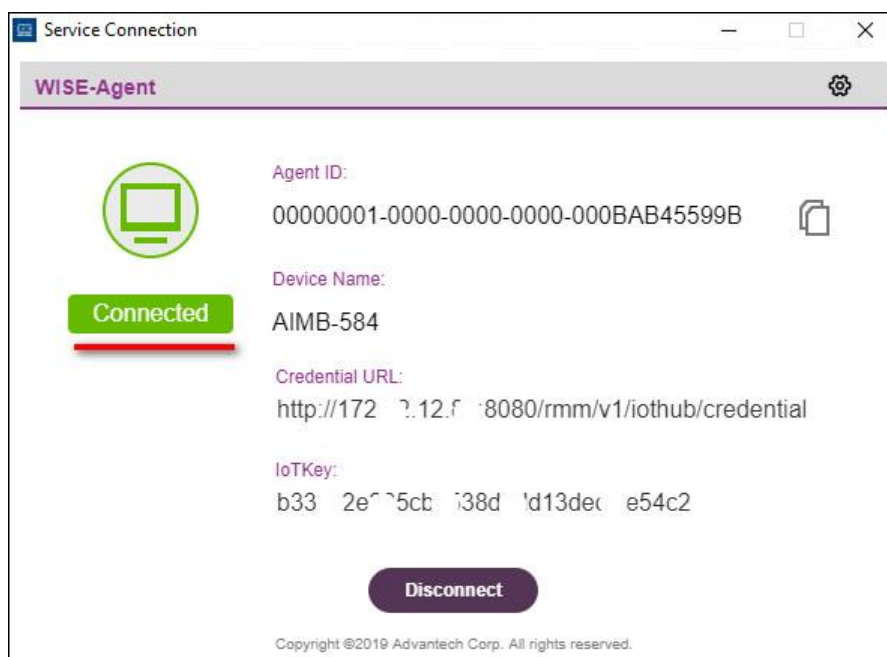


Step 4: Launch the WISE-Agent

Click on the “WISE-Agent” icon on the Windows Desktop to open the WISE-Agent user interface.

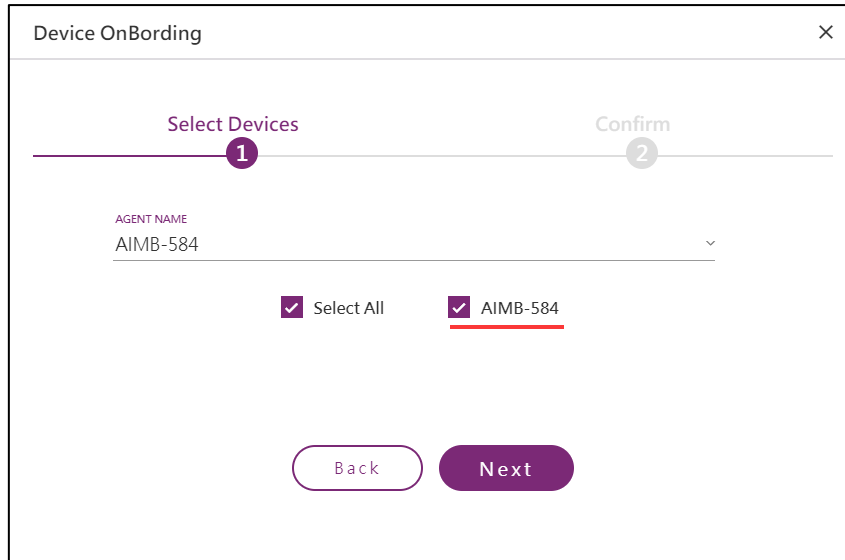


If the status shows “Disconnected”, please make sure your network settings are configured correctly and that you have access to the DeviceOn server-side application, either located in a public cloud (WISE-PaaS, MS Azure) or on premise (standalone server version) depending on deployment scenario. Then, please click the “Connect” button to try to reconnect.

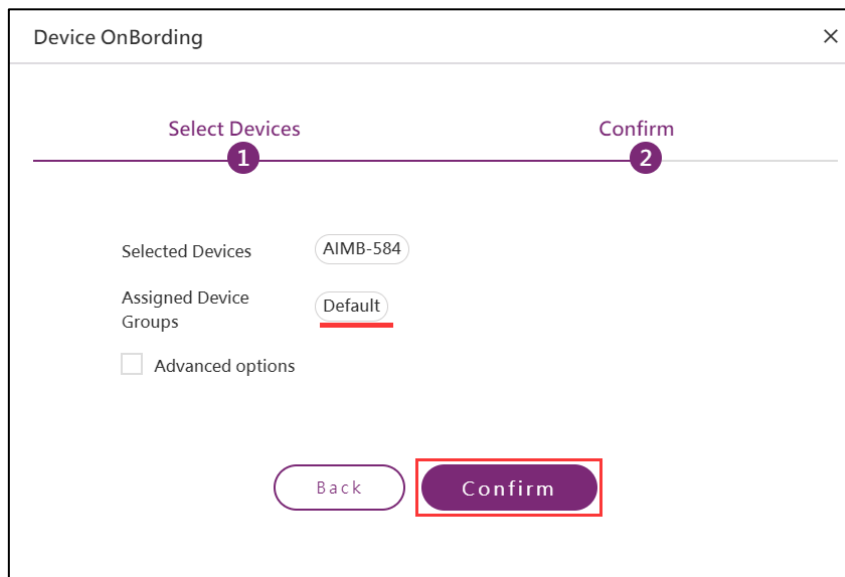


Step 5: Grouping Your Devices

Once the device connects, the DeviceOn user interface will move on to the device grouping page, where the device group for these devices can be selected.

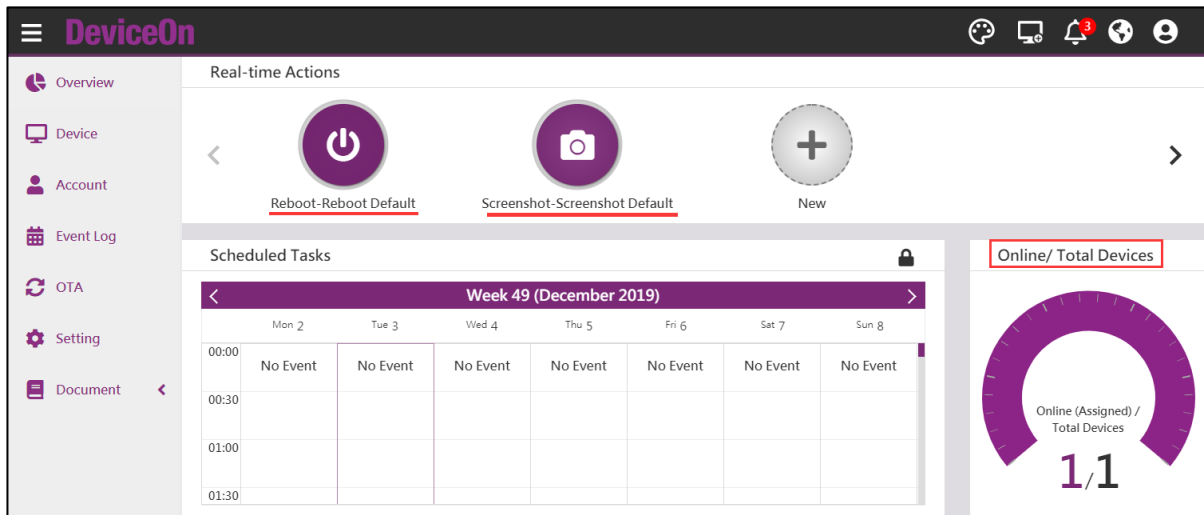


There is a “**Default**” group that can be used, or other groups for this device can be created after checking “Advanced options”. Click “**Confirm**” to start device management.



Step 6: Start Device Management

By default, two “Real-time Actions” are created for a group, one is “Screenshot” and the other one is “Reboot”. The overview page further shows the online status of registered.



3. DeviceOn User Interface & Functions

3.1 DeviceOn Server (Standalone)

The standalone version provides all packages of the DeviceOn software in one installer package, including RabbitMQ as a message broker, MongoDB, PostgreSQL as databases, Grafana for visualization, Tomcat for web services, and a watchdog service that protects DeviceOn core components from crashing or becoming unresponsive.

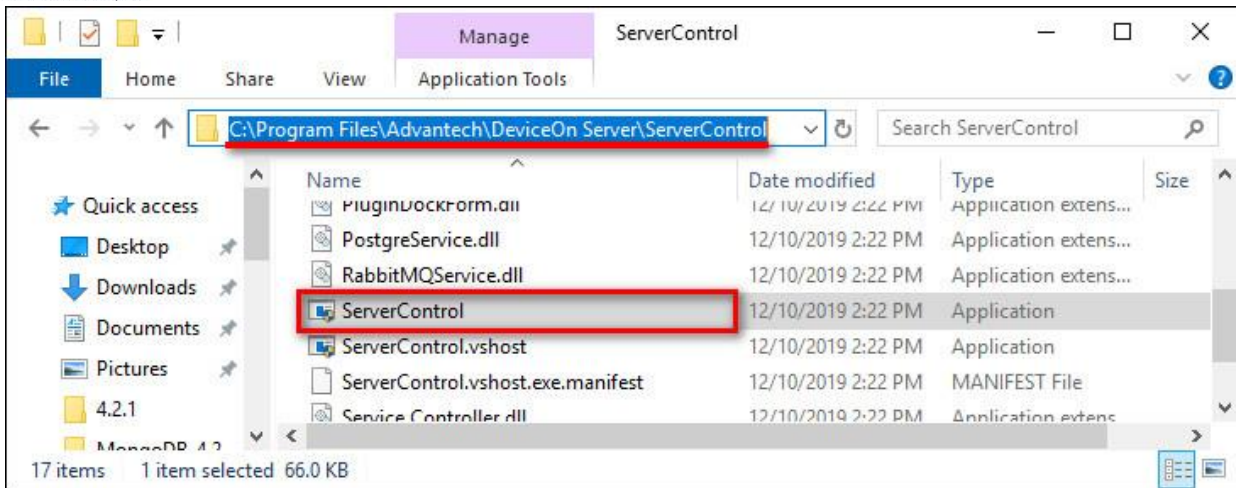
The following section (3.1.1) introduces the “Standalone Server Control” tool that allows to monitor and enable/disable DeviceOn core components. The watchdog service is explained in section 3.1.2.

3.1.1 Standalone Server Control

After the DeviceOn standalone version has been installed, a “**Server Control**” icon should show up in the system tray.



If it does not show up for some reason, please go to installation path and launch the program (ServerControl.exe) manually as shown here:

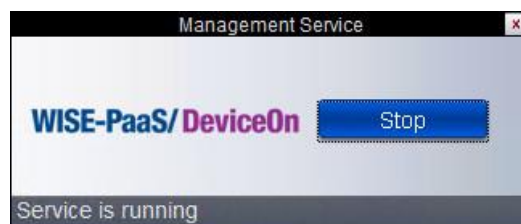


Right click on the tray icon to bring up an overview of each core component status. The green light indicates normal status and a red light means the respective service is stopped.



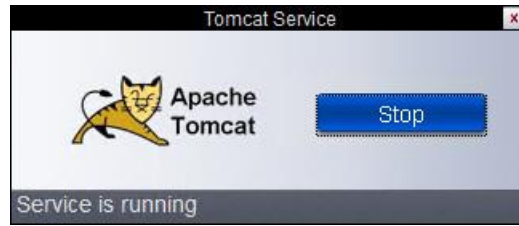
● Management Service

The “Management” service includes the DeviceOn backend core function and consists of two Java processes (DeviceOn and Provisioning Worker) that handle messages and process OTA traffic between the client and server. Click “Stop” to stop the management service.

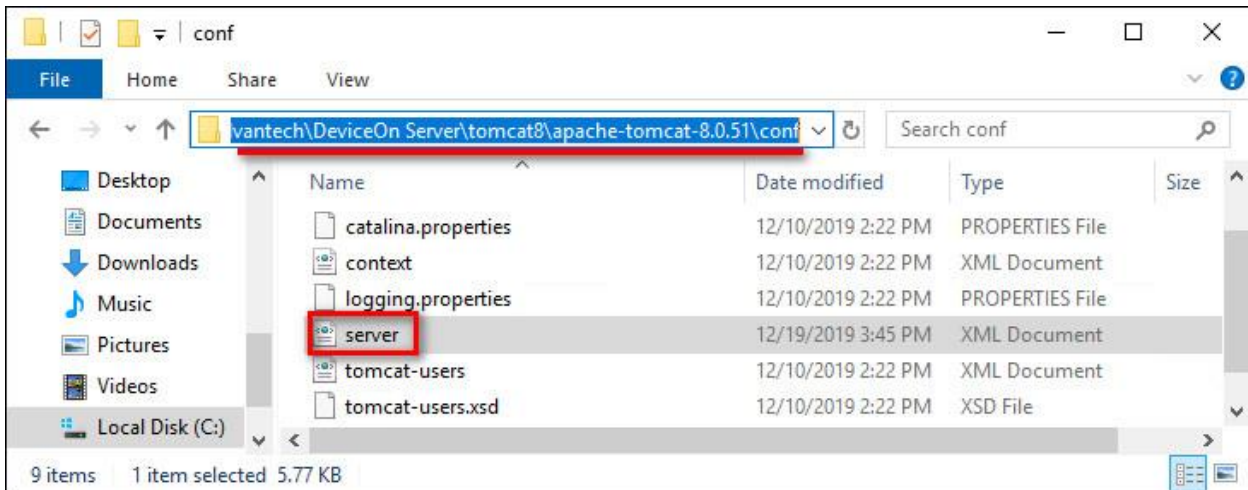


● Tomcat Service

The DeviceOn web service uses Apache Tomcat to provide the user interface, APIs and WebSockets. Click “**Stop**” to stop the Apache Tomcat service.



For advanced configuration (SSL, connection pool, etc.), you may modify “**server.xml**” located in the installation folder.

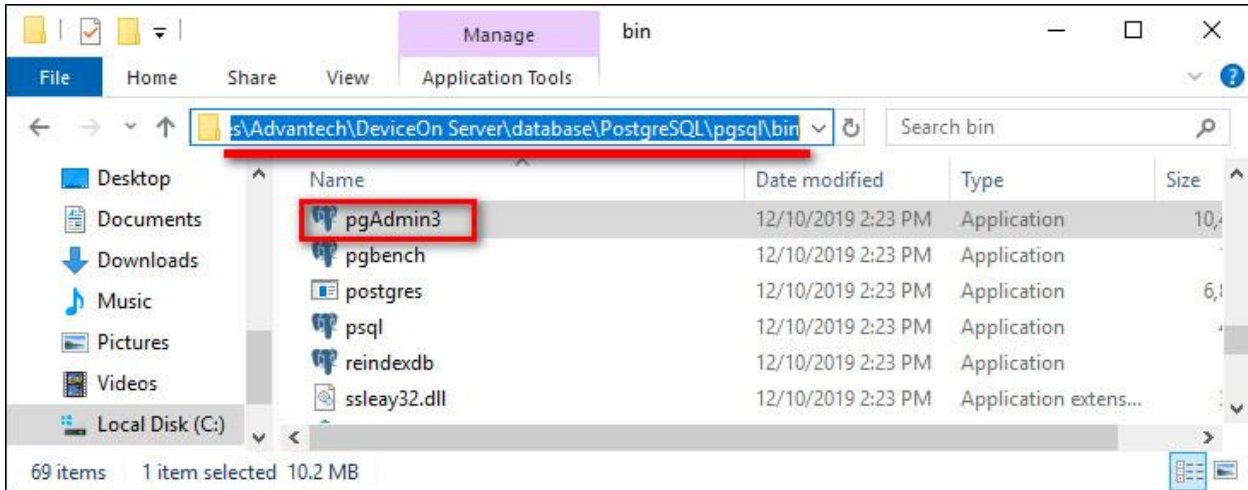


- PostgreSQL Service

The relational database (PostgreSQL) is used to store account, device, map, permission data etc. Click “**Stop**” to stop the PostgreSQL service.

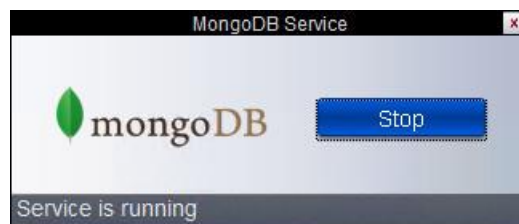


A GUI tool called “**pgAdmin3.exe**” providing access to the PostgreSQL database comes with the PostgreSQL installation and is located in the installation folder as shown below. The default account is “**postgres**” and the password is the one you defined during the installation. We recommend you do not delete/edit any schema, table or data , since DeviceOn might stop to work if data is corrupt or missing.



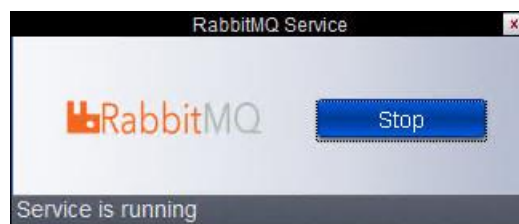
- **MongoDB Service**

To process sensor data from client devices, DeviceOn leverages MongoDB to provide better performance and compression rates than relational databases. Click **“Stop”** to stop the MongoDB service.



- **RabbitMQ Service**

RabbitMQ is one of the most popular open source message brokers, and is used as “IoT Hub” to exchange messages between the server and client devices. Click **“Stop”** to stop the RabbitMQ service.



- **Grafana Service**

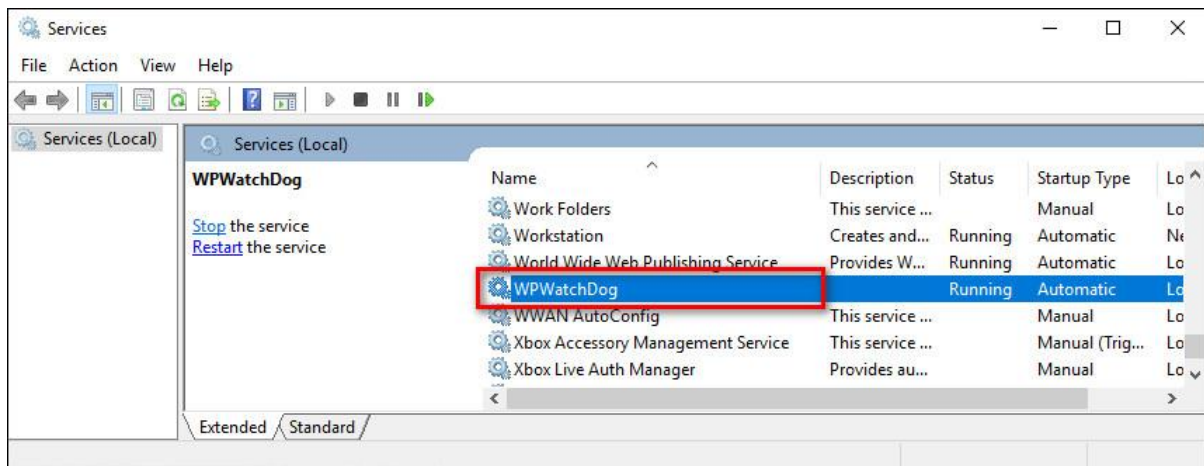
Grafana is a popular framework that allows you to query, visualize and alert on data from various data sources. DeviceOn supports a simple JSON API that as can be used as data source in Grafana, effectively making all DeviceOn data available to Grafana. Click **“Stop”** to stop the Grafana service.



3.1.2 Background Watchdog Service

- Watchdog Service

There is a Watchdog service (WP) that monitors the management service (DeviceOn and Provisioning Worker) and ensures all the functions work as expected.

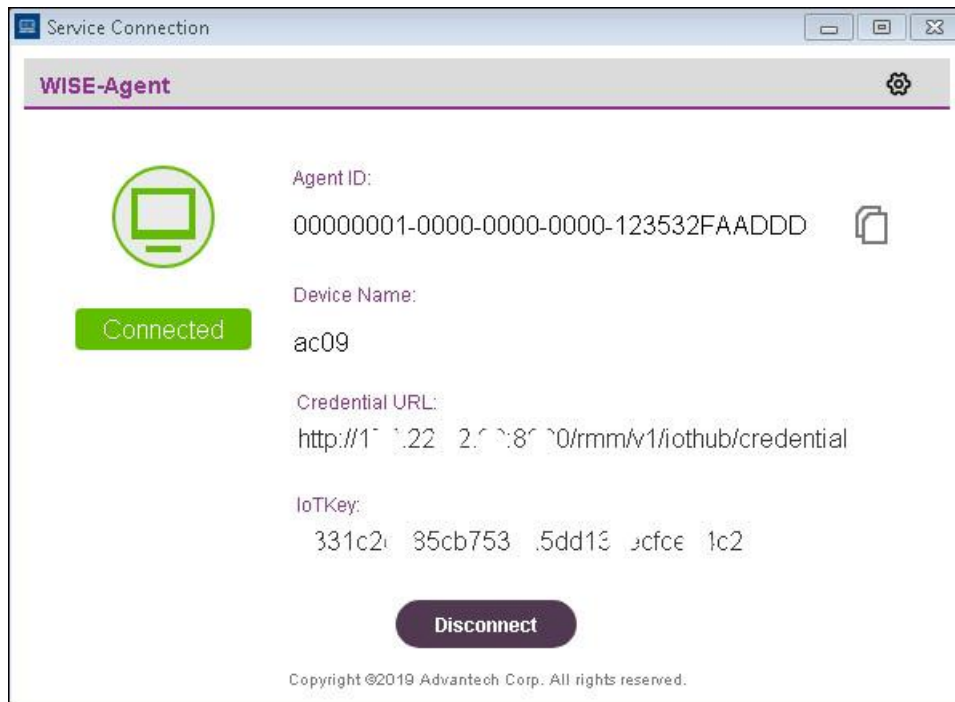


3.2 DeviceOn WISE-Agent

WISE-Agent runs as Windows service, so even without any user logged in, WISE-Agent will establish a connection to the DeviceOn server and the most of the features are supported. Section 3.2.1 explains how to use the WISE-Agent user interface to verify the current connection status and retrieve basic information of the client device. There is another Watchdog service monitoring the WISE-Agent client in order to avoid impact due to crashed or hanging processes.

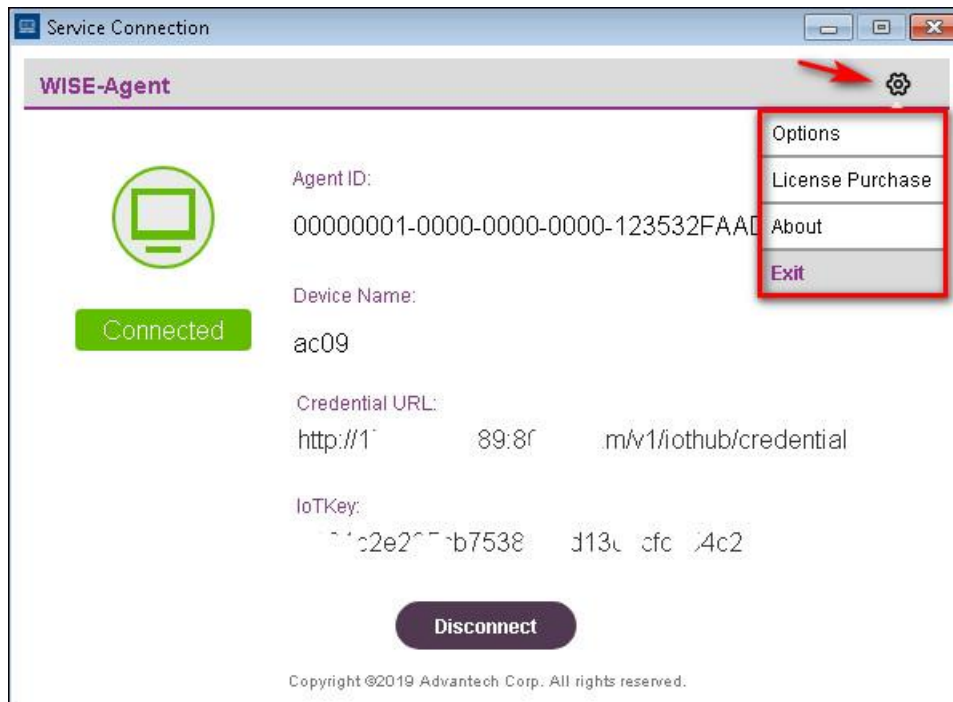
3.2.1 WISE-Agent Connection

If you followed the instructions to set up WISE-Agent and connect to the DeviceOn server/cloud, there should be a WISE-Agent shortcut on your desktop. If not, please refer to Section 2.3 to install WISE-Agent. After launching the WISE-Agent user interface, it will provide an overview of the connection status, device information (AgentID, Device Name) as well as connection credentials (Credential URL, IoTKey).



- **Agent ID:** Device unique ID - the default is 32 characters, prefix (20 characters) and MAC address (12 Characters)
- **Device Name:** Device name as shown on the DeviceOn server
- **Credential URL:** Connection URL, used to authenticate to DeviceOn Server
- **IoTKey:** Connection Key - each DeviceOn client has a unique key that will be used to establish the MQTT session
- **Disconnect:** To stop the device connection and data transmission, you can click “Disconnect” to stop the WISE-Agent service

If you would like to adjust the device name or connection parameters, please click the “Settings” icon on the top right and select “**Options**”.



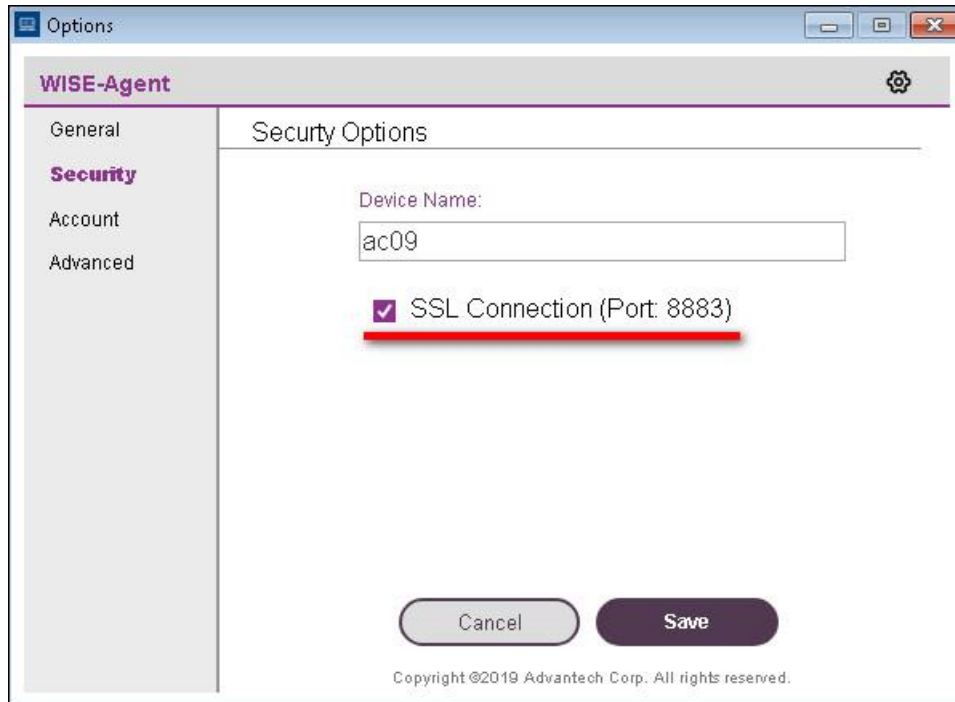
- Option -> **General**

This overview page provides information about “Device Name”, “Operating System” (Windows 7, 8, 10), “MAC Address” of the client, “Memory Capacity” and version of the Advantech SUSI Driver (if applicable). The version of the “Operating System” represents the [Windows kernel version](#). If the client device is an Advantech platform that is supported by SUSI, we recommend to download the latest SUSI driver from the [Advantech Support](#) site first. Please click [here](#) to obtain the latest driver version.



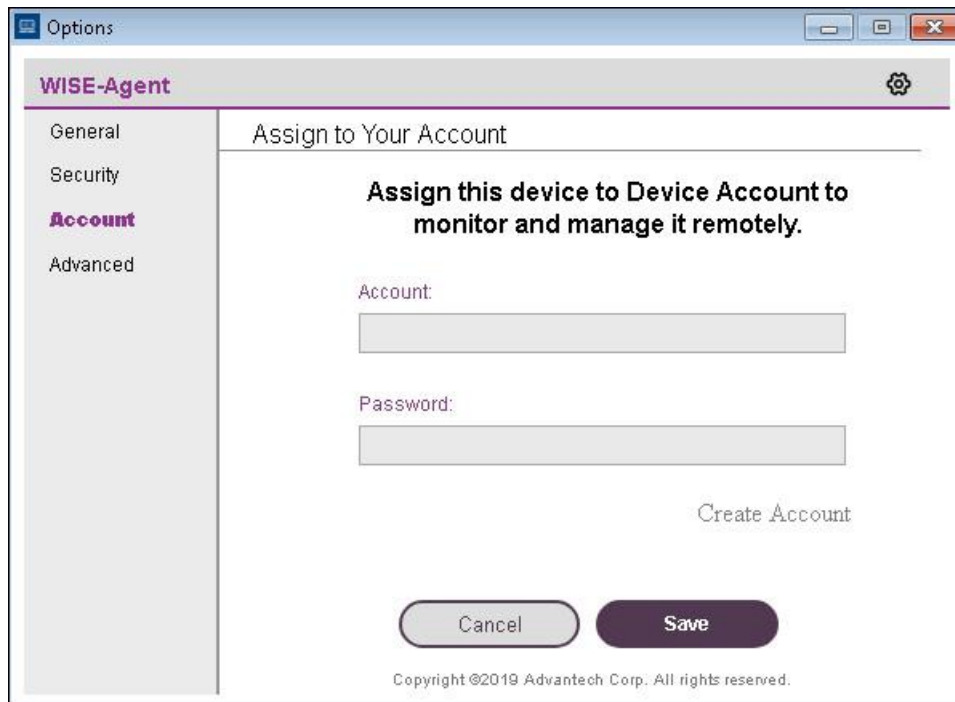
- Option -> **Security**

The communication protocol used for message exchange between the server and client is MQTT, an industry standard lightweight messaging protocol for small sensors and mobile devices. WISE-Agent provides the option to use MQTT with SSL encryption on port 8883, or MQTT without SSL on port 1883.



- Option -> **Account**

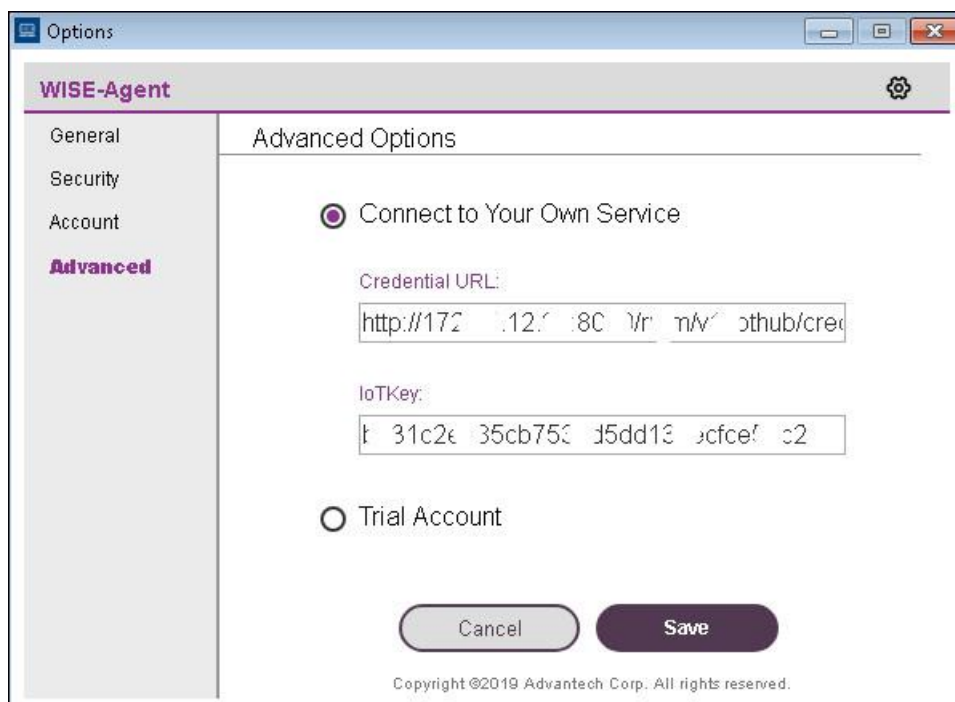
You can register on the DeviceOn trial site (<https://deviceonapp.wise-paas.com>) for a six-month trial account and use it with your device. Before you can create a trial account or enter trial account information, please go to the "Advanced" tab and select "Trial Account".



The screenshot shows the 'Options' window for 'WISE-Agent'. The 'Account' tab is selected in the left sidebar. The main area is titled 'Assign to Your Account' and contains the instruction: 'Assign this device to Device Account to monitor and manage it remotely.' Below this, there are two input fields: 'Account:' and 'Password:'. A 'Create Account' button is positioned to the right of the password field. At the bottom, there are 'Cancel' and 'Save' buttons. A copyright notice at the very bottom reads: 'Copyright ©2019 Advantech Corp. All rights reserved.'

- Option -> **Advanced**

Under the “Advanced” tab, you can select whether to connect to a DeviceOn server/cloud service, or whether to connect to the DeviceOn trial site (<https://deviceonapp.wise-paas.com/>). In case of trial site, you need to enter account information under the “Account” tab (see previous step) while for a regular DeviceOn server or cloud service, you need to enter the “Credential URL” and “IoT Key” here. Refer to “Step 2” in Section 2.3 on information how to obtain those.

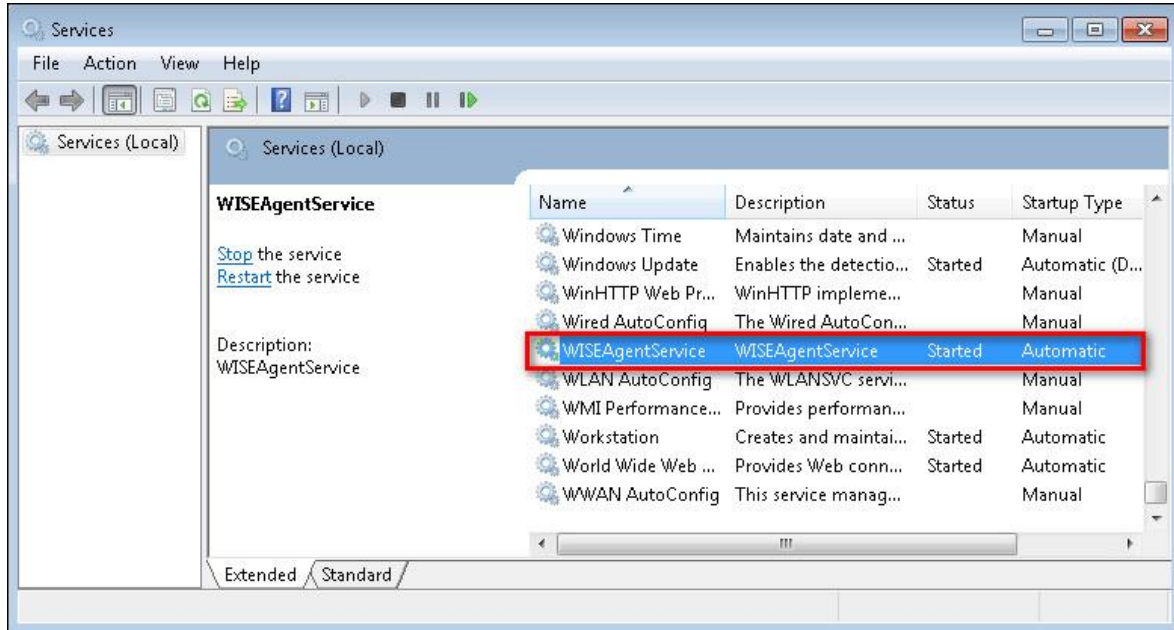


The screenshot shows the 'Options' window for 'WISE-Agent' with the 'Advanced' tab selected. The main area is titled 'Advanced Options'. It features two radio buttons: 'Connect to Your Own Service' (which is selected) and 'Trial Account'. Below the 'Connect to Your Own Service' option, there are two input fields: 'Credential URL:' with the value 'http://172.17.0.1:8080/v1/auth/cred' and 'IoTKey:' with the value 't-31c2e-35cb753-d5dd13-ecfce-c2'. Below these fields are 'Cancel' and 'Save' buttons. The same copyright notice is at the bottom: 'Copyright ©2019 Advantech Corp. All rights reserved.'

3.2.2 WISE-Agent Services

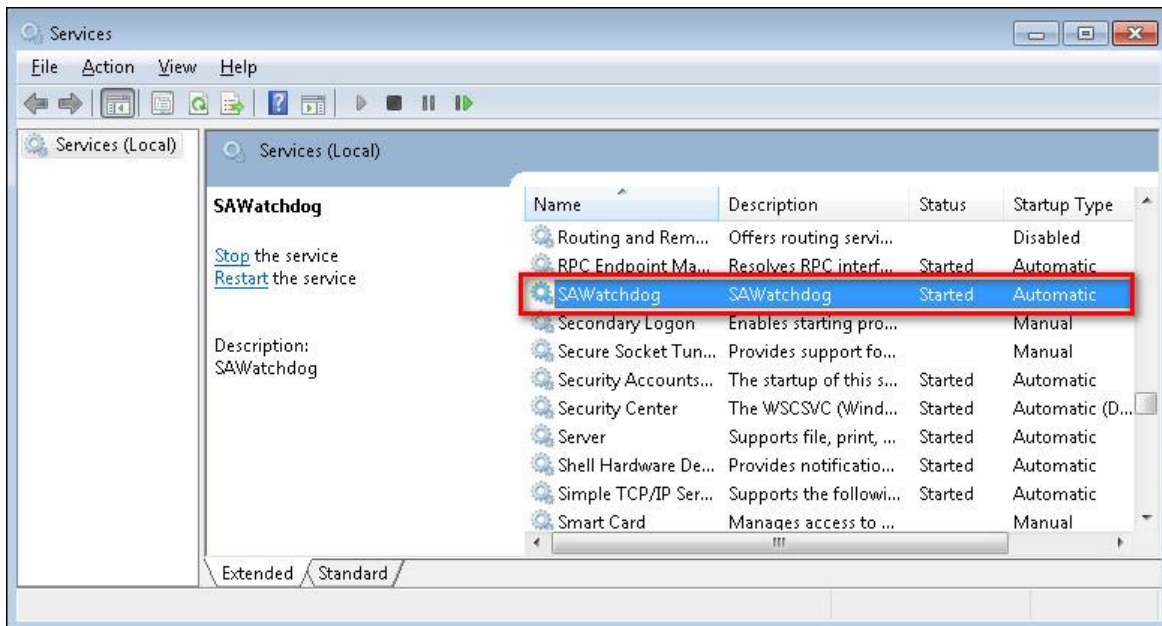
- Main Service

“WISEAgentService” is the main services that connects to the DeviceOn server/cloud service. The service is set to start automatically by default.



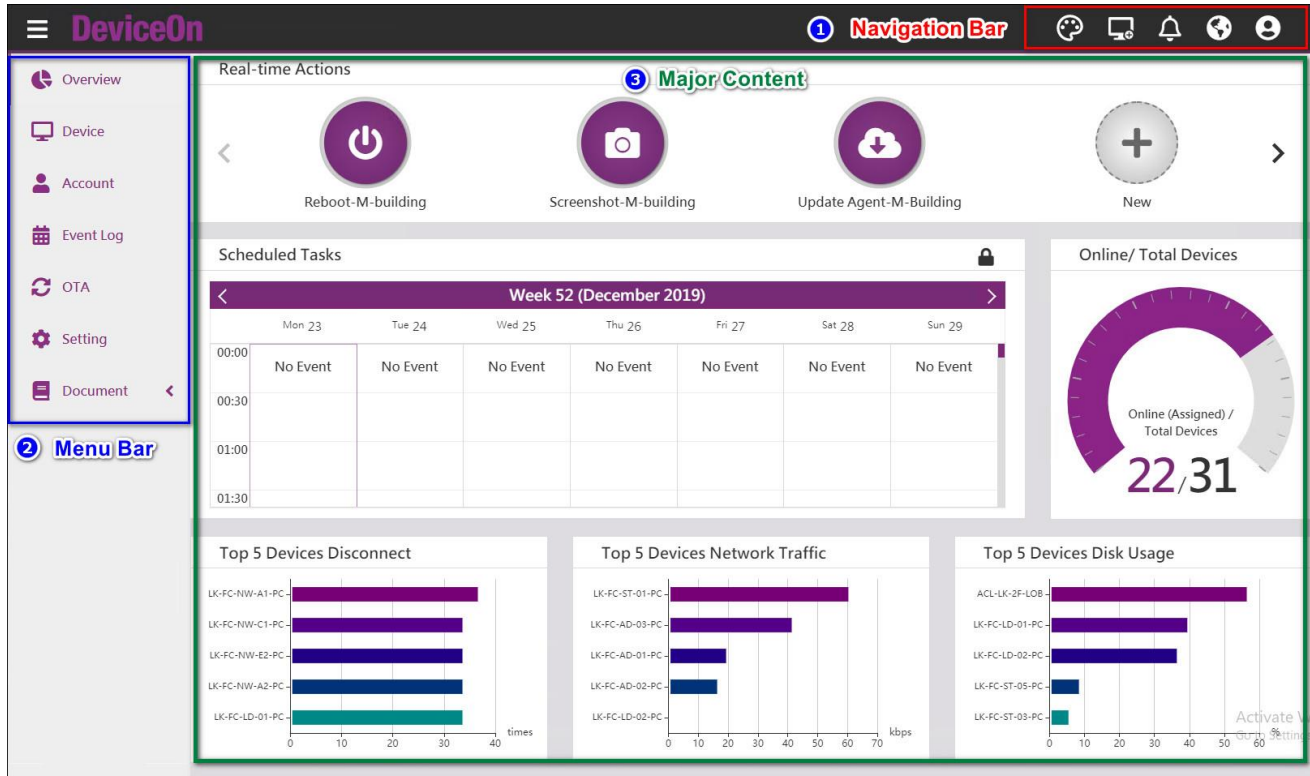
- Watchdog Service

The “SAWatchdog” service is a basic watchdog governing “WISEAgentService” in order to ensure service quality.



3.3 DeviceOn User Interface

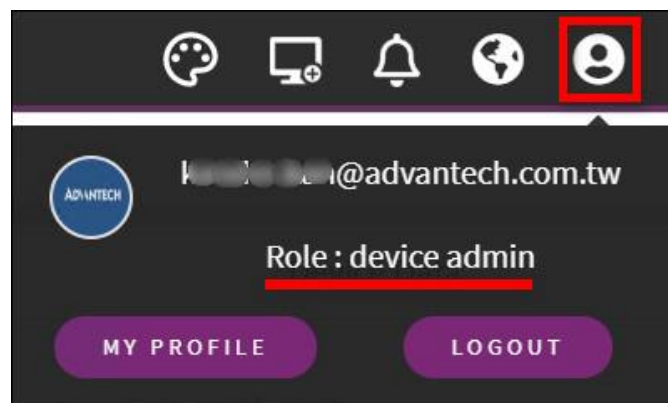
The DeviceOn web interface is based on the VUE framework and leverages the [Vuestic Admin](#) template. The user interface is divided into three main parts - the navigation bar at the top, the menu bar at the left and the main content in the center with.



Navigation Bar:

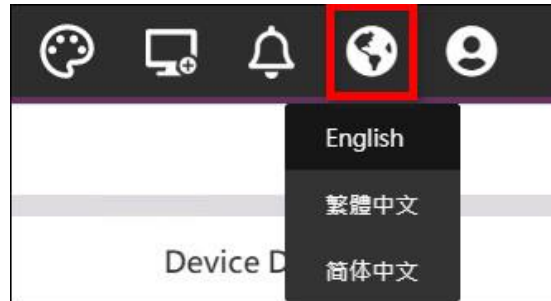
- Account Information

Click the account icon to show the currently logged in account and respective role. For more information, click “My Profile” to open the account page. (Menu Bar -> Account). Click “Logout” to log out from DeviceOn and remove personal information like cookies or tokens.



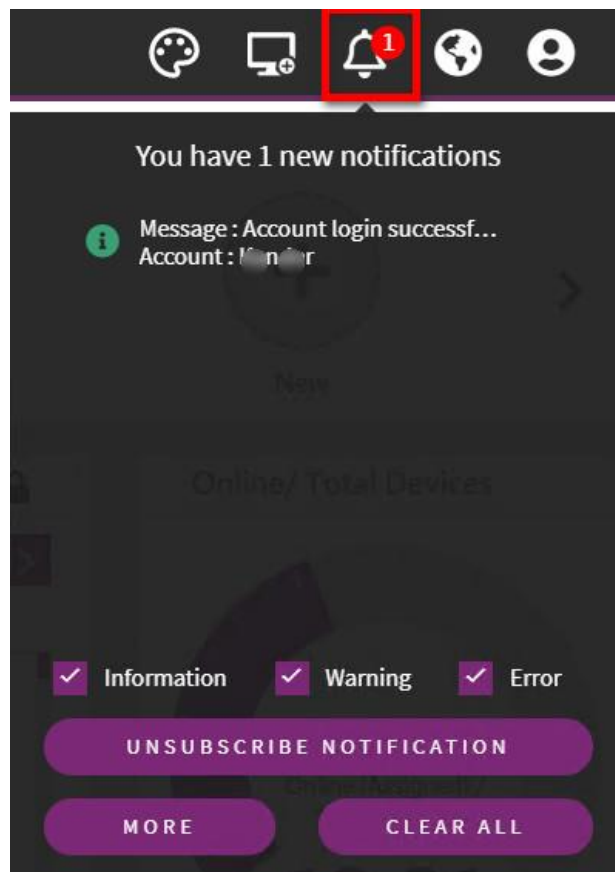
- Languages

DeviceOn supports multiple languages that can be changed by clicking the globe icon in the navigation bar. Currently there are three languages to choose from: English, Traditional Chinese and Simplified Chinese.



- Notification

If there are any active notifications, the number of event log messages is shown on the notification icon. Click the notification icon to see the event message summary. Three levels of events are supported: **“Information”**, **“Warning”** and **“Error”**, and the user can select which type of events should be shown on the user interface. For example, clicking the **“Unsubscribe Notification”** would disable any events in the screenshot shown below. Please note that after disabling events, the UI will not refresh automatically but needs to be refreshed manually. Click **“More”** to open the event log page (**Menu Bar -> Event Log**)



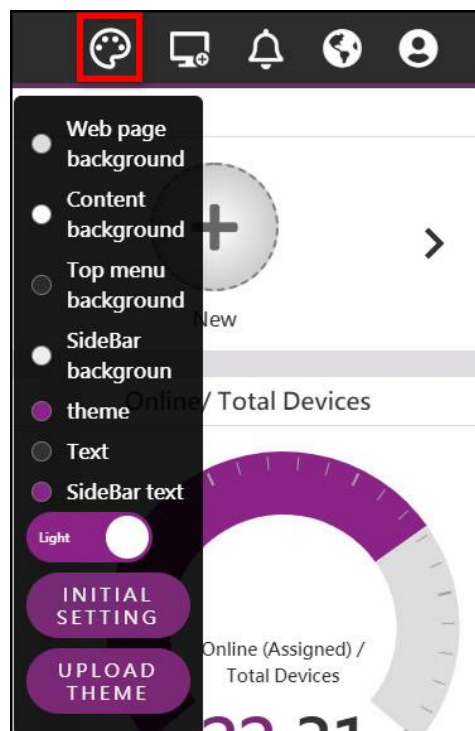
- **Device Onboarding**

To onboard devices, click the onboarding icon in order to download the WISE-Agent installer and in order to look up the required connection credentials. For more details on onboarding, please refer to Section 2.2.



- **Themes & Colors**

By default, DeviceOn uses a purple main color scheme. By clicking the color palette symbol, you can customize the UI theme and select individual colors for background, menu bar text etc.



3.3.1 DeviceOn Overview

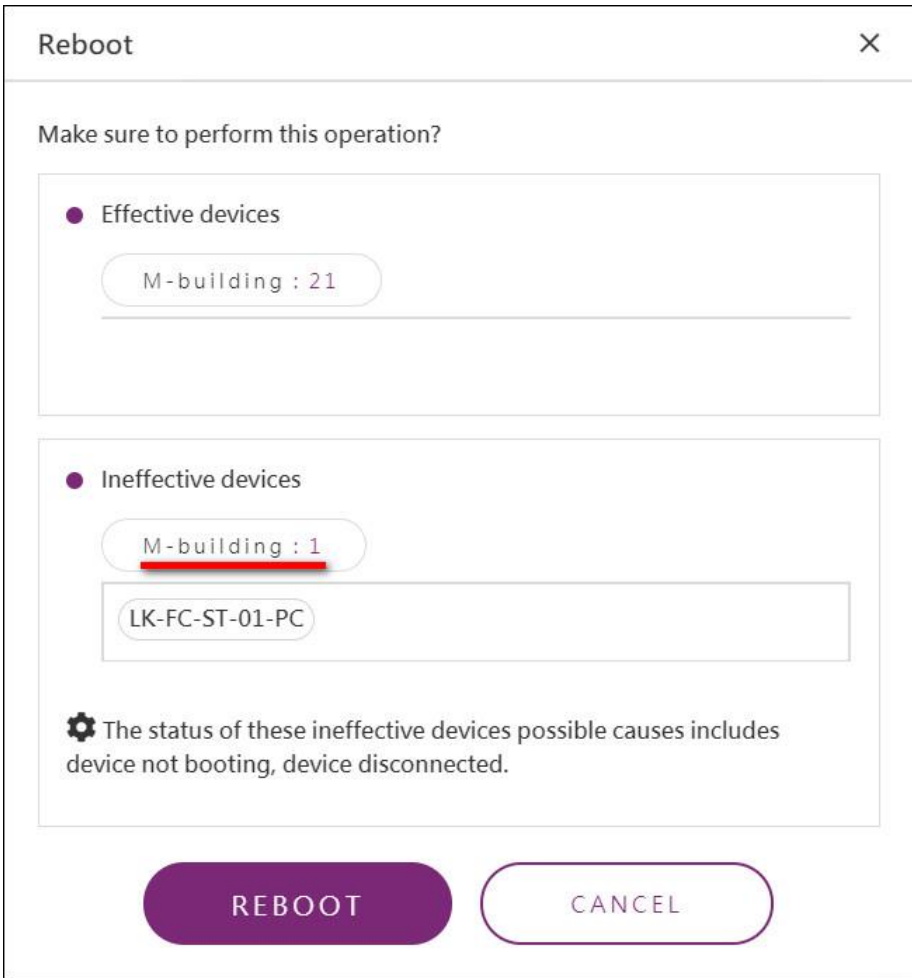
The overview provides quick access to real-time statistics for your managed devices. This information helps to monitor overall status as well as identifying high risk devices. Currently the overview includes Real-time Action, Scheduled Tasks, Online/Total Devices, Top 5 Statistics and Device Map.

- **Real-time Actions**

Real-time actions provide one-click access to certain actions defined for specific device groups, providing a shortcut for efficient management. Examples for actions are batch reboot, batch screenshot or batch updates.

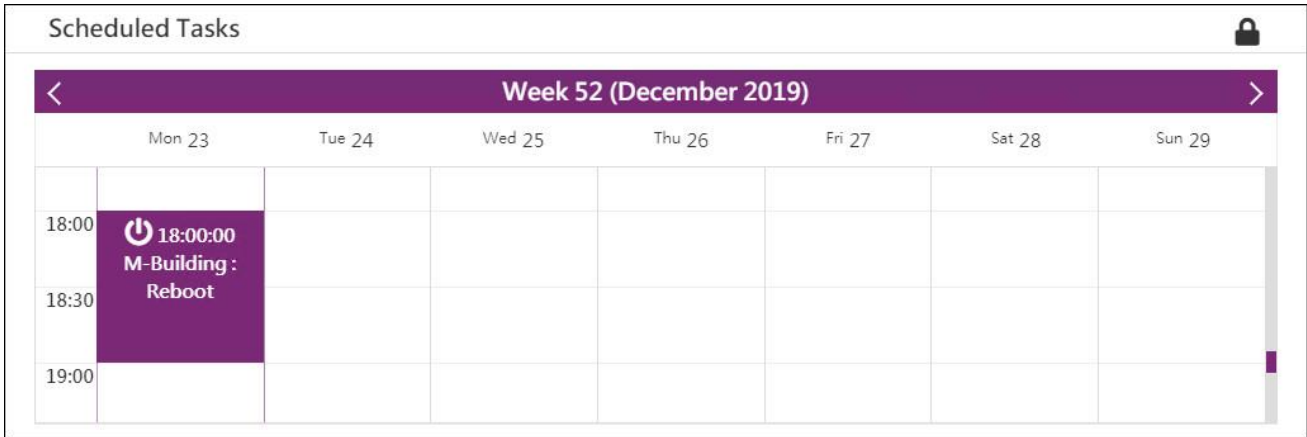


For example, once you click “Reboot”, a confirmation dialog will pop up and will indicate which devices will actually be affected. Click on the device group button to get more details (individual devices names).



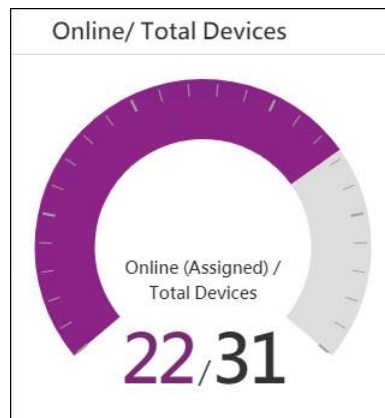
- Scheduled Tasks

In addition to real-time action, actions can be scheduled. An example for this is powering off or rebooting devices at a certain time of day. A calendar view is used to visualize upcoming tasks.












- Online / Total Devices

Shows the number of currently online devices as well as total number of managed devices (assigned to account).



Clicking this overview will bring up a detailed device list including status as well as group membership information.

DeviceList 

SETTING STATUS 	DEVICE NAME 	DEVICE GROUP NAME 	WAKE-ON-LAN 	MESSAGE 
	ACL-LK-2F-LOB	E-building 2F	Direct Mode	
	LK-FC-AD-01-PC	M-building aisle	Direct Mode	
	LK-FC-AD-02-PC	M-building aisle	Direct Mode	

- Top 5 (High-Risk) Statistic

The figure consists of six horizontal bar charts arranged in a 2x3 grid, each displaying the top 5 devices for a specific metric. The bars are color-coded: purple for the top two devices, blue for the next two, and green for the bottom one.

- Top 5 Devices Disconnect:** Shows the number of disconnects. LK-FC-NW-A1-PC is the highest at approximately 37.
- Top 5 Devices Network Traffic:** Shows network traffic in kbps. LK-FC-ST-01-PC is the highest at approximately 62.
- Top 5 Devices Disk Usage:** Shows disk usage in %. ACL-LK-2F-LOB is the highest at approximately 55%.
- Top 5 High Risk (Disk Health):** Shows disk health percentage. LK-FC-ST-02-PC is the lowest at approximately 35%.
- Top 5 Devices CPU Usage:** Shows CPU usage in %. LK-FC-LD-02-PC is the highest at approximately 42%.
- Top 5 Devices Memory Usage:** Shows memory usage in %. LK-FC-AD-03-PC is the highest at approximately 43%.

Metric	Device	Value
Top 5 Devices Disconnect	LK-FC-NW-A1-PC	37
	LK-FC-NW-C1-PC	33
	LK-FC-NW-E2-PC	33
	LK-FC-NW-A2-PC	33
	LK-FC-LD-01-PC	33
Top 5 Devices Network Traffic	LK-FC-ST-01-PC	62
	LK-FC-AD-03-PC	35
	LK-FC-AD-01-PC	15
	LK-FC-AD-02-PC	12
	LK-FC-LD-02-PC	0
Top 5 Devices Disk Usage	ACL-LK-2F-LOB	55
	LK-FC-LD-01-PC	38
	LK-FC-LD-02-PC	35
	LK-FC-ST-05-PC	8
	LK-FC-ST-03-PC	5
Top 5 High Risk (Disk Health)	LK-FC-ST-02-PC	35
	LK-FC-NW-C2-PC	85
	LK-FC-LD-01-PC	95
	LK-FC-NW-A2-PC	98
	LK-FC-NW-D2-PC	100
Top 5 Devices CPU Usage	LK-FC-LD-02-PC	42
	LK-FC-NW-A1-PC	40
	LK-FC-NW-C1-PC	35
	LK-FC-LD-01-PC	33
	LK-FC-NW-A2-PC	32
Top 5 Devices Memory Usage	LK-FC-AD-03-PC	43
	LK-FC-AD-02-PC	42
	LK-FC-AD-01-PC	40
	LK-FC-ST-02-PC	38
	LK-FC-ST-03-PC	38

- Device Map

The map displays the Taipei metropolitan area, highlighting the distribution of various device groups across the region. Major landmarks and locations include:

- Taoyuan:** Taoyuan International Airport, Sun Yat-sen Memorial Hall, National Sun Yat-sen Memorial Hall, and various parks and museums.
- New Taipei City:** Sun Yat-sen Memorial Hall, National Sun Yat-sen Memorial Hall, and various parks and museums.
- Taipei:** Sun Yat-sen Memorial Hall, National Sun Yat-sen Memorial Hall, and various parks and museums.

The map is titled "Device Map" and includes a legend for "SELECT DEVICE GROUPS".

3.3.2 Device Management

DeviceOn

Home > Device

Device List 1 Device Monitoring 2 Remote Control 3 Device Data 4

SELECT ACCOUNT: Kander SELECT DEVICE GROUPS: --- All --- SELECT STATUS: All Keyword Search

SETTING STATUS	DEVICE NAME	UPGRADE	POWER	PROTECTION	BACKUP&RECOVERY	DEVICE GROUP NAME	WAKE-ON-LAN	MESSAGE
●	ACL-LK-2F-LOB	Upgrade	Power off Restart Sleep Intel AMT			E-building 2F	Direct Mode	
●	LK-FC-AD-01-PC	Upgrade	Power off Restart Sleep Intel AMT			M-building aisle	Direct Mode	
●	LK-FC-AD-02-PC	Upgrade	Power off Restart Sleep Intel AMT			M-building aisle	Direct Mode	
●	LK-FC-AD-03-PC	Upgrade	Power off Restart Sleep Intel AMT			M-building aisle	Direct Mode	
●	LK-FC-LD-01-PC	Upgrade	Power off Restart Sleep Intel AMT	Upgrade Protect		M-building aisle	Direct Mode	
●	LK-FC-LD-02-PC	Upgrade	Power off Restart Sleep Intel AMT	Upgrade Protect		M-building aisle	Direct Mode	

● Device List

The device could be assigned to multiple accounts and device groups; therefore, you could leverage filter to find your device through **Account**, **Device Group** or **Keyword**.

Device List Device Monitoring Remote Control Device Data

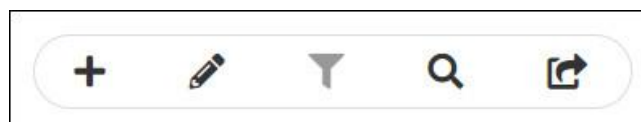
SELECT ACCOUNT: dandan.yao@advantech.com.cn SELECT DEVICE GROUPS: --- All --- SELECT STATUS: All Keyword Search

Filter

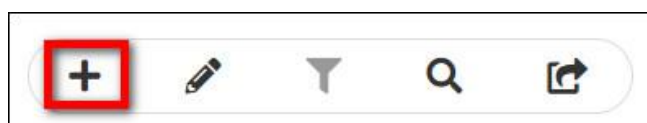
DEVICE STATUS	DEVICE NAME	UPGRADE	POWER	PROTECTION	BACKUP&RECOVERY	DEVICE GROUP NAME	WAKE-ON-LAN	MESSAGE
●	DESKTOP-NRB0J...		Power off Restart Sleep Hibernate			Default	Not Set	
●	ac09	Device Upgrade	Power off Restart Sleep	Protect	Backup Recovery	Default	Not Set	

2 records

Here is action bar for add, edit, search or export for below table devices.



Click the icon to add devices, that's similar to device onboarding, download WISE-Agent, setup to your local device and grouping.



1
 Device OnBording

2
 Select Devices

3
 Confirm

Setup your local device

Try to setup your local device, install WISE-Agent and connect to DeviceOn

Credential URL

https://api-.../v1/serviceCredentials

IoT Key

f5c...bc1...22c...n

Download

(WISE-Agent : Available for Windows 7+ , If Available for Ubuntu 16.04 please [contact us](#))

Hint: To fast device onboarding, please put the WISE-Agent and credential file (Agent.config) into same folder.

Next

Click the edit icon to display “Delete” and “Edit” options on each device list.

+	1				
DELETE	EDIT	DEVICE STATUS	DEVICE NAME		
		2	DESKTOP-NRB0...		
			ac09		
2 records					

You could edit device name, assign to different accounts, device groups in “Edit Device”

← Edit Device

AGENT ID
00000001-0000-0000-0000-000BAB7E1D30

AGENT NAME
DESKTOP-NRB0J2A


SELECT ACCOUNT
c...@advantech

DEVICE GROUPS
Default

y...@advantech.com.cn : Default
 x
 c...@advantech.com.cn : Default
 x

Save

If you would like to know a device be assigned to which account and device group, click search icon to enter Agent ID (from your WISE-Agent UI) to understand.



Device Belonging Search

AGENT ID

00000001-0000-0000-0000-00003A7E03

Search

CANCEL

Click on export icon to export devices that in the table as CSV file.



Device Name	Agent ID	WAKE-ON-LAN	Mac	Message	Status
DESKTOP-NRB0J2A	00000001-0000-0000-0000-00003A7E03	Not Set	000E...7E1 30		Device Online
ac09	00000001-0000-0000-0000-1234567890	Not Set	12 321 AD 0		Device Offline

Actually, you cloud do lots of remote action on the device.

DEVICE STATUS	DEVICE NAME	UPGRADE	POWER	PROTECTION	BACKUP&RECOVERY	DEVICE GROUP NAME	WAKE-ON-LAN	MESSAGE
	DESKTOP-NRB0J2A...					Default	Not Set	
	ac09	 Device Upgrade				Default	Not Set	


- ✧ **Device Status:** Green light represent device connected, gray for disconnected and orange for device abnormal, due to device over threshold.
- ✧ **Device Name:** Device name, click name to get more deice information, such as platform, operation system, MAC, memory, etc.

Device Detailed Information		
AGENT NAME DESKTOP-NR80J2A	AUTO REPORT ON	BIOS (D570X036)
AGENT ID 00000001-0000-0000-0000-000B87E1D30	STATUS MESSAGE None	MAC 000B87E1D30
DEVICE GROUPS Default	PRODUCT WISE-Agent	CPU Intel(R) Celeron(R) CPU N2930 @ 1.83GHz
WAKE-ON-LAN Not Set	MANUFACTURER Advantech	MEMORY 4083144 KB
CONNECTION STATUS Connected	VERSION 1.3.3.0	LAST CONNECTED AT 2019/12/24 14:35
	PLATFORM DS-570	
	OPERATING SYSTEM Windows 10 Enterprise LTSC 2019 X64	

- ✧ **Upgrade:** WISE-Agent upgrade icon, if there is new version released by Advantech, it will check and show the icon automatically.

Upgrade

DeviceName	ac09
Device Version	<u>1.2.16.0</u>
Latest Version	<u>1.3.3.0</u>



CONFIRM

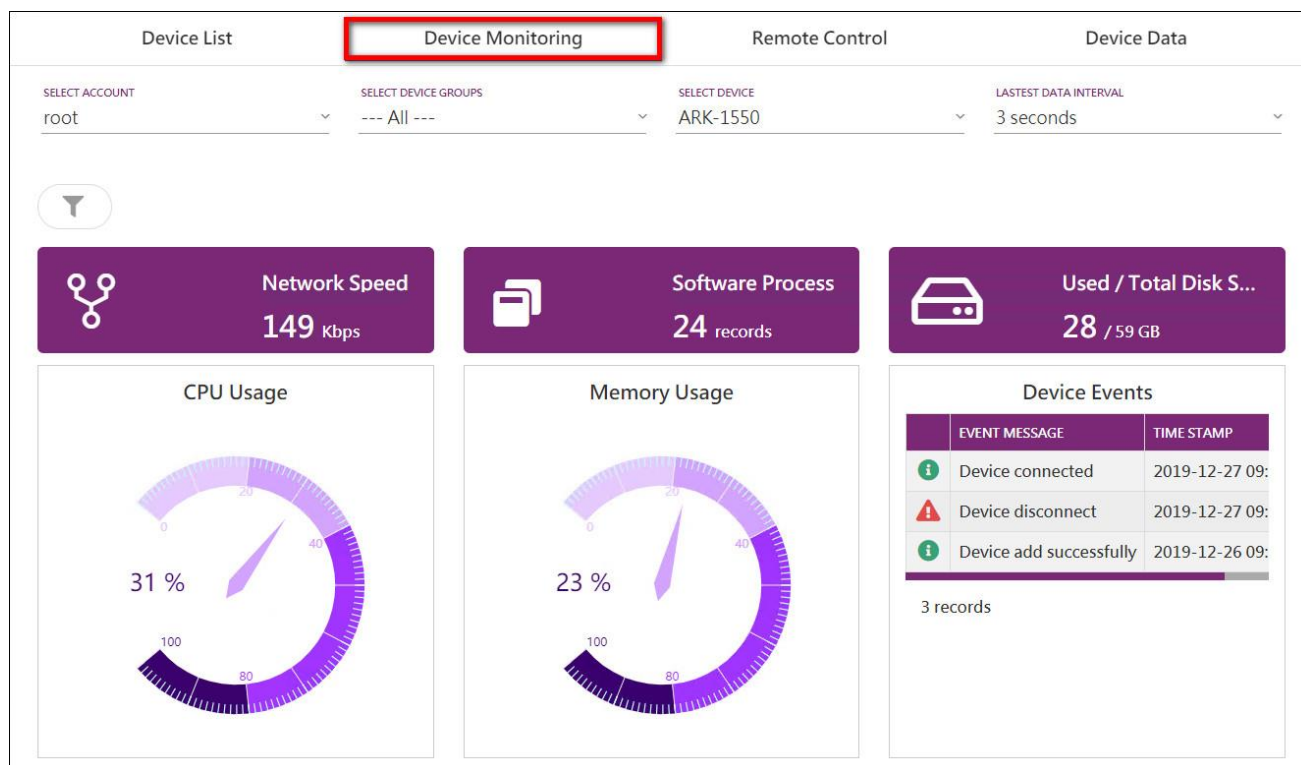
CANCEL

- ✧ **Power:** Power On/Off, Restart, Sleep and hibernate, the actions depend on your device supported.
- ✧ **Protection:** Power-by McAfee white-list protection mechanism to solidify device system. After enable, 3rd execution file, bat, DLL cannot be launch. Please go to **Setting** -> **Provision**-> **Protection** to install first.
- ✧ **Backup & Recovery:** Power-by Acronis to backup/recovery device runtime system partition. Please go to **Setting** -> **Provision**-> **Backup/Recovery** to install first.
- ✧ **Device Group Name:** Device belong to which device groups.
- ✧ **Wake-On-LAN:** Wake-On-LAN mode for device, three mode to power your device up, “**Direct Mode**”, “**Agent Mode**” and “**Repeater Mode**”. The magic package sent by DeviceOn Server call “Direct Mode”, but cannot through different network. Therefore, to overcome this limitation, through another Agent or Router to send, forward magic packet. Please go to **Setting** -> **Provision**-> **Power On** to configure.
- ✧ **Message:** Device current status

● Device Monitoring

On this page, you could get real-time information about the device that you selected. The information

includes general PC status, such as network speed, software process, disk healthy, CPU and memory usage. If the device is Advantech industrial PC and SUSI driver supported, the RPM (Revolution(s) Per Minute) of CPU FAN, system, board level voltage, temperature is displayed on the page.



Some of devices support multiple network cards, especial industrial PC. Click on the network button to retrieve others.



Network Usage Detail

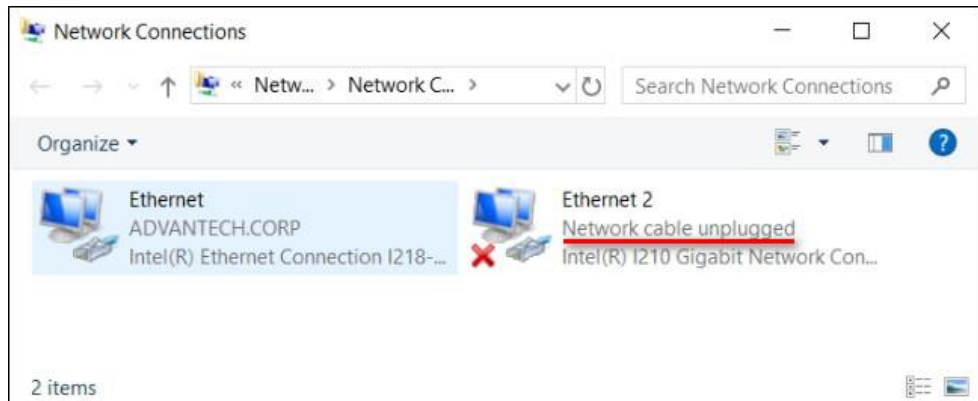
NAME	DESCRIPTION	STATUE	LINK SPEED (MBPS)	US
Index1^--Ethernet	Intel(R) Ethernet Connection I218-LM	Connected	1000	0.0
Index2^--Ethernet 2	Intel(R) I210 Gigabit Network Connection	Disconnect	0	0.0

2 records

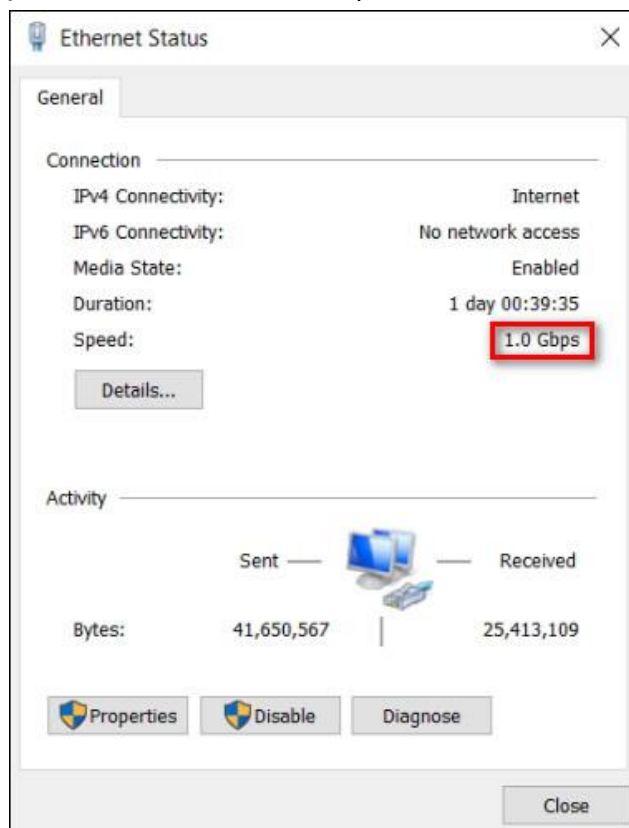
CONFIRM

✧ **Name:** Name of network card

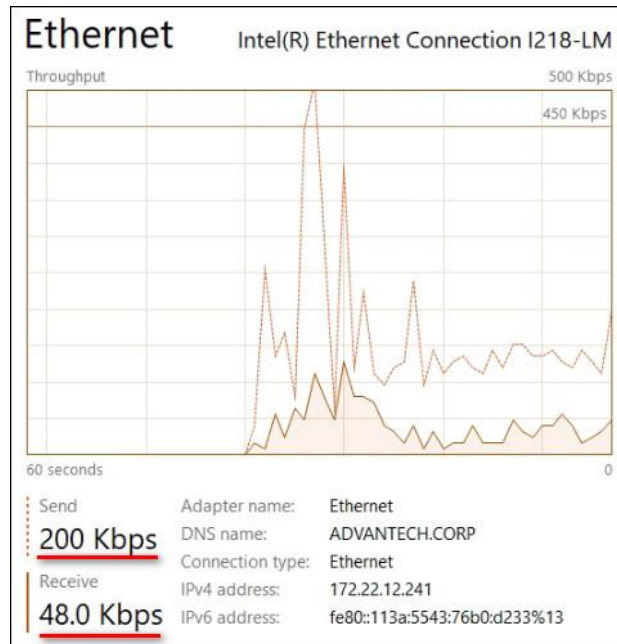
- ✧ **Description:** network description
- ✧ **State:** Network connected or disconnected, for example, ethernet cable plugin or not.



- ✧ **Link Speed (MBPS):** Network maximum link speed



- ✧ **Usage:** Network current usage, **Speed/Link Speed**.
- ✧ **Speed (MBPS):** Send plus receive data rate.



Click on **Software Process** to show **current user process** list, if your device system not login, the result might be zero.



Hover your mouse on the process list, you could restart or terminal it.

Software Process Detail

PROCESS NAME	PID	CPU USAGE	MEMORY USAGE
SearchUI.exe	6964	0	130,628
explorer.exe	5488	0	111,336
ServerConnection.exe	7372	0	39,800
ServerConnection.exe	1548	0	33,276
RuntimeBroker.exe	7108	0	29,116
AnyDesk.exe	7400	0	21,460
AnyDesk.exe	4968	0	17,848
smartscreen.exe	3272	0	17,292
ShellExperienceHost.exe	6700	0	17,248
sihost.exe	676	0	13,772

<< < 1 2 3 > >>

Showing 1 to 10 of 25 records

CONFIRM

For hard drive status, not only include current **Used Storage**, but **Healthy** and **Power on Time**. The healthy is based on Acronis healthy model, that calculate on edge side, if you are interested, reference the [official page](#).

Disk Storage Detail
×

Disk Partition

DISK NAME	USED STORAGE (MB)	TOTAL STORAGE (MB)
Disk C:	29,454	60,505

1 record

Disk Hardware

INDEX	NAME	TYPE	HEALTH (%)	TEMPERATURE (°C)	POWER ON TIME (HOUR)
0	SQF-S25M4-64G-S9C	SQFlash	99	0	7789289

1 record

CONFIRM

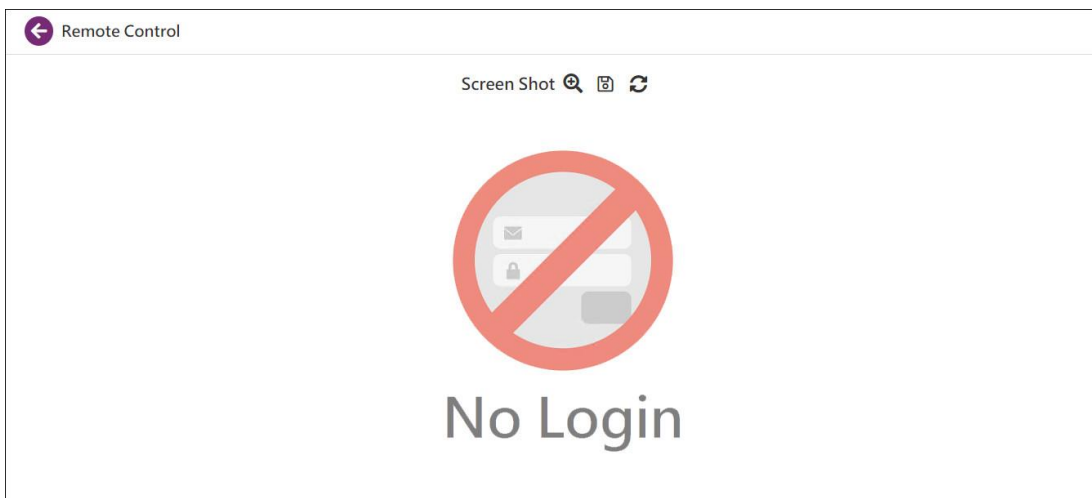
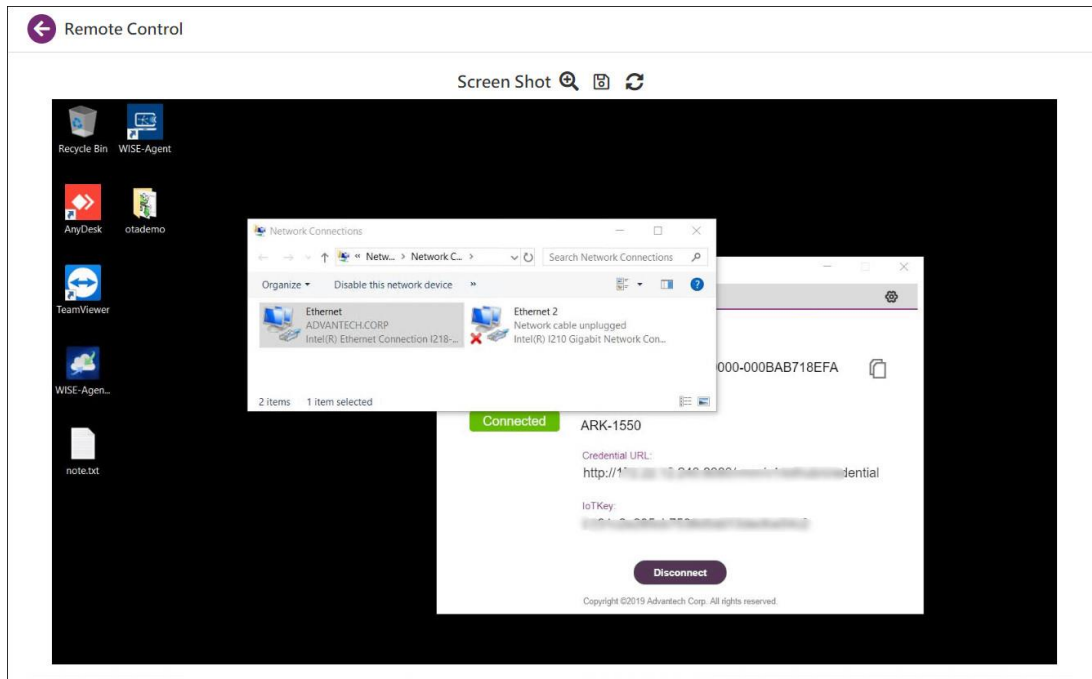
- Remote Control

If you need to debug, diagnostic to your devices, actually, do not need go to field side. Through DeviceOn remote control to manage to reduce your operation effort. Basically, there are three functions (**Screenshot**, **Terminal** and **Remote Desktop**) for most devices.

Device List	Device Monitoring	Remote Control	Device Data
SELECT ACCOUNT root	SELECT DEVICE GROUPS --- All ---	SELECT DEVICE ARK-1550	
<div> </div> <div> <div> Screen Shot </div> <div> Terminal </div> <div> Remote Desktop </div> <div> Audio Volume Control <div> <div></div> <div></div> </div> </div> <div> LVDS Screen Brightness <div> <div></div> <div></div> </div> </div> <div> USB Drives Free to Access </div> <div> Function Key Available </div> <div> WatchDog Protection Disabled </div> <div> Windows Notification Enabled </div> <div> Touch Screen Enabled </div> <div> Touch Gesture Disabled </div> <div> UWF Protection Disabled </div> </div>			

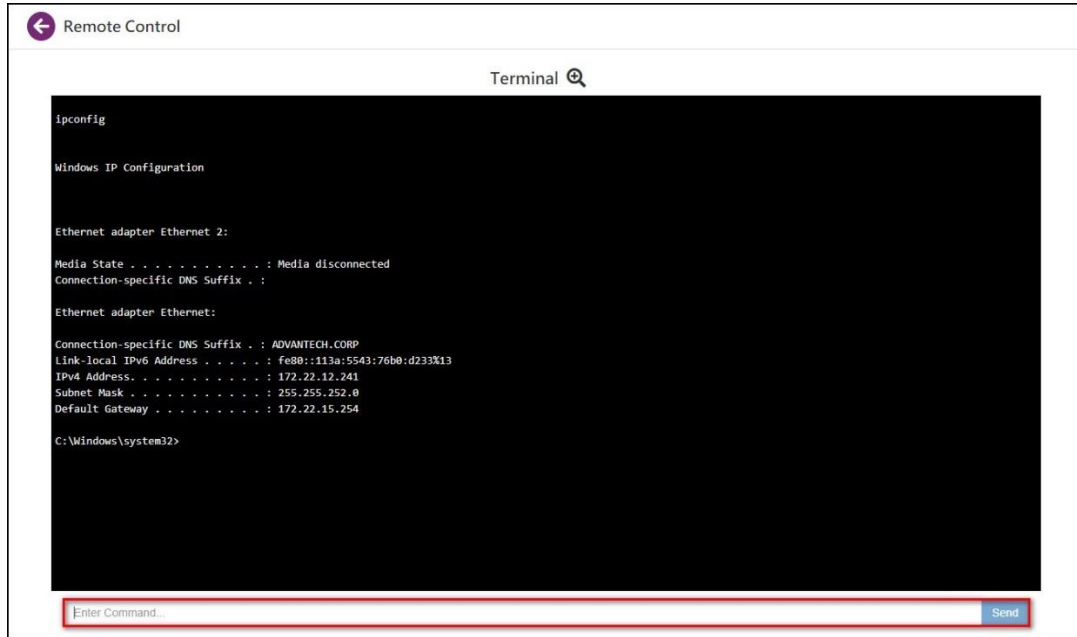
[Screenshot]

Through the Screenshot to get device real-time screen, there is a limitation, your device **must login to operation system**, otherwise, cannot capture screen and shown “No Login”



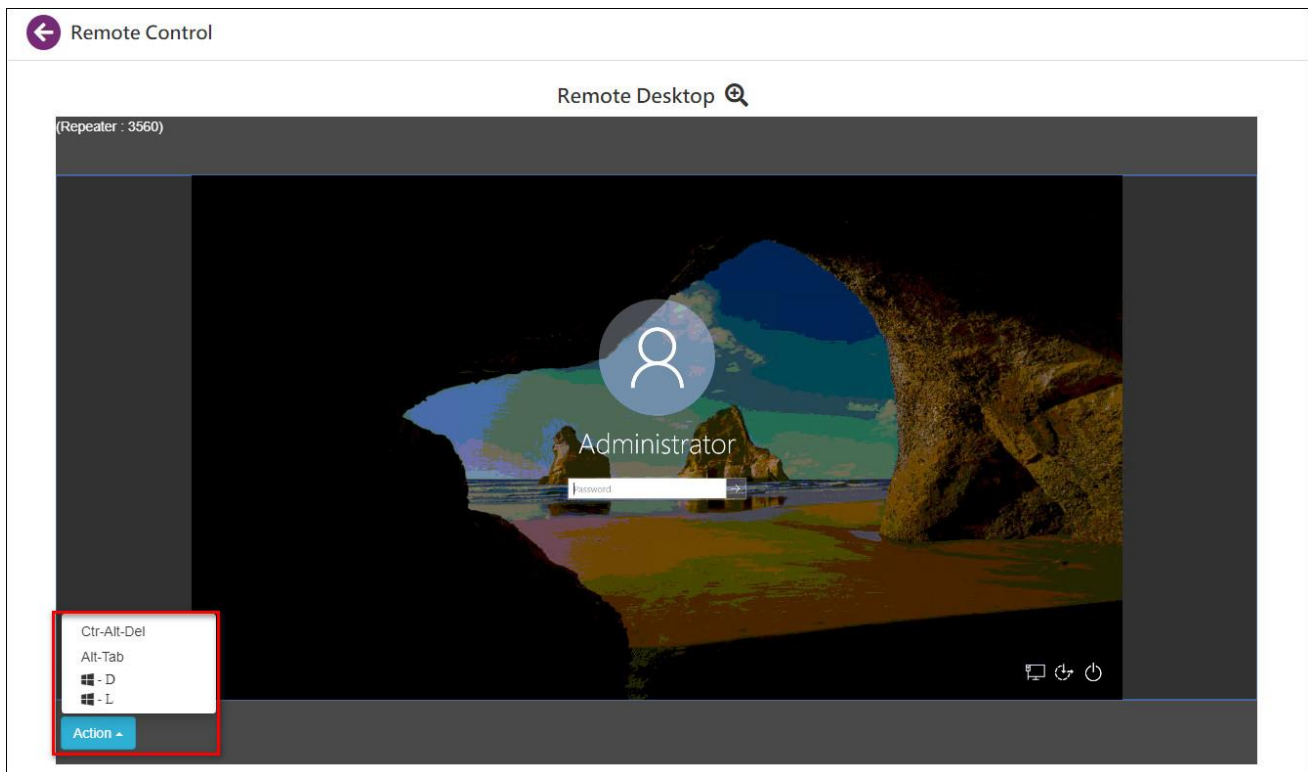
[Terminal]

To terminal support any command to your devices, for instance, realize your device IP, traceroute the network or copy/view file on the device.



[Remote Desktop]

DeviceOn leverage VNC (Virtual Network Computing) technology to achieve remote desktop, to bridge different network between public and private. User do not need to install any program, App on their laptop or mobile devices. Through DeviceOn website to remote desktop to debug and diagnostic.



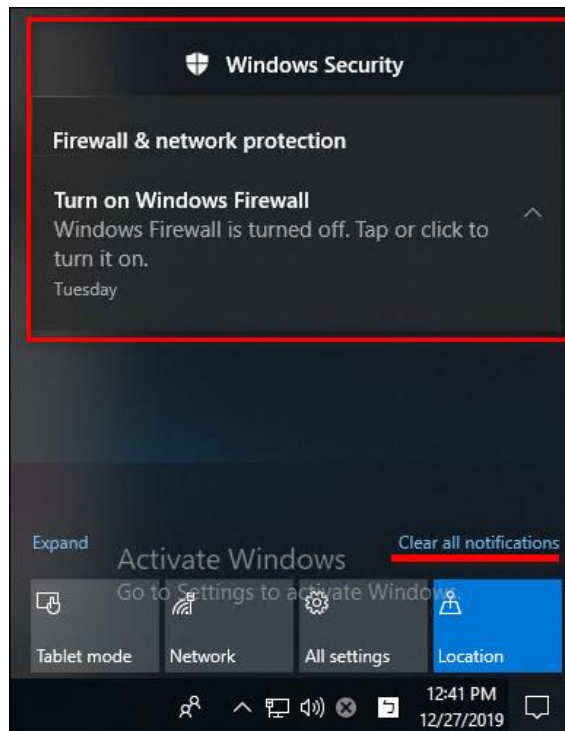
[Advanced Control]

For others features depend on your device operation system and hardware. DeviceOn integrate Windows Lockdown features on LTSC (Long Time Service Channel) and LTSB (Long Time Service Branch) to provide advanced control, such as “**Block USB Drives**”, “**Keyboard Filter**”, “**Block Windows Notification**”, “**Block Touch, Gesture**” and “**UWF (Unified Write Filter)**”.

[USB Drive]: Prevent threats from outside **USB drives**, not include keyboard, mouse.

[Function Key]: Disables **Ctrl**, **Alt**, and **WinKey**.

[Windows Notification]: Block application notification.



[Touch Screen]: Disable touch control

[Tough Gesture]: Disable gesture control

[UWF Protection]: To protect your drives by intercepting and redirecting any writes to the drive (app installations, settings changes, saved data) to a virtual overlay. The virtual overlay is a temporary location that is usually cleared during a reboot or when a guest user logs off.

Benefits:

- Provides a clean experience for thin clients and workspaces that have frequent guests, like school, library or hotel computers. Guests can work, change settings, and install software. After the device reboots, the next guest receives a clean experience.
- Increases security and reliability for kiosks, IoT-embedded devices, or other devices where new apps are not expected to be frequently added.
- Can be used to reduce wear on solid-state drives and other write-sensitive media.

For **backlight**, **brightness** and **Watchdog** only support on Advantech hardware platform with SUSI

driver, please download from [Advantech Support](#) site.

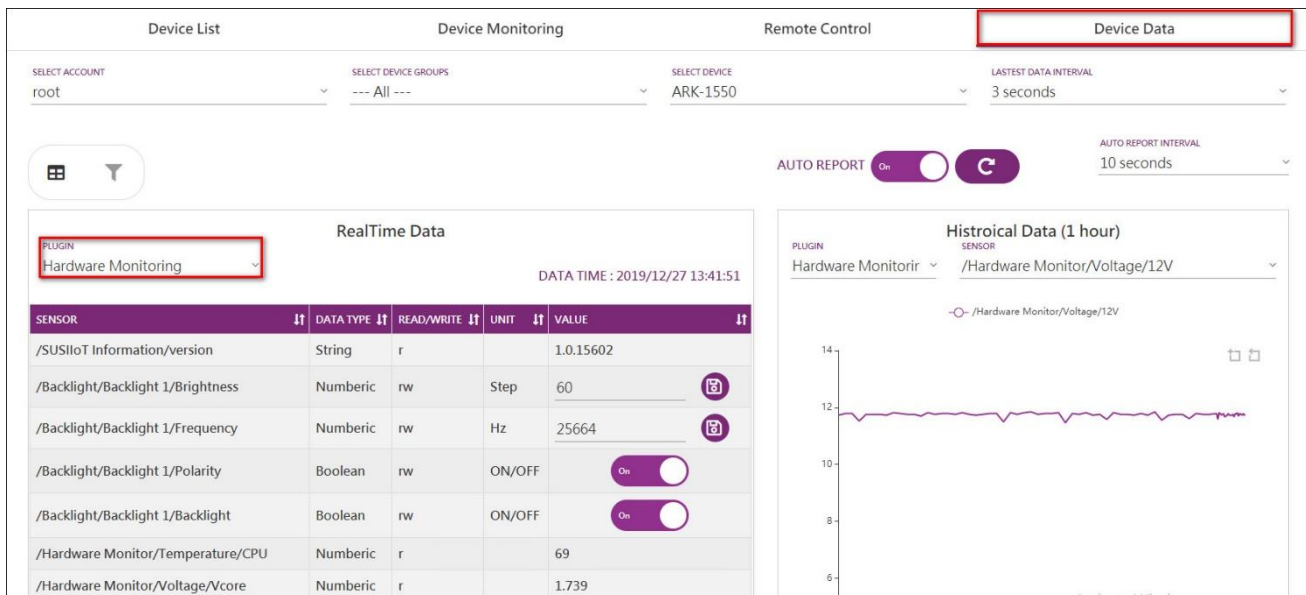
[LVDS, Backlight and Brightness]: Turn on/off LVDS backlight for power saving.

[Watchdog Protection]: Hardware level watchdog to prevent BSoD (Blue Screen of Death) or system hang without any response. If happened, watchdog will restart your device automatically. There is an tool call [NotMyFault](#) that you can use to crash, hang, and cause kernel memory leaks on your Windows system.

Benefits: Avoid embarrassing moment, if BSoD on your Signage devices over the airport, department store and public area.

● Device Data

Raw data of each plugin on devices, user could get real-time and historical data on this page. To data analysis and aggregation, user could adjust data report interval or reset to default (60s) for basic sensors.



3.3.3 Account Management

The first step to manage device is login to DeviceOn, therefore, you could start to invite, edit other accounts on this page. There are 3 tabs on account management.

DeviceOn

Home > Account

Overview

Device

Account

Event Log

OTA

Setting

Document

1 My Profile

2 Management

3 Device Group

Account Information

Role	super admin
Account Name	root
Email	root@advantech.com.tw
First Name	root
Last Name	root
Phone (optional)	
Login At	2019/12/26 09:57:29
Created At	2017/1/1 00:00:00

Personal Alert Services

Email Notify	On
SMS Notify	Not set
WeChat Notify	Not set
WeChat SC Key	Not set
LINE notify	Not set
LINE Notify Token	Not set
WhatsApp notify	Not set

- My Profile

On “**My Profile**”, shows your account information and personal alert service, such as LINE, WeChat token.

- Management

Every account belongs to a role, you could use the filter to find account. There are 3 roles in the DeviceOn system. One is “**Super Admin**”, only one account in the system belongs to “**Super Admin**”. The other role is “**Admin**” and “**Device Admin**”. For detail role permission, please reference Section 7.1.

My Profile

Management

Device Group

ROLE

super admin

Keyword Search

Filter

+

✎

⏏

NAME	SOURCE	EMAIL	PHONE	FULL NAME	ENABLE
root	DeviceOn	root@advantech.com.tw	Not set	root	●

1 record

Click on the icon to “Add Account”



Add Account

ASSIGNED ROLE
admin

ACCOUNT NAME
Sephiroth

PASSWORD

EMAIL
sephiroth.wang@advantech.com.tw

FIRST NAME
Sephiroth

LAST NAME
Wang

EMAIL NOTIFY
On
CARBON COPY(SEPARATED BY:)
sephiroth.wang@gmail.com

SMS NOTIFY
On
+886 0912 345 678

WECHAT NOTIFY
Off
WeChat SC Key

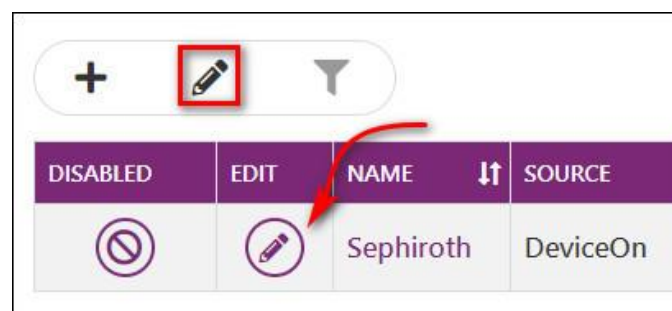
LINE NOTIFY
Off
LINE Notify Token

WHATSAPP NOTIFY
Off

Save

Enter your account, role, password, etc. to create an account. If the user would to receive notify from device, system alert, please enable these alert services on “**Mail**”, “**SMS**”, “**WeChat**”, “**LINE**” and **WhatsApp**. These alert services are personal setting, please make sure the “**Setting -> Notification**” is configured, enabled on DeviceOn System.

Click on the icon to “**Edit**” or “**Disable**” account.





● Device Group

Every account could group their device into different groups to manage, for example, device over different floor on the building. User could create 1F, 2F group to easy management.

My Profile
Management

Device Group

ACCOUNT
Sephiroth
Keyword Search

+



DEVICE GROUP NAME	DESCRIPTION
No matching records	

Click on the icon to add “Device Group”.



Add Device Group

DEVICE GROUP NAME
1F Lobby

DESCRIPTION
Linkou 1F Lobby Room

Save

Click on the icon to “Edit” or “Delete” account.

+



DELETE	EDIT	DEVICE GROUP NAME
		1F Lobby

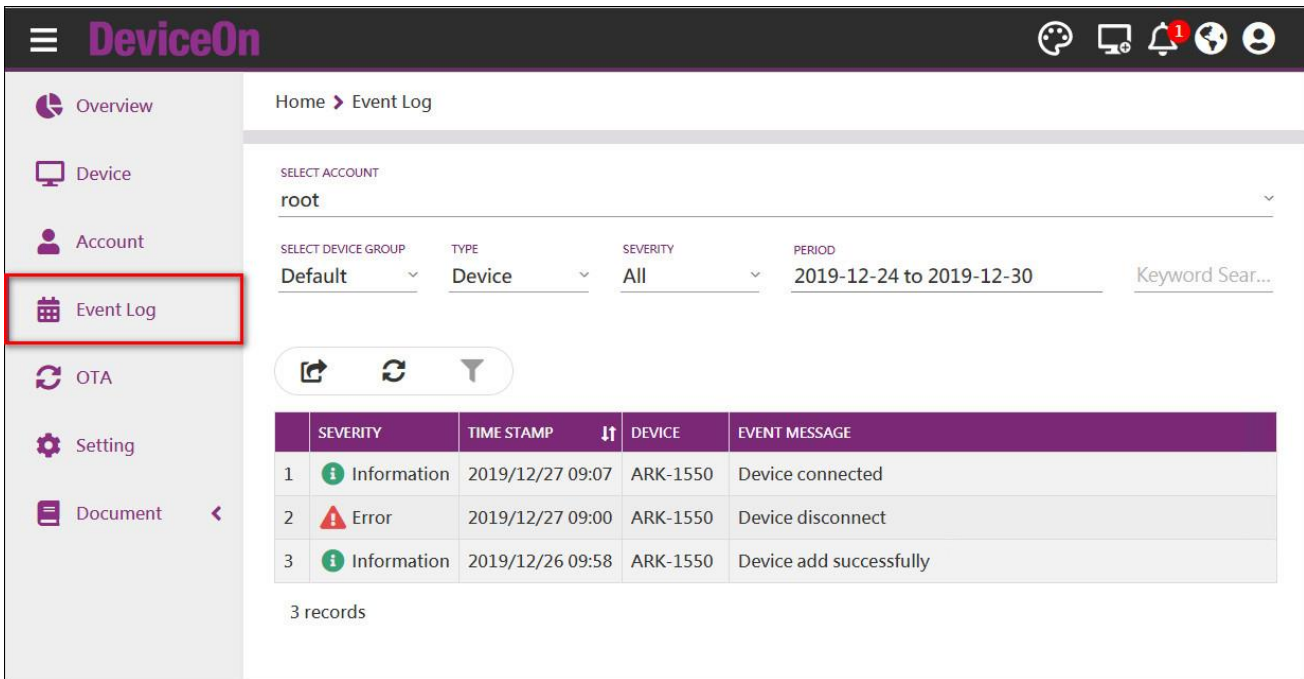
3.3.4 Event Logs

Device management is complex with device log and user behavior. Logging data can provide insights about your devices and help you:

- Troubleshoot past problems or prevent potential ones
- Improve device healthy or maintainability
- Real-time alert through 3rd notification

DeviceOn logs are categorized into the following types:

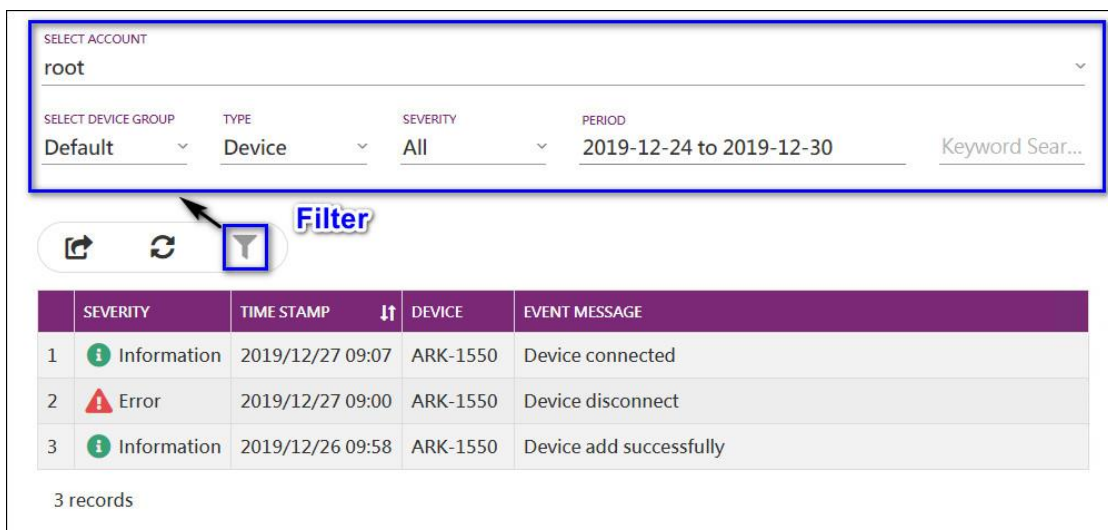
- Operation log provide information about DeviceOn resource CREATE, UPDATE and DELETE operation, like set device power off, update device name or delete account.
- Device log provide information about events raised as device side resources, like connected, disconnected, over the threshold,
- System log provide information about analyzed; scheduling event/alert that have been process on DeviceOn server. Example of this type are queue buffer alerts where server has processed and measured IoT Hub queue and provides concise alerts.



	SEVERITY	TIME STAMP	DEVICE	EVENT MESSAGE
1	Information	2019/12/27 09:07	ARK-1550	Device connected
2	Error	2019/12/27 09:00	ARK-1550	Device disconnect
3	Information	2019/12/26 09:58	ARK-1550	Device add successfully

3 records

There are three type of Event Logs as mentioned above and each event log with different severity, **Information, Warning and Error**. Through the filter to find your device log.



	SEVERITY	TIME STAMP	DEVICE	EVENT MESSAGE
1	Information	2019/12/27 09:07	ARK-1550	Device connected
2	Error	2019/12/27 09:00	ARK-1550	Device disconnect
3	Information	2019/12/26 09:58	ARK-1550	Device add successfully

3 records

Click on the icon to refresh event log by manual.

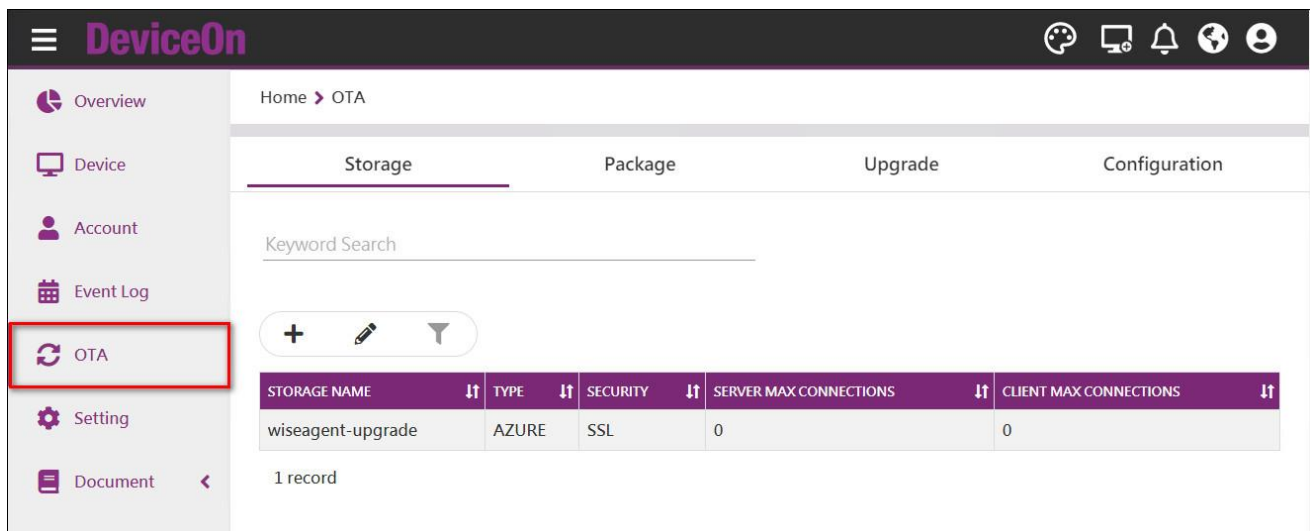


Click on export icon to export devices that in the table as CSV file.



3.3.5 OTA (Remote Provisioning)

OTA (Over-The-Air) is one of powerful feature DeviceOn provides. Users can deploy **software** packages, **configuration**, **Windows QFE** (Quick Fix Engineering), **Advantech BIOS** update onto a device remotely, or even many devices broadly.



Home > OTA

Storage Package Upgrade Configuration

Keyword Search

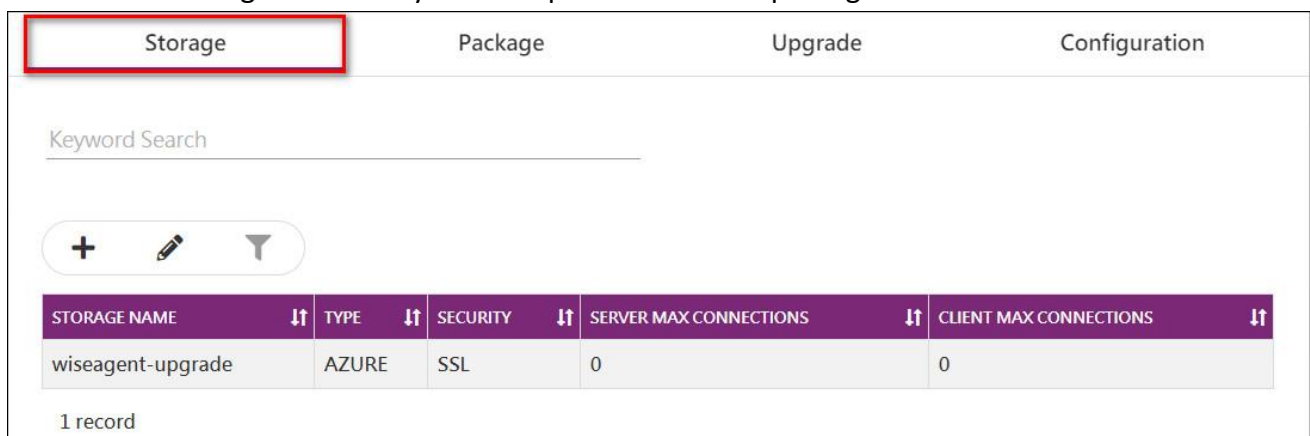
+ ✎ 🔍

STORAGE NAME	TYPE	SECURITY	SERVER MAX CONNECTIONS	CLIENT MAX CONNECTIONS
wiseagent-upgrade	AZURE	SSL	0	0

1 record

● Storage

There is a default Azure blob storage called “**wiseagent-upgrade**”, host by Advantech DeviceOn team. If there is a new version of WISE-Agent released, all of user could get the update and upgrade their devices. The storage is read only cannot upload user’s OTA package.



Storage Package Upgrade Configuration

Keyword Search

+ ✎ 🔍

STORAGE NAME	TYPE	SECURITY	SERVER MAX CONNECTIONS	CLIENT MAX CONNECTIONS
wiseagent-upgrade	AZURE	SSL	0	0

1 record

Click on add icon to add new storage.



For cloud storage, DeviceOn provide “**Amazon S3**”, “**S3 Compatible**”, “**Azure Blob**” and traditional FTP services.

[Amazon S3]

You could create and get Access Key, Secret Key from Amazon Web service.

← Add New Storage

STORAGE

Amazon S3

Security

☒ SSL

Storage Name

Region

Access Key

Secret Key

DESCRIPTION

Save

- ✧ Storage Name: Your storage name, define by yourself.
- ✧ Region: Region of AWS S3
- ✧ Access Key: Access Key for AWS S3
- ✧ Secret Key: Secret Key for AWS S3

Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, use the [IAM Console](#).

To learn more about the types of AWS credentials and how they're used, see [AWS Security Credentials](#) in AWS General Reference.

- ▲ Password
- ▲ Multi-factor authentication (MFA)
- ▼ Access keys (access key ID and secret access key)

Use access keys to make programmatic calls to AWS from the AWS CLI, Tools for PowerShell, the AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. [Learn more](#)

Created	Access Key ID	Last Used	Last Used Region	Last Used Service	Status	Actions
Aug 8th 2019	[REDACTED]	2019-12-27 14:57 UTC+0800	ap-southeast-1	s3	Active	Make Inactive Delete

[Create New Access Key](#)

Root user access keys provide unrestricted access to your entire AWS account. If you need long-term access keys, we recommend creating a new IAM user with limited permissions and generating access keys for that user instead. [Learn more](#)

Create Access Key

✓ **Your access key (access key ID and secret access key) has been created successfully.**

Download your key file now, which contains your new access key ID and secret access key. If you do not download the key file now, you will not be able to retrieve your secret access key again.

To help protect your security, store your secret access key securely and do not share it.

▼ [Hide Access Key](#)

Access Key ID: [REDACTED]

Secret Access Key: [REDACTED]

[Download Key File](#) [Close](#)

[S3 Compatible]

The setting similar to Amazon, only **endpoint** must be configured to yourself.

Add New Storage

STORAGE
S3 Compatible

Security ☒ NONE ☐ SSL

Storage Name

Endpoint

Access Key

Secret Key

DESCRIPTION

[Azure Blob]

For Azure Blob, supports two mechanisms to access, one is **"Storage Account"** and **"Access Key"** with

full access permission of container. The other is “**container**” SAS token generated via [Microsoft Azure Storage Explorer](#).

← Add New Storage

STORAGE
Azure Blob

Security ☒ SSL

Storage Name

ENDPOINTSUFFIX
core.windows.net (AzureCloud)

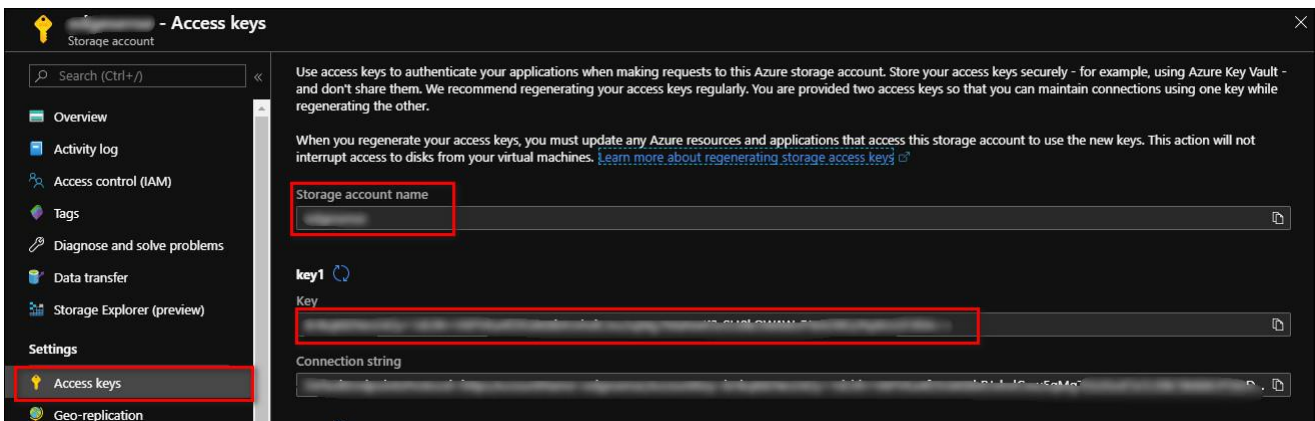
SAS ☐ Use Shared Access Signature

Account Name

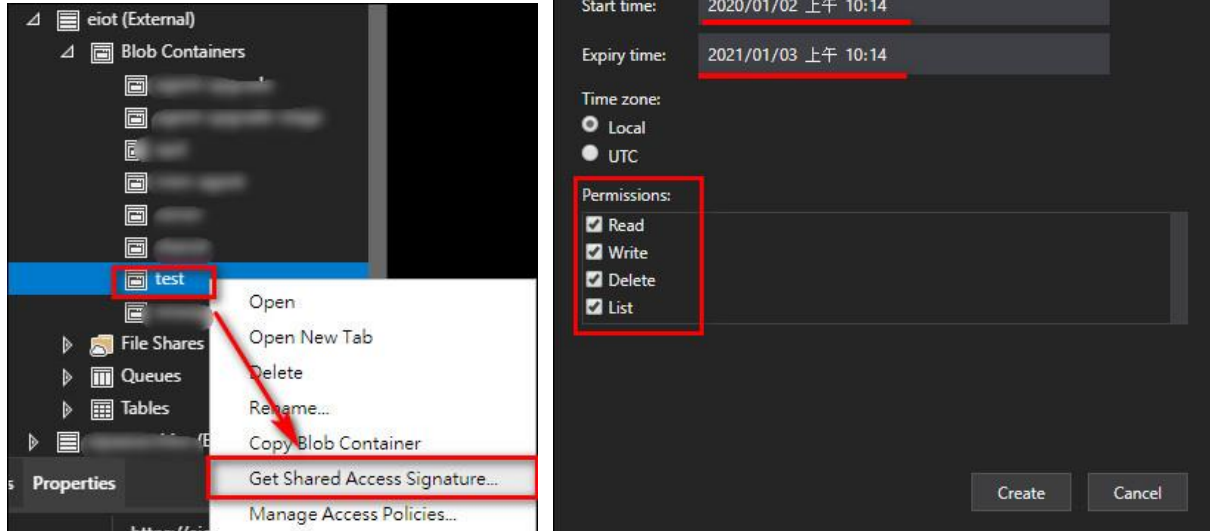
Access Key

DESCRIPTION

Through Azure portal to get your **Storage Account** and **Access Key**.

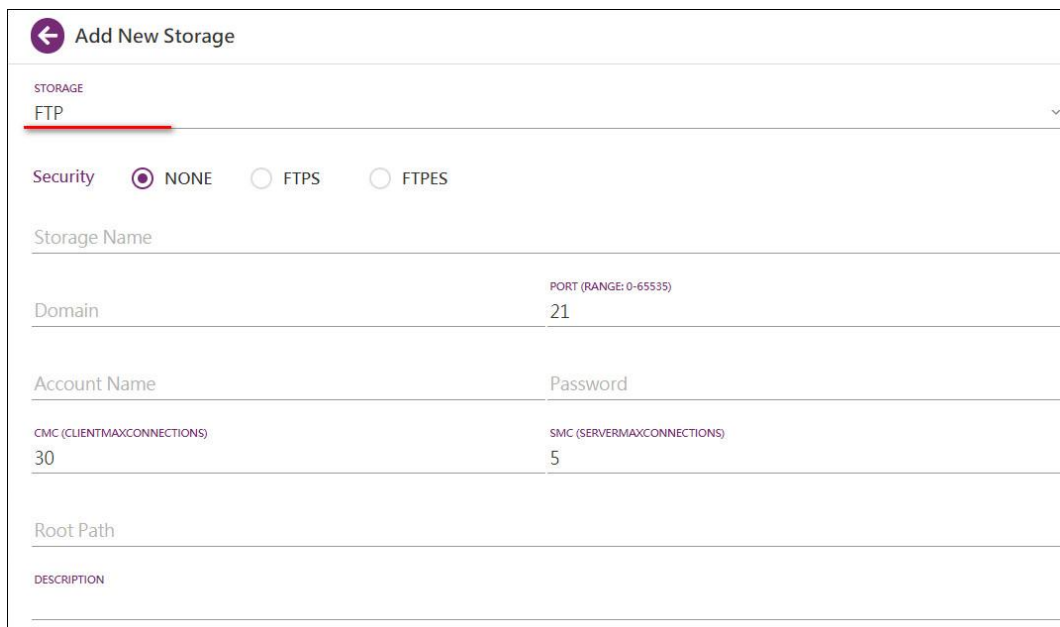


Get **container's SAS token** via Azure Storage Explorer, please make sure your permission (Read, Write, Delete, List) and valid period (Start and Expiry time)



[FTP]

For FTP, you might setup another FTP server with security and account, password.





- ✧ **Security:** Leave it as “**NONE**”, the default value. If your FTP server running on FTPS protocol, pick “**FTPS**”.
- ✧ **SOTRAGE NAME:** Enter “**MyFTP**”.
- ✧ **DOMAIN:** Enter the FQDN of your FTP server, or its IP address.
- ✧ **PORT:** Should be **21** if the FTP server runs on a standard port number.


- ✧ **ACCOUNT NAME:** A valid username that can connect to the FTP server, and upload files onto the server as well.
- ✧ **PASSWORD:** The password to login.
- ✧ **CMC/SMC:** Maximum Client & Server Connection.
- ✧ **ROOT PATH:** FTP server access path (root folder)
- ✧ **DESCRIPTION:** It's optional information.

Click on edit icon to adjust a storage.



You could edit yourself storage, but the default storage cannot.

DELETE	EDIT	STORAGE NAME	TYPE
		Testing	AZURE
		<u>wiseagent-upgrade</u>	AZURE
2 records			


Edit Storage

STORAGE
Azure Blob

Security ☒ SSL

STORAGE NAME
Testing

SAS ☒ Use Shared Access Signature

SAS URI

DESCRIPTION

● Package

View and edit OTA package on select storage, user could edit, delete upload their package to selected storage, but default storage (**wiseagent-upgrade**) cannot. To ensure the security and data format on OTA package, user should wrap their software, firmware via DeviceOn toolkit. The toolkit not only command-line tool but support online UI mechanism.

Storage

Package

Upgrade

Configuration

STORAGE

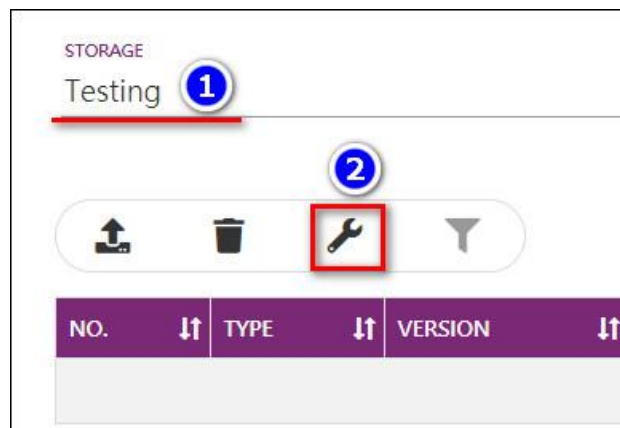
wiseagent-upgrade

Keyword Search

NO. <div></div>	TYPE	<div></div>	VERSION <div></div>	TAGS	STORAGE <div></div>	NAME
1	WISEAgentSetup	1.2.17.0	win,x86	wiseagent-upgrade	WISEAgentSetup-v1.2.17.0-cb8b3c38dbf9	
2	IMX6WISEAgentSetup	1.2.17.0	fsl,imx6,yocto	wiseagent-upgrade	IMX6WISEAgentSetup-v1.2.17.0-ef955f3c:	

2 records

Select to your storage and click on the toolkit icon to start to warp your OTA package.



Prepare your software, configuration and installation script first, gives below information. The operation system and architecture might be different. Therefore, to determine the OTA package be deployed on which devices, please pick-up the **“Tag Name”** on **“Supported Arch”**. All **“Tags”** must match with devices, the OTA package will be executed. For example, there is two devices (ARK-1123, UTC-520) with different tag attribute. The ARK-1123 device is Windows based and support x64 and x86 OTA package. The UTC-520 is Ubuntu system also support x64, x86.

- ARK-1123 (Tags): win, x64, x86
- UTC-520 (Tag): ubuntu, x64, x86

If your OTA package tags are **“win”**, **“x64”**, **“x86”**, the package only support and executed on **“ARK-1123”**. Otherwise, if the tag is **“x64”**, both devices could be affected.

- ✧ **Package Type:** Name of package
- ✧ **Package Version:** Version of Package
- ✧ **Supported Arch:** Select **“Tag Name”** from of device (Account -> Device Group -> Device)
- ✧ **Deploy File:** Installation script (batch file or shell script)

- ✧ **Storage: Upload to storage or download**
- ✧ **Advanced options: Reboot or run the script after deployed.**

Package Toolkit

PACKAGE TYPE

notepad

PACKAGE VERSION

1.0.0.1

ACCOUNT

root

DEVICE GROUP

1F Lobby

DEVICE

ac09

SUPPORTED ARCH

☒ x64
☒ x86
☒ win

SOURCE DIR

otademo

Browser

DEPLOY FILE

installNotepad.bat

STORAGE

Testing

☐ Advanced options

Click on the delete icon to delete your OTA package.

DELETE	NO. ↑↓	TYPE ↑↓	VERSION ↑↓	TAGS
	1	notepad	1.0.0.1	x64,x86,win
1 record				

Click on the upload icon to upload your OTA package.

Upload Package

Upload file

CONFIRM

● Upgrade

On the upgrade tab, start to select your device or device group and pick-up your OTA package that you upload before. On the device list to configure schedule, check the result status and program list

that installed.

Home > OTA

Storage Package **Upgrade** Configuration

SELECT ACCOUNT: root SELECT DEVICE GROUP: 2F Demo Room Keyword Search

1 record

NAME	UPGRADE	PROCESSING	SCHEDULE SETTING	DEPLOYED SOFTWARE STATUS	PACKAGE	PROGRAM	PLATFORM	S/N
ARK-1550		↓ 0 ↺ 0	↓ 0 ↺ 0	4/4	0		ARK-1550	000BAB

Click on upgrade icon to select OTA package.

1 record

NAME	UPGRADE	PROCESSING	SCHEDULE SETTING	DEPLOYED SOFTWARE STATUS	PACKAGE	PROGRAM
ARK-1550		↓ 0 ↺ 0	↓ 0 ↺ 0	4/4	0	

Select your package to “**Upgrade**”, “**Download**” or “**Deploy**”. The “Upgrade” represents download OTA package from storage and execute (Deploy) immediately. Every package would be kept on device side as “Upgrade” or “Download”.

← Upgrade Operation

DEVICE: ARK-1550




CHOOSE ACTION: ☒ Upgrade ☐ download ☐ deploy

Keyword Search

4 records

CHOOSE	TYPE	VERSION	OS	ARCH	STORAGE	NAME
<input checked="" type="checkbox"/>	notepad	1.0.0.1	n/a	n/a	Testing	notepad-v1.0.0.1-357a65f072edcd7fb866f038
<input type="checkbox"/>	WISEAgentSetup	1.3.4.0	n/a	n/a	wiseagent-upgrade	WISEAgentSetup-v1.3.4.0-ffb9b7ec0e9a0fe2ef
<input type="checkbox"/>	WISEAgentSetup	1.2.17.0	n/a	n/a	wiseagent-upgrade	WISEAgentSetup-v1.2.17.0-cb8b3c38dbf94771
<input type="checkbox"/>	IMX6WISEAgentSetup	1.2.17.0	n/a	n/a	wiseagent-upgrade	IMX6WISEAgentSetup-v1.2.17.0-ef955f3c3c90

To check the deploy status, please click on process icon.

NAME	UPGRADE	PROCESSING	SCHEDULE SETTING	DEPLOYED SOFTWARE STATUS	PACKAGE
ARK-1550		 1 0	 ↓ 0 ↺ 0	4/4	0

1 record




← Upgrade Processing Information

DEVICE ARK-1550

ACTION	NAME	STAGE	PROGRESS	MESSAGE
download	notepad-v1.0.0.1-357a65f072edcd7fb866f038741e0ba6.zip	NORMAL	<div><div>100%</div></div>	Download task doing, download pe

1 record

To avoid burst download on large number of devices upgrade at the same time, user could add schedule to check and upgrade by schedule.

NAME	UPGRADE	PROCESSING	SCHEDULE SETTING	DEPLOYED SOFTWARE STATUS	PACKAGE	PROGRAM
ARK-1550		↓ 0 ↺ 0	 ↓ 0 ↺ 0	4/4	0	

1 record

Click on add icon to create a schedule.



← Add Schedule

DEVICE ARK-1550

PACKAGE TYPE notepad

ACTION TYPE ☒ download ☐ deploy

UPGRADE MODE ☒ max ☐ increment

FREQUENCY Daily

ACTION START TIME 11:28

ACTION END TIME 11:58

- ✧ Package Type: Select your OTA package from storage.
- ✧ Action Type: Download or Deploy the package.
- ✧ Upgrade Mode: If the mode is **Max**, the action would download/deploy **the latest version** on the package. Otherwise, if the mode “**Increment**”, The deploy, or download behavior will gradually increase from the lower version to the latest version.
- ✧ Frequency: **Daily, Weekly, Monthly** or **Once** to check.
- ✧ Action Start Time: Check time on start.
- ✧ Action End Time: End time for download, if download exceeds the end time, the action will be terminated.

Click on edit icon to modify, delete OTA schedule.

DELETE	EDIT	TYPE	PACKAGE TYPE	ACTION TYPE
		Device	notepad	download

1 record

To check deployed software, configurate status on device, please click on the numbers.

← Deployed software List

DEVICE ARK-1550

NAME	VERSION	DEPLOYMENT STATUS
Cfg_Default	1.0.0.1	✓
Cfg_DeviceOn	1.0.0.1	✓
WISEAgentSetup	1.3.4.0	✓
notepad	1.0.0.1	✓

4 records

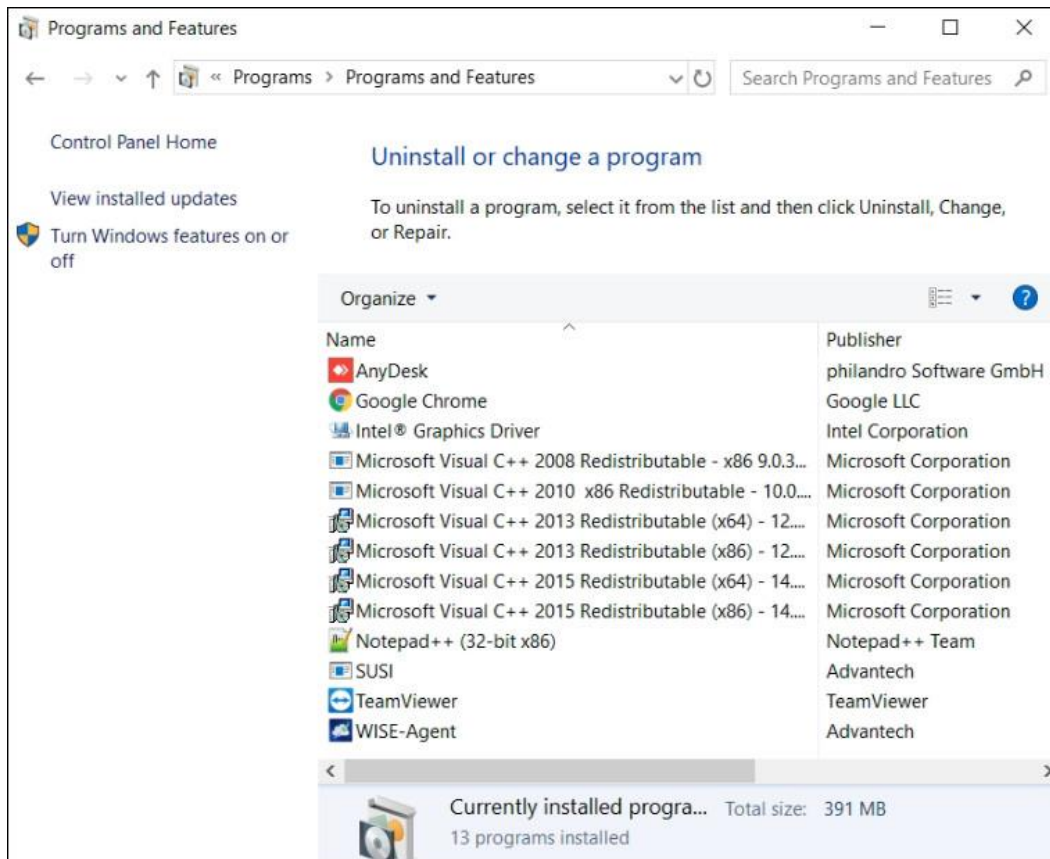
Furthermore, user could view the program list on the device. (Windows Only)

NAME	UPGRADE	PROCESSING	SCHEDULE SETTING	DEPLOYED SOFTWARE STATUS	PACKAGE	PROGRAM
ARK-1550		↓ 0 ↺ 0	↓ 1 ↺ 0	4/4	0	

1 record

Device Program List				
DEVICE ARK-1550				
NO.	DISPLAY NAME	PUBLISHER	INSTALL DATE	ESTIMATED SIZE
1	SUSI	Advantech	2019926	13706 KB
2	AnyDesk	philandro Software GmbH	20191129	2048 KB
3	Google Chrome	Google LLC	20191226	0 KB
4	Notepad++ (32-bit x86)	Notepad++ Team	202017	8757 KB
5	TeamViewer	TeamViewer	20191129	0 KB
6	Microsoft Visual C++ 2015 Redistributable (x86) - 14.0.24212	Microsoft Corporation	2019117	20018 KB
7	WISE-Agent	Advantech	202016	196627 KB
8	Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161	Microsoft Corporation	2019726	10440 KB
9	Microsoft Visual C++ 2015 Redistributable (x64) - 14.0.23026	Microsoft Corporation	20191018	22986 KB
10	Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.40660	Microsoft Corporation	2019925	21062 KB

This program information retrieves from device operation system, same as below figure.



- Configuration

There are three options for OTA to deploy your package, one is “**Rollback**” that means if a new version

deploys failed, the WISE-Agent would try the best to rollback to previous version that successfully. But there is a prerequisite, the previous version of the package exists on the device side. The remaining two options are the retry times. Due to network instability or other factors causing the download fail, OTA provide the retry times to ensure successful deployment as possible.

Storage	Package	Upgrade	Configuration
<div> <div>Notify Device Setting</div> <div> <p>We provide three options that allow you to set the number of repeated downloads or deployments, and notice that settings provided here are master switches, which make influence to all download or deployment tasks.</p> </div> <div> <div>Rollback <input type="checkbox"/> Off</div> <div> <div>DOWNLOAD RETRY COUNT</div> <div>3</div> </div> <div> <div>DEPLOY RETRY COUNT</div> <div>0</div> </div> </div> </div>			

3.3.6 System Configuration

A System Configuration defines advanced settings including real-time **"Action"**, device **"Provision"**, **"Event Alert"**, **"Rule Engine"**, **"Notification"** services, product **"Activation"**, and **"System Menu"**. These settings are usually changed less often or only need to be modified once. Some functions require root, admin to modify or be visible, and product activation only shown on prefecture license, such as Standalone, Azure Kubernetes version.

DeviceOn

Overview

Device

Account

Event Log

OTA

Setting

Document

Home > Setting

Assign Action

Provision

Event Alert

Rule Engine

Notification

Activate Server

System Menu

+

KEYWORD SEARCH

PIN TO HOME	SCHEDULE	ACTION TYPE	ACTION DESCRIPTION	DEVICE GROUP NAME	CREATED DATETIME
		Screenshot	Screenshot Default	Default	2019/12/26 09:58:35
		Reboot	Reboot Default	Default	2019/12/26 09:58:35

2 records

- Assign Action

The real-time actions on the overview that are defined, created on here, you could add a new action and pin to overview. These actions are binding to personal account, cannot view, edit, delete others.

Assign Action	Provision	Event Alert	Rule Engine	Notification	Activate Server	System Menu
KEYWORD SEARCH						
<div> <div>+</div> <div></div> </div>						
PIN TO HOME	SCHEDULE	ACTION TYPE	ACTION DESCRIPTION	DEVICE GROUP NAME	CREATED DATETIME	
		Screenshot	Screenshot Default	Default	2019/12/26 09:58:35	
		Reboot	Reboot Default	Default	2019/12/26 09:58:35	
2 records						

Click on the icon to add action.



Enter your description and select an “**Action**” from three categories, **Power Saving**, **Security** and **System**.

← New Action

Select Action

Select Device Groups

Confirm

1

2

3

Action Description

Power Saving

Security

System

☐ Power On
 ☐ Power Off
 ☐ Reboot
 ☐ Backlight On
 ☐ Backlight Off

☐ Protection On
 ☐ Protection Off
 ☐ Backup
 ☐ Recovery
 ☐ USB Lock
 ☐ USB Unlock
 ☐ Keyboard Lock
 ☐ Keyboard Unlock
 ☐ Touch Lock
 ☐ Touch Unlock
 ☐ Touch Gesture Lock
 ☐ Touch Gesture Unlock

☐ Update Agent
 ☐ Screenshot
 ☐ Audio Mute
 ☐ Audio Unmute
 ☐ Watchdog Enable
 ☐ Watchdog Disable
 ☐ Notification Block
 ☐ Notification Unblock
 ☐ UWF Enable
 ☐ UWF Disable

Select “**Device Groups**” for the action that you picked up.

←

New Action

Select Action

Select Device Groups

Confirm

1

2

3

Add Device Groups

+

☒ Default

Back

Next

To confirm information, action, group and devices, and enable pin on overview, please click on **“Confirm”** to complete the wizard.

←

New Action

Select Action

Select Device Groups

Confirm

1

2

3

Action Description	Linkou Lobby
Action Type	Power Off
Pin to home	<input checked="" type="checkbox"/> On
Group And Device	<div> <div>Default</div> <div>ARK-1550</div> </div> <div> <div>Device Group</div> <div>Devices</div> </div>

Back

Confirm

After created, you could find a new action on below actions list, click the PIN icon to determine the action shown on overview or not.

PIN TO HOME	SCHEDULE	ACTION TYPE	ACTION DESCRIPTION	DEVICE GROUP NAME	CREATED DATETIME
<input checked="" type="checkbox"/>		Screenshot	Screenshot Default	Default	2019/12/26 09:58:35
<input type="checkbox"/>		Reboot	Reboot Default	Default	2019/12/26 09:58:35
<input type="checkbox"/>		Power Off	Linkou Lobby	Default	2019/12/31 11:11:57

3 records

The actions support scheduling, click on the icon to define a schedule, daily, weekly, monthly, yearly or once.

PIN TO HOME	SCHEDULE	ACTION TYPE	ACTION DESCRIPTION	DEVICE GROUP NAME	CREATED DATETIME
		Screenshot	Screenshot Default	Default	2019/12/26 09:58:35
		Reboot	Reboot Default	Default	2019/12/26 09:58:35
		Power Off	Linkou Lobby	Default	2019/12/31 11:11:57

3 records


Enter to schedule list for all actions, and click on add icon to create new schedule.

Schedule List

ENABLE	SCHEDULE NAME	PERIOD	NEXT EXECUTION TIME
No matching records			

Given your schedule name, time zone, period and time and click **Save**.

- ✧ **Schedule Name:** Name of schedule
- ✧ **Time Zone:** Time zones tend to follow the boundaries of countries and their subdivisions instead of longitude, because it is convenient for areas in close commercial or other communication to keep the same time.
- ✧ **Period:** Repeat interval for Daily, Weekly, Monthly, Yearly or once at a time.
- ✧ **Time:** Execution time.

 Add Schedule

ACTION DESCRIPTION

Screenshot Default

ACTION TYPE

Screenshot

DEVICE GROUP NAME

Default

Schedule Name

1

TIMEZONE
(+08:00) Beijing, Shanghai

2

Enable

On

PERIOD
Daily



3


TIME
11:53

4

Save



Click on the edit icon to adjust schedule item.


+



EDIT	ENABLE	SCHEDULE NAME
	<div>On</div>	Sch1

1 record

Click on the delete icon to delete schedule item.

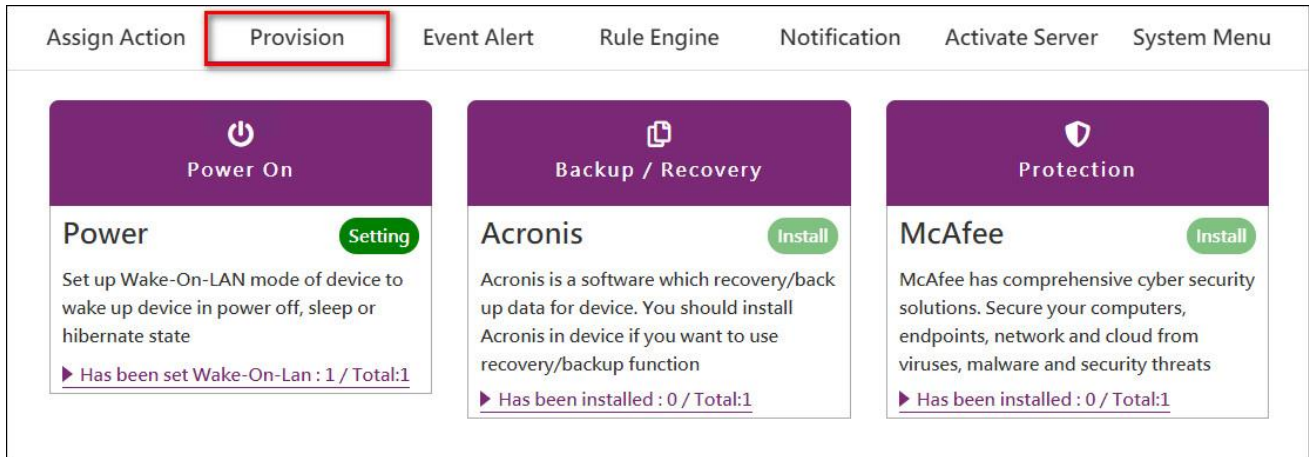
+



DELETE	ENABLE	SCHEDULE NAME
	<div>On</div>	Sch1

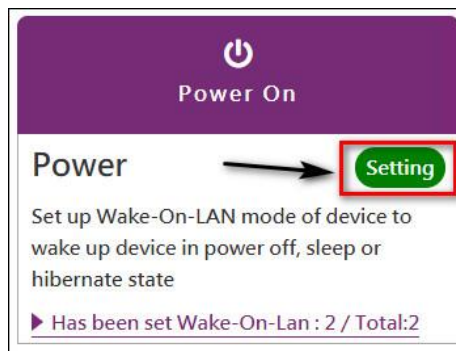
1 record

- Device Provision

For device provision, 3 types need be pre-configured. One is “**Power On**”, select which mode to enable device wake up. The others are 3rd party tool integration, **Acronis** to **backup/recovery** your device system and **McAfee** for white-list security **protection**. To install 3rd tools, you must purchase the license and activate the product.



Click on the Setting for “**Power On**”.



To power your device up, you might to configure the mode for your device. The mechanism is based on Wake-on-LAN to send magic packet to your device. There is a limitation on “**Direct Mode**”, the DeviceOn server and edge device must be on the same network.

←

Power mode Setting

WAKE-ON-LAN

Direct Mode

SELECT ACCOUNT

root

SELECT DEVICE GROUP

Default

root - Default ×

root - Default

ARK-1550

However, through the “**Agent Mode**” or “**Repeater**” could overcome the limitation. You need to pick-up a device that **always on** and on the same network with other devices.

←

Power mode Setting

WAKE-ON-LAN

Agent Mode

AGENT ID

00000001-0000-0000-0000-000BAB718EFA

SELECT ACCOUNT

root

SELECT DEVICE GROUP


1F Lobby

root - 1F Lobby ×

root - 1F Lobby

ac09

Select a Device



For **Repeater** mode, not only enter your repeater IP, but set your repeater to allow port forwarding (uses UDP port 7 and 9) and permit the packet to be broadcast to the entire LAN.

Power mode Setting

WAKE-ON-LAN

Repeater Mode

IP

172.11.22.33

Repeater IP

SELECT ACCOUNT

root

SELECT DEVICE GROUP

1F Lobby

root - 1F Lobby

root - 1F Lobby

ac09

Click on the Install for “**Acronis**”.

Backup / Recovery


Acronis

Install

Acronis is a software which recovery/back up data for device. You should install Acronis in device if you want to use recovery/backup function

Has been installed : 1 / Total:2

Select the free space size to create Acronis Secure Zone (Hidden Partition) to backup system partition.
The free space size must larger than system used.


Install Acronis

Create a free space for Acronis Secure Zone for back-up functionality.

25

(unit: %)

Note: free space size would be at least the same as your current system used size

SELECT ACCOUNT

root

SELECT DEVICE GROUP


2F Demo Room

root - 2F Demo Room


root - 2F Demo Room

ARK-1550

Click on the Install for “**McAfee**”, and select device group to install.



Protection

McAfee



McAfee has comprehensive cyber security solutions. Secure your computers, endpoints, network and cloud from viruses, malware and security threats

► Has been installed : 1 / Total:2


Install McAfee

SELECT ACCOUNT

root

SELECT DEVICE GROUP

2F Demo Room

root - 2F Demo Room

root - 2F Demo Room



ARK-1550

● Event Alert







DeviceOn provide **Event Log** that describe on Section 3.3.4, user could decide to what kind of event should be notified.

Assign Action
Provision
Event Alert
Rule Engine
Notification
Activate Server
System Menu

TYPE
Device
SEVERITY
All

☐ Device Category

- ☒  Device add successfully
- ☒  Device add failed
- ☐  Device connected
- ☐  Device disconnect
- ☒  Device lost connected
- ☒  Device authentication refuse

☐ Power Category

☐ System Monitor Category

☐ Protection Category

☐ Recovery Category

☐ Threshold Category



☐ Intel AMT Category

● Rule Engine

DeviceOn provides the rule engine. Users can acquire anomaly situations by means of setting thresholds to those interested devices, and, once one or more thresholds meets, receive alerts via event notification services, another one indispensable feature for users.

Assign Action
Provision
Event Alert
Rule Engine
Notification
Activate Server
System Menu

SELECT ACCOUNT
root
RULE TYPE
Device

ENABLE	RULE TYPE	DEVICE / DEVICE GROUP NAME	↕	SENSOR NAME	ACTION	THRESHOLD
No matching records						

Click on the add icon to create a Rule.



Pick-up the sensor that you want to monitor, the steps are select **Rule Type**, **Device Group** and **Device**.

RuleEngine

Select Sensor

Define Threshold

Define Action

Confirm

SELECT RULE TYPE

Device

1

SELECT DEVICE GROUP

1F Lobby

2

SELECT DEVICE

ac09

3

Keyword Search

	SENSOR NAME	SENSOR ID
<input type="radio"/>	Network Utilization	NetMonitor/netMonInfoList/Index1^-Local Area Connection 2/nett
<input type="radio"/>	Network Throughput (Send)	NetMonitor/netMonInfoList/Index1^-Local Area Connection 2/sen
<input type="radio"/>	Network Throughput (Receive)	NetMonitor/netMonInfoList/Index1^-Local Area Connection 2/recv
<input checked="" type="radio"/>	System, Available Physical Memory	ProcessMonitor/System Monitor Info/availPhysMemKB
<input type="radio"/>	System, CPU Usage	ProcessMonitor/System Monitor Info/CPU Usage
<input type="radio"/>	System, Total Physical Memory	ProcessMonitor/System Monitor Info/totalPhysMemKB
<input type="radio"/>	Hardware, 12V	SUSIControl/Hardware Monitor/Voltage/12V
<input type="radio"/>	Hardware, 5V Standby	SUSIControl/Hardware Monitor/Voltage/5V Standby
<input type="radio"/>	Hardware, CMOS Battery	SUSIControl/Hardware Monitor/Voltage/CMOS Battery
<input type="radio"/>	Hardware, System (Temperature)	SUSIControl/Hardware Monitor/Temperature/System

<<

<

1

2

3

>

>>

Define the threshold, provide 3 types, **more than**, **less than** and **outside the range**. Also, you could realize current value on the page.

- ✧ Lasting Time (Second): means the sensor over the threshold and continue for a period time, avoid peak value to trigger.
- ✧ Notice Interval (Second): If over the threshold, the WISE-Agent will send a notify event, to avoid lots of message, user could adjust notice interval.

RuleEngine

Select Sensor

Define Threshold

Define Action

Confirm

Sensor Name : Hard Drive Health

Current Value : 18 Unit : %

☐ More than
 ☒ Less than
 ☐ Outside the range

0

20

40

60

80

100

Lasting Time(Second) : 10

Notice Interval (Second) : 60

Next, to define the action, if threshold reached. For example, you could power your device off, if the hard drive unhealthy.

←

RuleEngine

Select Sensor

Define Threshold

Define Action

1

2

3

TAKE A ACTION

Power On/Off

TAKE A SUB ACTION

System Power off

Trigger Frequency

☒ Always
 ☐ Back to Normal
 ☐ Once

Confirm the rule setting and click confirm.

←

RuleEngine

Select Sensor

Define Threshold

Define Action

Confirm

1

2


3

4

Enable	<input checked="" type="checkbox"/>
Rule Type :	Device
Device Group :	1F Lobby
Device :	ac09
Plugin :	HDDMonitor
SensorId :	HDDMonitor/hddInfoList/Disk0/health
Define Threshold :	Less than 10 %
Lasting Time(Second) :	10
Notice Interval (Second) :	60

The rule list shown as below, user could edit or disable through the switch.

+








ENABLE	RULE TYPE	DEVICE / DEVICE GROUP NAME	⌵⌴
<input checked="" type="checkbox"/>	Device	ac09	

1 record

● Notification Service

Here are five notification services, include tradition service (SMS, Email) and popular social media

(LINE, WeChat and WhatsApp), if you select the event type on **“Event Alert”**, the notify message will through these services. These notification services are global setting, if your account does not receive, please check the personal setting on **Account -> Personal Alert Service**.

Assign Action	Provision	Event Alert	Rule Engine	Notification	Activate Server	System Menu
<p> Email Email notifications deliver information about errors in your apps straight to your inbox.</p>						
<p> SMS Enable SMS notification service to receive notification messages vis SMS wun status changes or errors occur to th system</p>						
<p> WeChat Server Chan is a communication software between programmer and server.</p>						
<p> Line You can receive notifications from multiple services in groups or 1-on-1 chats.</p>						
<p> WhatsApp Wassenger is a serverless WhatsApp messaging API cloud solution that is easy to ues, cheap and scalable.</p>						

To configure these notification service, please reference Section 4.3.2 ~ Section 4.3.5.

- **Product Activation**


DeviceOn support online and offline to activate product, if your server could access to Advantech License Server, that would be simple. Enter your license key that you purchase the product from WISE-PaaS Marketplace.

Assign Action	Provision	Event Alert	Rule Engine	Notification	Activate Server	System Menu
<p><small>LICENSE KEY</small></p> <p><input type="text" value="L-00000000000000000000000000000000"/></p> <hr/> <p>2 / 10 (Assigned Quantity / Licensed Quantity)</p> <p><small>Server ID 0000000BAB45599B</small></p> <p>Activate</p>						

If your server environment without public network accessible, there is a QR code generated after enter the license key. Please leverage your mobile device to scan and retrieve the **“Activation Code”**.

Assign Action
Provision
Event Alert
Rule Engine
Notification
Activate Server
System Menu

Please scan with QRcode scanner and get an activate code to enter



Activate Code

Field is required

Activate

15:59

91%

wise-paas.com:8443

WISE-PaaS

Activate Product License

License Key

Machine/Server ID

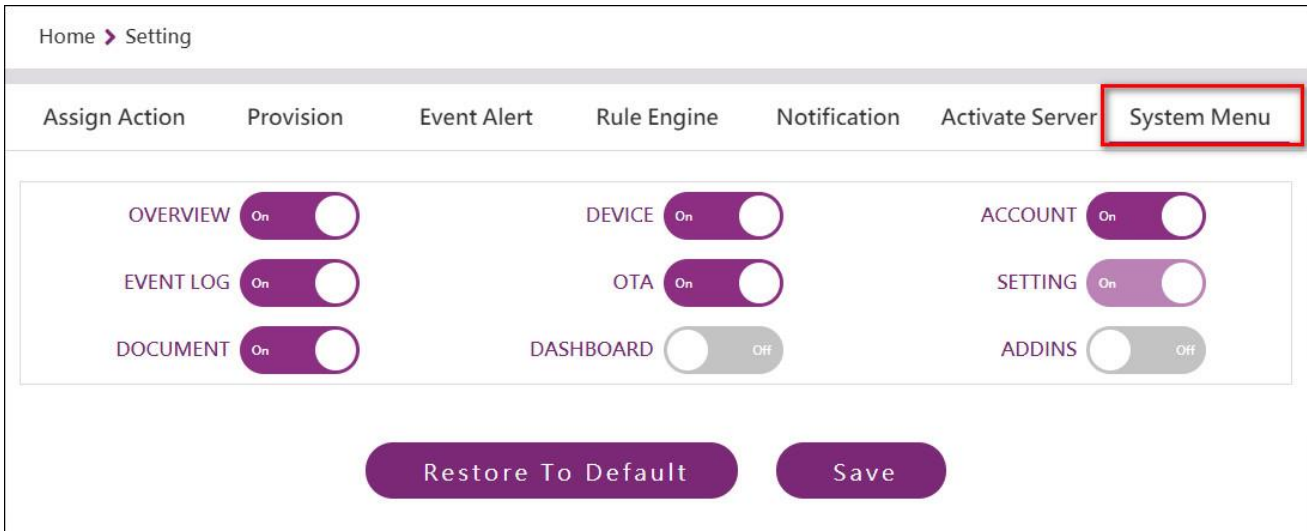
Product Name

Activate

© 1983-2019 Advantech Co., Ltd.

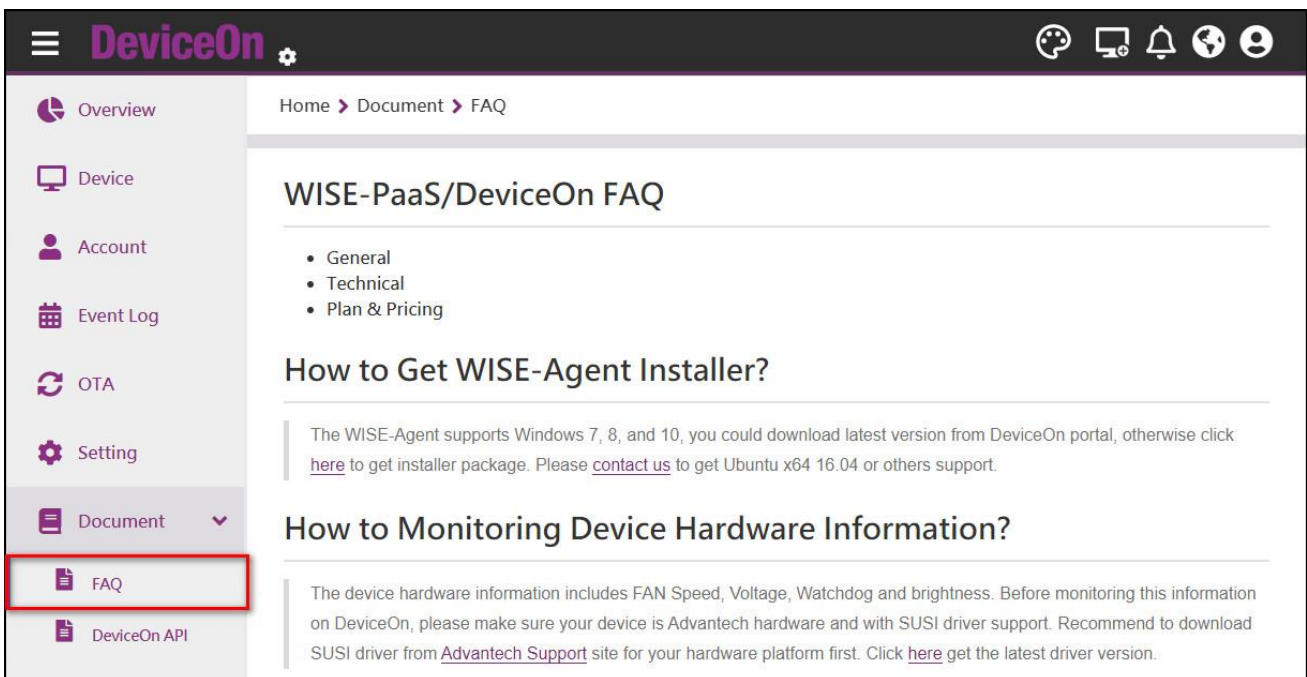
- System Menu

On System Menu, the user could determine which menu item to enable or disable. If you would like to adjust naming, sequence or icon, please reference Section 5.3 for advanced setting.



3.3.7 Documents

There are two documents on DeviceOn user interface, one is Restful APIs and another is FAQ that including technical and general questions.



DeviceOn provide hundreds of API for App engineer to build up their AIoT solution, through the APIs to get account, map, device data, and remote diagnostic on devices. The API document is generated by APIDoc, includes API method, request, response, header and testing.

DeviceOn

Home > Document > DeviceOn API

DeviceOn Restful API 1.1.40

User Guide - URL Path

The full format of URL Path for WISE-PaaS DeviceOn Restful API is "http(s)://{WISE-PaaS EdgeSense Server IP or Domain Name}:{Port}/{Relative Path of API}"

EXAMPLE

http://172.22.12.21:8080/APIInfoMgmt

AppInfo

AppInfo - Get Application Information 1.0.0

Get all information of application from environment variables.

GET

/rmm/v1/appinfo

Header

Field	Type	Description
Authorization	optional string	Basic Authorizaion/Bearer JWT
Cookie	optional string	EIToken JWT/EIRMMToken JWT

Actually, the developer could design a plugin on WISE-Agent to aggregate edge data (Reference Section 5.1), and get these data via Restful APIs, visualize on Grafana Dashboard (Reference Section 4.4) or develop a UI plugin to customize. (Reference 5.2)

4. Hands-On LABs

4.1 How to Create a Real-time Action into Overview

The real-time action is a handy way to execute a specific command to a bunch of devices. This lab guides you how to create a real-time action. And, after this lab, you should:

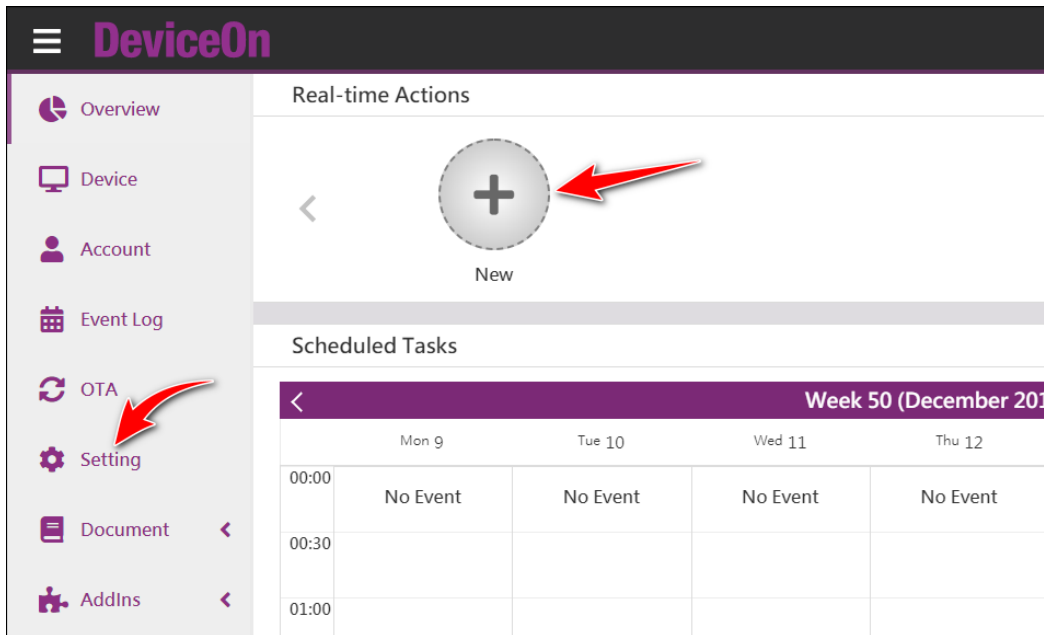
- Learn how to create a real-time action on demand.
- Know of what actions DeviceOn provides.
- Have an action named **"MyAction"** and pinned into your **"Overview"** page, that can reboot devices belong to group **"Default"**.

4.1.1 Prerequisite

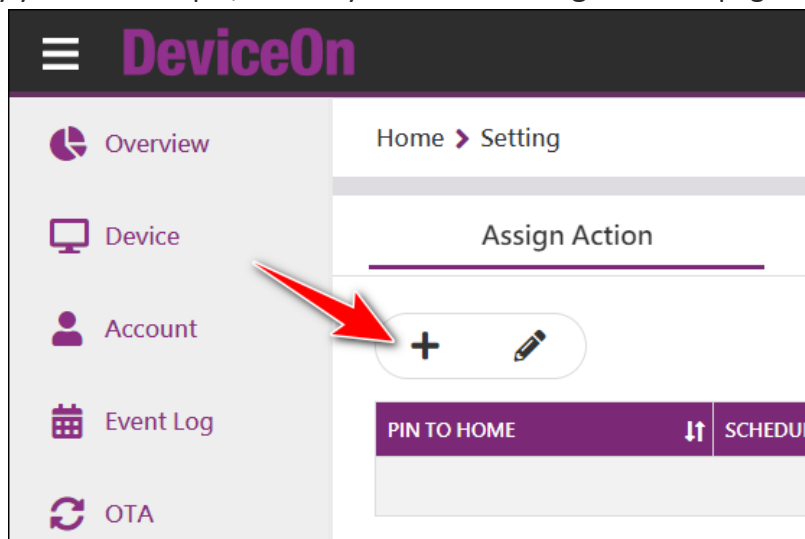
- A running DeviceOn server.
- A device that installed WISE-Agent connects to DeviceOn server.

4.1.2 Step-by-Step

Step 1: To create a real-time action, click the **“New”** icon in **“Overview”**. Alternate, click **“Setting”** from the menu populated in left hand side.



Step 2: Either way you use in step 1, it leads you into the **“Assign Action”** page. Click the **“+”** symbol.



Step 3: You now run into the first page **“Select Action”** to create a new real-time action. Enter the action name **“MyAction”** as well as choose the action **“Reboot”** within this page. From this page you can see all actions DeviceOn provides. Then end this page up with clicking **“Next”** button.

Home > Setting > New Action

New Action

Select Action 1 Select Device Groups 2 Confirm 3

ACTION DESCRIPTION MyAction ✓

Power Saving

- ☐ Power On
- ☐ Power Off
- ☒ Reboot
- ☐ Backlight On
- ☐ Backlight Off

Security

- ☐ Protection On
- ☐ Protection Off
- ☐ Backup
- ☐ Recovery
- ☐ USB Lock
- ☐ USB Unlock
- ☐ Keyboard Lock
- ☐ Keyboard Unlock
- ☐ Touch Lock
- ☐ Touch Unlock
- ☐ Touch Gesture Lock
- ☐ Touch Gesture Unlock

System

- ☐ Update Agent
- ☐ Screenshot
- ☐ Audio Mute
- ☐ Audio Unmute
- ☐ Watchdog Enable
- ☐ Watchdog Disable
- ☐ Notification Block
- ☐ Notification Unblock
- ☐ UWF Enable
- ☐ UWF Disable

Next

Choose an action

Action name here

Go to next page

Step 4: Choose the target group “Default” to execute the real-time action in “Select Device Groups” page.

New Action

Select Action 1 Select Device Groups 2 Confirm 3

Add Device Groups

☐ MyGroup

☒ Default

Back Next

1

2

Step 5: The last page “Confirm” provides you a summary like information and, more than those, lets you decide whether this action “Pin” to your “Overview” page or not. DeviceOn turns this feature on by default. Just toggle it if you don’t want this action pin to your home. Finally, click “Confirm” button to finish.

If everything goes well, you should see there is a new item generated within **“Assign Action”**. Meanwhile, if you go to your home (page **“Overview”**), you can see a new one action icon is populated there.

Assign Action	Provision	Event Alert	Rule Engine	Notification	System Menu
KEYWORD SEARCH					
PIN TO HOME	SCHEDULE	ACTION TYPE	ACTION DESCRIPTION	DEVICE GROUP NAME	CREATED DATETIME
		Reboot	MyAction	MyGroup Default AnotherGroup	2019/12/13 13:16:33

1 record

What should, or can, you do now? Yes, one-click that icon you created from **“Overview”** page, and watch the devices whether they execute reboot action.

4.2 How to Remote Software Provisioning via OTA

OTA (Over-The-Air) is another powerful feature DeviceOn provides. Users can deploy software packages onto a device remotely, or even many devices broadly. This lab guides you how to accomplish remote software provisioning via OTA. And, after this lab, you should:

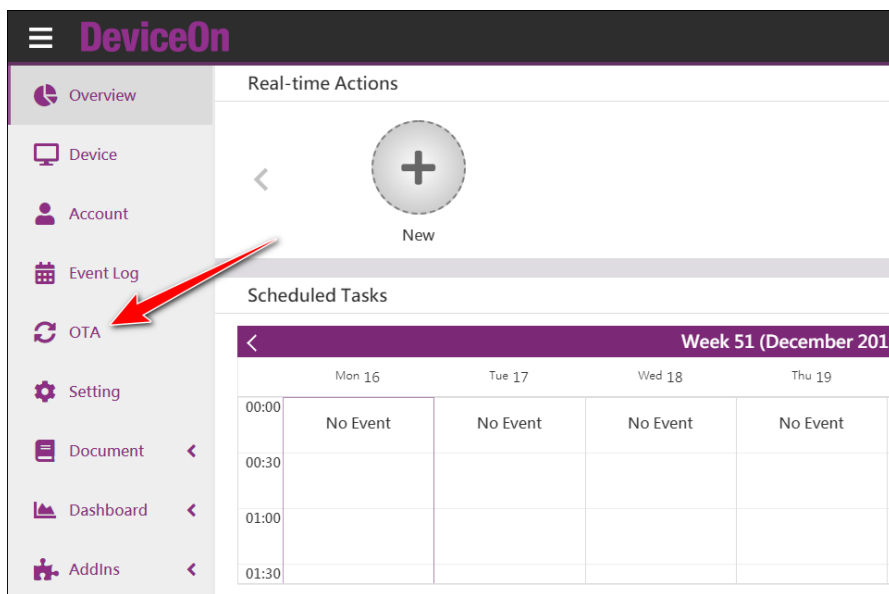
- Learn how to remote provisioning your software via OTA on demand.
- Learn how to package your software for remote provisioning.
- Have the NotePad++, a popular and famous text editor, populated within the target device.

4.2.1 Prerequisite




- A running DeviceOn server.
- A device which running on Windows operating system and installed WISE-Agent, that connects to DeviceOn server.
- A running, with well configured, FTP server as the storage.
- A NotePad++ installer, 32-bit edition is recommended. Its name is **“npp.7.8.2.Installer.exe”**, something like that. It can be downloaded from <https://notepad-plus-plus.org/downloads/>.
- Automation skills to install target software package. It is because that user intervention is not possible during provisioning via OTA. For Windows it can be batch file or power shell, while for Ubuntu it may be shell scripts.

4.2.2 Step-by-Step

Step 1: Click **“OTA”** from the menu on left hand side. It leads you into the **“Storage”** page.



Step 2: In **“Storage”** page, click the plus (+) sign. This step leads you into the **“Add New Storage”** page. You have to add a new storage to upload new packages.

Storage			
Keyword Search			
<div>    </div>			
STORAGE NAME	↕	TYPE	↕
wiseagent-upgrade		AZURE	SSL
Azure2		AZURE	SSL
Am1		S3	SSL

Step 3: Fill all fields in with proper values like following:

- **SOTRAGE:** Pick “FTP” from the dropdown lists.
- **Security:** Leave it as “NONE”, the default value. If your FTP server running on FTPS protocol, pick “FTPS”.
- **SOTRAGE NAME:** Enter “MyFTP”.
- **DOMAIN:** Enter the FQDN of your FTP server, or its IP address.
- **PORT:** Should be **21** if the FTP server runs on a standard port number.
- **ACCOUNT NAME:** A valid username that can connect to the FTP server, and upload files onto the server as well.
- **PASSWORD:** The password to login.
- **CMC/SMC:** Use defaults.
- **ROOT PATH:** Simply uses “/”.
- **DESCRIPTION:** Leave it empty. It’s optional information.


Finally, click “**Save**” button to finish this step. If it goes well, you should see a new table row regarding this FTP storage populated in “**Storage**” page.



← Add New Storage

STORAGE
FTP 1

Security 2 ☒ NONE ☐ FTPS ☐ FTPES


STORAGE NAME
MyFTP 3

DOMAIN 4  PORT (RANGE: 0-65535)
21 5

ACCOUNT NAME 6  PASSWORD 7 

CMC (CLIENTMAXCONNECTIONS)
30

SMC (SERVERMAXCONNECTIONS)
5

ROOT PATH 8 

DESCRIPTION

9 Save

Storage


Package


Upgrade

Configuration

Keyword Search

+





STORAGE NAME	TYPE	SECURITY	SERVER MAX CONNECTIONS	CLIENT MAX CONNECTIONS
agent-upgrade-stage	AZURE	SSL	0	0
MyFTP	FTP	NONE	5	30

2 records

Step 4: An extra step we need to execute prior to next step: prepare a valid package for OTA. DeviceOn provides users a toolkit to pack all stuff to be a valid OTA package.

1. Create a new folder names **"NPP"** in, say, your desktop.
2. Move the downloaded file **"npp.7.8.2.Installer.exe"** into.
3. Create a new file **"install.bat"**, contains only `start /wait npp.7.8.2.Installer.exe /S`, inside. This command, per its document in official web site, installs the downloaded NotePad++ software silently.

Step 5: Now click the **"Package"** tab next to **"Storage"** tab. And, then, choose **"MyFTP"** from **"STORAGE"** field. Last, click the **"Package Toolkit"** icon to enter **"Package Toolkit"** page.

Storage

Package 1


Upgrade


Configuration


STORAGE 2


MyFTP

Keyword Search









1

2

3

NO.	TYPE	VERSION	TAGS	STORAGE	NAME	UPLOAD TIME
1	largePack	1.1.1.1		MyFTP	largePack-v1.1.1.1-4531630409a5acc34286cfb6a67886ae.zip	2019/12/17 15:38
2	CreateDir	1.0.0.2		MyFTP	CreateDir-v1.0.0.2-a9d6612910a37dee7be162ca5bd985ff.zip	2019/12/17 15:36

2 records

Step 6: In “**Package Toolkit**” page, fill all mandatory field up with proper values. At last, click “**Generate**” button to package “**NPP**” software, and upload onto “**MyFTP**” storage as well.

- **Package Type:** Fill “**NPP**” up.
- **Package Version:** Fill “**1.0.0.0**” up.
- **Device Group:** Choose “**Default**”.
- **DEVICE:** Choose the target device. “**AA-Win**” in this lab environment.
- **SOURCE DIR:** Click “**Browser**” to point to the location of “**NPP**” folder we created in step 4.
- **DEPLOY FILE:** DeviceOn chooses “**install.bat**” for you.
- **STORAGE:** Choose “**MyFTP**” from dropdown list.

The screenshot shows the 'Package Toolkit' form with the following fields and annotations:

- 1** PACKAGE TYPE: NPP
- 2** PACKAGE VERSION: 1.0.0.0
- 3** DEVICE GROUP: Default
- 4** DEVICE: AA-Win
- 5** SOURCE DIR: NPP (with a 'Browser' button next to it)
- 6** DEPLOY FILE: install.bat
- 7** STORAGE: MyFTP
- 8** Generate button

At the bottom, there is a footer: 'Version 4.0.0 ©2019 Advantech corp All rights reserved.'

Step 7: Now, in “**Package**” page, a new one table row represents the “**NPP**” package has been added.

Storage

Package

Upgrade

Configuration

STORAGE

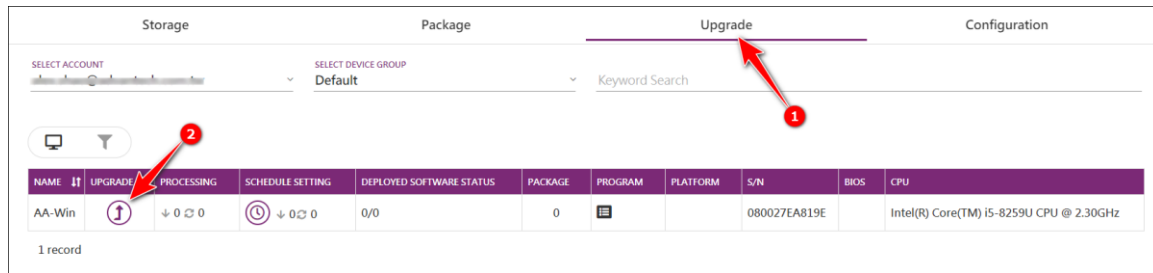
MyFTP

Keyword Search

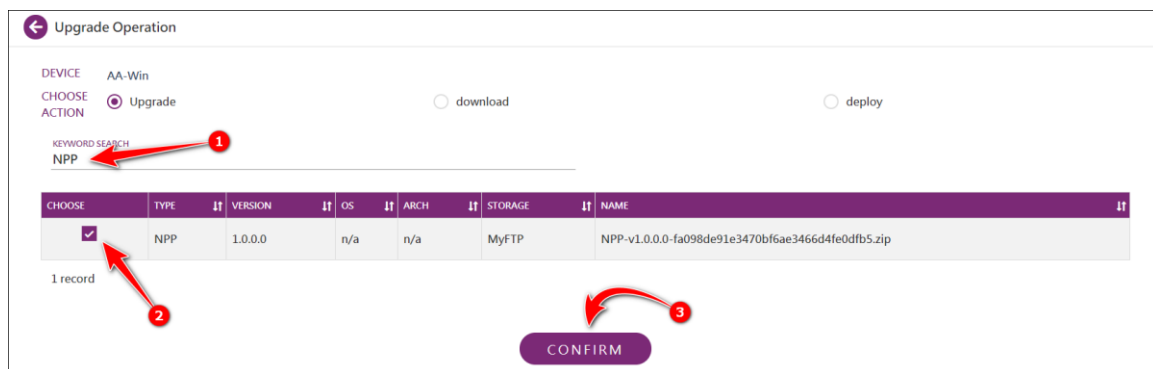
NO.	TYPE	VERSION	TAGS	STORAGE	NAME	UPLOAD TIME
1	NPP	1.0.0.0	x64,x86,win	MyFTP	NPP-v1.0.0.0-fa098de91e3470bf6ae3466d4fe0dfb5.zip	2019/12/18 13:35
2	largePack	1.1.1.1		MyFTP	largePack-v1.1.1.1-4531630409a5acc34286cfb6a67886ae.zip	2019/12/17 15:38
3	CreateDir	1.0.0.2		MyFTP	CreateDir-v1.0.0.2-a9d6612910a37dee7be162ca5bd985ff.zip	2019/12/17 15:36

3 records

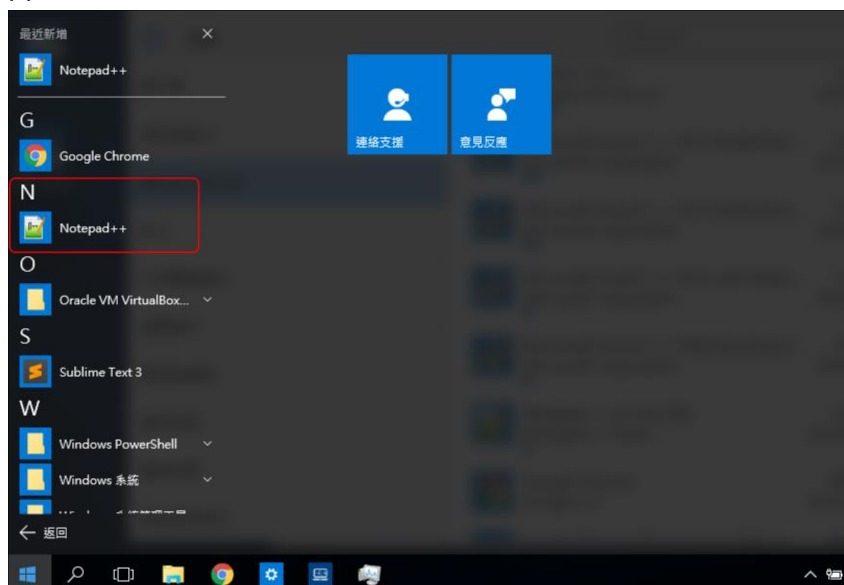
Step 8: It is time to install NotePad++ onto the target device remotely. Based on previous step, click “**Upgrade**” tab next to “**Package**” tab. You should find the target device shows there within the table view. Click the icon locates in target device row and “**UPGRADE**” column. It leads you into the “**Upgrade Operation**” page.



Step 9: In “Upgrade Operation” page, fill “NPP” up in “KEYWORD SEARCH” field so that the package can be filtered out of all packages. Check the box accordingly and click “CONFIRM” button.



Step 10: Now the NotePad++ should be installing and, after a while, if everything went well, a corresponding application item should be created in Windows menu.



4.3 How to Set a Device Threshold and Event Notify Services

For devices monitoring, DeviceOn provides the rule engine. Users can acquire anomaly situations by means of setting thresholds to those interested devices, and, once one or more thresholds meets,

receive alerts via event notification services, another one indispensable feature for users. This lab guides you how to set thresholds to a device and how to set event notification services as well. As such, after this lab, you should:

- Learn how to set thresholds to a device on demand.
- Learn how to set event notification services, including email, LINE, and WeChat as well.

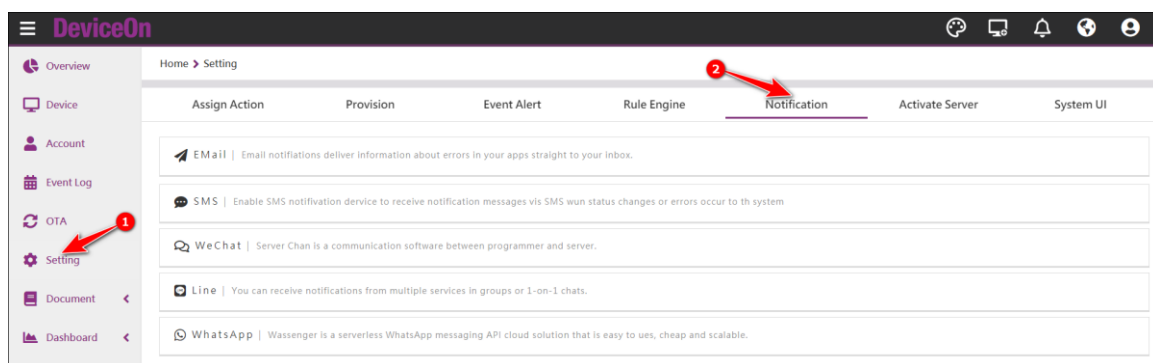
4.3.1 Prerequisite

- A running DeviceOn server.
- A device that installed WISE-Agent connects to DeviceOn server.
- A valid, send-able, email account to enable Email notification service.
- A valid LINE account to enable LINE notification service.
- A valid WeChat account, as well as a valid GitHub account, to enable WeChat notification service.

4.3.2 Steps to Set Event Notification Service – Email

The configuration of using email as one of event notification services is a system-wide setting. This means DeviceOn uses the server, the one you set in this step, to send all emails. Therefore, uses email settings from your organization is recommended, rather than uses your personal Gmail. If you really want to use Gmail, the situations you are running into may vary and depends on your google account settings. So, in this lab, we assume that you have already a valid business email address from your company.

Step 1: Click **“Setting”** menu on the left-hand side of DeviceOn portal and, then, **“Notification”**.



Step 2: Click **“EMail”** bar to open settings regarding email notification service.

Assign Action Provision Event Alert Rule Engine **Notification** Activate Server System UI

Email | Email notifications deliver information about errors in your apps straight to your inbox.

EMAIL NOTIFICATION

Email notifications deliver information about errors in your apps straight to your inbox. You can turn on notifications to get alerts on your phone or computer when you get new emails.

PORT (RANGE: 0-65535)
25

SSL TLS

Email Server

Email Account

Email Password

Sender Email

EMAIL SUBJECT
DeviceOn

Test Save

Step 3: Toggle “On/Off” switch to enable this feature. Then fill fields up with proper values. And end up this step by clicking “Test” button.

- **EMAIL SERVER:** The email server host name.
- **PORT:** The email server port. Normally this is 25.
- **SSL/TLS:** Toggle to a proper setting.
- **EMAIL ACCOUNT:** Your email account name. If takes the windows domain into account, a value format like “DOMAIN\USER” should be used.
- **EMAIL PASSWORD:** Your password to sign in to the email server.
- **SENDER EMAIL:** Your email address.
- **EMAIL SUBJECT:** Leave it the default.

Assign Action Provision Event Alert Rule Engine **Notification** Activate Server System UI

Email | Email notifications deliver information about errors in your apps straight to your inbox.

EMAIL NOTIFICATION

Email notifications deliver information about errors in your apps straight to your inbox. You can turn on notifications to get alerts on your phone or computer when you get new emails.

PORT (RANGE: 0-65535)
25

SSL TLS

EMAIL SERVER
mailapp.advantech.com

EMAIL ACCOUNT
advantech\alexsahao

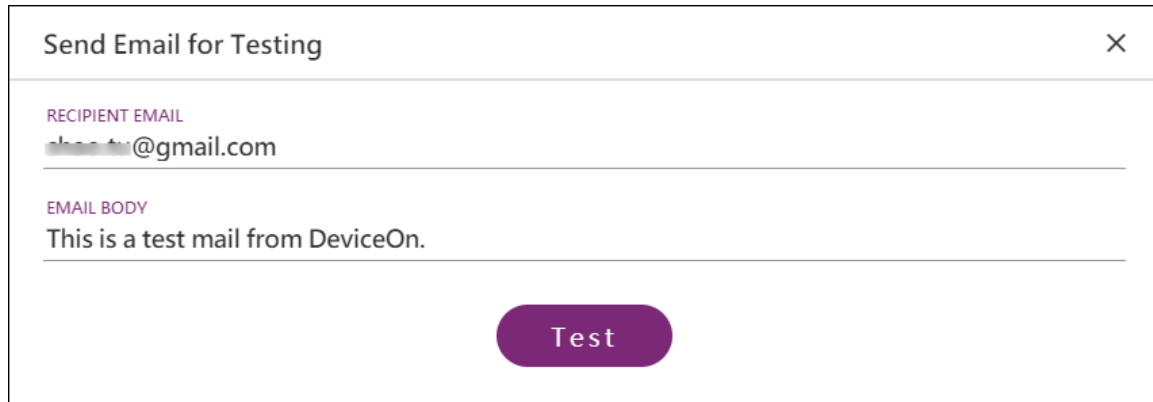
EMAIL PASSWORD

SENDER EMAIL
alexsahao@advantech.com.tw

EMAIL SUBJECT
DeviceOn

Test Save

Step 4: To assert all values are correct, click **“Test”** button, on the bottom right of the page, to open the **“Send Email for Testing”** dialog for testing purpose. And fill a recipient email as well as email body. Then click **“Test”** on this dialog. An email you should receive in a while later. Revise them until you got a test email.

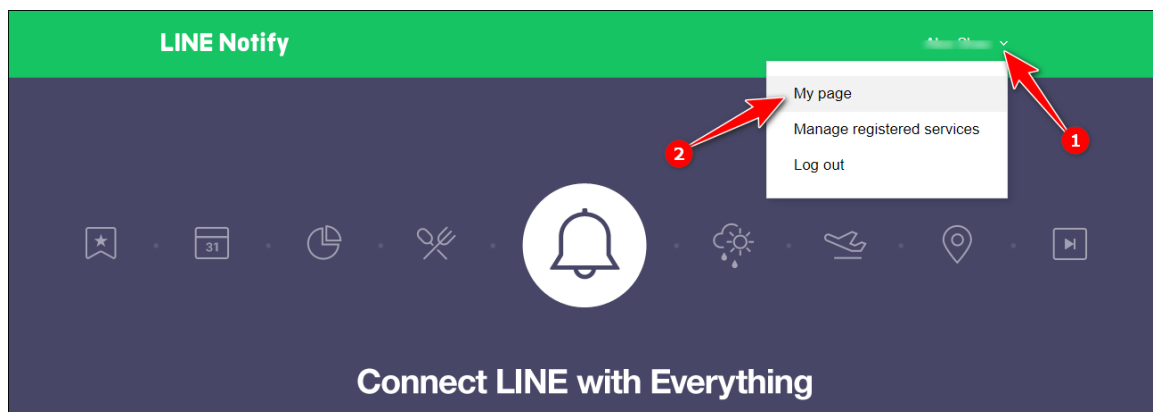


The dialog box titled "Send Email for Testing" has a close button (X) in the top right corner. It contains two input fields: "RECIPIENT EMAIL" with the value "shane.tu@gmail.com" and "EMAIL BODY" with the value "This is a test mail from DeviceOn." At the bottom center is a purple button labeled "Test".

Step 5: Click **“Save”** on the bottom right of the page that shows in step 3 to keep all settings and enable email notification service.

4.3.3 Steps to Set Event Notification Service – LINE

Step 1: Go to <https://notify-bot.line.me/> and sign in with your LINE account. Click **“My Page”** from your account’s dropdown menu in the upper right of the page.



Step 2: Click **“Generate token”** under **“Generate access token (For developers)”**. It pops up the **“Generate token”** dialog.

Generate access token (For developers)

By using personal access tokens, you can configure notifications without having to add a web service.

Generate token

LINE Notify API Document

Step 3: Fill token field up with **“DeviceOn”** and click the **“1-on-1 chat with LINE Notify”** item. Then click the **“Generate token”** button in green at bottom.

Generate token

Please enter a token name to be displayed before each notification.

DeviceOn 1

Select a chat to send notifications to.

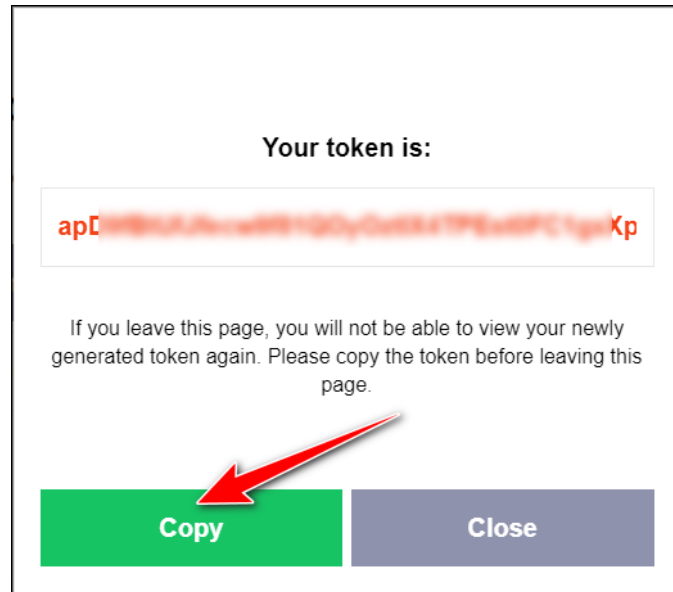
Search by group name

1-on-1 chat with LINE Notify 2

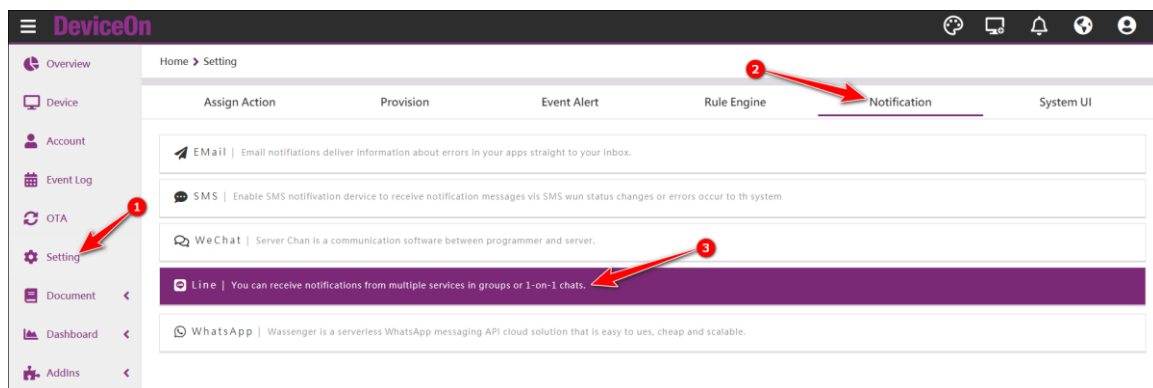
Note: Revealing your personal access token can allow a third party to obtain the names of your connected chats as well as your profile name.

Generate token 3

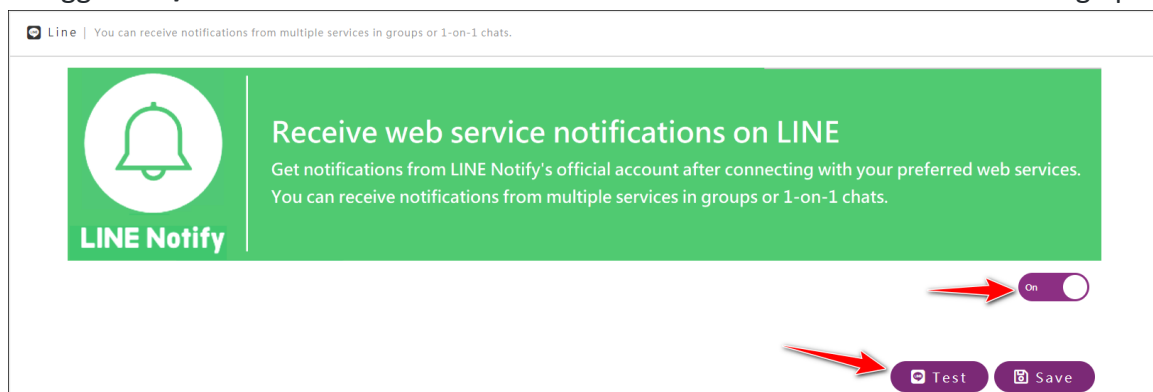
Step 4: A new window pops up with token. Meanwhile, a LINE message about this token generation received immediately. Click **“Copy”** to keep the token in memory, or any file you like.



Step 5: Now switch your browser to DeviceOn portal. Click **“Setting”** menu on the left-hand side, then **“Notification”**, and last **“LINE”** bar to open settings regarding LINE event notification service.



Step 6: Toggle **“On/Off”** switch to enable this feature. Click **“Test”** to show the test dialog up.



Step 7: Paste the copied token into the first field (LINE Token) and write something into the second field (LINE Message Content). Click **“Test”**, you should receive the messages you wrote with **“DeviceOn”** as the prefix.

Send LINE Message for Testing

LINE TOKEN
ap[REDACTED]GQt 1

LINE MESSAGE CONTENT
Hello DeviceOn !!! 2

3
Test

Step 8: Click “Save” button that shows in **Step 6** to keep your settings and enable LINE event notification service.

4.3.4 Steps to Set Event Notification Service – WeChat

Step 1: Go to <http://sc.ftqq.com/3.version>. Click “登入网站” hyperlink.

Server酱

首页 发送消息 微信推送 TalkAdmin 一对多推送 登入

是什么

「Server酱」，英文名「ServerChan」，是一款「程序员」和「服务器」之间的通信软件。

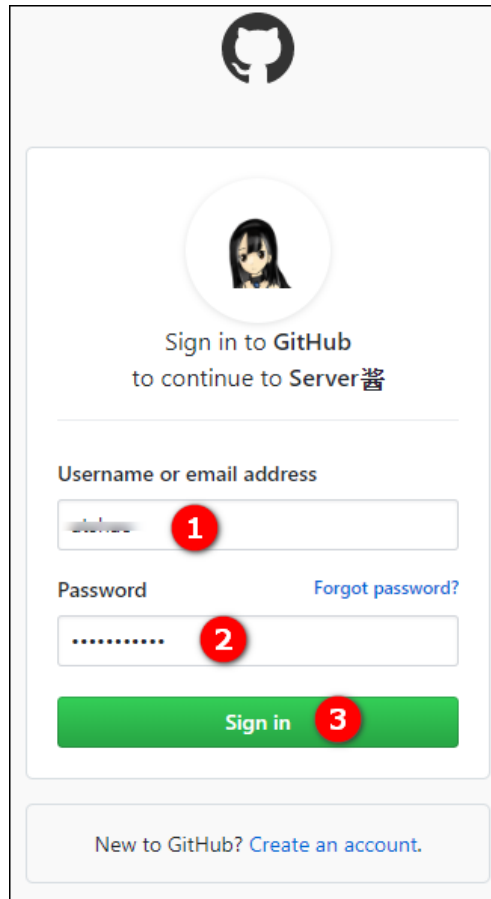
说人话？就是从服务器推报警和日志到手机的工具。

开通并使用上它，只需要一分钟：

1. 登入：用GitHub账号 **登入网站**，就能获得一个SCKEY（在「发送消息」页面）
2. 绑定：点击「微信推送」，扫码关注同时即可完成绑定
3. 发消息：往 <http://sc.ftqq.com/SCKEY.send> 发GET请求，就可以在微信里收到消息啦

来个示意图：

Step 2: Sign in with your GitHub account.



The image shows a GitHub login page for 'Server酱'. At the top is the GitHub logo. Below it is a circular profile picture of a character. The text 'Sign in to GitHub to continue to Server酱' is centered. There are two input fields: 'Username or email address' with a red circle '1' next to it, and 'Password' with a red circle '2' next to it. A 'Forgot password?' link is next to the password field. A green 'Sign in' button with a red circle '3' next to it is below the fields. At the bottom, there is a link 'New to GitHub? Create an account.'

Step 3: Click “微信推送” hyperlink.

Server酱

是什么

「Server酱」，英文名「ServerChan」，是一款「程序员」和「服务器」之间的通信软件。

说人话？就是从服务器推报警和日志到手机的工具。

开通并使用上它，只需要一分钟：

1. 登入：用GitHub账号[登入网站](#)，就能获得一个SCKEY（在「[发送消息](#)」页面）
2. 绑定：点击「[微信推送](#)」 扫码关注同时即可完成绑定
3. 发消息：往 <http://sc.ftqq.com/SCKEY.send> 发GET请求，就可以在微信里收到消息啦

Step 4: Click “开始绑定”. It opens a QR code image.



Step 5: Take your mobile up, swipe and open WeChat App to scan this generated QR code so that the service can bind with your WeChat account.



Step 6: Once it is done. The page changes, like below.



Step 7: Click “**SCKEY**” hyperlink and copy, from the opened page, the SCKEY value.

Step 10: Paste the copied SCKEY, copied in step 7, into the first field **“WECHAT SC KEY”**. Give a title to the second field **“WECHAT MESSAGE TITLE”**. Write some message content to the last field **“WECHAT MESSAGE CONTENT”**. And click **“Test”** to see if it works or not.

Send WeChat Message for Testing

WECHAT SC KEY
SCI...e3f 1

WECHAT MESSAGE TITLE 2
DeviceOn

WECHAT MESSAGE CONTENT 3
Notification testing!!!

Test 4

Step 11: Click **“Save”** button that shows in step 9 to keep your settings and enable WeChat event notification service.

4.3.5 Other Event Notification Services – SMS/WhatsApp

DeviceOn provides 2 more event notification services other than mentioned previously. They are SMS (Clickatell) and WhatsApp. Those two are provided by third party service and purchase required. Please contact us if it is necessary for you to use one of them as the event notification service.

4.3.6 Steps to Set Thresholds to a Device

Step 1: Click **“Setting”** menu on the left-hand side of DeviceOn portal and, then, **“Rule Engine”**

DeviceOn

Home > Setting

Assign Action Provision Event Alert Rule Engine 2 Notification System UI

SELECT ACCOUNT Alex.Shao@advantech.com.tw RULE TYPE Device

+ -

ENABLE	RULE TYPE	DEVICE / DEVICE GROUP NAME	SENSOR NAME	ACTION	THRESHOLD
No matching records					

Step 2: Click the plus (+) sign to enter **“Rule Engine”** page.

ENABLE	RULE TYPE	DEVICE / DEVICE GROUP NAME	SENSOR NAME	ACTION	THRESHOLD
No matching records					

Step 3: Choose each setting with a proper value within step 1 – Select Sensor.

- **SELECT RULE TYPE:** Shows the new rule engine applies to a single device or a device group. Please pick “**Device**” here.
- **SELECT DEVICE GROUP:** Also, leave it the default, “**Default**”.
- **SELECT DEVICE:** Which device the new rule engine will apply? We choose “**AA-Win**” in this lab environment.
- **KEYWORD SEARCH:** Please enter “**hard**” so that only hard drive relevant items available.

Here, to ease this lab, we pick **“Hard Drive Free Space”** as a threshold of the rule engine. In addition, like the picture shows, it illustrates the disk C is the target hard drive in this lab. Click **“Next”** to go to next step.

	SENSOR NAME	SENSOR ID
<input type="radio"/>	Hard Drive Health	HDDMonitor/hddInfoList/Disk0/health
<input type="radio"/>	Hard Drive Power on Time	HDDMonitor/hddInfoList/Disk0/powerOnTime
<input type="radio"/>	Hard Drive Total Space	HDDMonitor/DiskInfo/Disk C:/Total Disk Space
5 <input checked="" type="radio"/>	Hard Drive Free Space	HDDMonitor/DiskInfo/Disk C:/Free Disk Space

Step 4: Now we need to define a threshold for this rule engine in this step. Based on **“Current Value”** shows on top right, check the **“Less than”** radio button and slide to a maximum value that just on less than **“Current Value”**.

Leave **“Lasting Time”** as well as **“Notice Interval”** the defaults. **“Lasting Time”** indicates that the target device runs into the abnormal condition only when it reaches the set threshold and last the set time. While **“Notice Interval”** tells the interval of users receive an event, until the condition back to normal. Then click **“Next”** to go to next page.

Step 5: We are now in “Define Action” step. Pick “Power On/Off” from “TAKE A ACTION”, “System Restart” from “TAKE A SUB ACTION”, and “Back to Normal” for “Trigger Frequency”. These combination means that the target device will reboot once it backs to normal, after it enters the threshold we set. Also, click “Next” to go to next page.

Step 7: Review all information within this page. Leave “Enable” the default and click “Confirm” button to set this rule, and apply it to the target device as well.

Enable	ON
Rule Type	Device
Device Group	Default
Device	AA-Win
Plugin	HDDMonitor
SensorId	HDDMonitor/DiskInfo/Disk C:/Free Disk Space
Define Threshold	Less than 39543.66 Megabyte
Lasting Time(Second)	10
Notice Interval (Second)	60
Trigger Frequency	Back to Normal
Action	power_onoff

Step 8: The new item should be populated as the image shows.

Assign Action

Provision

Event Alert

Rule Engine

Notification

System UI

SELECT ACCOUNT

Alex.Shao@advantech.com.tw

RULE TYPE

Device

+

ENABLE	RULE TYPE	DEVICE / DEVICE GROUP NAME	SENSOR NAME	ACTION	THRESHOLD
<div>On</div>	Device	AA-Win	HDDMonitor/DiskInfo/Disk C:/Free Disk Space	Power On/Off--System Restart	Less than39543.66 Megabyte

1 record

Step 9: Click “Device” menu item on left hand side of DeviceOn portal. You can see a green circle represents the target device accordingly.

Device List

SELECT ACCOUNT
AlexShao@advantech.com.tw

Device Monitoring

SELECT DEVICE GROUPS
--- All ---

Remote Control

SELECT STATUS
All

Device Data

Keyword Search

+

SETTING STATUS	DEVICE NAME	UPGRADE	POWER	PROTECTION	BACKUP&RECOVERY	DEVICE GROUP NAME	WAKE-ON-LAN	MESSAGE
	AA-Win		 Power off Restart	 Install	 Install	Default	Not Set	
	A9449-NB		 Power on			MyGroup	Not Set	
	AA-Ubuntu		 Power on			Default	Not Set	
	PC060303		 Power on			Default	Not Set	

4 records

Step 10: We can do something so that the target device meets the threshold we set previous. Here we download the newest Ubuntu ISO image to the target device. The green circle shows in step 9 changes, a while later, to an orange one, of which indicates it runs into an abnormal condition.

Device List

Device Monitoring

Remote Control

Device Data

SELECT ACCOUNT

Alex.Shao@advantech.com.tw

SELECT DEVICE GROUPS





--- All ---

SELECT STATUS

All

Keyword Search

+

SETTING STATUS	DEVICE NAME	UPGRADE	POWER	PROTECTION	BACKUP&RECOVERY	DEVICE GROUP NAME	WAKE-ON-LAN	MESSAGE
	AA-Win		 Power off Restart	 Install	 Install	Default	Not Set	
	A9449-NB	 Device Upgrade	 Power on	 Install	 Install	MyGroup	Not Set	
	AA-Ubuntu		 Power on			Default	Not Set	
	PC060303	 Device Upgrade	 Power on			Default	Not Set	

4 records

Step 10: Interrupt the download action at any time, or wait until it finishes. Purge the downloaded file so that the target device has free space more than the threshold we set previous. After a while, the target device should reboot due to the rule engine we set. Note here that it may necessary to purge the recycle bin to achieve our goal.

4.4 How to Visualize Device Data via Grafana Dashboard

Grafana is an open-source software for monitoring and analysis. One of its major characteristics is it supports many different data sources, from popular CloudWatch, Elasticsearch, Graphite, and influxDB, to OpenStack Gnocchi or Google Calendar. Its range is very extensive. However, for others data source require to implement [SimpleJson](#) to access your data. The DeviceOn native support SimpleJson APIs and data source plugin on Grafana. This lab guides you how to visualize device data via Grafana dashboard.

4.4.1 Prerequisite

- A running DeviceOn server.
- A running Grafana service with DeviceOn data source plugin.
- A device which installed WISE-Agent, that connects to DeviceOn server.

4.4.2 Step-by-Step

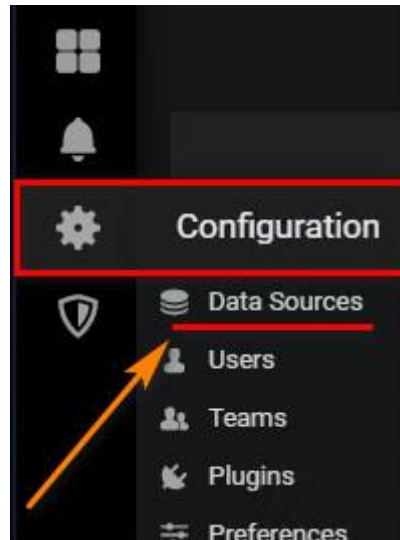
Step 1: Launch Grafana Web Service Shortcut on Desktop, or access the Grafana service endpoint.



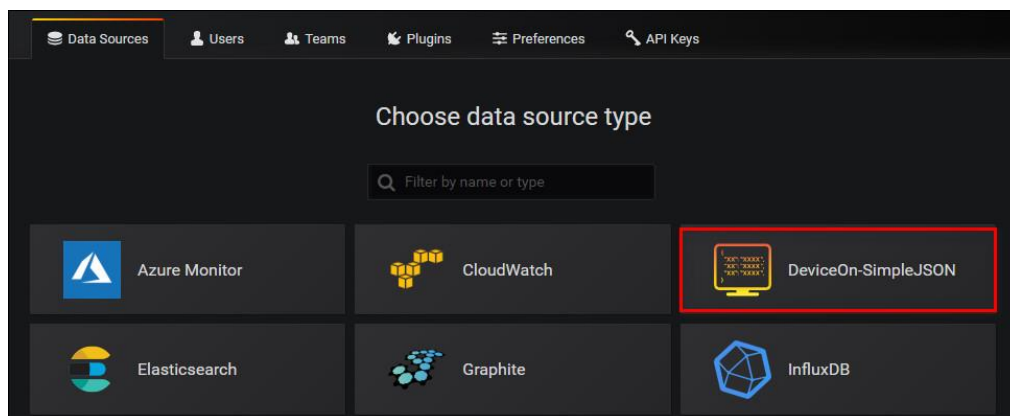
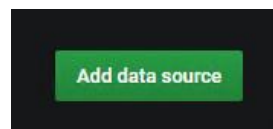
Step 2: Login to Grafana portal with your account, password (Default: admin/admin)



Step 3: Create a data source to access DeviceOn SimpleJson API.



Click on “**Add data source**” and select “**DeviceOn-SimpleJson**”, (for previous version might be RMM-SimpleJson)



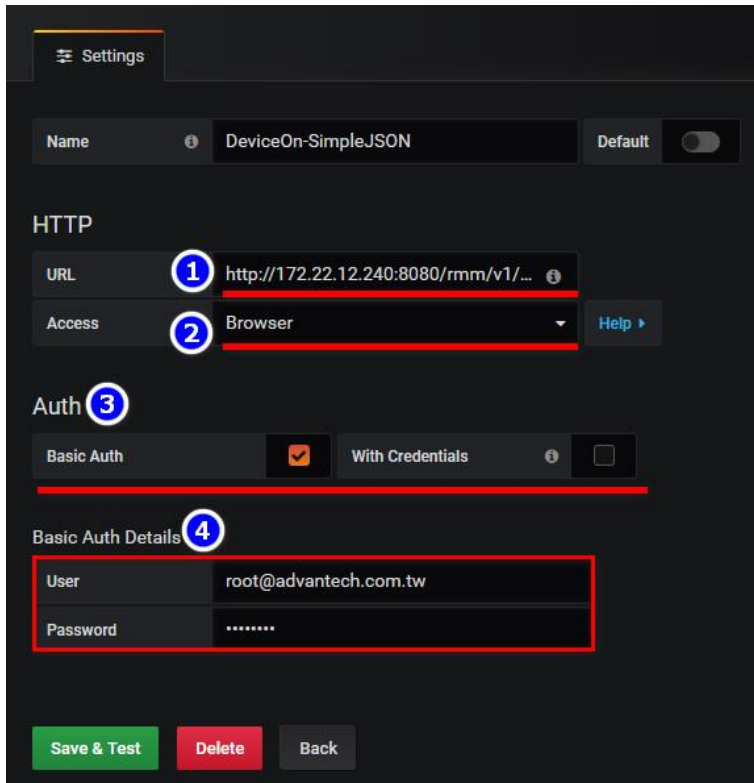
Step 4: Given below parameters for data source plugin to retrieve device data from DeviceOn APIs.

URL: http://<DEVICEON_SERVER>:8080/rmm/v1/grafana/simplejson

Access: Browser

Auth: Basic Auth (Support on prefecture version)

Basic Auth: DeviceOn Account & Password

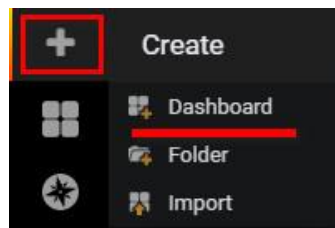


The screenshot shows the 'Settings' page for a device named 'DeviceOn-SimpleJSON'. The 'HTTP' section is expanded, and the following steps are highlighted with numbered circles and red boxes:

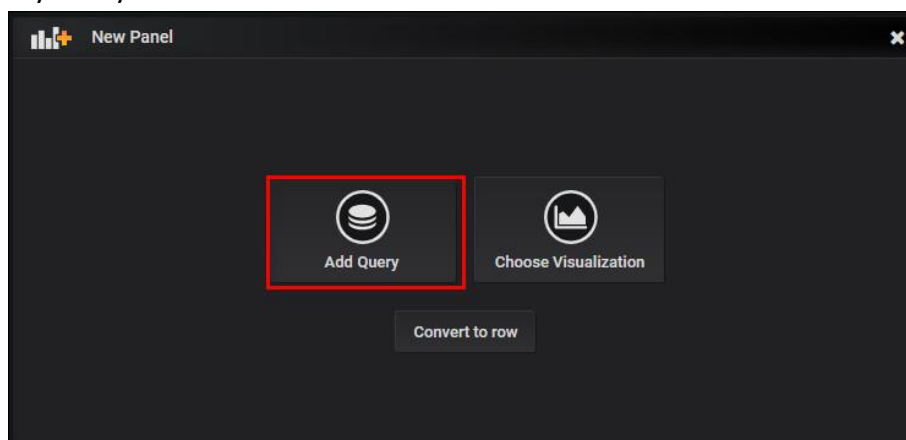
- URL:** `http://172.22.12.240:8080/rmm/v1/...`
- Access:** `Browser`
- Auth:** `Basic Auth` is selected, and the `With Credentials` checkbox is checked.
- Basic Auth Details:** The `User` field is set to `root@advantech.com.tw` and the `Password` field is masked with dots.

At the bottom, there are three buttons: `Save & Test` (green), `Delete` (red), and `Back` (grey).

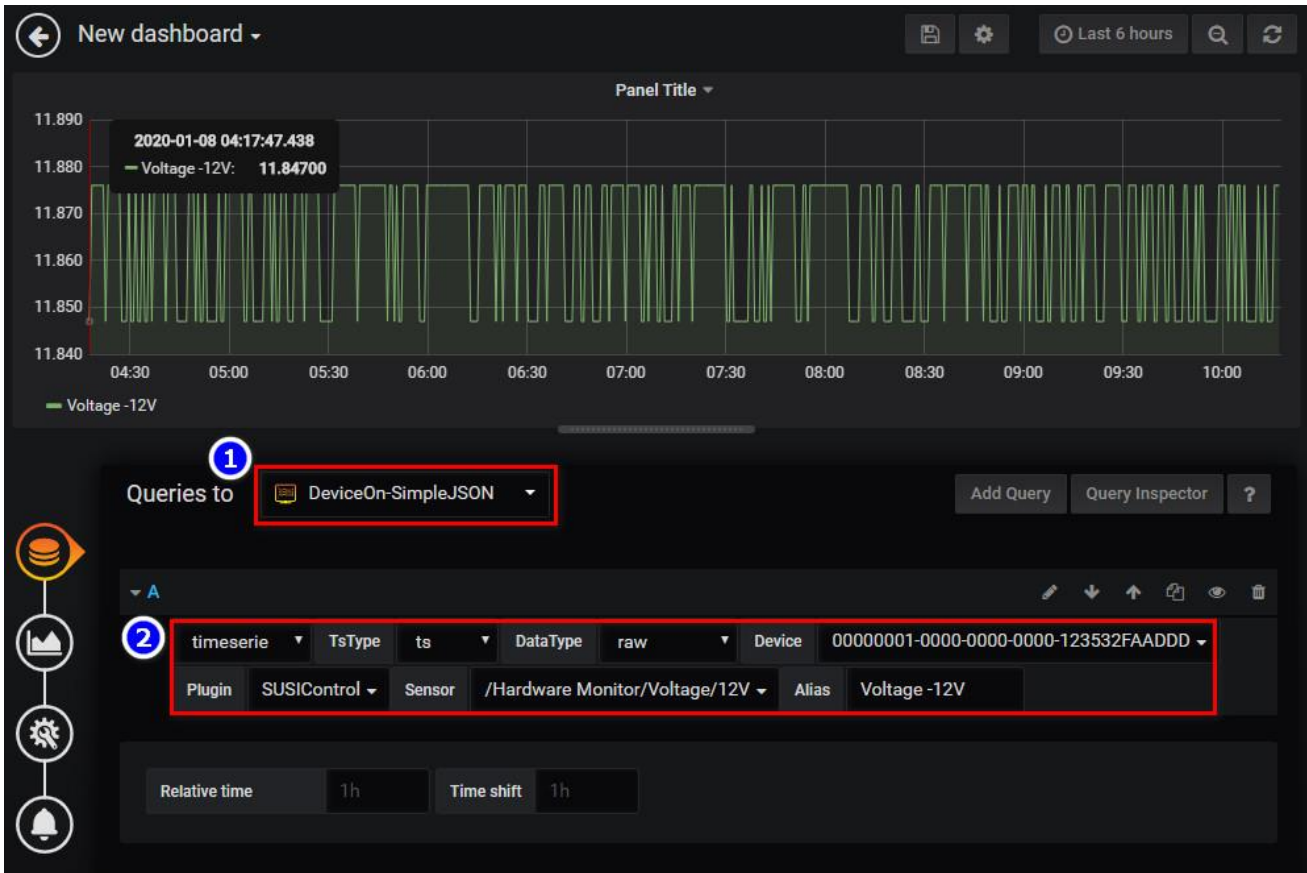
Step 5: Create a dashboard to visualize your device data.



Select "Add Query" for your device.



Select **DeviceOn-SimpleJson** from "Queries to", and pick-up your device with **AgentID**, **Plugin**, **Sensor** and **Alias Name** (Option).



4.5 How to Enable/Disable Windows Lockdown Features

For devices protection, Windows built many nice features in natively. For instance, function key protection disables Ctrl, Alt, and WinKey. UWF protection guarantees your disk C (System Partition) rollbacks to the original state after you reboot the Windows operating system. This lab guides you how to enable Windows lockdown features, and how to active/inactive them via DeviceOn portal. After this lab, you should:

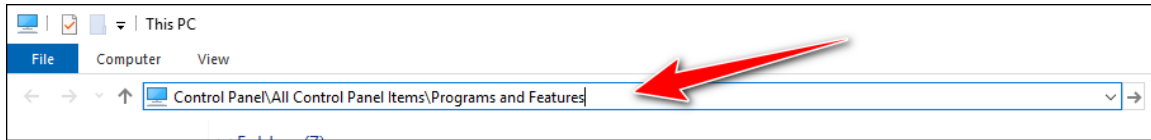
- Learn how to enable **“Keyboard Filter”** and **“Unified Write Filter”** (a.k.a. UWF) in Windows lockdown features.
- Know what lockdown features can be controlled via DeviceOn portal.

4.5.1 Prerequisite

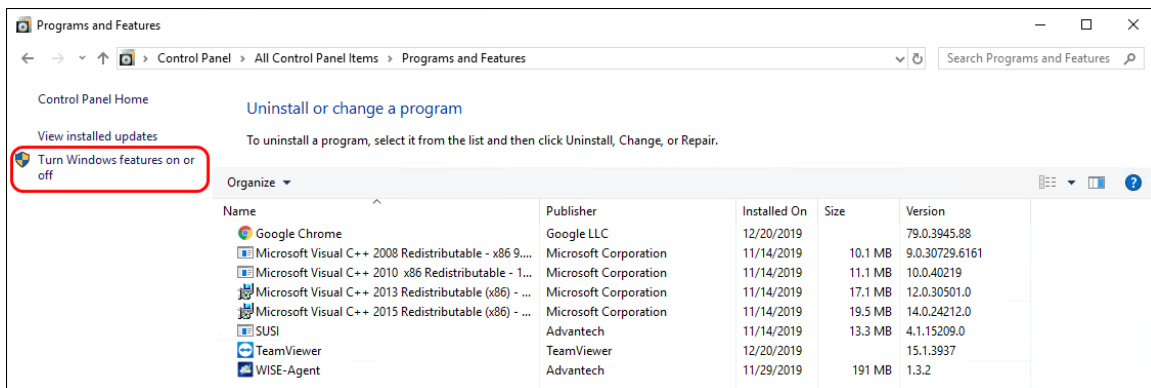
- A running DeviceOn server.
- A device which running on Windows 10 operating system (LTSB, LTSC) and installed WISE-Agent, that connects to DeviceOn server. Besides, this agent must install Advantech SUSI driver, or lockdown feature should not work properly.

4.5.2 Step-by-Step

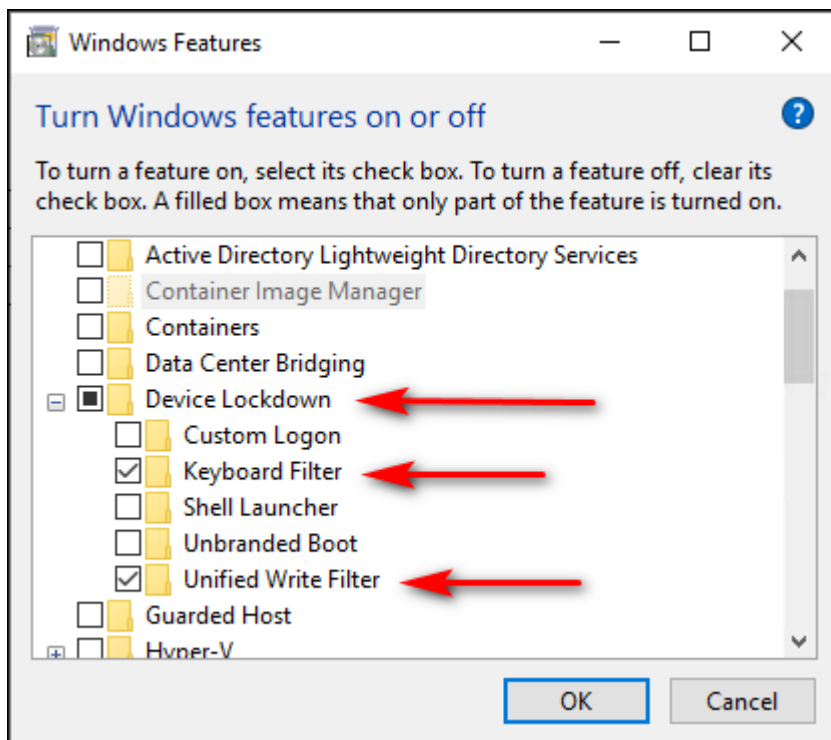
Step 1: Go to the target agent device and open the file explorer window. In address bar, key “**Control Panel\All Control Panel Items\Programs and Features**” in and followed by pressing “**ENTER**”. It opens the “**Programs and Features**” window.



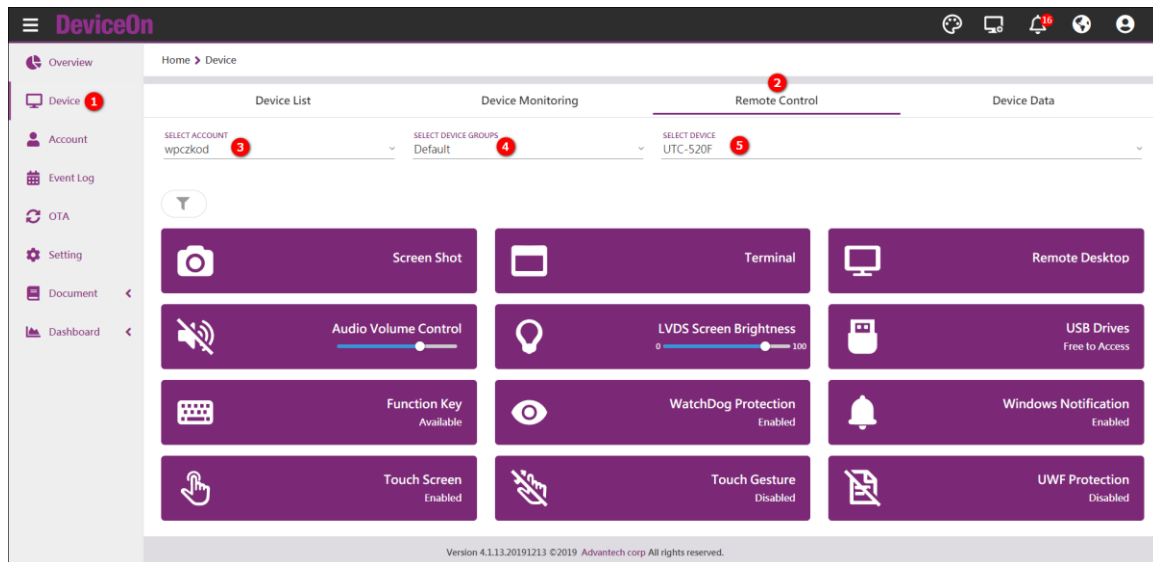
Step 2: Click “**Turn Windows features on or off**” on left hand side to open “**Windows Features**” window.



Step 3: Scroll down the window, find and open the “**Device Lockdown**” item. Make sure both “**Keyboard Filter**” and “**Unified Write Filter**” are checked. Then click “**OK**”.



Step 4: Now back to DeviceOn portal. Click **“Device”** menu item, then **“Remote Control”** tab. And choose proper account, group, and device from **“SELECT ACCOUNT”**, **“SELECT DEVICE GROUPS”**, and **“SELECT DEVICE”** fields accordingly. You can see **“Function Key”**, **“UWF Protection”** control buttons there. Also, other than these two mentioned, **“WatchDog Protection”**, **“Windows Notification”** and more relevant features are available as you can see.



Step 5: Click **“Function Key”** control button. You would find, after a while, the description of **“Function Key”** changes from **“Available”** to **“Ctrl, Alt, WinKey Lockdown”**. If you try to press such keys on the target device, they should not work as expected. Okay, you learned how to enable, disable **“Function Key”** lockdown. Let’s go ahead and learn something regarding UWF.

Step 6: Click **“UWF Protection”** control button. A dialog pops up and the message shows that this action will reboot the device. Click **“CONFIRM”**, its description changes from **“Disabled”** to **“Enabled”**. Just wait for the reboot completed.

Step 7: Now, write some data into disk C. You can, for example, download files into disk C, copy files into disk C. Or even generate by programmatically. Just do whatever you can do to mimic that you are working on disk C.

Step 8: Once you finish your tasks, reboot the target device. You would find that all those data you made at previous step disappear. The disk C rollbacks to the original state and just like you did nothing at all.

4.6 How to Manage DeviceOn on AKS

Since the DeviceOn service container are running the Azure Kubernetes, that's much easier to upgrade to new version, if released. There

4.6.1 Prerequisite

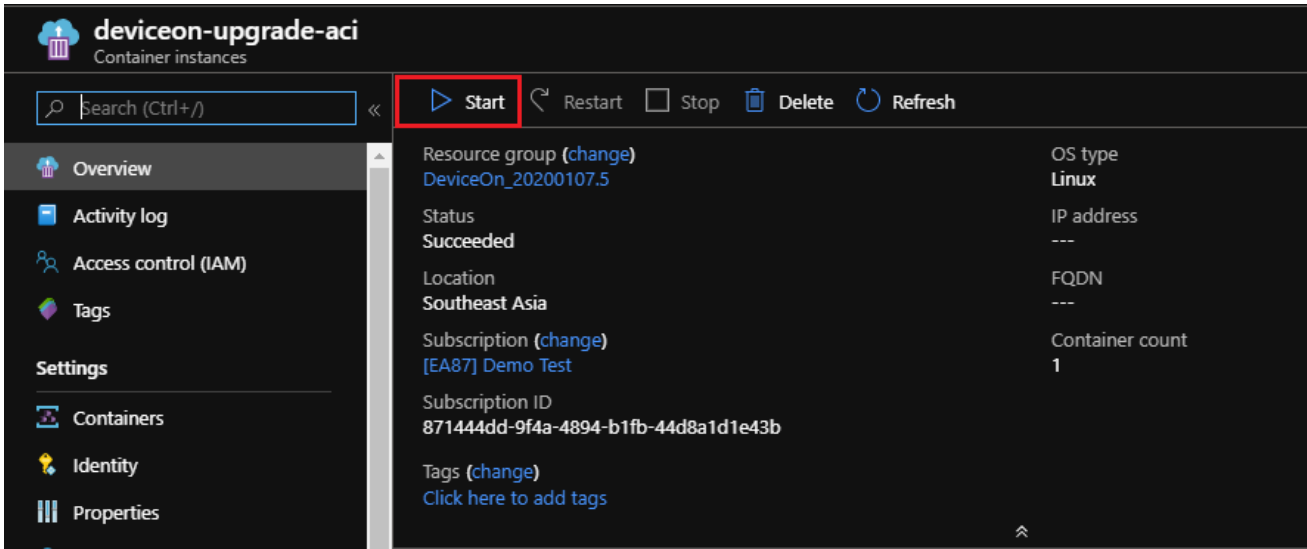
- A running DeviceOn server on Azure Kubernetes
- Azure Account

4.6.2 Steps to Upgrade DeviceOn

Step 1: Login to Azure Portal and find your AKS solution resource group.

Step 2: Click **deviceon-upgrade-aci** service.

Step 3: Click **Start** button to upgrade latest version DeviceOn server.

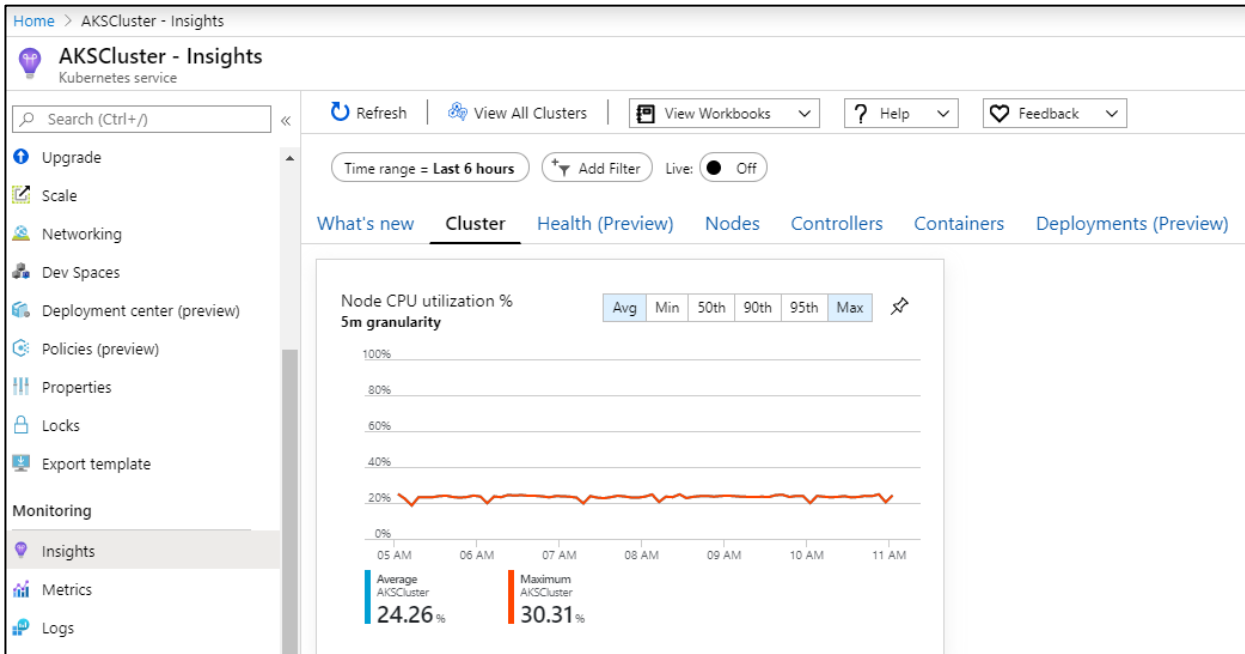


Step 4: After upgrade container instances finish, please go to DeviceOn portal check server version.

4.6.3 Step to Monitor Container Healthy and Status

● Monitor Container Status

Step 1: In AKS service, select "Insights" on the left tab.



Step 2: Click on “Containers” on the top tab. Check if status of each container is running.

** Init container will show completed. **

















What's new Cluster Health (Preview) Nodes Controllers Containers Deployments (Preview)

Search by name...

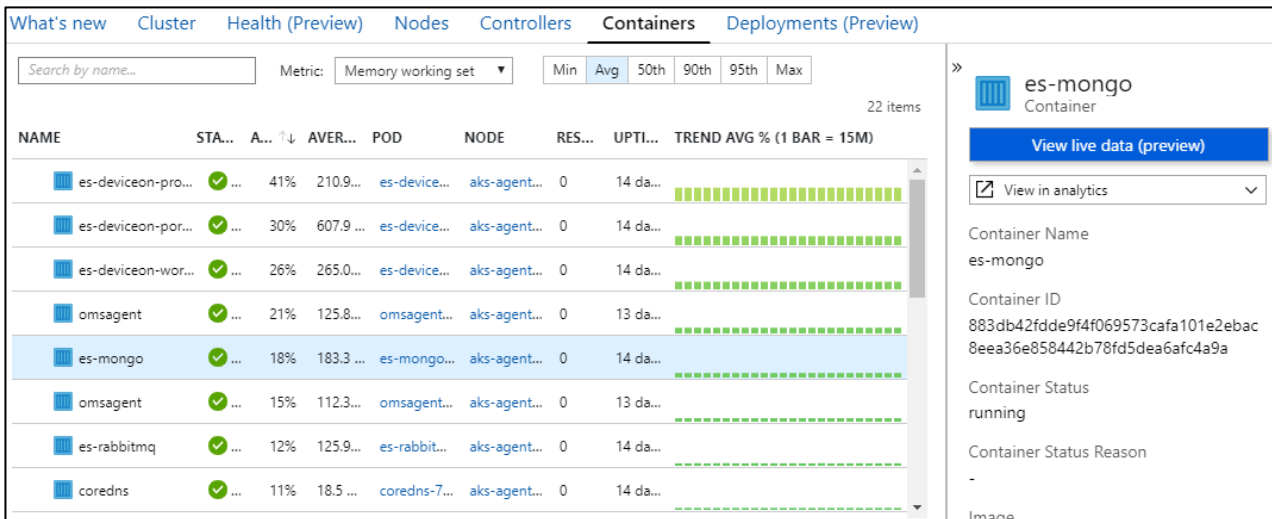
Metric: Memory working set

Min Avg 50th 90th 95th Max

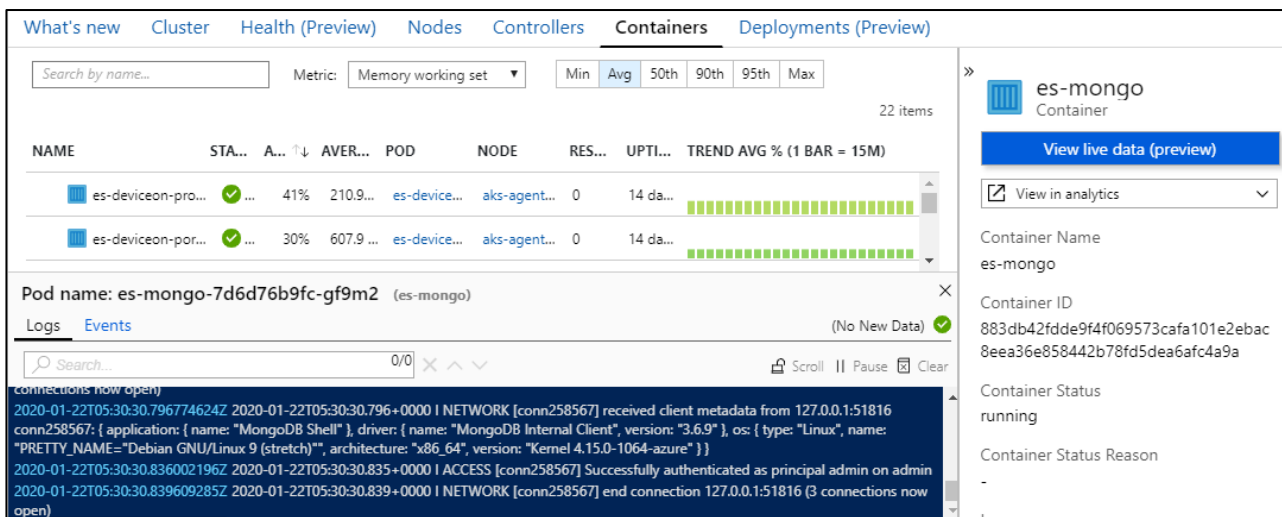
22 items

NAME	STA...	A... ↑↓	AVER...	POD	NODE	RES...	UPTI...	TREND	AVG % (1 BAR = 15M)
 es-deviceon-pro...		...	41%	210.9...	es-device...	aks-agent...	0	14 da...	<div><div></div></div>
 es-deviceon-por...		...	30%	607.8...	es-device...	aks-agent...	0	14 da...	<div><div></div></div>
 es-deviceon-wor...		...	26%	265.0...	es-device...	aks-agent...	0	14 da...	<div><div></div></div>
 omsagent		...	21%	125.7...	omsagent...	aks-agent...	0	13 da...	<div><div></div></div>
 es-mongo		...	18%	183.2...	es-mongo...	aks-agent...	0	14 da...	<div><div></div></div>
 omsagent		...	15%	112.2...	omsagent...	aks-agent...	0	13 da...	<div><div></div></div>
 es-rabbitmq		...	12%	125.6...	es-rabbit...	aks-agent...	0	14 da...	<div><div></div></div>
 coredns		...	11%	18.51 ...	coredns-7...	aks-agent...	0	14 da...	<div><div></div></div>

Step 3: View the container log by clicking on container name. Take es-mongo for example.



Step 4: Click on “View live data” to view live log of container.



● Monitor Usage of Persistent Volume (PV)

Step 1: Open PowerShell and login

Follow the instruction to login your account

```
# az login
```

Select your subscription, if you have multiple subscription, you have to set which subscription AKS service is located.

```
# az account set --subscription "SUBSCRIPTION_NAME"
```

Try to install AKS command line.

```
# az aks install-cli
```

To get AKS credential to access.

```
# az aks get-credentials --resource-group RESOURCE_GROUP --name K8S_CLUSTER
```

Step 2: Use kubectl command to get k8s information

```
# kubectl get pod --all-namespaces (check all pods)
```

```
PS Azure:\> kubectl get pod --all-namespaces
```

NAMESPACE	NAME	READY	STATUS	RESTARTS	AGE
default	es-deviceon-portal-6d6574b65-tp744	1/1	Running	0	13d
default	es-deviceon-provisioning-fc74b9cd7-cnwl	1/1	Running	0	13d
default	es-deviceon-worker-5f88997ccb-292pl	1/1	Running	0	13d
default	es-mongo-7d6d76b9fc-gf9m2	1/1	Running	0	13d
default	es-rabbitmq-7cb946db6c-5sqk5	1/1	Running	0	13d
default	rmm-iothub-bridge-6cf98f5f4-cvqf4	1/1	Running	13	13d
kube-system	coredns-7fc597cc45-ht4jc	1/1	Running	0	13d
kube-system	coredns-7fc597cc45-r98l4	1/1	Running	0	13d
kube-system	coredns-autoscaler-7ccc76bfbd-bjwpc	1/1	Running	0	13d
kube-system	kube-proxy-zsfmx	1/1	Running	0	7d9h
kube-system	kubernetes-dashboard-6fbc7f598b-klcbg	1/1	Running	5	13d
kube-system	metrics-server-58b6fcfd54-8jpn8	1/1	Running	0	13d
kube-system	omsagent-nwrnl	1/1	Running	0	12d
kube-system	tiller-deploy-59b99695d8-2x4pf	1/1	Running	0	13d

Try to shows all PVs in the cluster, it also includes which PVCs (Persistent Volume Claim) are requesting for the resources.

```
# kubectl get pv --all-namespaces (check PV)
```

```
PS Azure:\> kubectl get pv --all-namespaces
```

NAME	STORAGECLASS	REASON	AGE	CAPACITY	ACCESS MODES	RECLAIM POLICY	STATUS	CLAIM
pvc-e967a374-3115-11ea-a6bc-6201b0e63488	managed-premium		13d	500Gi	RWO	Delete	Bound	default/es-mongo
pvc-e9eb4084-3115-11ea-a6bc-6201b0e63488	managed-premium		13d	8Gi	RWO	Delete	Bound	default/es-postg
pvc-ea66f281-3115-11ea-a6bc-6201b0e63488	managed-premium		13d	32Gi	RWO	Delete	Bound	default/es-rabbi

Take es-mongo as example, the capacity of es-mongo PV is 500Gi, and default/es-mongo is requesting it as PVC. If you'd like to know the PV usage, you need to access es-mongo container.

```
# kubectl exec -it es-mongo-7d6d76b9fc-gf9m2 -- /bin/bash
```

Please replace the **pod** name to yours. To display disk available space on the file system, you could enter:

```
# df -h
```

```

root@es-mongo-7d6d76b9fc-gf9m2:/# df -h
Filesystem      Size  Used Avail Use% Mounted on
overlay         97G   19G   79G   20% /
tmpfs           64M    0    64M    0% /dev
tmpfs           7.9G    0   7.9G    0% /sys/fs/cgroup
/dev/sdc        493G  448M  492G    1% /data/db
/dev/sda1       97G   19G   79G   20% /etc/mongo
shm             64M    0    64M    0% /dev/shm
tmpfs           7.9G   12K   7.9G    1% /run/secrets/kubernetes.io/serviceaccount
tmpfs           7.9G    0   7.9G    0% /proc/acpi
tmpfs           7.9G    0   7.9G    0% /proc/scsi
tmpfs           7.9G    0   7.9G    0% /sys/firmware

```

4.6.4 Steps to Expose Database/RabbitMQ to Access

Step 1: Download [Database/RabbitMQ](#) yaml files.

Step 2: Open PowerShell and login

Follow the instruction to login your account

```
# az login
```

Select your subscription, if you have multiple subscription, you have to set which subscription AKS service is located.

```
# az account set --subscription "SUBSCRIPTION_NAME"
```

Try to install AKS command line.

```
# az aks install-cli
```

To get AKS credential to access.

```
# az aks get-credentials --resource-group RESOURCE_GROUP --name K8S_CLUSTER
```

Step 3: Expose MongoDB/PostgreSQL/RabbitMQ

```
# kubectl create -f service-mongodb.yaml
```

```
# kubectl create -f service-postgres.yaml
```

```
# kubectl create -f service-rmq.yaml
```

Step 4: Use Kubernetes Dashboard to check service public address

```
# az aks browse --resource-group RESOURCE_GROUP --name K8S_CLUSTER
```

✓ es-rabbitmq-worldwide	app: rabbitmq heritage: Tiller release: es-rabbitmq	10.0.230.154	es-rabbitmq-worldwide:5672 TCP es-rabbitmq-worldwide:30050 TCP es-rabbitmq-worldwide:5671 TCP es-rabbitmq-worldwide:30051 TCP es-rabbitmq-worldwide:15672 TCP es-rabbitmq-worldwide:30052 TCP es-rabbitmq-worldwide:1883 TCP es-rabbitmq-worldwide:30053 TCP es-rabbitmq-worldwide:8883 TCP es-rabbitmq-worldwide:30054 TCP		3 分	...
✓ es-postgres-worldwide	app: postgres heritage: Tiller release: es-postgres	10.0.38.44	es-postgres-worldwide:5432 TCP es-postgres-worldwide:30066 TCP		3 分	...
✓ es-mongo-worldwide	app: mongo heritage: Tiller release: es-mongo	10.0.44.25	es-mongo-worldwide:27017 TCP es-mongo-worldwide:30063 TCP		3 分	...

Port for DeviceOn Server Used

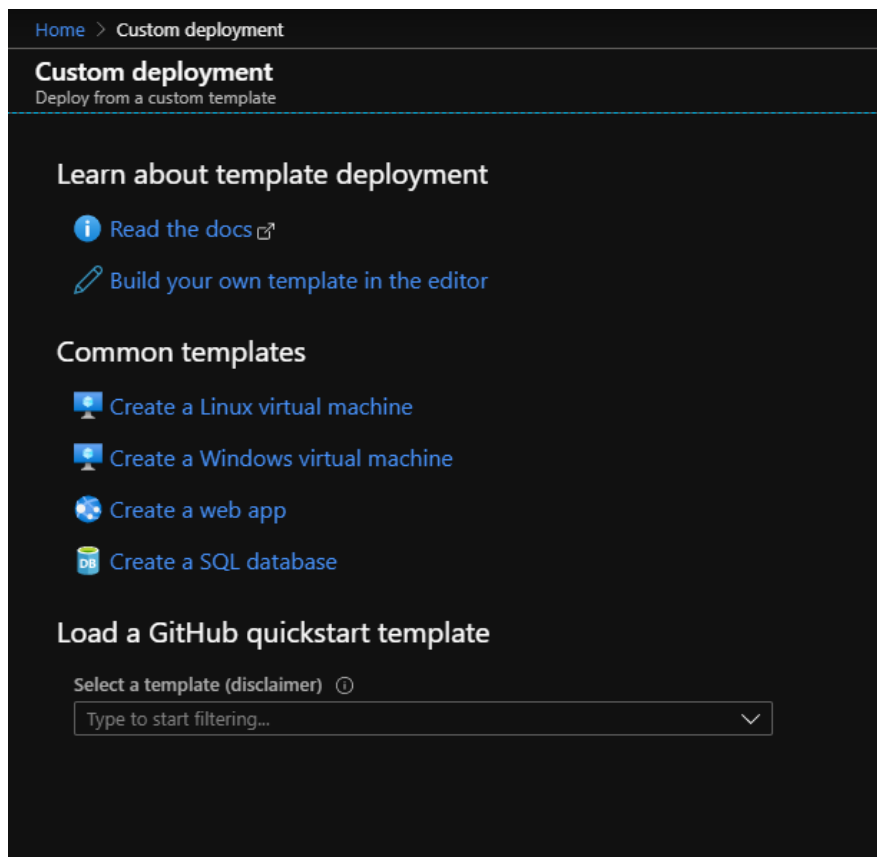
Name & Description		Inbound Port
1	Message Broker (RabbitMQ) MQTT, MQTTs	1883, 8883
2	Message Broker (RabbitMQ) AMQP, AMQPs	5671, 5672
3	Message Broker (RabbitMQ) Management Console	15672
4	Database for MongoDB	27017
5	Database for PostgreSQL	5432

4.6.5 Steps to Deploy DeviceOn to AKS by Manual

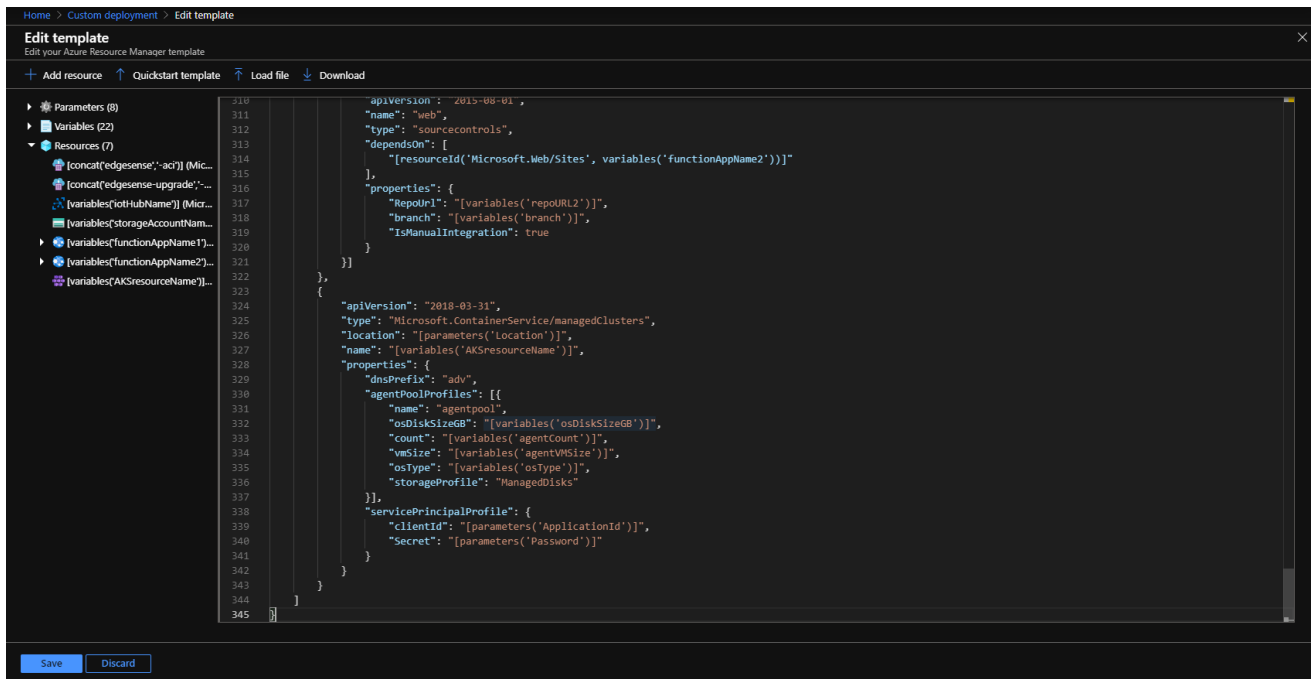
Step 1: Download [ARM template](#) and use notepad to open the file.

Step 2: Copy all content from the template

Step 3: Login [Azure Portal](#) to start custom deployment



Step 4: Select **Build your own template in the editor** and paste the content from Step 2, then click save button.



Step 5: Please enter these parameters to start deploy, the **Application Id**, **Password (Client Secrets)**, **Tenant Id**, please refer to Section 2.1.2.

Home > Custom deployment

Custom deployment

Deploy from a custom template

TEMPLATE

Customized template

7 resources

Edit template

Edit paramet...

Learn more

BASICS

Subscription *

[EA87] Demo Test

Resource group *

Select a resource group

Create new

Location *

(Asia Pacific) Japan East

SETTINGS

Application Id * ⓘ

Password * ⓘ

Tenant Id * ⓘ

Email * ⓘ

Location * ⓘ

Io T Hub Sku * ⓘ

Io T Hub Unit * ⓘ

Activate Key * ⓘ

TERMS AND CONDITIONS

Azure Marketplace Terms | Azure Marketplace

Purchase

- Email: The email address to get deployment status.
- Location: Please refer below table

Data Center	Location name
Asia East	eastasia
Asia Southeast	southeastasia
Japan East	japaneast
US East	eastus
Europe North	northeurope

- IoT Hub SKU: S1/S2/S3, default is S1
- IoT Hub Unit: 1 to 10, default is 1
- Activate key: Enter **N/A** to skip activate DeviceOn server automatically or please [contact us](#) to purchase license key.

Step 6: Pick-up agreement item and click **Purchase** button to start deployment process.

TERMS AND CONDITIONS

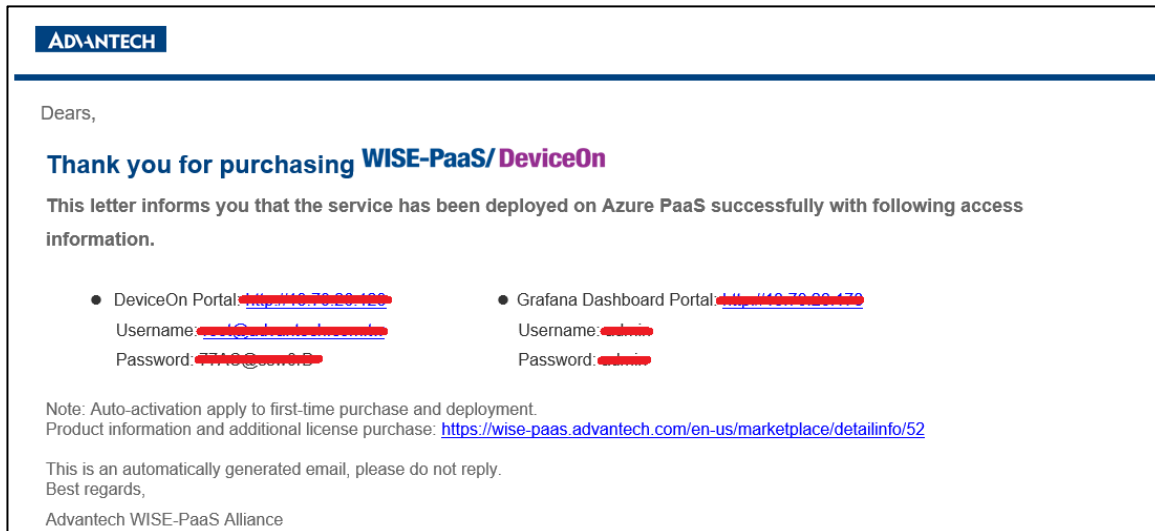
[Azure Marketplace Terms](#) | [Azure Marketplace](#)

By clicking "Purchase," I (a) agree to the applicable legal terms associated with the offering; (b) authorize Microsoft to charge or bill my current payment method for the fees associated the offering(s), including applicable taxes, with the same billing frequency as my Azure subscription, until I discontinue use of the offering(s); and (c) agree that, if the deployment involves 3rd party offerings, Microsoft may share my contact information and other details of such deployment with the publisher of that offering.

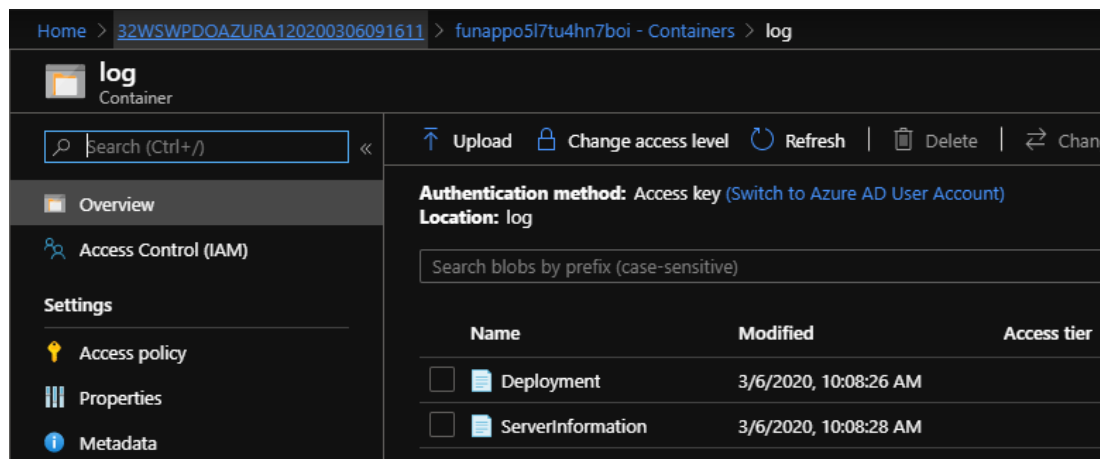
☒ I agree to the terms and conditions stated above

Purchase

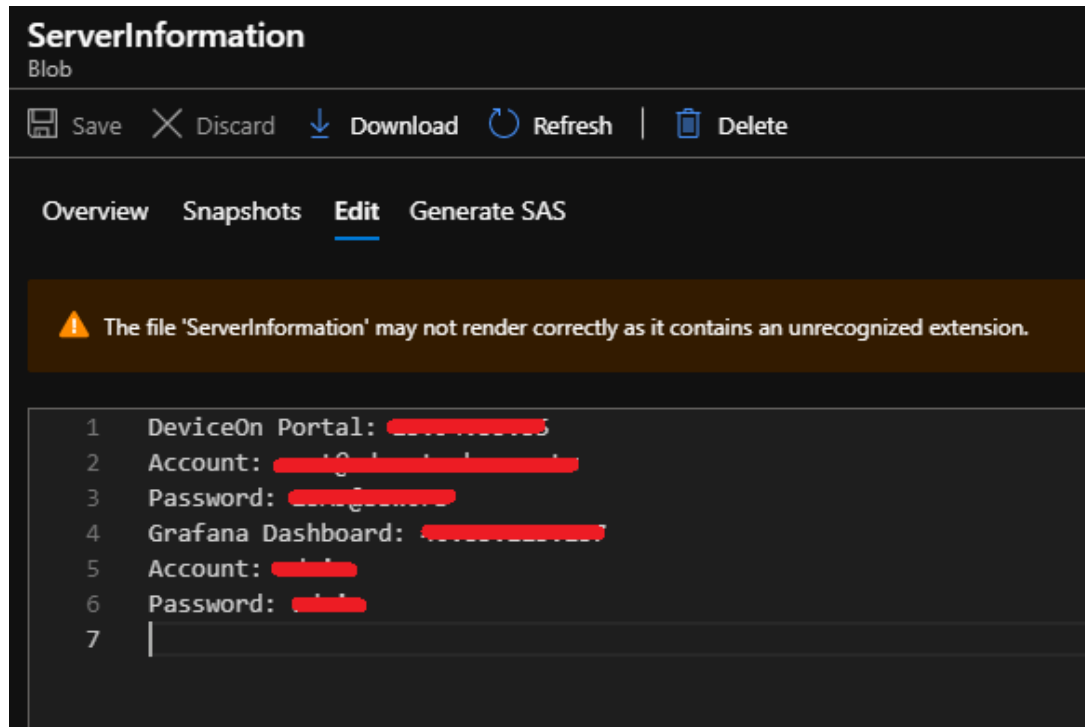
Step 7: After deployment, you will receive a mail to get server information, including account, password and URL.



To prevent your mail blocked, we write the server information in Azure blob simultaneously.



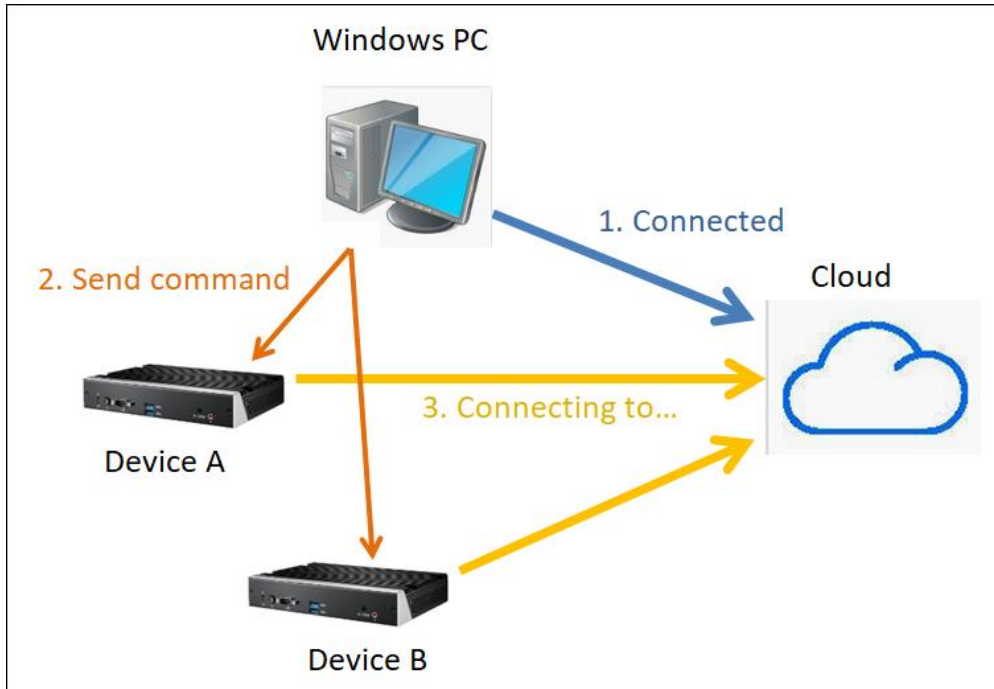
The credential and access information also on the “ServerInformation”.



4.7 How to Batch Provision to Your Devices

WISE-Agent will connect to DeviceOn server through **Credential URL** and **IoT Key** and those setting in **agent_config.xml**, if you have many devices (that has WISE-Agent in it) need to connect to the server, it takes time to modify agent_config.xml in each device. Here, we build-in the “**Local Provision**” Plugin to speed up this process. You will learn how to trigger all local devices to connect to the server with the same Credential URL and IoT Key.

The WISE-Agent local provision plugin will send Credential URL and IoT key to other local agent devices, and the local agent devices can connect to the server successfully. In following figure, you can send trigger command to make device A and B connect to a server with a Windows GUI tool.



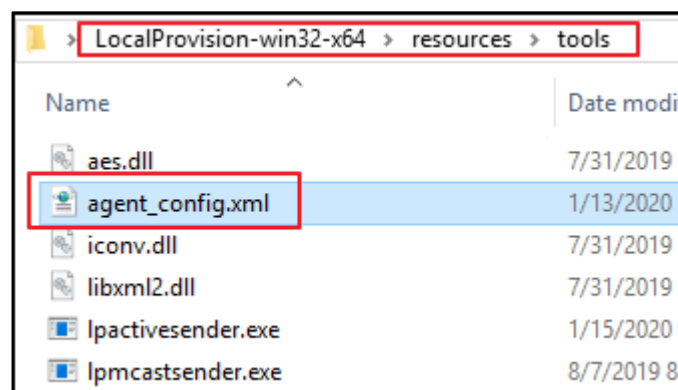
4.7.1 Prerequisite

- All devices must install WISE-Agent in it.
- All devices and the control PC must in the same local network (The multicast packet will not be filtered)
- All devices have the capability to connect to DeviceOn server.

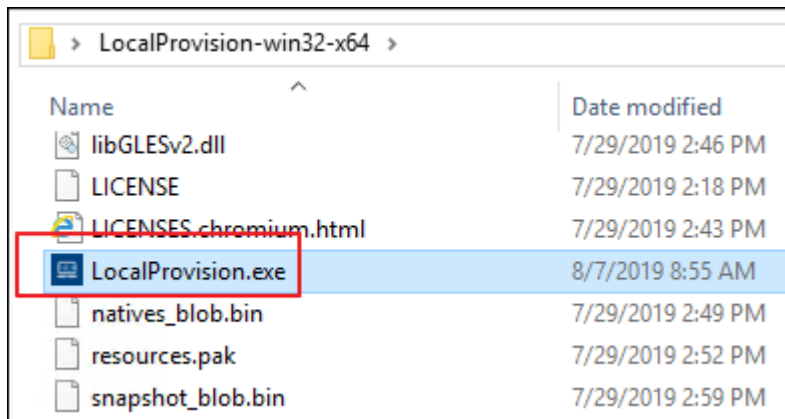
4.7.2 Steps to Local Provisioning

Step 1: Download and unzip the [local provision GUI tool](#).

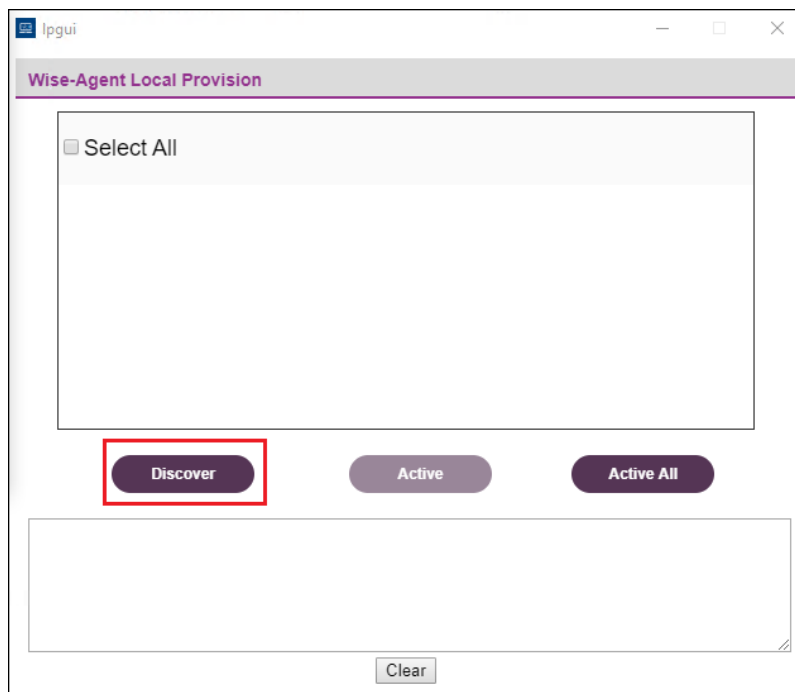
Step 2: Place valid “**agnet_config.xml**” file (with correct Credential URL and IoT Key) to “**GUI tool\resources\tools**” folder



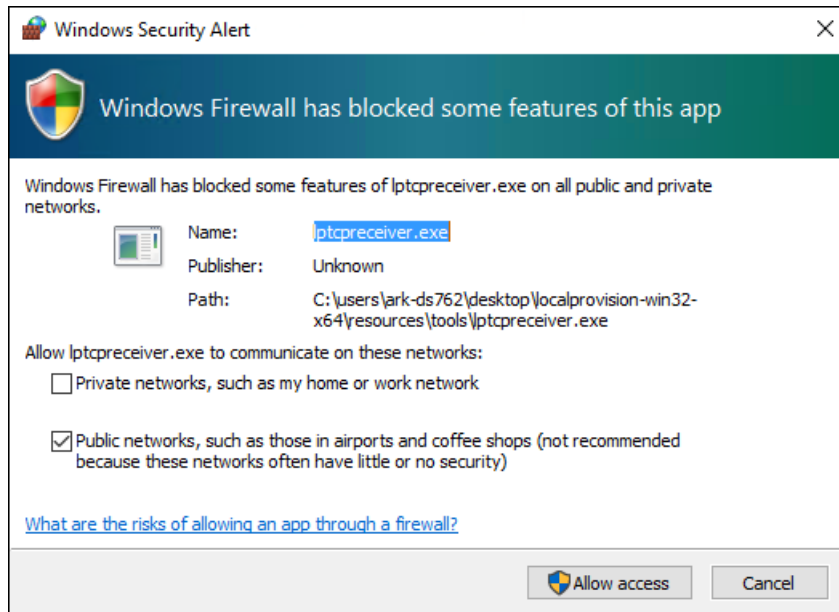
Step 3: Double click “LocalProvision.exe”



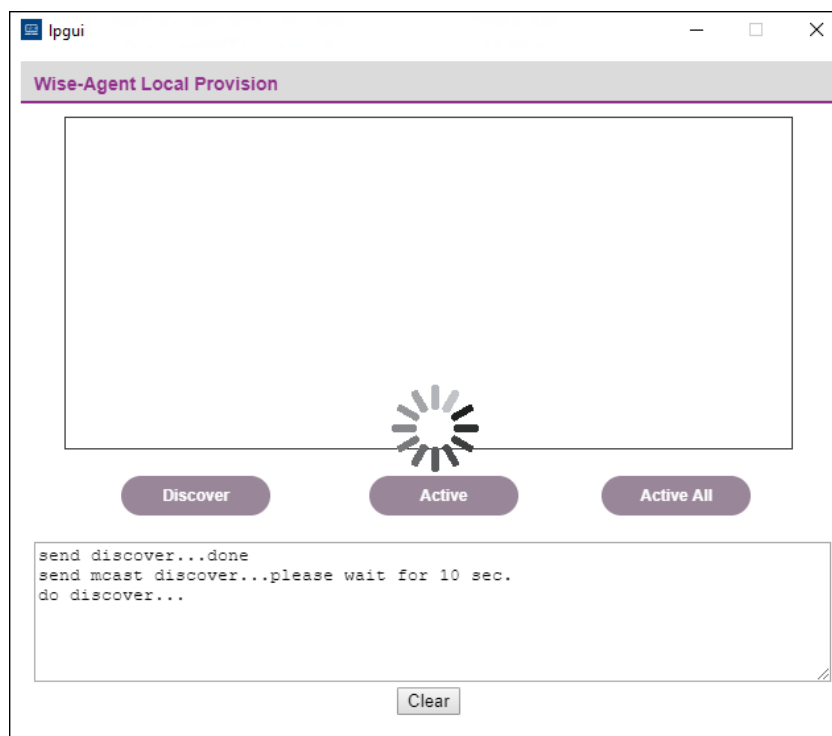
Step 4: Click **Discover** button

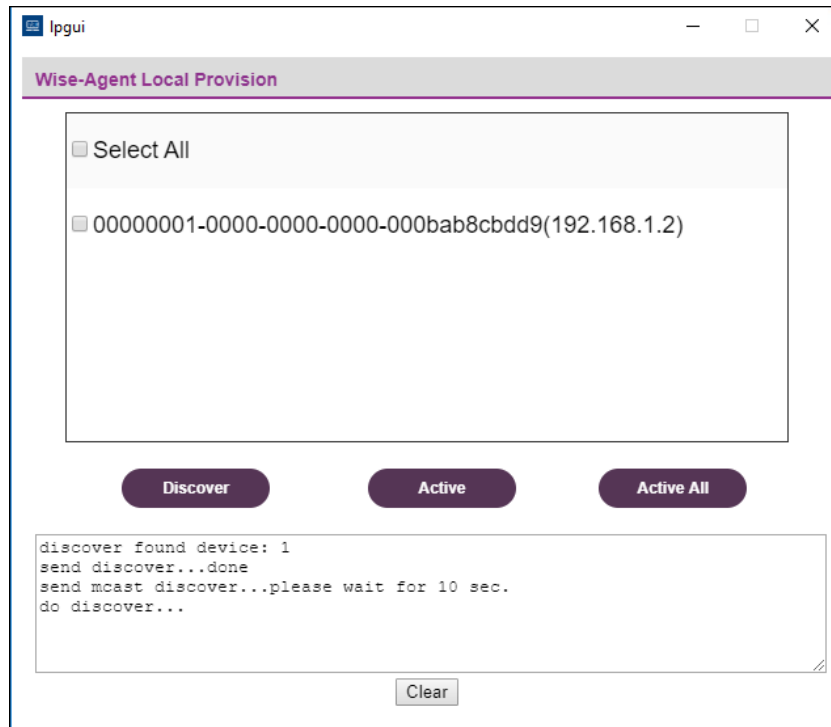


If windows display a firewall dialog, please click allow to enable TCP server permission in tool.

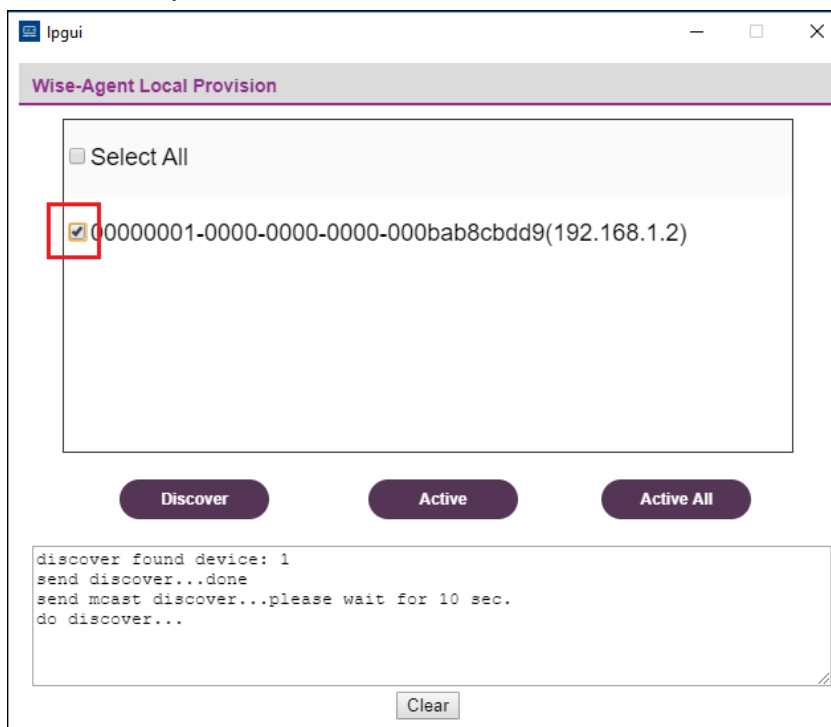


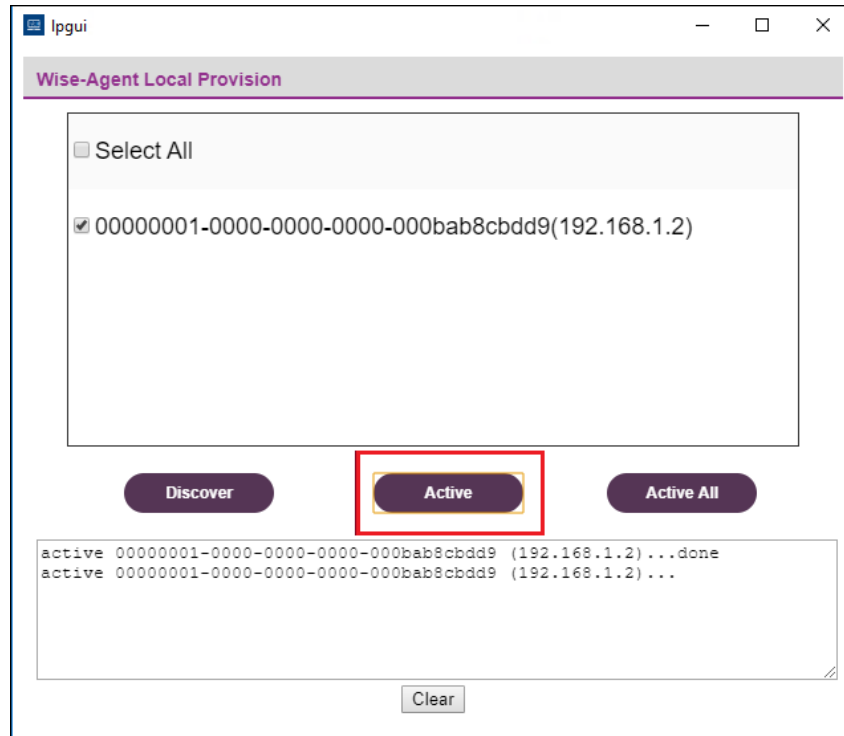
Step 5: Wait for 10 second and then you can get the devices on checkbox list.





Step 6: Pick-up the device that you would like to connect to the server and click **Active**.





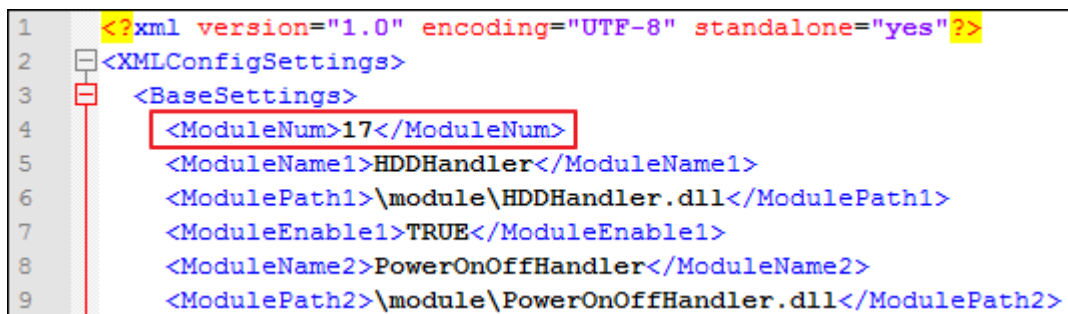
Until now, the checked devices should connect to server after few second later.

4.7.1 Troubleshooting

Why can't I find some WISE-Agent devices? Please help check following:

A. Please check if your local provision plugin is enabled.

Open the **module_config.xml** in "Installation path\module\" to check if local provision handler is enabled.



```

50      <ModuleName16>EmbIPC</ModuleName16>
51      <ModulePath16>\module\EmbIPC.dll</ModulePath16>
52      <ModuleEnable16>TRUE</ModuleEnable16>
53      <ModuleName17>HDDPMQ</ModuleName17>
54      <ModulePath17>\module\HDDPMQ.dll</ModulePath17>
55      <ModuleEnable17>TRUE</ModuleEnable17>
56      <ModuleName18>LocalProvision</ModuleName18>
57      <ModulePath18>\module\LocalProvisionHandler.dll</ModulePath18>
58      <ModuleEnable18>TRUE</ModuleEnable18>
59  </BaseSettings>
60 </XMLConfigSettings>

```

- B. Please check if your device and windows PC is in the same local network and can transfer multicast packets.
- C. Because the local provision discovers wise-device by UDP port **9178** and TCP port **9177**, please check if your IT block these ports in your local network.

5. DeviceOn Development Guide

5.1 WISE-Agent Plugin Development

Advantech provides an edge software tool to communicate and exchange information between IoT (Internet of Thing) devices and DeviceOn cloud, called a WISE-Agent. The WISE-Agent not only provides a rich set of users friendly, intelligent, standardization and scalability.

- **Standardization**

The communication protocol is based on the MQTT protocol to communicate and exchange data with DeviceOn cloud. The IoT sensor data report format is following the IPSO Alliance. in JSON format.

- **Portability**

The whole framework is written in C language and follow the ANSI C Standard, that C compilers are available for most systems and are often the first compiler provided for a new system, such as OpenWRT, Yacto and Linux based system.

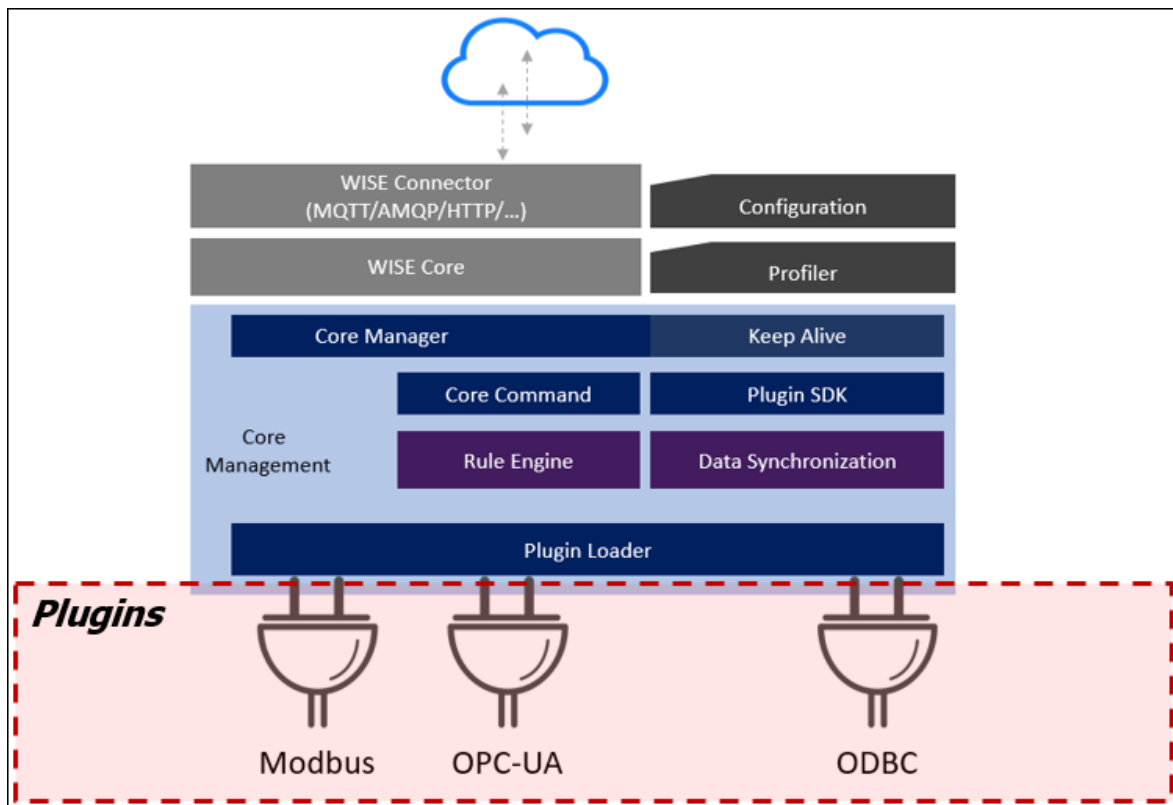
- **Scalability**

The WISE-Agent is modular design and offering plugin concept to Plug & Play (PnP) which is one with a specification that facilitates the discovery of a Plugin in a system without the need for a physical device to advanced configuration or user intervention in resolving resource conflicts.

Besides the basic device connectivity, the WISE-Agent provides an advanced heartbeat solution to synchronize device status. On the different network environment, how to keep your device data without loss? The WISE-Agent has built-in “**Data Synchronization**” to avoid and overcome the disconnect for a long time. For various protocols, we offer a plugin SDK, users only focus on how to retrieve the data, do not worry about the connectivity and stability.

5.1.1 WISE-Agent Architecture

WISE-Agent includes two parts, one is the **Core Framework** and **Plugins**.



- **Core Framework**

The main library used to communicate with WISE-PaaS IoT Hub or standard MQTT broker and include below components.

- ✧ **Platform Profiler:** describes the target platform (e.g., OS version, SN, Device name, MAC address)
- ✧ **Configuration:** describes how to connect to MQTT broker (e.g., Credential URL, IoTKey, TLS/SSL settings)
- ✧ **Core Manager:** integrates and manages the resources and keeps them alive.
- ✧ **Core Command:** responsible for handling commands that interact with internal components (e.g., rename, update, get capability, auto report start/stop)
- ✧ **Plugin SDK:** A plugin framework that makes plugin implement more easily.

- ✧ **Keep Alive:** A component to detect the connection between WISE-Agent and DeviceOn Server.
- ✧ **Data Synchronization:** kernel plugin that caches and restores data to ensure zero downtime.
- ✧ **Rule Engine:** kernel plugin that supports the threshold rule check and then sends event or trigger actions
- ✧ **Plugin Loader:** responsible for loading and managing plugins indicated in module_config.xml

● The plugins

The plugins include IPC monitoring (Advantech Hardware, HDD/SSD, Networks, Process...etc.), control function (Backup/Recovery, Protection, Remote Desktop, Terminal...), and sensor protocol collection. Following are the list of supported plugins in WISE-Agent.

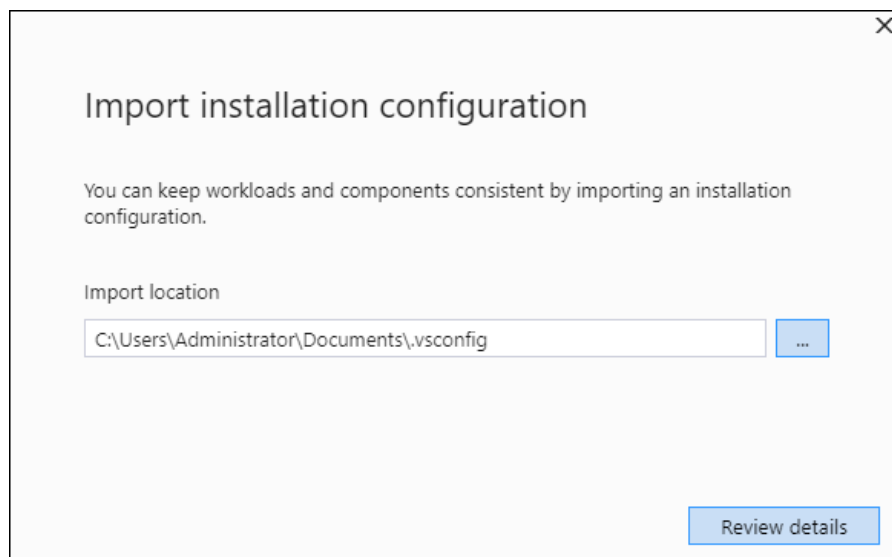
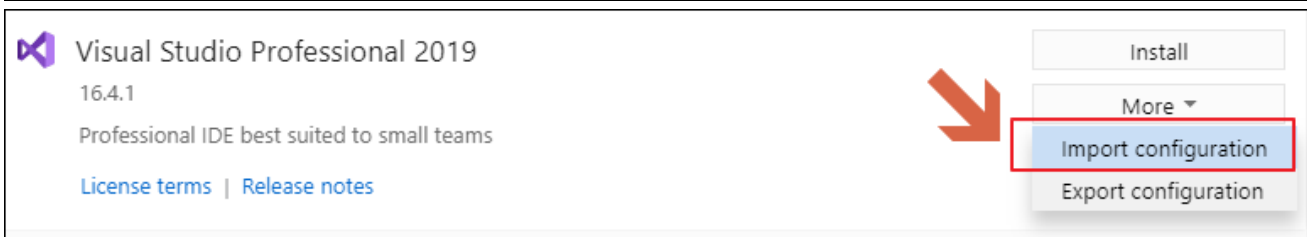
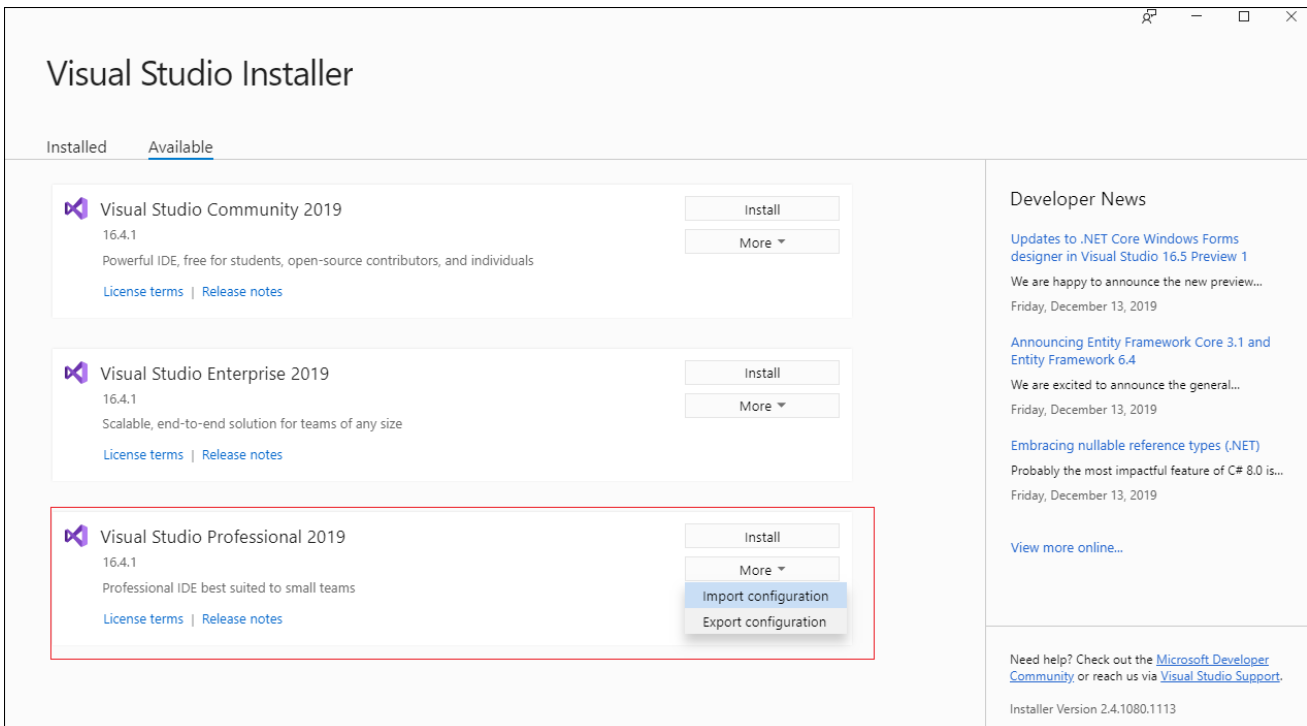
- ✧ **SUSI Control:** Monitoring and Control Advantech Hardware Platform
- ✧ **HDD Monitoring:** Monitoring Hard Drives (HDD, SSD) Usage, Healthy and S.M.A.R.T Information, especially for Advantech SQFlash.
- ✧ **Network Monitoring:** Monitoring Network Interface Usage, Throughput...
- ✧ **Process Monitoring:** Monitoring System Process Status, CPU, Memory Usage.
- ✧ **Power Management:** Remote Control Power On, Off, Reboot, Sleep, Hibernate.
- ✧ **Backup/Recovery:** Remote Backup/Recovery System via Acronis
- ✧ **Protection:** Remote System Protection via McAfee
- ✧ **Remote Desktop:** Remote Desktop via VNC Viewer
- ✧ **Remote Terminal:** Remote Terminal Command
- ✧ **Remote Screenshot:** Remote Screenshot on Current Screen
- ✧ **OTA (Over-the-Air):** Remote Software, Firmware Update
- ✧ **System Program Monitoring:** System Program Information
- ✧ **Embedded Control:** Advanced Control (UWF, USB Lock, Keyboard Filter, ...etc.) for Windows 10 Embedded, LTSC, LTSB
- ✧ **HDD Prediction:** Build-in Hard Drives (HDD, SSD) Failure Prediction Model
- ✧ **Modbus:** Modbus Device Data Gathering
- ✧ **Service Plugin:** Bridge Southbound Device Service

5.1.2 Prerequisite

- Visual Studio 2019.
- A WISE-Agent that is running on your system.

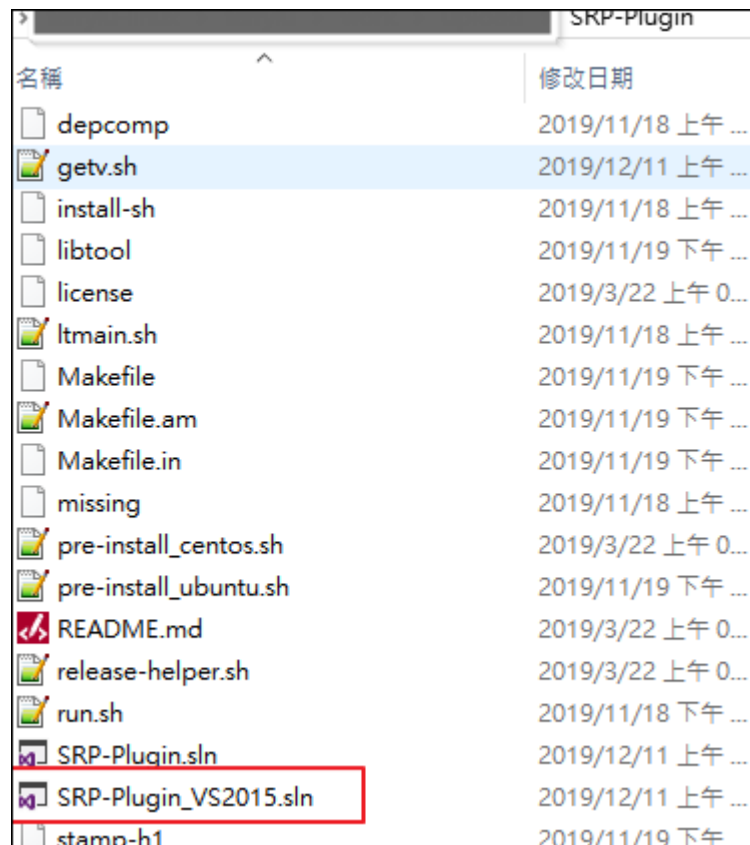
5.1.3 Develop a Plugin on Windows Environment

Step 1: You can configure Visual Studio across your organization with installation configuration files, [.vsconfig](#)

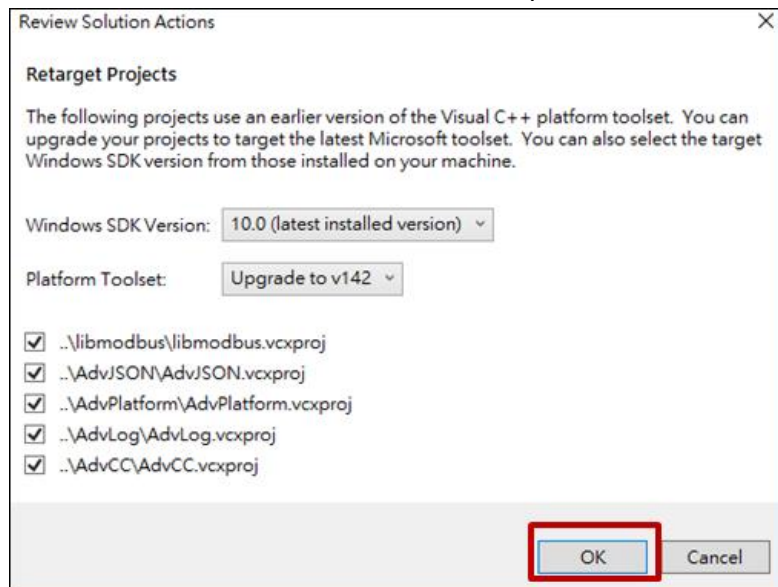


Step 2: Download SRP-Plugin,
git clone <http://advgitlab.eastasia.cloudapp.azure.com/SRP-Connect/SRP-Plugin.git>

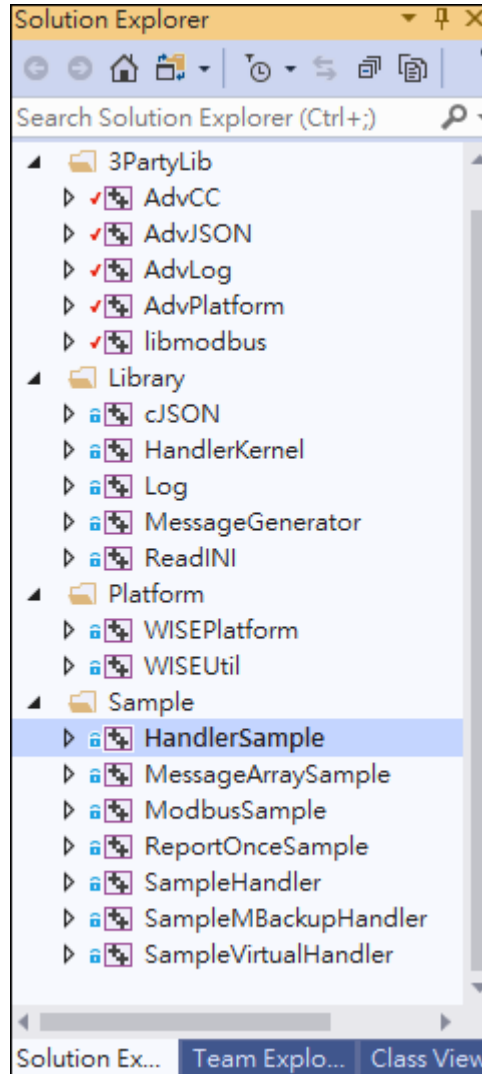
Step 3: Open SRP-Plugin solution file, **SRP-Plugin-V2015.sln**



Step 4: Click OK to update the SDK and Toolset for current compile environment







Step 5: You can implement new plugin base on plugin sample project.



Step 6: It is more easily to create a new plugin by Web-Simulator tools. Web-Simulator is an auxiliary tool that helps you quickly simulate data on the cloud via MQTT over WebSocket (network port: 15675) and directly generate the corresponding code. Following step will introduce how to create a new plugin by Web-Simulator tools. If you want to know exactly how this tool is used, you can refer Web-Simulator [QuickStart](#).

Step 7: Download [Web-Simulator](#) tools.

Step 8: The sample code can be generated in the fourth step. Please save it as **handler_data.c** and replace it in the “SRP-Plugin\Sample\HandlerSample” path.

Step 3 - Create Grafana board

Now you can open the [RMM Portal](#) to check the reltime value or go to the next step, automatically generate a grafana board for you.

Or you can reference the [Sample Handler](#) sample code , according to previous step.

Grafana url:

Name:

Password:

Previous
Next

Step 9: Right click the “**HandlerSampe**” project in Step 5 and choose “**Solution**”.

Step 10: Check output without error message. If appear error message, suggest to copy the error message search in google or ask Advantech technical people.

Step 11: After successfully completing the compilation, you can find all the **.dll** files in below path
“**SRP-Plugin\Debug\module**”

Step 12: Download and install [WISE-Agent](#) for Windows. The default installation path is
C:\Program Files (x86)\Advantech\WISE-Agent

Step 13: After install the WISE-Agent, copy “**HandlerSample.dll**” file to
“C:\Program Files (x86)\Advantech\WISE-Agent**module**” folder.

Step 14: Modify **module_config.xml** on
“C:\Program Files (x86)\Advantech\WISE-Agent\module**module_config.xml**”

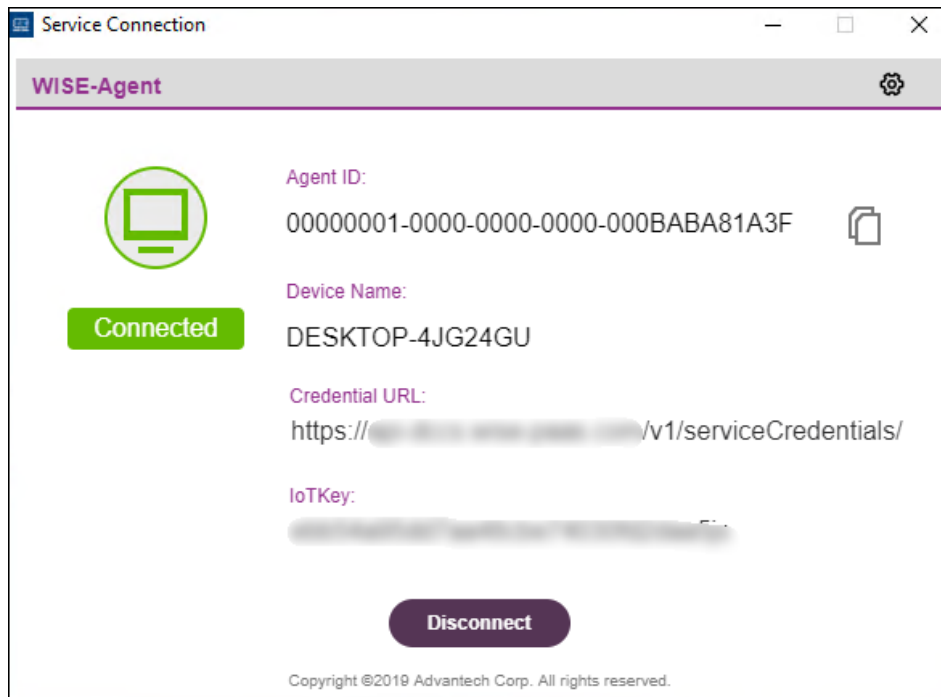
- Increase **ModuleNum** value in below line 3
- Add **HandlerSample.dll** item in below line 7.

```

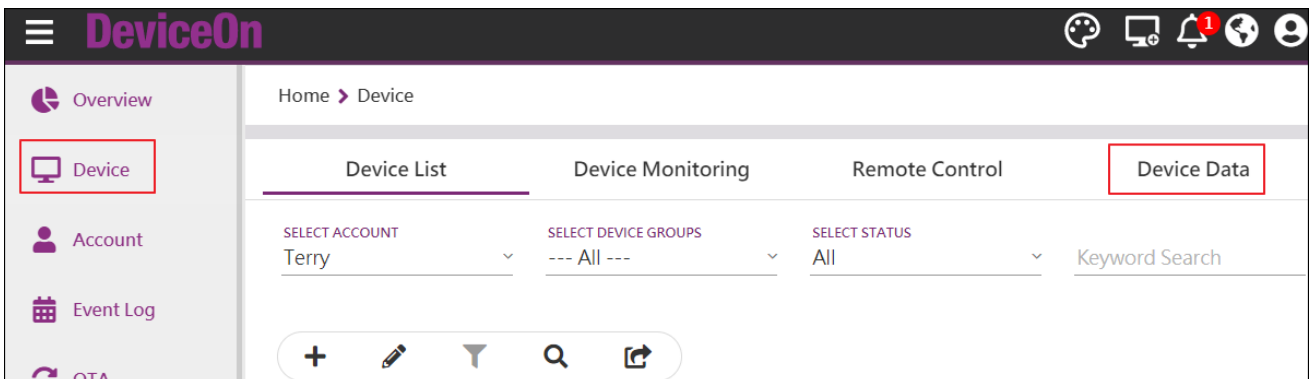
01. <?xml version="1.0"?>
02. <XMLConfigSettings><BaseSettings>
03. <ModuleNum>15</ModuleNum>
04. <ModuleName1>HDDHandler</ModuleName1><ModulePath1>module/HDDHandler.so</ModulePath1><ModuleEnable1>TRUE</ModuleEnable1>
05. ...
06. <ModuleName14>ServiceHandler</ModuleName14><ModulePath14>module/ServiceHandler.so</ModulePath14><ModuleEnable14>TRUE</ModuleEnable14>
07. <ModuleName15>HandlerSample</ModuleName15><ModulePath15>module/HandlerSample.so</ModulePath15><ModuleEnable15>TRUE</ModuleEnable15>
08. </BaseSettings>
09. </XMLConfigSettings>

```

Step 15: Reconnect WISE-Agent by “Server Connection” tools. Press “Disconnect” then “Connect”.



Step 16: Check if your plugin appears in DeviceOn Page, (Device -> Device Data -> PLUGIN)



RealTime Data

PLUGIN
usrPlugin

DATA TIME : 2019/12/17 16:49:51

SENSOR	DATA TYPE	READ/WRITE	UNIT	VALUE
/usrPlugin/PM2.5	Numeric			37.44721560340238
/usrPlugin/CO	Numeric			4.090449359957392

2 records

5.1.4 Develop a Plugin on Linux Environment

The following steps are handled in Ubuntu or Debian system. If your target device is Yocto Linux, you have to set up cross-compile environment on your host PC. The example below shows how to set up for NXP i.MX8 projects.

```
$ /opt/fsl-imx-xwayland/4.14-sumo
$ source environment-setup-aarch64-poky-linux
```

From now, the DeviceOn supports the following RISC platform, please refer to the SDK links relating to the platform you are developing for details.

Platform	OS	Architecture	SDK
NXP i.MX8	Yocto 2.5.2	aarch64	Link
NXP i.MX6	Yocto 2.1.1	armv7-a	Link
Qualcomm APQ8016	Yocto 2.1.3	aarch64	Link
TI AM335x	Yocto 2.4	armv7-a	Link
RK3288	Debian 9.8	arm	N/A
RK3399	Debian 9.9	aarch64	N/A

[http://ess-wiki.advantech.com.tw/view/AIMLinux/AddOn/DeviceOn#Supported Platforms](http://ess-wiki.advantech.com.tw/view/AIMLinux/AddOn/DeviceOn#Supported+Platforms)

Step 1: Download SRP-Plugin as Section 5.1.3 Step 2.

Step 2: In Plugin SDK (SRP-Plugin) folder, execute ‘`sudo ./pre-install_ubuntu.sh`’ with root user authority to install compile tools and dependency libraries

Note: If you are developing with cross-compile, you can skip this step.

```
test@ubuntu: ~/GitLab/SRP-Plugin
test@ubuntu:~/GitLab/SRP-Plugin$ sudo ./pre-install_ubuntu.sh
[sudo] password for test:
=====
Now will check whether the following packages installed:
 libxml2 libx11-6 libxext6 libxtst6 libmosquitto1 sqlite3 xterm ethtool gcc g++
 make libxml2-dev libx11-dev libxtst-dev libxext-dev libmosquitto-dev autoconf a
 utotools-dev build-essential libtool libcurl4-openssl-dev libssl-dev
=====
All the packages is installed!
test@ubuntu:~/GitLab/SRP-Plugin$
```

Step 3: You can implement new plugin base on plugin sample project or Web-Simulator in Section 5.1.3 Step 6 to Step 8.

Step 4: Copy `handler_data.c` that generated by Web-Simulator to
“SRP-Plugin/Sample/HandlerSample”.

Step 5: Build SRP-Plugin by “build-srpplugin.sh”

```
$ ./build-srpplugin.sh
```

Step 6: You can find the release build file in “SRP-Plugin/Release/module” folder.

```
test@ubuntu: ~/GitLab/SRP-Plugin/Release/module
test@ubuntu:~/GitLab/SRP-Plugin$ cd Release/
test@ubuntu:~/GitLab/SRP-Plugin/Release$ ls
libAdvCC.so          libAdvJSON.so.0.0.0  libmodbus.so.5
libAdvCC.so.0        libAdvLog.so         libmodbus.so.5.1.0
libAdvCC.so.0.0.0    libAdvLog.so.0       libWISEPlatform-1.1.1.so
libAdvCompression.so libAdvLog.so.0.0.0   libWISEPlatform.so
libAdvCompression.so.0 libLog.so            libWISEUtil-1.1.1.so
libAdvCompression.so.0.0.0 libLog.so.0         libWISEUtil.so
libAdvJSON.so        libLog.so.0.0.0      module
libAdvJSON.so.0      libmodbus.so
test@ubuntu:~/GitLab/SRP-Plugin/Release$ cd module/
test@ubuntu:~/GitLab/SRP-Plugin/Release/module$ ls
HandlerSample.so      MessageArrayHandler.so.0  ModbusSample.so.0.0.0
HandlerSample.so.0    MessageArrayHandler.so.0.0.0  module_config.xml
HandlerSample.so.0.0.0 ModbusSample.so
MessageArrayHandler.so ModbusSample.so.0
```

Step 7: Please download [WISE-Agent](#) for Ubuntu 16.04 x64. The default installation path is /usr/local/AgentService.

Step 8: After install the WISE-Agent, copy “HandlerSample.so.0.0.0” and “HandlerSample.so” files to “/usr/local/AgentService/module/” folder.

```
$ sudo cp -a Release/module/HandlerSample.so* /usr/local/AgentService/module/
```

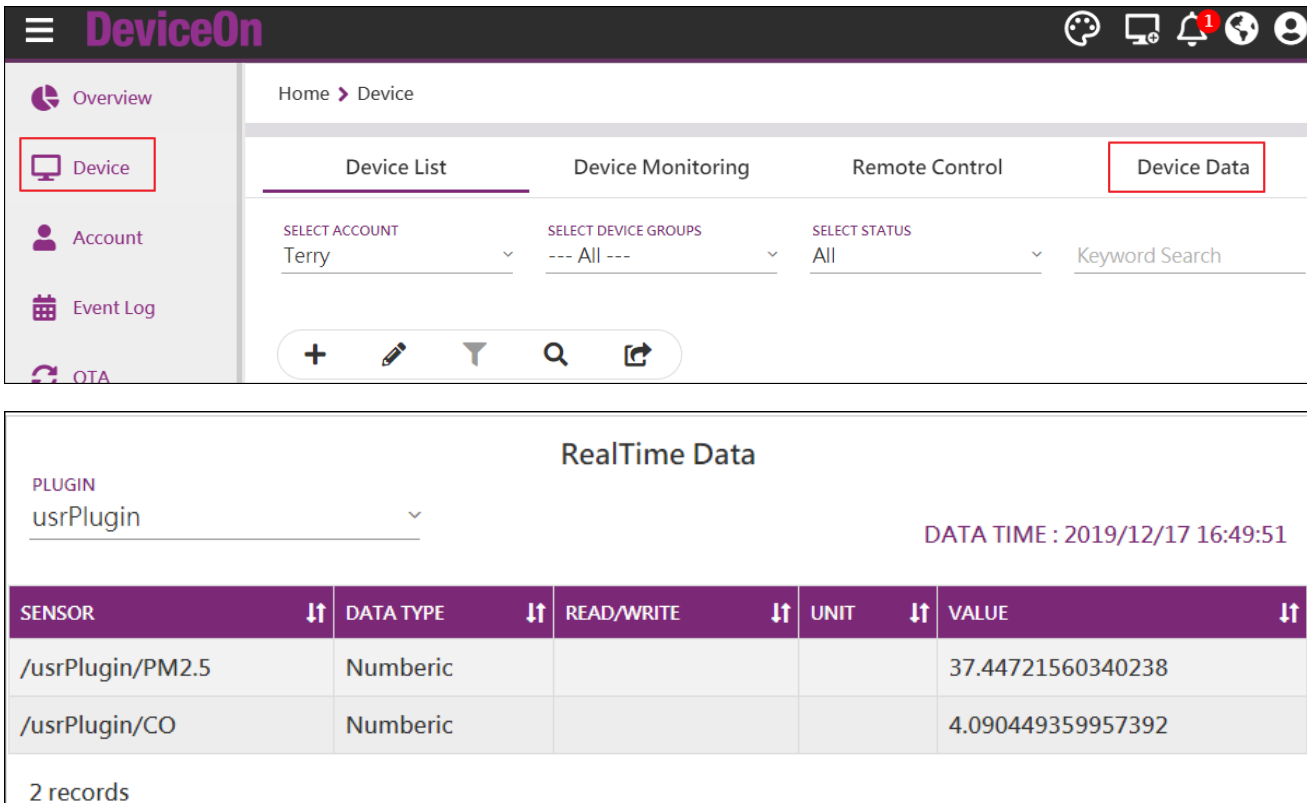
Step 9: Modify “/usr/local/AgentService/module/module_config.xml” Increase **ModuleNum** value in below line 3. Add HandlerSample.so item in below line 7.

```
01. <?xml version="1.0"?>
02. <XMLConfigSettings><BaseSettings>
03.   <ModuleNum>15</ModuleNum>
04.   <ModuleName1>HDDHandler</ModuleName1><ModulePath1>module/HDDHandler.so</ModulePath1><ModuleEnable1>TRUE</ModuleEnable1>
05.   ...
06.   <ModuleName14>ServiceHandler</ModuleName14><ModulePath14>module/ServiceHandler.so</ModulePath14><ModuleEnable14>TRUE</ModuleEnable14>
07.   <ModuleName15>HandlerSample</ModuleName15><ModulePath15>module/HandlerSample.so</ModulePath15><ModuleEnable15>TRUE</ModuleEnable15>
08. </BaseSettings>
09. </XMLConfigSettings>
```

Step 10: Restart WISE-Agent

```
$ sudo systemctl restart saagent
```

Step 11: Check if your plugin appears in DeviceOn Page, (Device -> Device Data -> PLUGIN)



The screenshot shows the DeviceOn web interface. The left sidebar contains navigation links: Overview, Device (highlighted with a red box), Account, Event Log, and OTA. The main content area is titled 'Home > Device'. It features four tabs: Device List, Device Monitoring, Remote Control, and Device Data (highlighted with a red box). Below the tabs are filters for 'SELECT ACCOUNT' (Terry), 'SELECT DEVICE GROUPS' (--- All ---), and 'SELECT STATUS' (All). A 'Keyword Search' field is also present. Below the filters is a toolbar with icons for adding, editing, filtering, searching, and sharing. The main data section is titled 'RealTime Data' and shows a dropdown for 'PLUGIN' set to 'usrPlugin'. The data time is '2019/12/17 16:49:51'. A table displays the real-time data for the selected plugin.

SENSOR	DATA TYPE	READ/WRITE	UNIT	VALUE
/usrPlugin/PM2.5	Numeric			37.44721560340238
/usrPlugin/CO	Numeric			4.090449359957392

2 records

5.2 DeviceOn UI Plugin Development

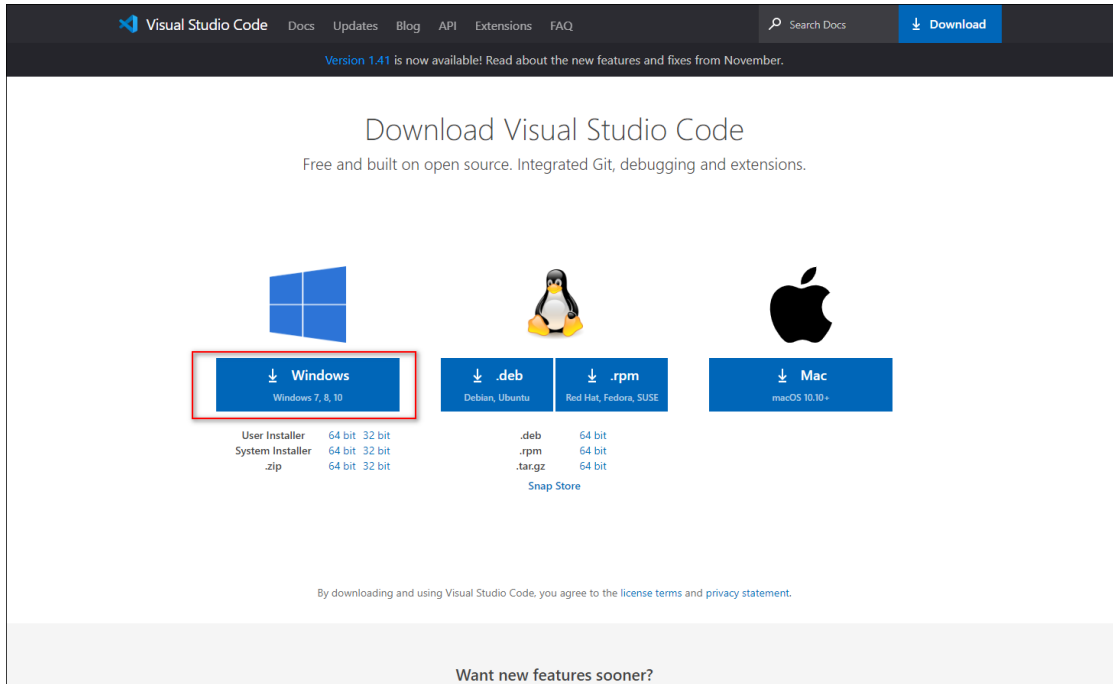
Actually, DeviceOn provide plenty of features to remote management, control to your edge devices, but it's hard to meet all domains application, such as, medical, traffic, energy system and etc. Fortunately, DeviceOn provide APIs and Addins (web user interface) for users to develop their own solution.

5.2.1 Prerequisite

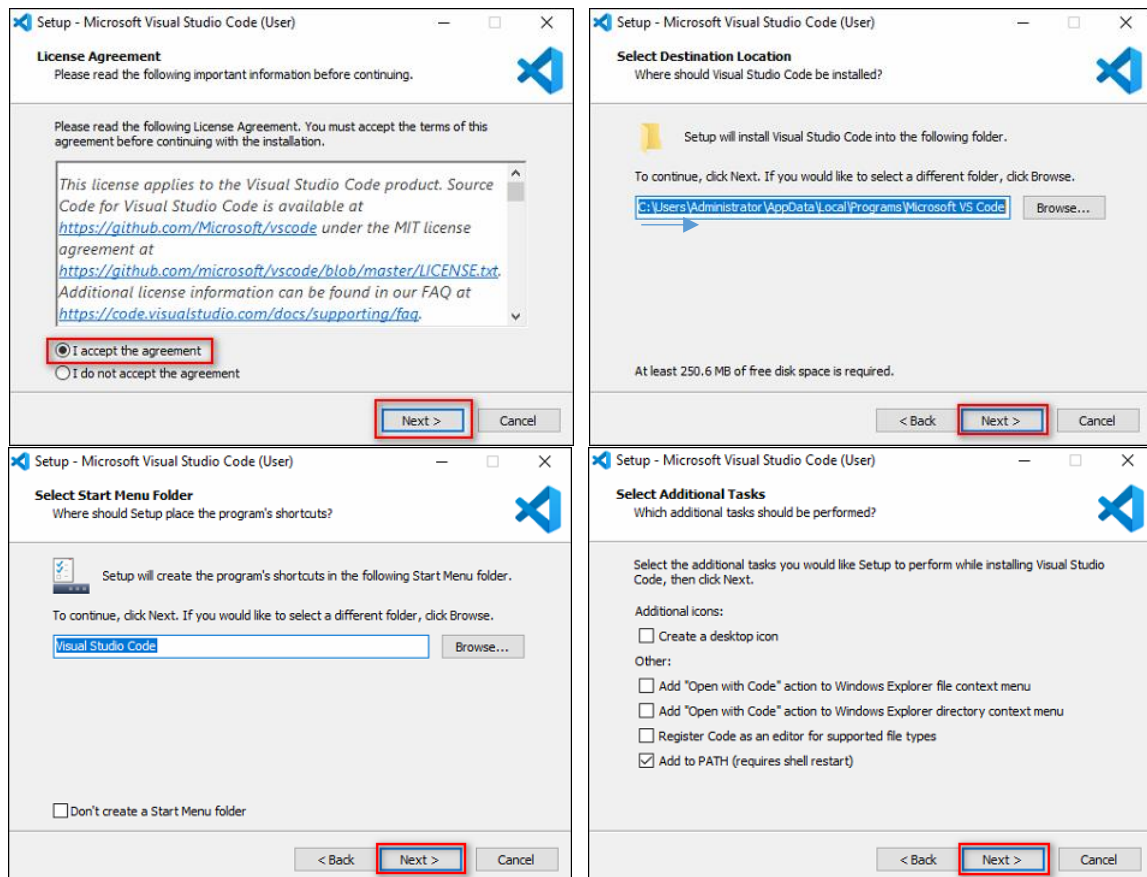
- Visual Studio Code V 1.4.1
- DeviceOn Server

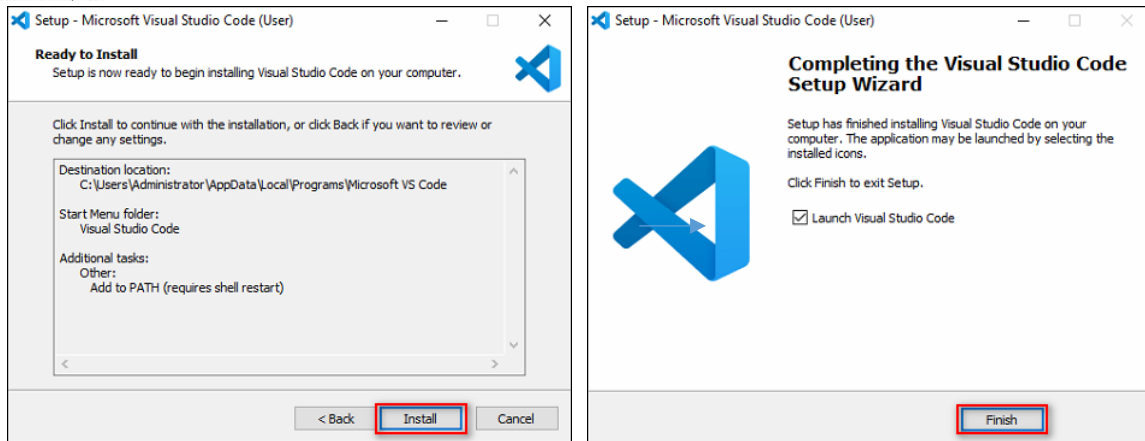
5.2.2 Environment Setup

Step 1: Download [Visual Studio Code v-1.4.1](#) and launch VSCodeUserSetup-x64-1.41.1.exe.



Step 2: Install Visual Studio Code, step by step.





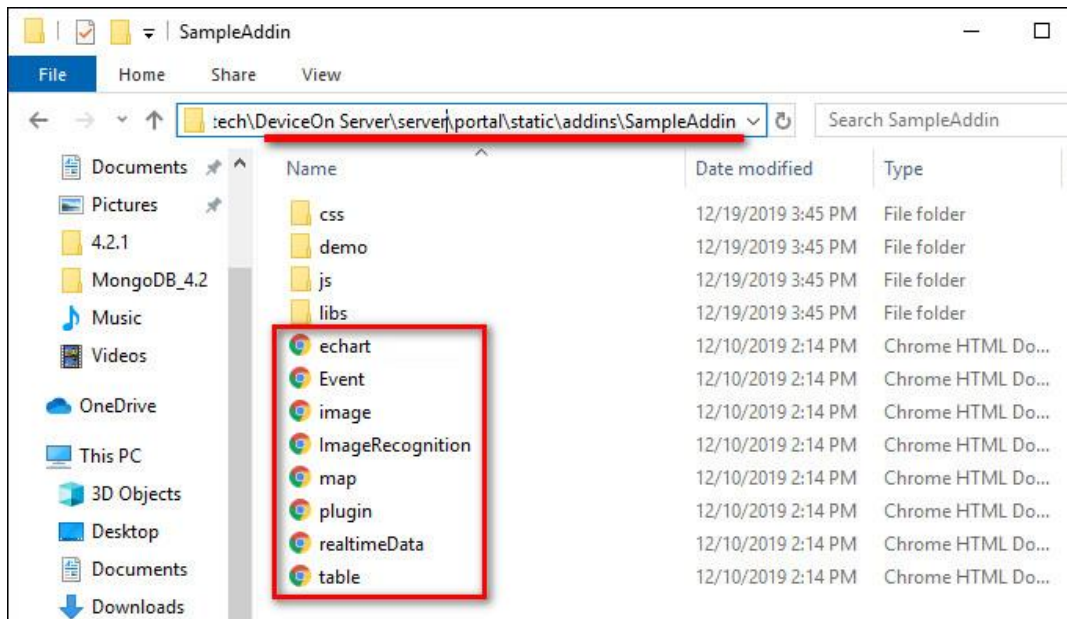
Step 3: Install DeviceOn Server, if you don't install DeviceOn Server before, please reference Section 2.2.

5.2.3 Develop a Sample Add-in

Step 1: Open DeviceOn Server folder and go to the installation path:

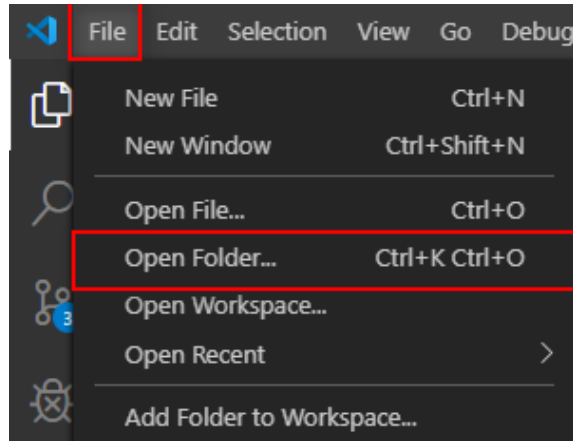
`\DeviceOn Server\server\portal\static\addins\SampleAddin.`

Here are several Add-in examples (*.html) that we provide, for your reference.

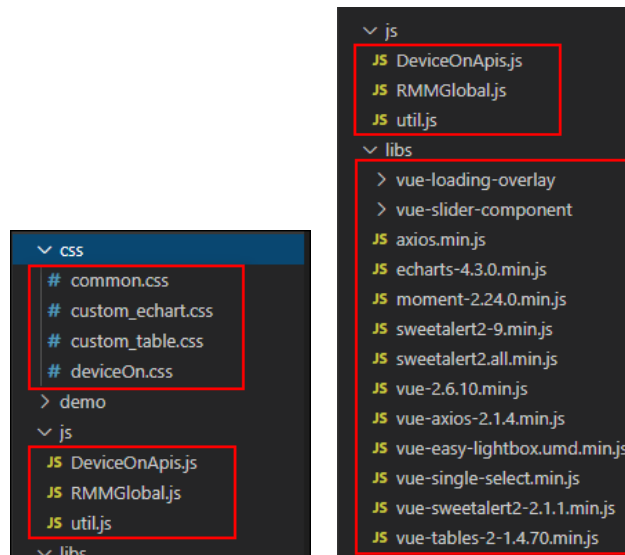


Step 2: Open Visual Studio Code -> Open the path:

`\DeviceOn Server\server\portal\static\addins\SampleAddin\`



Step 3: Here are several resources for you to develop your function.



- **CSS folder** that include *.css style to describes how HTML elements are to be displayed on screen, paper, or in other media.
- **js folder** provides DeviceOnApis.js which is the API for get or set Data from Database on the server and RMMGlobal.js which is the function to get or set the data from the local storage of Website.
- **libs** folder provides simple library, if you need another library, please download from [CDN.js](#) and place in this folder.

Step 4: Download [sample code](#), there are two files (demo.html, demo2.html), please place **demo.html** into "SampleAddin" folder.

Line 18 to 30 (demo.html) to include java script library, you could place your library in the relative path, or alternatively, given library URL from [CDN.js](#).

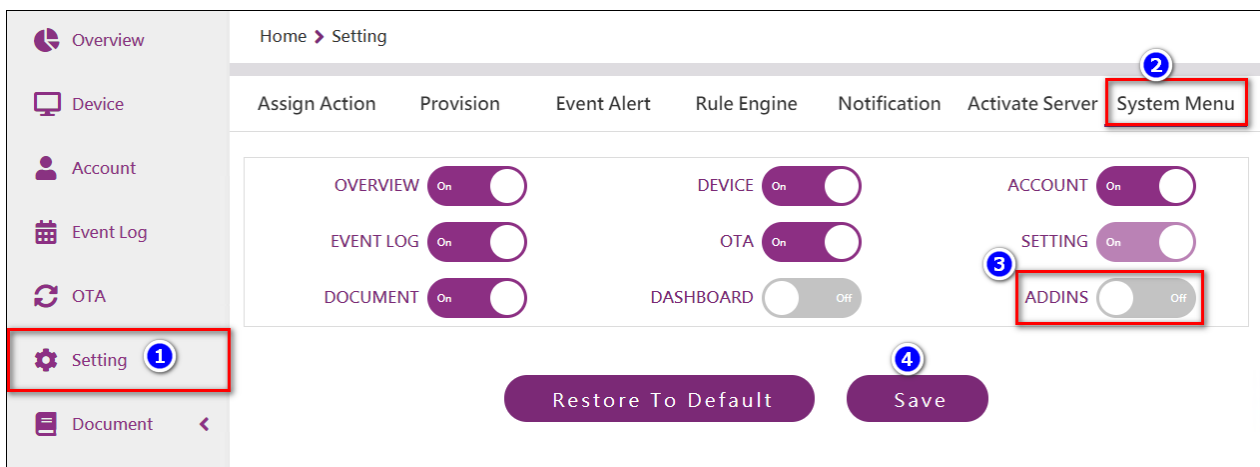
```

17 <!-- javascript plugins -->
18 <script src="/static/addins/SampleAddin/libs/vue-2.6.10.min.js"></script>
19 <script src="/static/addins/SampleAddin/libs/vue-tables-2-1.4.70.min.js"></script>
20 <script src="/static/addins/SampleAddin/libs/axios.min.js"></script>
21 <script src="/static/addins/SampleAddin/libs/sweetalert2.all.min.js"></script>
22 <script src="/static/addins/SampleAddin/libs/vue-sweetalert2-2.1.1.min.js"></script>
23 <script src="/static/addins/SampleAddin/libs/echarts-4.3.0.min.js"></script>
24 <script src="/static/addins/SampleAddin/libs/moment-2.24.0.min.js"></script>
25 <script src="/static/addins/SampleAddin/libs/vue-single-select.min.js"></script>
26
27 <!-- javascript common plugins -->
28 <script src="/static/addins/SampleAddin/js/RMMGlobal.js"></script>
29 <script src="/static/addins/SampleAddin/js/DeviceOnApis.js"></script>
30 <script src="/static/addins/SampleAddin/js/util.js"></script>
31

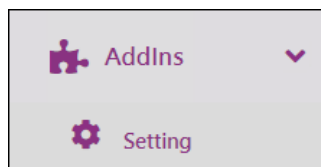
```

1. <!-- CDNjs-->
2. <script src="https://code.jquery.com/jquery.js"></script>
3. <script src="https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/3.3.7/js/bootstrap.min.js"></script>

Step 5: Enable “AddIN” option from DeviceOn Server. (Setting -> System Menu -> ADDINS)



After the option is enabled, the “Addins” will appear in the menu item.



Step 6: Click on the “Setting” (Addins -> Setting) to add your Addins.

+		
DELETE	↑↓	ENABLE
		Setting
1 record		

Add New Addins

NAME 1
demo

URL 2
/static/addins/SampleAddin/demo.html

ICON (FONT AWESOME, EX: FA-CHART-LINE) 3
fa-smile-beam

Save CANCEL

- **Name:** Label name on the menu item
- **URL:** Relative path, **/static/addins/SampleAddin/demo.html**
- **Icon:** Reference [Fontawesome](#) site to get the string of icon

After that, the “**demo**” shown on the menu item, if not, please enable the “**Addin**” on Setting page.

Overview

Device

Account

Event Log

OTA

Setting

Document

AddIns

Setting 1

demo

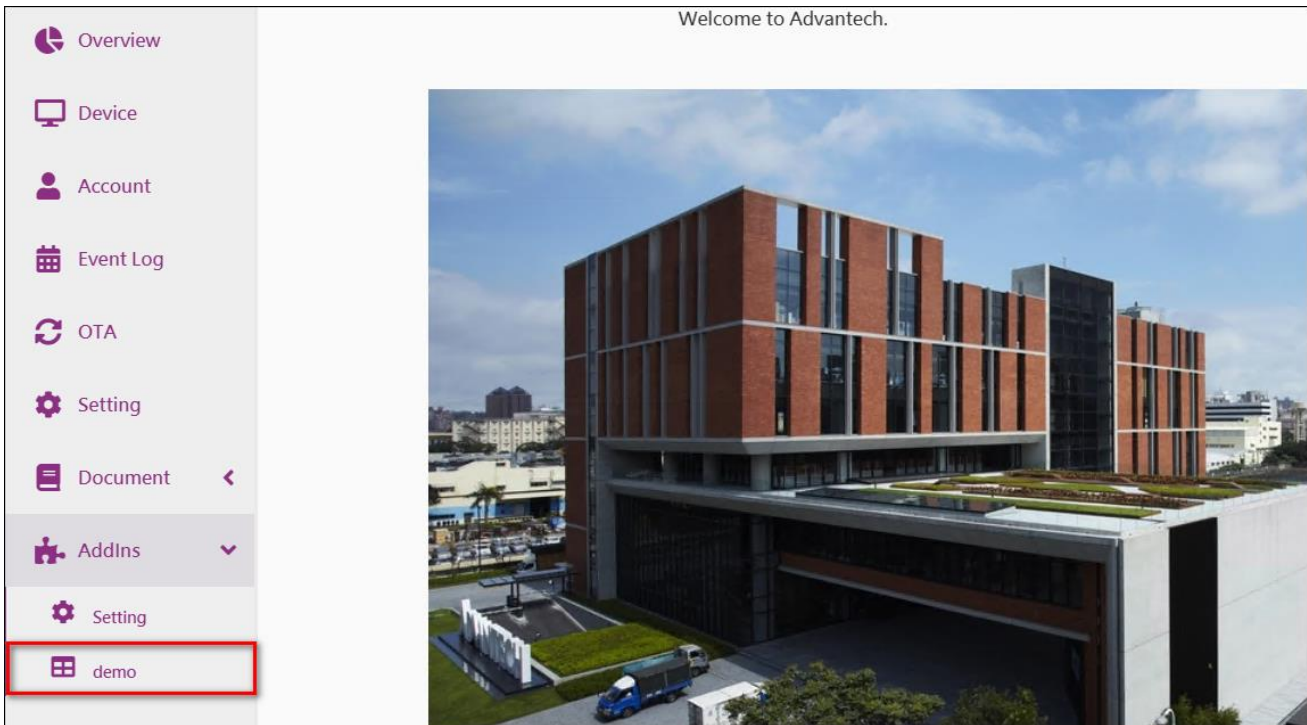
+

DELETE	↑↓	ENABLE	↑↓	LABEL	↑↓	ROUTER	↑↓	PATH	↑↓
		2		Setting		addins			
		<input checked="" type="checkbox"/>		demo		addins		/static/addins/SampleAddin/demo.html	

2 records

Version 4.1.13 ©2019 Advantech corp All rights reserved.

Step 7: Click on the “**demo**” addins.



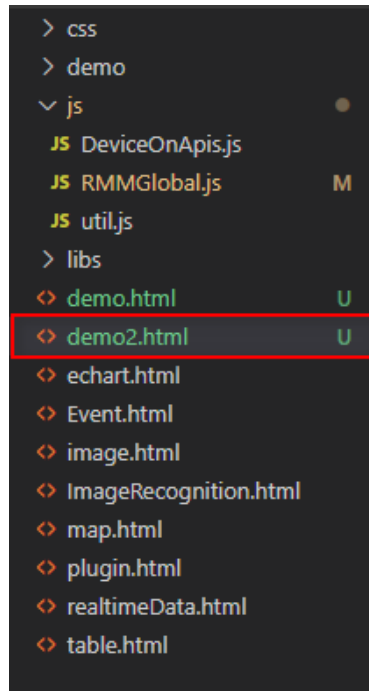
5.2.4 Develop an Add-in to Access DeviceOn API

This example will show you how to get all accounts, groups and devices.

APIs used on below sample

1. DeviceOnApis.accounts.get.accounts(aid)
To get all accounts information from database.
2. DeviceOnApis.accounts.get.deviceGroups(aid)
To get all groups which under this aid's account from database.
3. DeviceOnApis.devicegroups.get.devicesAll(data)
To get all devices which under this aid's account from database.
4. DeviceOnApis.devicegroups.get.devices(gid, data)
To get all devices which under this gid's group from database.

Step 1: Download [sample code](#), there are two files (demo.html, demo2.html), please place **demo2.html** into "SampleAddin" folder.



Step 2: Line 10 ~22 (demo2.html) that describe library used in the Add-in.

```

8
9      <!-- css plugins -->
10     <link rel="stylesheet" href="/static/addins/SampleAddin/css/deviceOn.css">
11     <link rel="stylesheet" href="/static/addins/SampleAddin/css/common.css">
12     <link rel="stylesheet" href="/static/addins/SampleAddin/css/custom_echart.css">
13
14     <!-- javascript plugins -->
15     <script src="/static/addins/SampleAddin/libs/vue-2.6.10.min.js"></script>
16     <script src="/static/addins/SampleAddin/libs/axios.min.js"></script>
17     <script src="/static/addins/SampleAddin/libs/vue-single-select.min.js"></script>
18
19     <!-- javascript common plugins -->
20     <script src="/static/addins/SampleAddin/js/RMMGlobal.js"></script>
21     <script src="/static/addins/SampleAddin/js/DeviceOnApis.js"></script>
22     <script src="/static/addins/SampleAddin/js/util.js"></script>
23
  
```

Use single-select component to build demo view. (Line 27 ~ 57)

```

26 <body style="background: #FAFAFA;">
27 <div id="app">
28   <div class="content">
29     <div class="row">
30       <div class="col-md-4">
31         <div class="cus-label">Account: </div>
32         <vue-single-select v-model="selectedAccount" :options="accountOptions" option-label="name">
33           <template slot="option" slot-scope="{option, index}">
34             <div>
35               <span style="margin-left: 1rem;">{{option.name}}</span>
36             </div>
37           </template>
38         </vue-single-select>
39       </div>
40       <div class="col-md-4">
41         <div class="cus-label">Device Group: </div>
42         <vue-single-select v-model="selectedGroup" :options="groupOptions" option-label="name"></vue-single-select>
43       </div>
44       <div class="col-md-4">
45         <div class="cus-label">Device: </div>
46         <vue-single-select v-model="selectedDevice" :options="deviceOptions" option-label="name">
47           <template slot="option" slot-scope="{option, index}">
48             <div>
49               <i :class="option.iconClass" :style="{ 'color': option.iconColor}" aria-hidden="true"></i>
50               <span style="margin-left: 1rem;">{{option.name}}</span>
51             </div>
52           </template>
53         </vue-single-select>
54       </div>
55     </div>
56   </div>
57 </div>
58 </body>

```

Use RMMGlobal() to get your login account ID (aid), through the aid as parameter to request API.

```

70 mounted: function () {
71   //get current user aid
72   var aid = RMMGlobal.get().Login.aid;
73   this.getAccounts(aid);
74 },

```

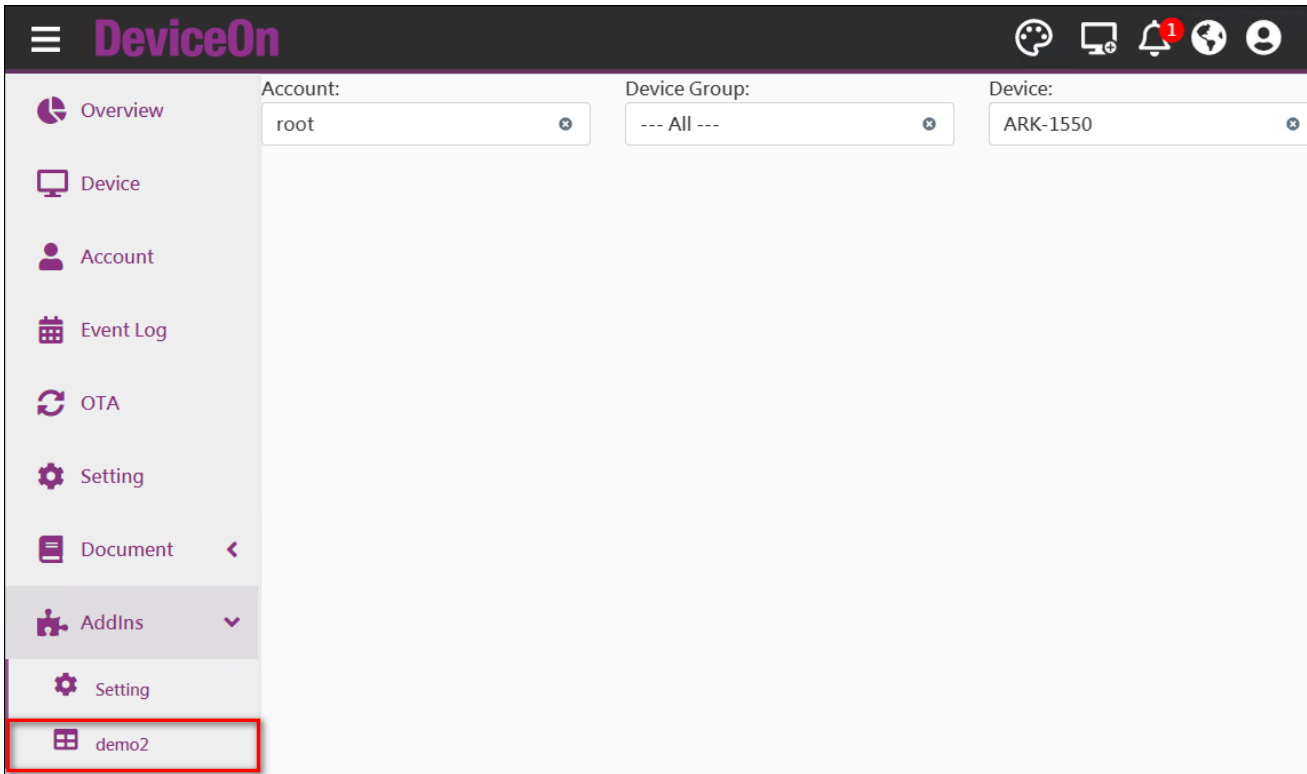
The API (**DeiceOnApis.accounts.get.accounts(aid)**) will send request to server, and return all account data.

```

83 methods: {
84   getAccounts: function (aid) {
85     DeviceOnApis.accounts.get.accounts(aid)
86       .then(function (xhr) {
87         if (xhr && xhr.data && xhr.data.accounts) {
88           vue.accountOptions = xhr.data.accounts;
89           let aAccount = vue.accountOptions.filter(function (g, i) {
90             return g.aid === Number(aid);
91           });
92           if (aAccount.length === 0 && vue.accountOptions.length > 0) {
93             vue.selectedAccount = vue.accountOptions[0];
94           } else {
95             vue.selectedAccount = aAccount[0];
96           }
97         }
98       });
99 },

```

Step 3: Add an Addin (demo2) as before steps.



5.3 Customization DeviceOn Logo, Theme and Menu

DeviceOn supports simple way to replace “**Logo**”, “**Theme**” and “**Menu Item**” to meet diverse domain demands. There are two themes that we provided, one is “Shiny White” and another is “Dark Night”. This lab guides you how to update the logo and select color to change through web user interface quickly. For advanced, if user would like to change the initial settings (Logo, Theme and Menu Items), you could adjust “**defaultConfig**” file to replace default parameters on DeviceOn.

The “**defaultConfig**” file not only provides basic modifications provided by website UI, but also has more detailed parameters to modify:

- **Logo:** Support two sizes of logo, one is for desktop mode, and another is for mobile devices, and the image format should be SVG.
- **Theme:** The gradient background of the login page can be modified.
- **Menu:** The menu items could adjust the order and icon.

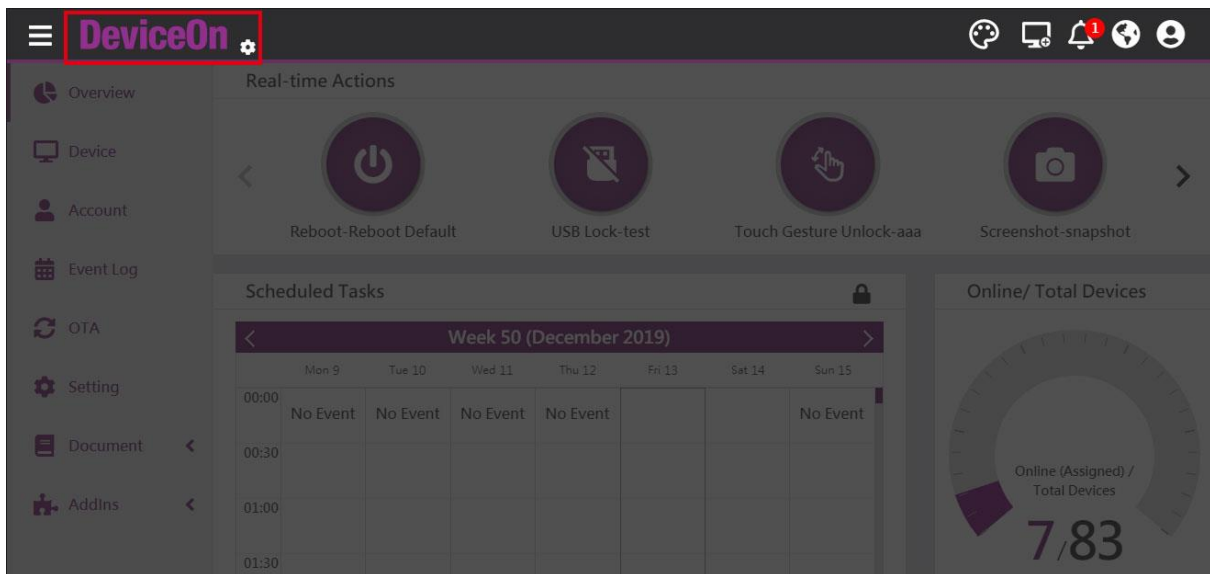
5.3.1 Prerequisite

- DeviceOn Server
- Visual Studio Code V 1.4.1

5.3.2 Steps to Change Logo via Web UI

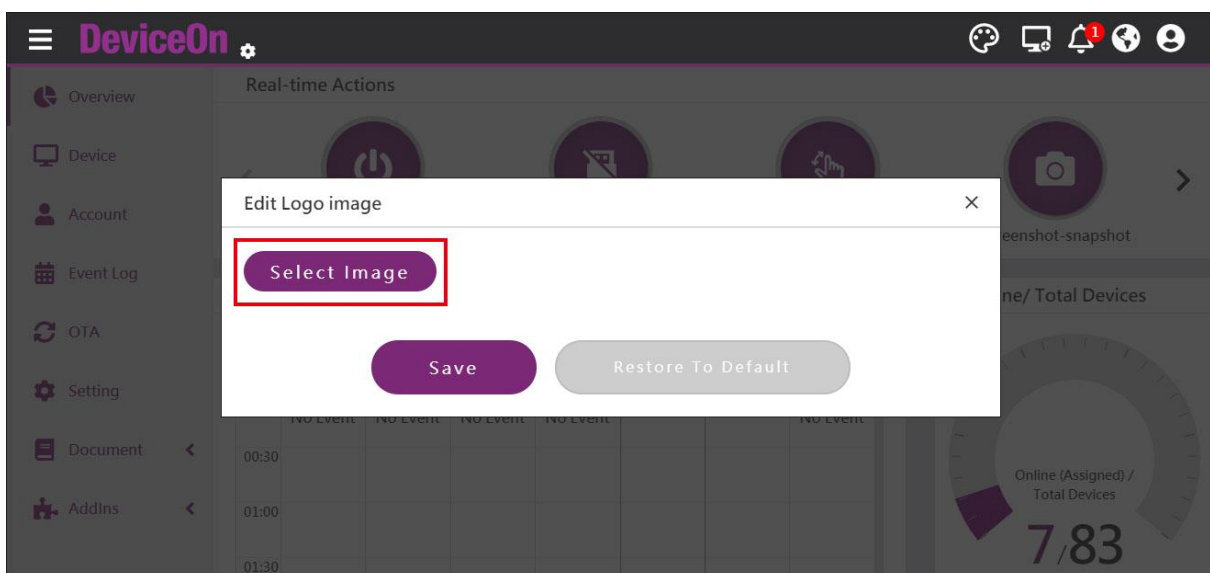
Note: This change will affect the whole system setting.

Step 1: Hover logo and click gear icon.

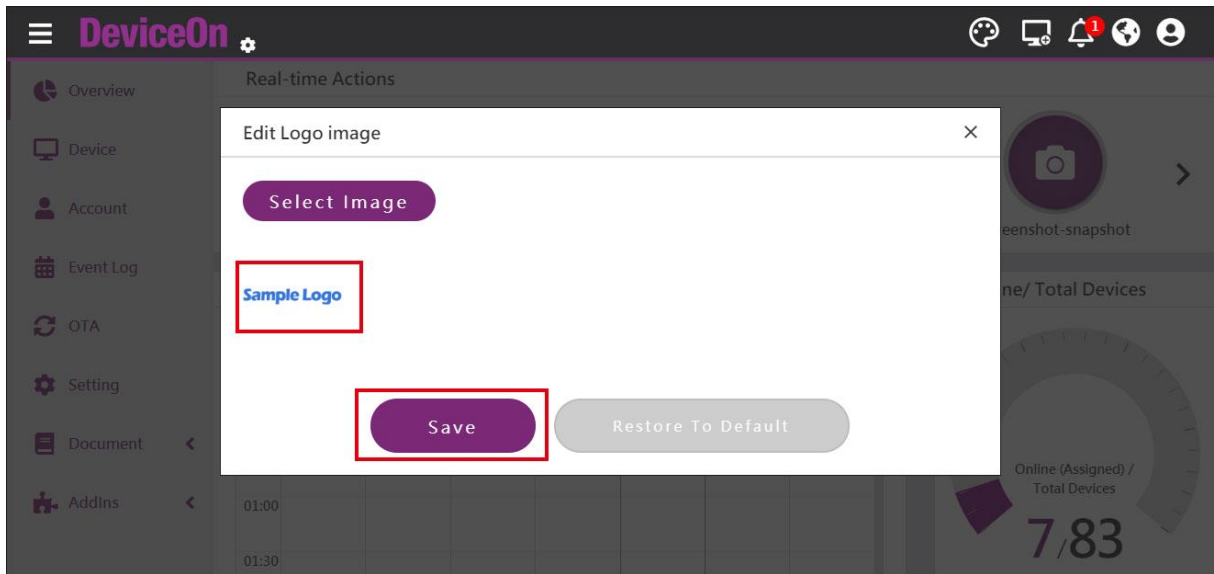


Step 2: Click “Select Image” button to select image file, the image format suggestion as below.

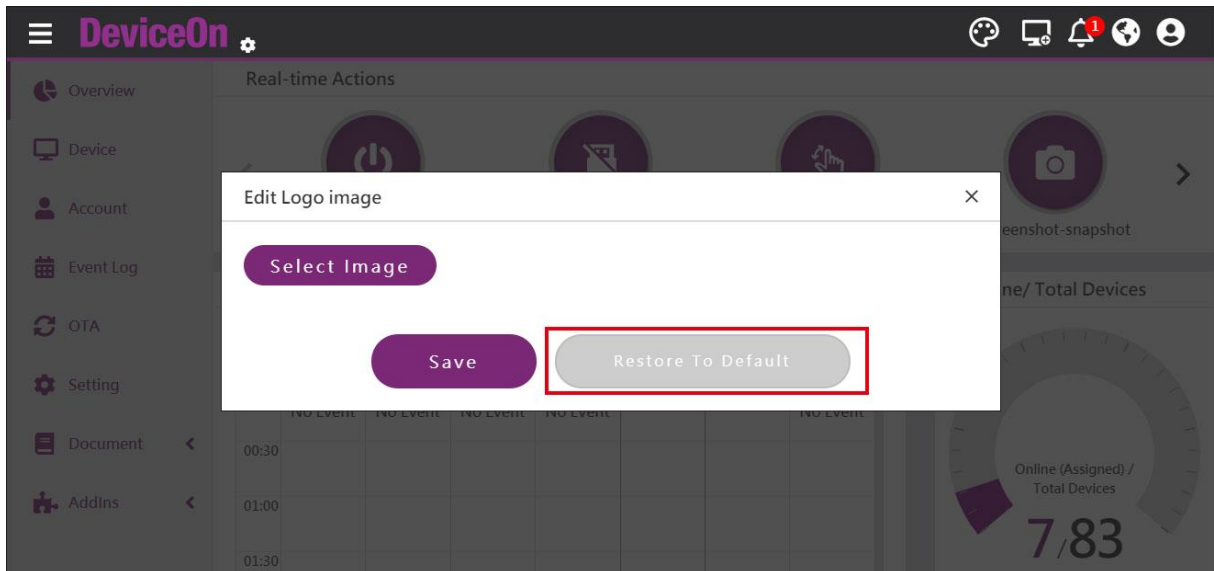
- **Accept file type:** .PNG .JPEG .JPEG .GIF
- **Suggestion file type:** The image file format is PNG and has a transparent background.
- **Size:** 350*150px



Step 3: You will see the image you selected, click the “Save” button when you are sure, and the picture will be uploaded to the cloud.



If you want to restore the initial logo, you can click “**Restore to Default**” button.



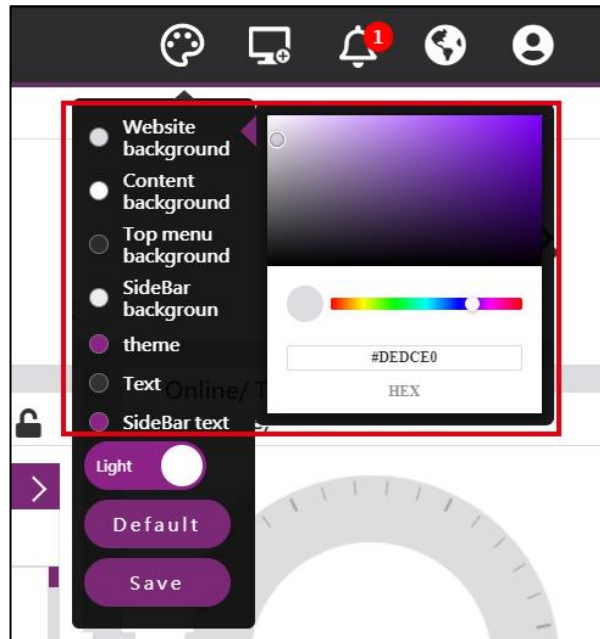
5.3.3 Steps to Change Theme via Web UI

Note: This change will affect on personal account not the system.

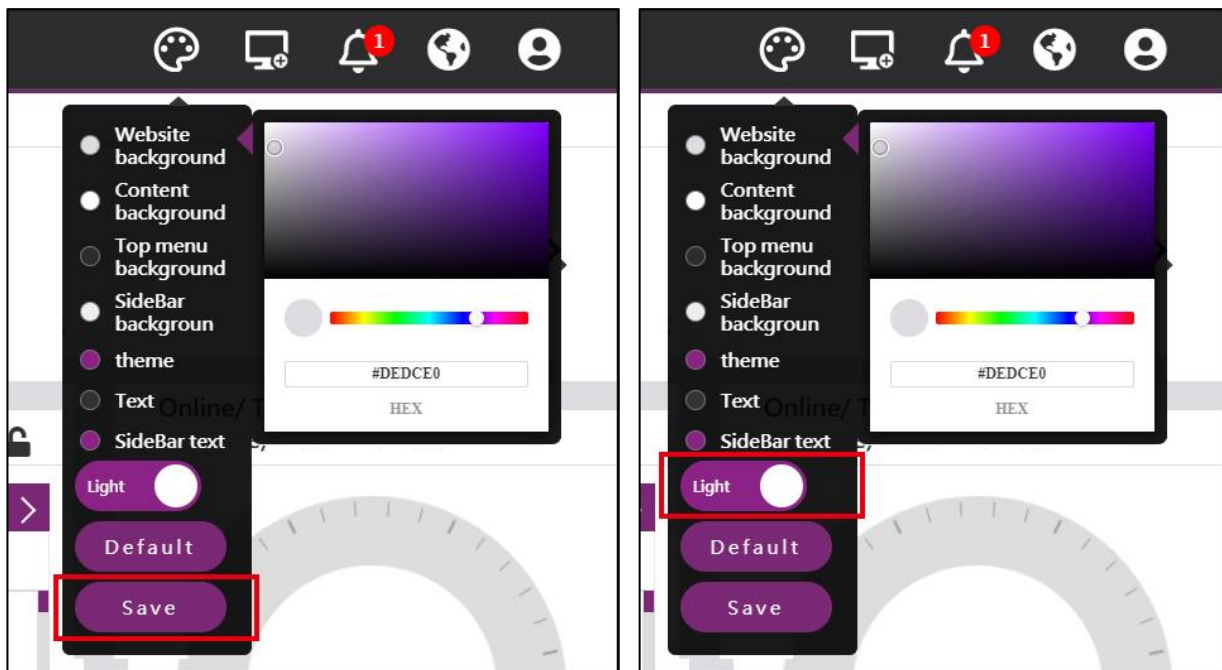
Step 1: Click Palette icon



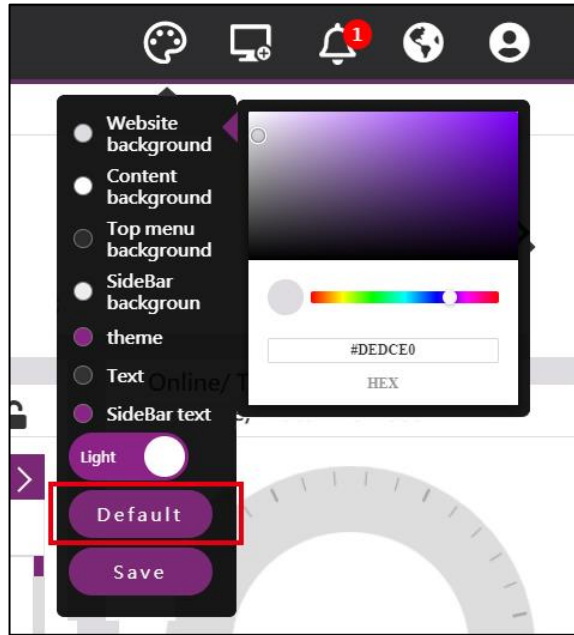
Step 2: You can choose the background of the webpage, content, header, menu, theme color, text and menu text color.



Step 3: Click “Save” button to save your color settings and Switch button to quickly change the theme of Light and Dark.



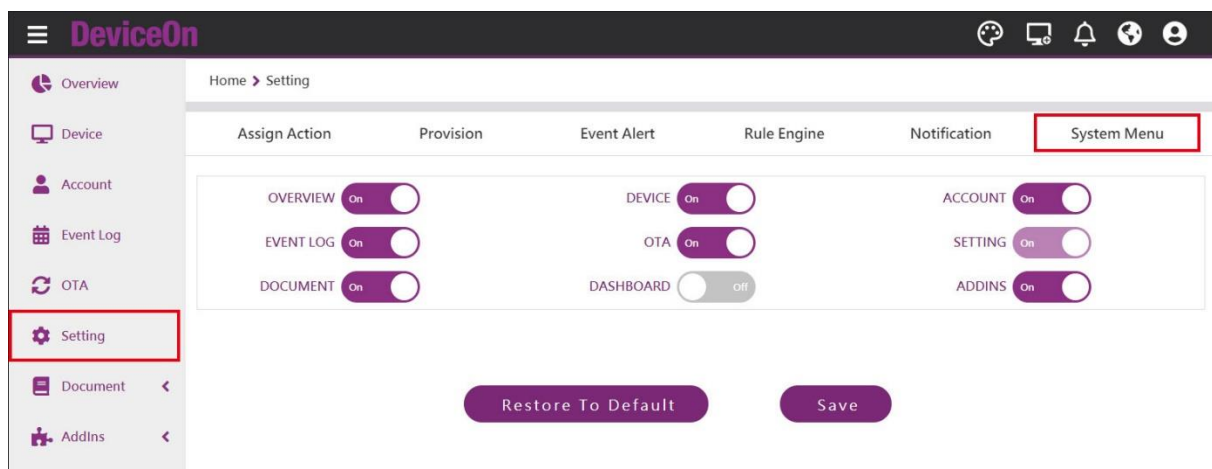
Click “Default” button can return to initial settings.



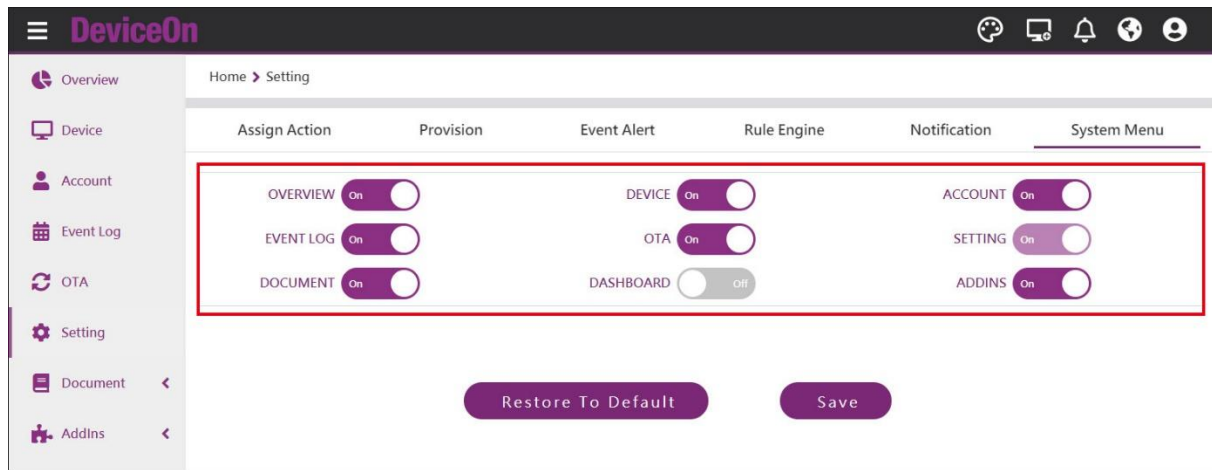
5.3.4 Steps to Adjust Menu Items via Web UI

Note: This change will affect the whole system setting.

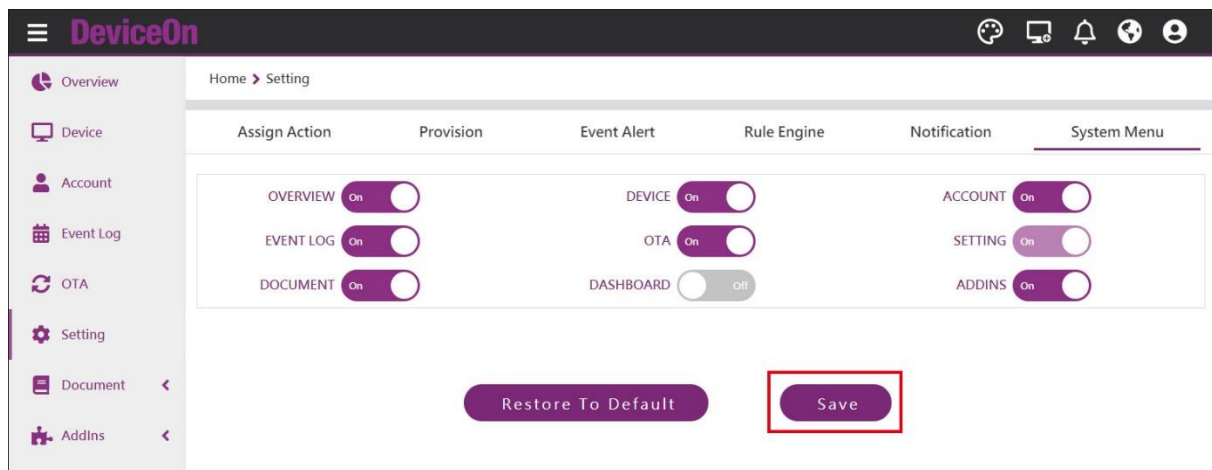
Step1: Go to Setting → System Menu



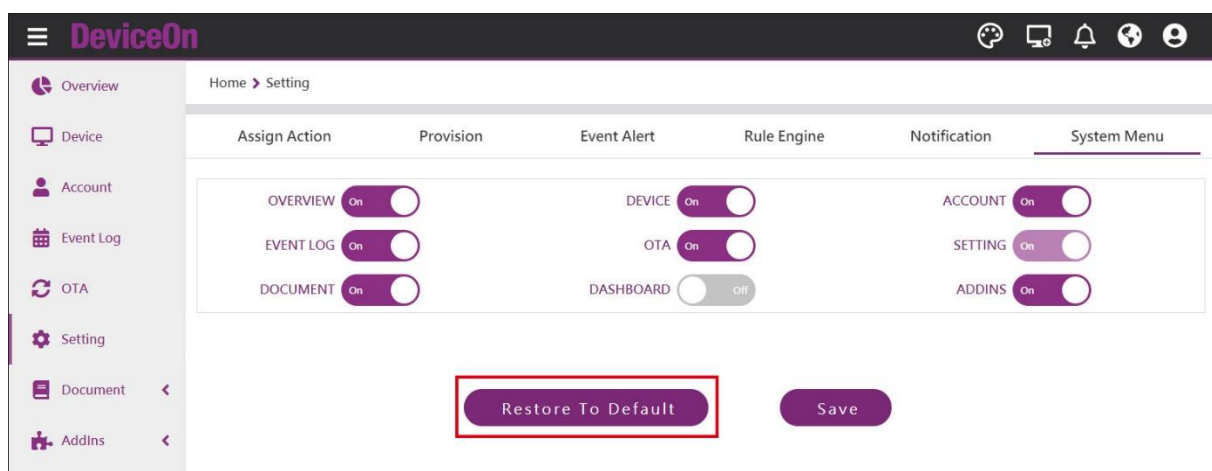
Step 2: Switch menus button, control the opening and closing of items.



Step 3: Click “Save” button to save setting.



Click “Restore to Default” button can return to initial setting.

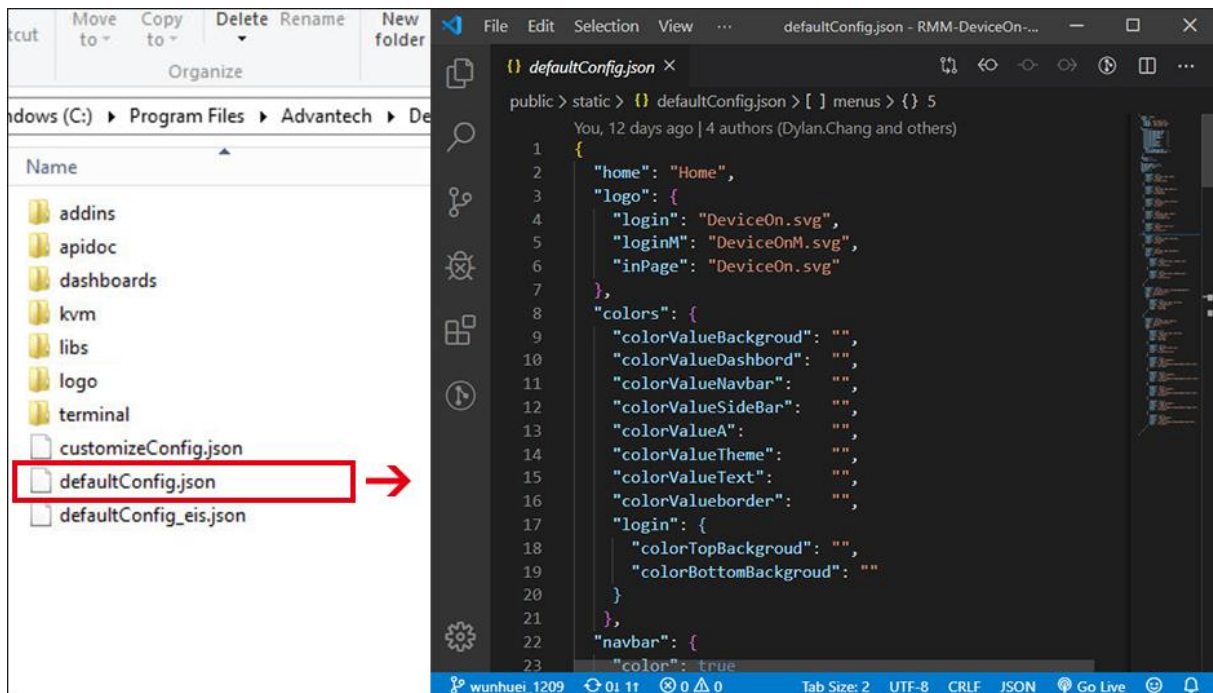


5.3.5 Introduce Advanced Configuration

Configuration File:

C:\Program Files\Advantech\DeviceOn Server\server\portal\static\

Open “defaultConfig” file use Visual Studio Code.



Program Architecture:

This file is the appearance preset value that the DeviceOn website relies on. The picture below is the current setting value. If it is modified, it is a custom preset value, not the default style of DeviceOn.

```

1  {
2    "home": "Home",
3    "logo": {
4      "login": "DeviceOn.svg",
5      "loginM": "DeviceOnM.svg",
6      "inPage": "DeviceOn.svg"
7    },
8    "colors": {
9      "colorValueBackgroud": "",
10     "colorValueDashbord": "",
11     "colorValueNavbar": "",
12     "colorValueSideBar": "",
13     "colorValueA": "",
14     "colorValueTheme": "",
15     "colorValueText": "",
16     "colorValueborder": "",
17     "login": {
18       "colorTopBackgroud": "",
19       "colorBottomBackgroud": ""
20     }
21   },
22   "navbar": {
23     "color": true
24   },
25   "breadcrumbs": true,
26   "grafanaAccount": "",
27   "grafana": "",
28   "menus": [
29     {
30       "enable": true,
31       "label": "deviceon.menu.home",
32       "router": "Home",

```

- **Logo:** Replace the default logo of the website.
- **Colors:** Replace the default color system of the website, including background, content, header, menu, menu text, theme color, text, border
- **Colors -> login:** Adjust the default gradient background color of the login page.
- **Menus:** Adjust the default menu items, show or hidden, order of items, and icon image.

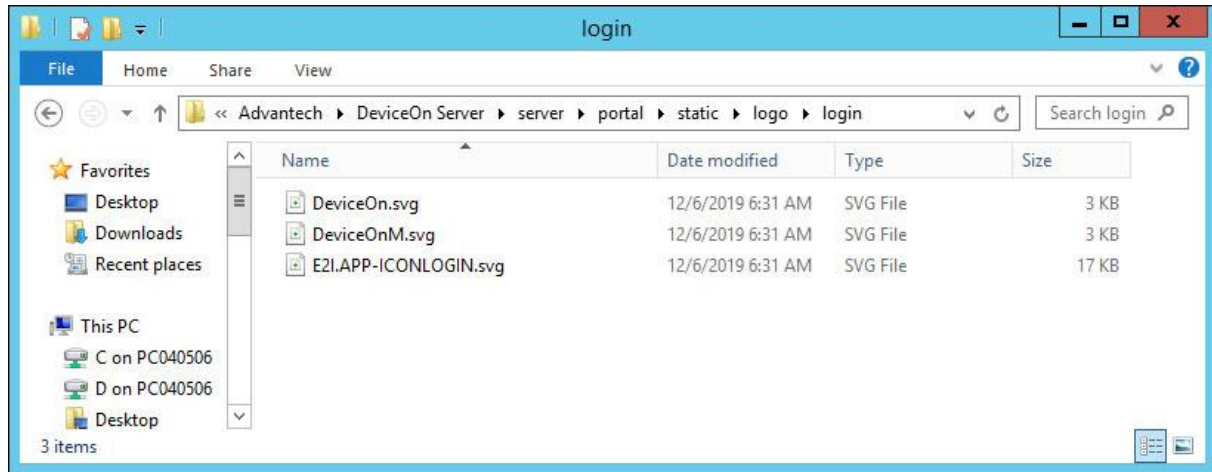
Once again, if you make changes, the value set in the file is the customer's initial value, and it will no longer be DeviceOn style.

5.3.6 Steps to Change Logo via Advanced Configuration

User could control logo displayed on the desktop size and phone size.

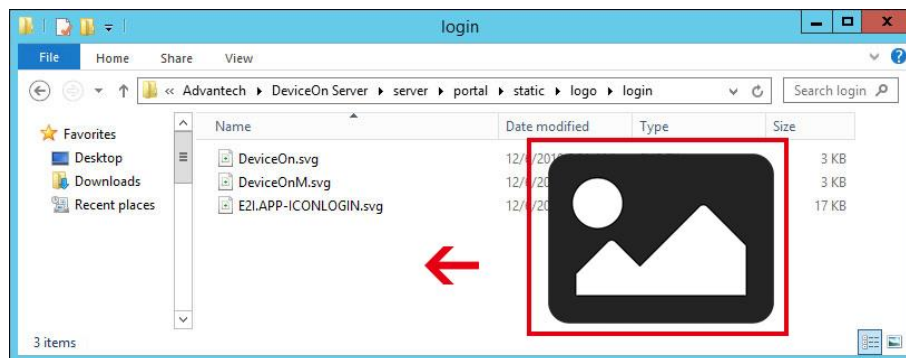
Step 1: Open the folder

"C:\Program Files\Advantech\DeviceOn Server\server\portal\static\logo\login"

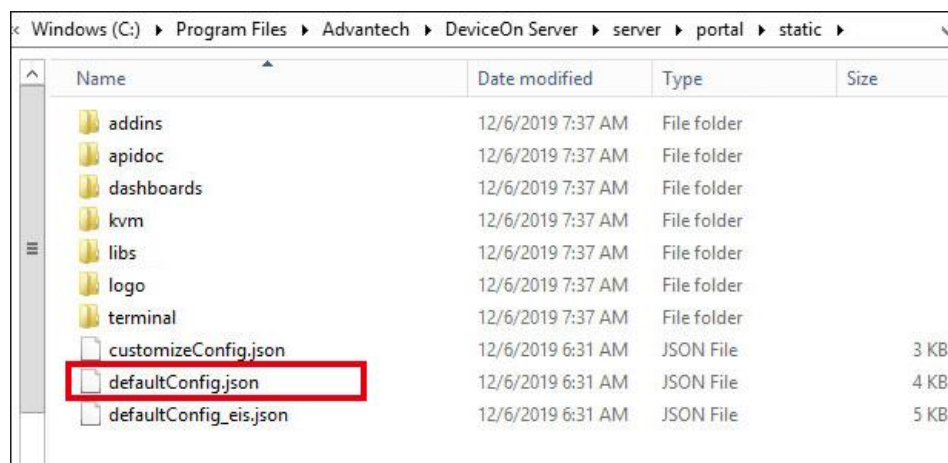


Step 2: Place the logo image to be replaced. You can prepare two images to change the screen size of the desktop and mobile.

- **Accept file Type:** .PNG .JPG .JPEG .GIF .SVG
- **Suggestion file Type:** PNG or SVG with a transparent background.
- **Size:** 350*150px



Step 3: To C:\Program Files\Advantech\DeviceOn Server\server\portal\static
 Open “defaultConfig” file use Visual Studio Code



Step 4: Rewrite the code parameter of defaultConfig file.

```

1  {
2      "home": "Home",
3      "logo": {
4          "login": "DeviceOn.svg",
5          "loginM": "DeviceOnM.svg",
6          "inPage": "DeviceOn.svg"
7      },

```

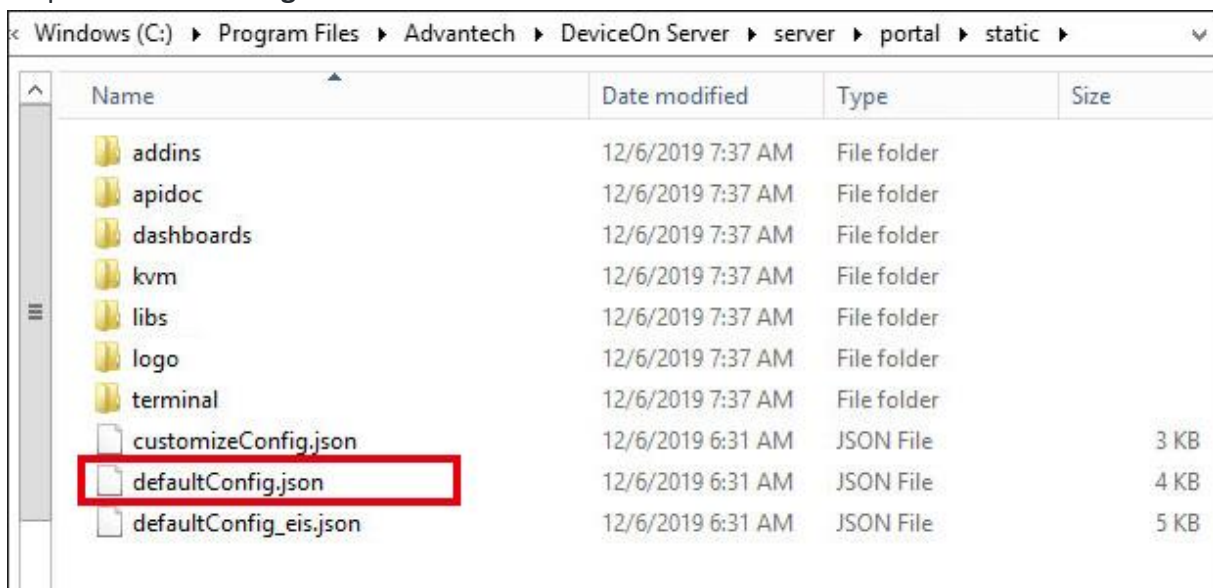
- "login": For desktop size
- "loginM": For phone size
- "inPage": Reserve special settings

5.3.7 Steps to Change Theme, Color via Advanced Configuration

User can modify the web page color of the basic inner page, and **modify the gradient color of the login page also.**

Step 1: To C:\Program Files\Advantech\DeviceOn Server\server\portal\static

Open "defaultConfig" file use Visual Studio Code



Name	Date modified	Type	Size
addins	12/6/2019 7:37 AM	File folder	
apidoc	12/6/2019 7:37 AM	File folder	
dashboards	12/6/2019 7:37 AM	File folder	
kvm	12/6/2019 7:37 AM	File folder	
libs	12/6/2019 7:37 AM	File folder	
logo	12/6/2019 7:37 AM	File folder	
terminal	12/6/2019 7:37 AM	File folder	
customizeConfig.json	12/6/2019 6:31 AM	JSON File	3 KB
defaultConfig.json	12/6/2019 6:31 AM	JSON File	4 KB
defaultConfig_eis.json	12/6/2019 6:31 AM	JSON File	5 KB

Step 2: Rewrite the code parameter of defaultConfig file

- Parameter must be capitalized
- Use Hex Code #RRGGBB (ex: #AD8641)

*References: <https://htmlcolorcodes.com/color-picker/>

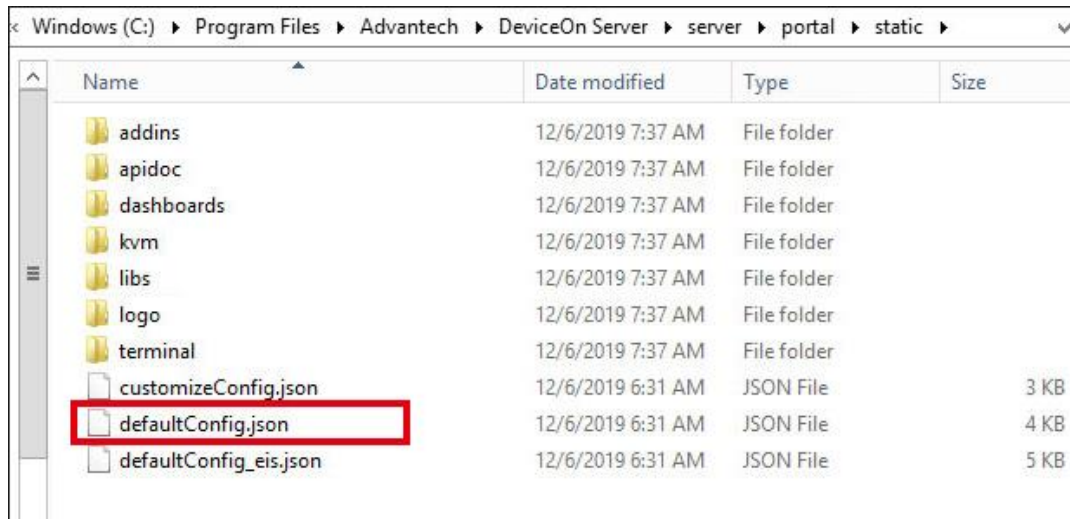
8	"colors": {	8	"colors": {
9	"colorValueBackgroud": "",	9	"colorValueBackgroud": "#0E0E0E",
10	"colorValueDashbord": "",	10	"colorValueDashbord": "#1B1B1B",
11	"colorValueNavbar": "",	11	"colorValueNavbar": "#151515",
12	"colorValueSideBar": "",	12	"colorValueSideBar": "#151515",
13	"colorValueA": "",	13	"colorValueA": "#FFFFFF",
14	"colorValueTheme": "",	14	"colorValueTheme": "#405594",
15	"colorValueText": "",	15	"colorValueText": "#FFFFFF",
16	"colorValueborder": "",	16	"colorValueborder": "#AEAEAE",
17	"login": {	17	"login": {
18	"colorTopBackgroud": "",	18	"colorTopBackgroud": "#408A94",
19	"colorBottomBackgroud": ""	19	"colorBottomBackgroud": "#405394"
20	}	20	}
21	},	21	},
DeviceOn Parameter		Example Parameter	

1. "colorValueBackgroud": //Web background
2. "colorValueDashbord": //Content background
3. "colorValueNavbar": //Header background
4. "colorValueSideBar": //Menu background
5. "colorValueA": //Menu text
6. "colorValueTheme": //Main color
7. "colorValueText": //Text
8. "colorValueborder": //Border color
9. "login": {
10. "colorTopBackgroud": //Login page top gradient
11. "colorBottomBackgroud": //Login page bottom gradient
12. }

5.3.8 Steps to Adjust Menu Items via Advanced Configuration

Step 1: To C:\Program Files\Advantech\DeviceOn Server\server\portal\static

Open "defaultConfig" file use Visual Studio Code.



Step 2: Rewrite the menus code parameter of defaultConfig.

```

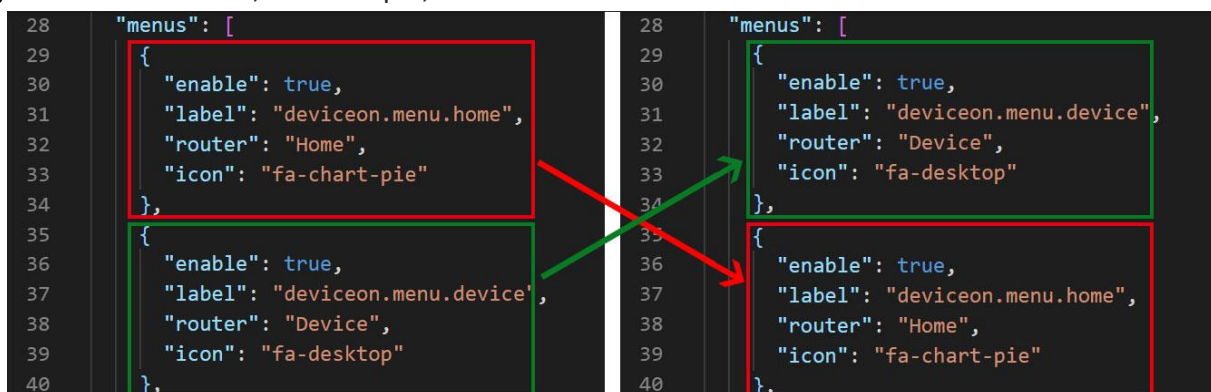
28  "menus": [
29    {
30      "enable": true,
31      "label": "deviceon.menu.home",
32      "router": "Home",
33      "icon": "fa-chart-pie"
34    },

```

- **"enable"**: Change the parameters "true" or "false" to switch the menu item.
- **"icon"**: Change the parameters can show different icon.

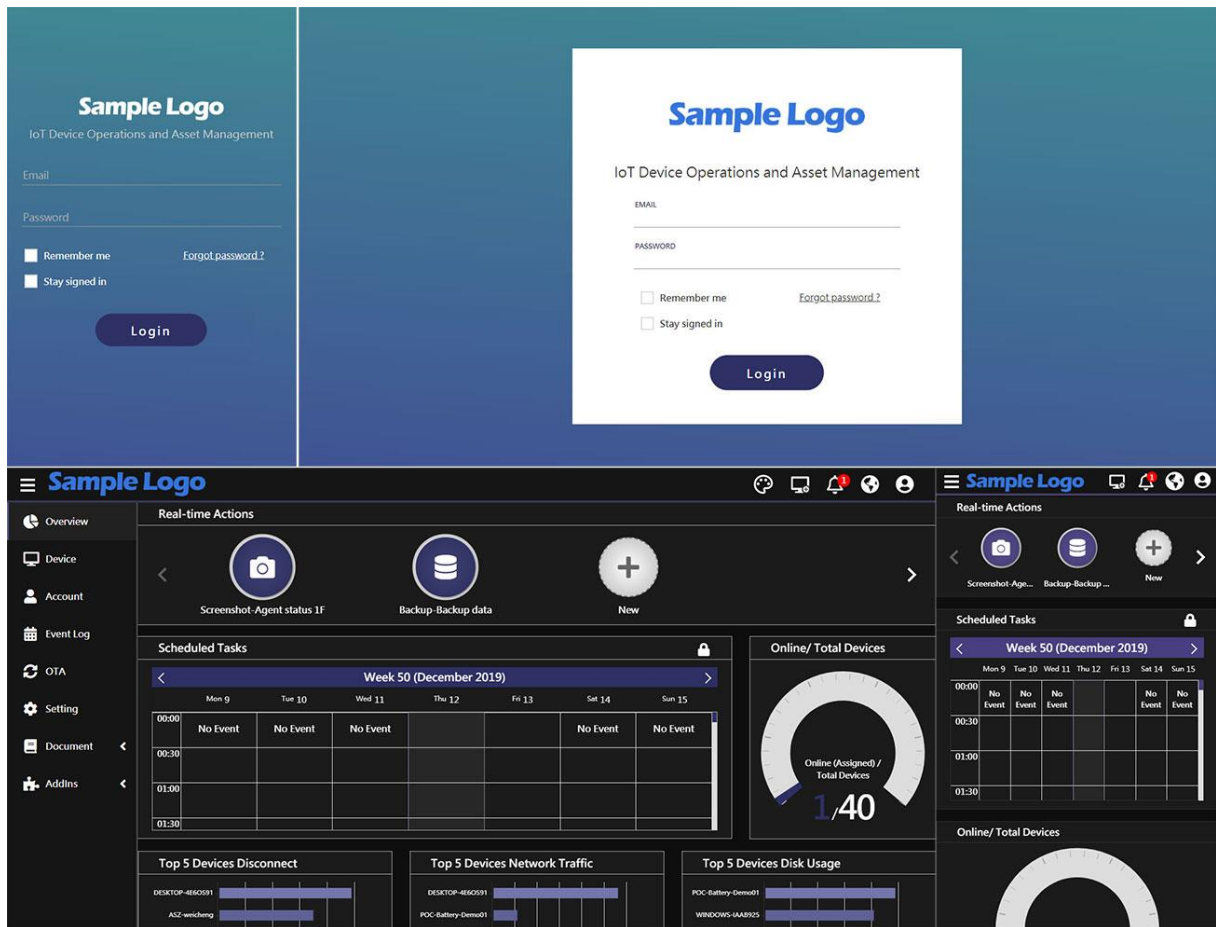
*References: <https://fontawesome.com/v5.12.0/icons?d=gallery&m=free>

Adjust the menu order, for example, switch these items as below.



System with initial value setting is completed and saves; you can see it when you open the Device On web page. The logo image changes on the desktop and mobile phone. The gradient color of the login page is not the initial purple setting of DeviceOn. All changes are presented through the parameters

of defaultConfig file.



6. FAQ

6.1 Why Some of Devices Cannot Power On

REF: <https://www.lifewire.com/wake-on-lan-4149800/>

The DeviceOn leverage Wake-on-LAN (WoL) mechanism to remote power your device on, there are 2 steps to should be configured at first. Wake-on-LAN (WoL) is a network standard that allows a computer to be turned on remotely, whether it's hibernating, sleeping, or even completely powered off. It works by receiving what's called a "magic packet" that's sent from a WoL client.

It also doesn't matter what operating system the computer will eventually boot into (Windows, Mac, Ubuntu, etc.), Wake-on-LAN can be used to turn on any computer that receives the magic packet. A computer's hardware does have to support Wake-on-LAN with a compatible BIOS and network interface card, so not every computer is automatically able to use Wake-on-LAN.

Two-step WoL Setup

Enabling Wake-on-LAN is done in two steps, both of which are described below. The first sets up the motherboard by configuring Wake-on-LAN through BIOS before the operating system boots, and the next logs into the operating system and makes some small changes there. The first step with the BIOS is valid for every computer, but after following the BIOS setup, skip down to your operating system instructions, whether it be for Windows, Mac, or Linux.

Step 1: BIOS Setup

The first thing you need to do to enable WoL is to set up BIOS correctly so that the software can listen for incoming wake up requests.

Every manufacturer will have unique steps, so what you see below may not describe your setup exactly. If these instructions aren't helping, find out your BIOS manufacturer and check their website for a user manual on how to get into BIOS and find the WoL feature.

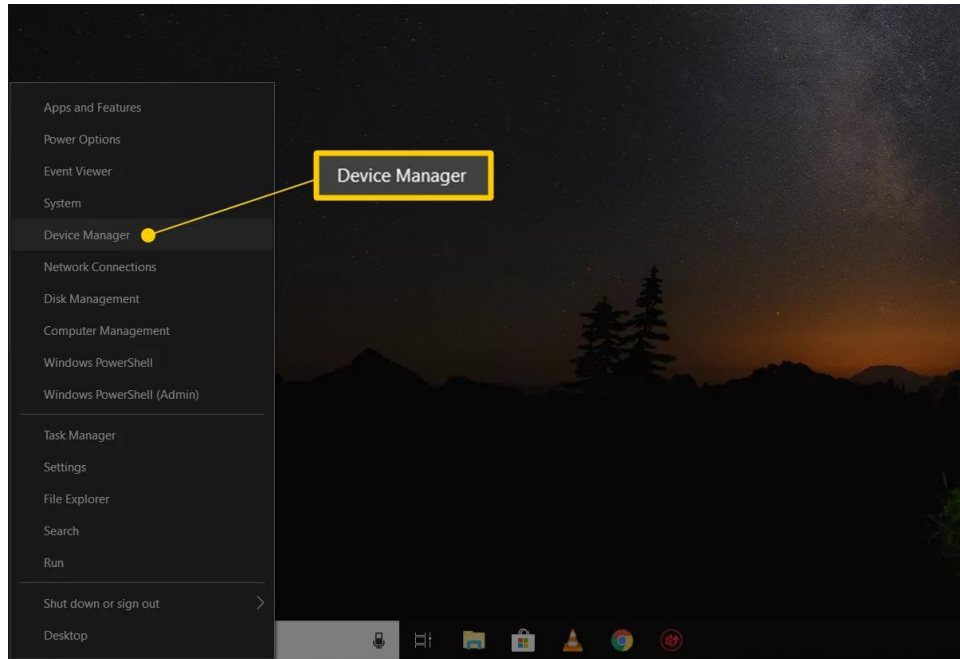
1. Enter BIOS instead of booting to your operating system.
2. Look for a section that pertains to power, such as Power Management. This may be under an Advanced section. Other manufacturers might call it Resume On LAN, such as on the Mac.
Most BIOS screens have a help section off to the side that describes what each setting does when enabled. It's possible that the name of the WoL option in your computer's BIOS isn't clear.
3. Once you find the WoL setting, you can most likely press **Enter** to either immediately toggle it on or to show a small menu that allows you to toggle it on and off, or enable it and disable it.
4. Save the changes. This isn't the same on every computer, but on many the **F10** key will save and exit BIOS. The bottom of the BIOS screen should give some instructions about saving and exiting.



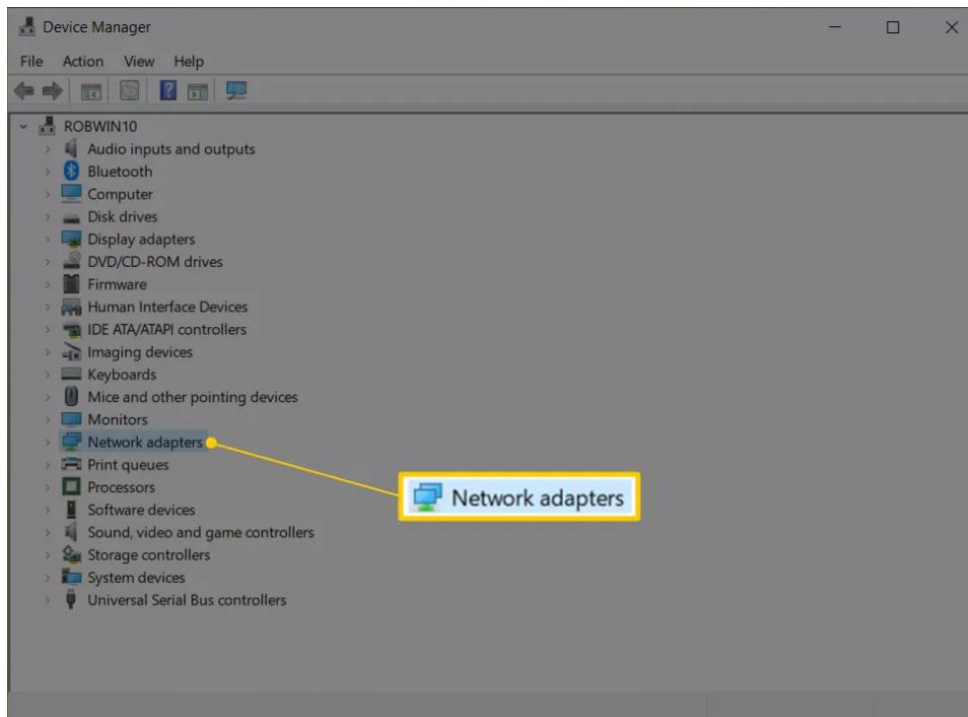
Step 2: Windows operating system WoL setup

[Windows Wake-on-LAN](#) is set up through Device Manager. There are a few different settings to enable here:

1. Open Device Manager

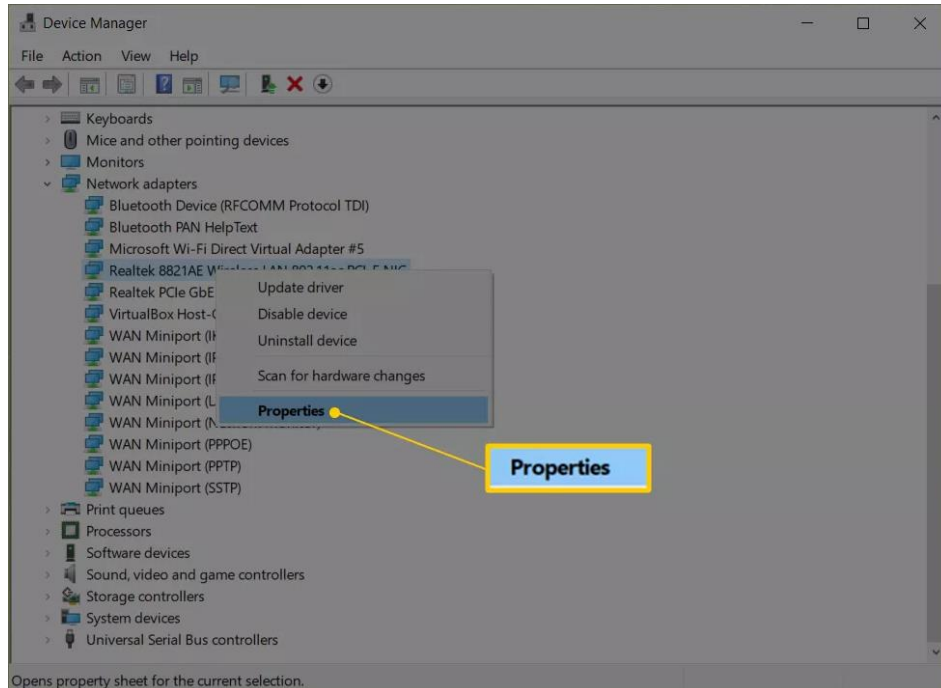


2. Find and open the Network adapters section.

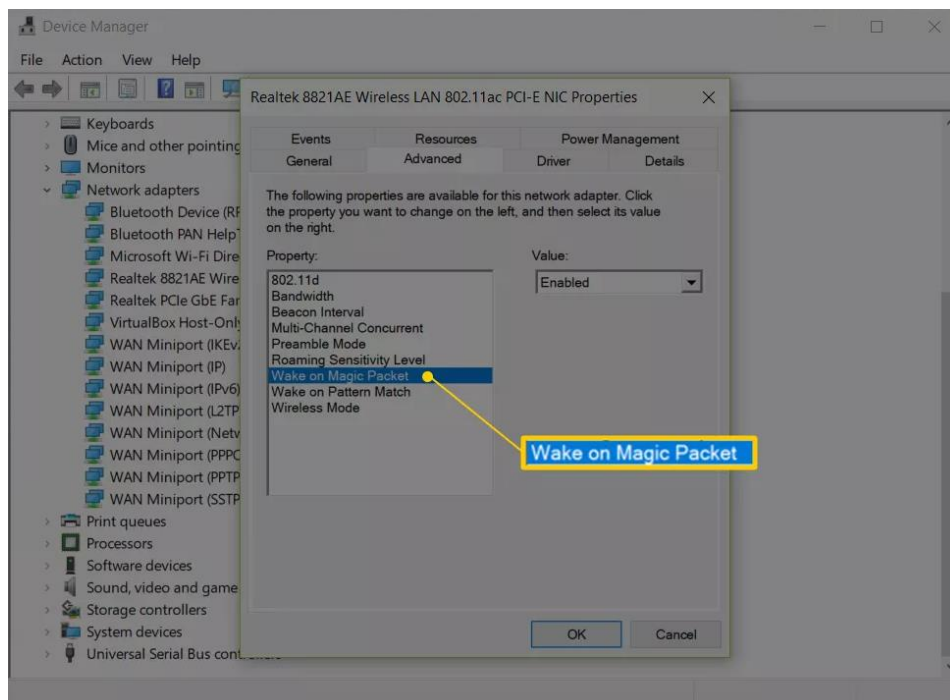


You can ignore any Bluetooth connections and virtual adapters. Double-click (or double-tap) **Network adapters** or select the small + or > button next to it to expand that section.

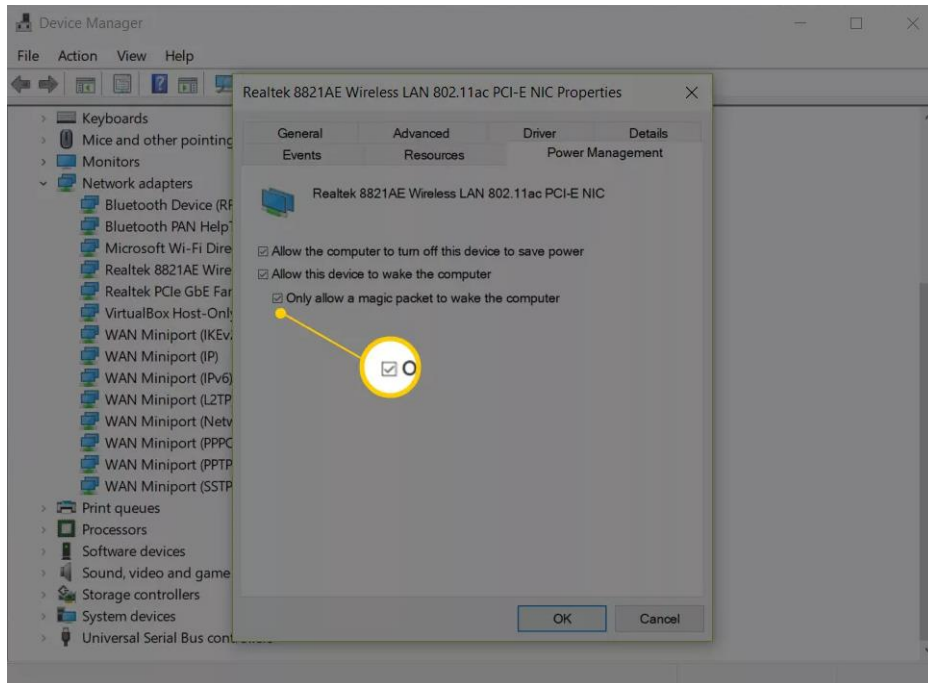
3. Right-click or tap-and-hold the adapter that belongs to the active internet connection. Examples of what you might see are **Realtek PCIe GbE Family Controller** or **Intel Network Connection**, but it will vary depending on your computer.
4. Choose **Properties**.



5. Open the **Advanced** tab.
6. Under the **Property** section, click or tap **Wake on Magic Packet**. If you can't find this, skip to Step 8; Wake-on-LAN might still work anyway.



7. From the **Value** menu on the right, choose **Enabled**.
8. Open the **Power Management** tab. It might be called **Power** depending on your version of Windows or network card.
9. Make sure these two options are enabled: **Allow this device to wake the computer** and **Only allow a magic packet to wake the computer**.

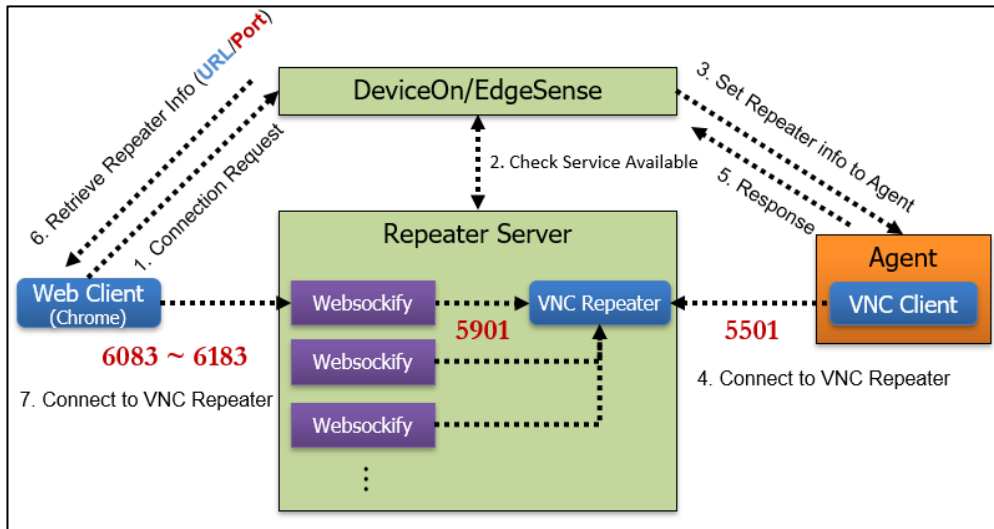


These settings might instead be under a section called Wake-on-LAN and be a single setting called **Wake on Magic Packet**.

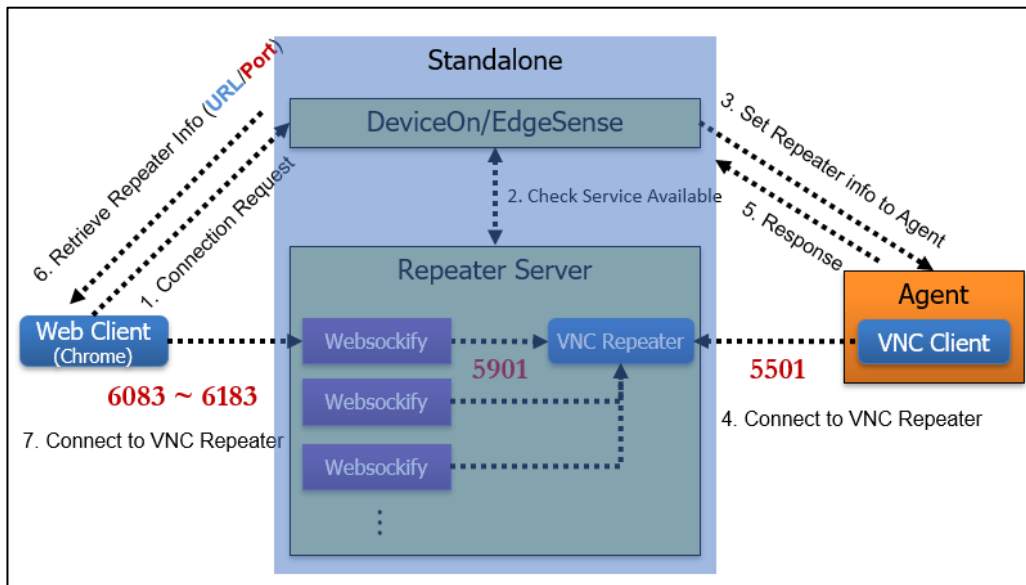
10. Click or tap **OK** to save the changes and exit that window. You can also close down Device Manager.

6.2 Why Cannot Remote Control via KVM (Remote Desktop)

The DevicOn leverage VNC (Virtual Network Computing) technology to achieve remote desktop, to bridge different network between public and private. We build-up a Repeater server on public site for WISE-PaaS/EnSaaS and Azure PaaS. There is a web-client through WebSocket (port: 6083 ~6183) mechanism connect to Repeater and device via 5501 to Repeater, the structure as below. Please help confirm the port available on your browser and device side.

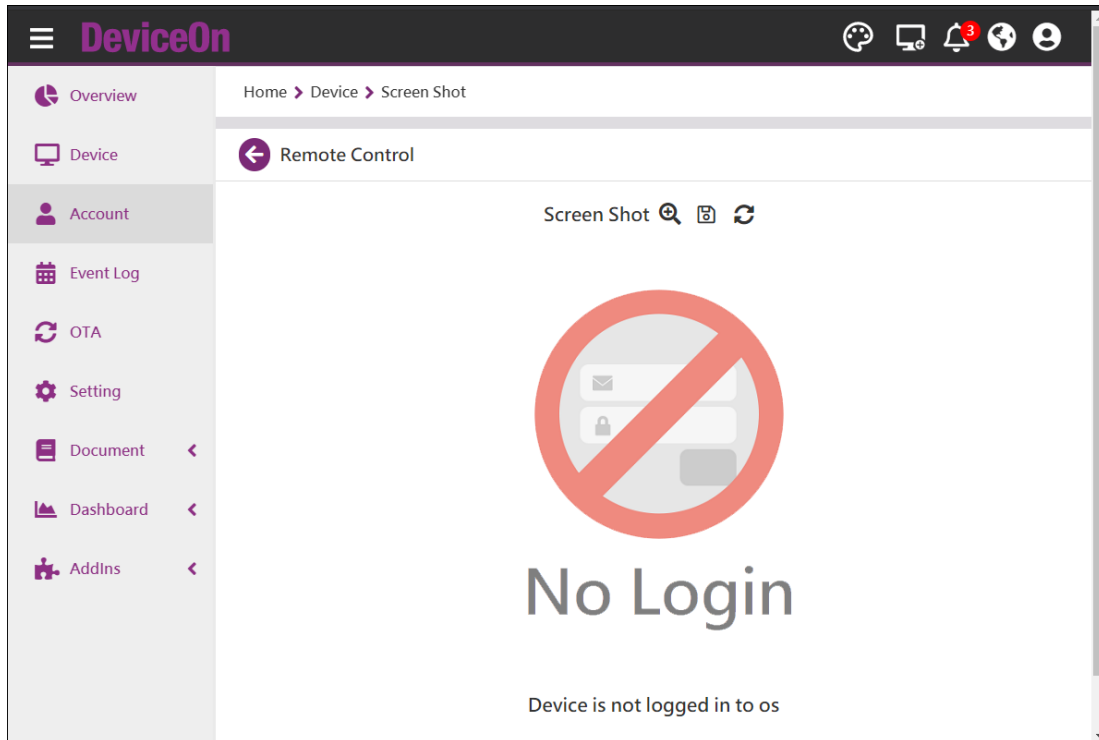



If the DeviceOn running on VM, standalone version, the Repeater also build into same machine, please reference the structure, make sure the VM available for these inbound and outbound ports.

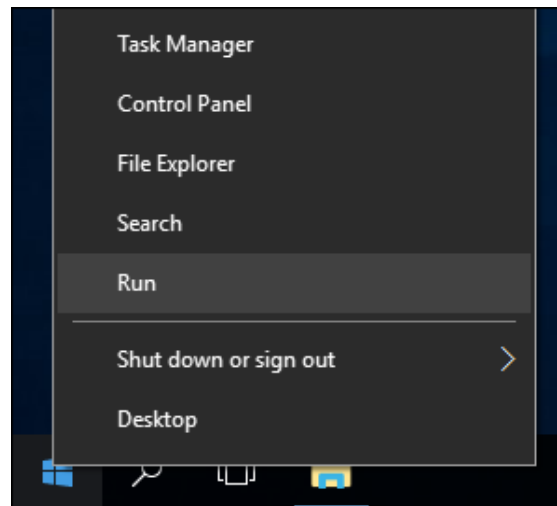


6.3 Why Cannot Screenshot and Always Show Device “No Login”

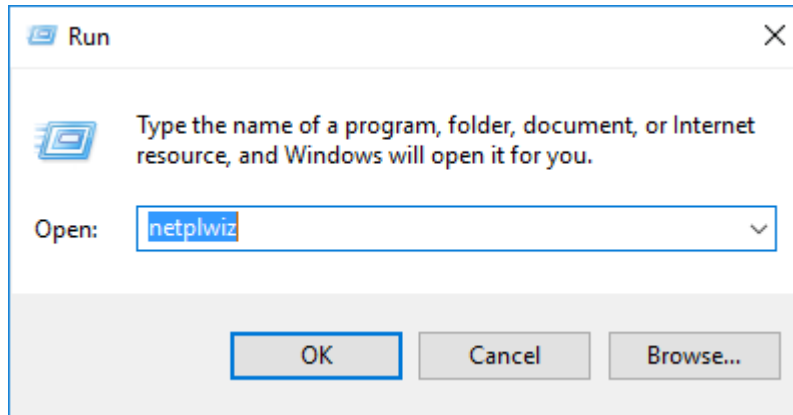
To fix the “No Login” error, you can sign into the system manually, or set the “Automatically Sign in to Windows 10”.



Step 1, Right-click the Start button and select Run from the hidden quick access menu, or use the keyboard shortcut Windows Key  + R to bring up the Run dialog.

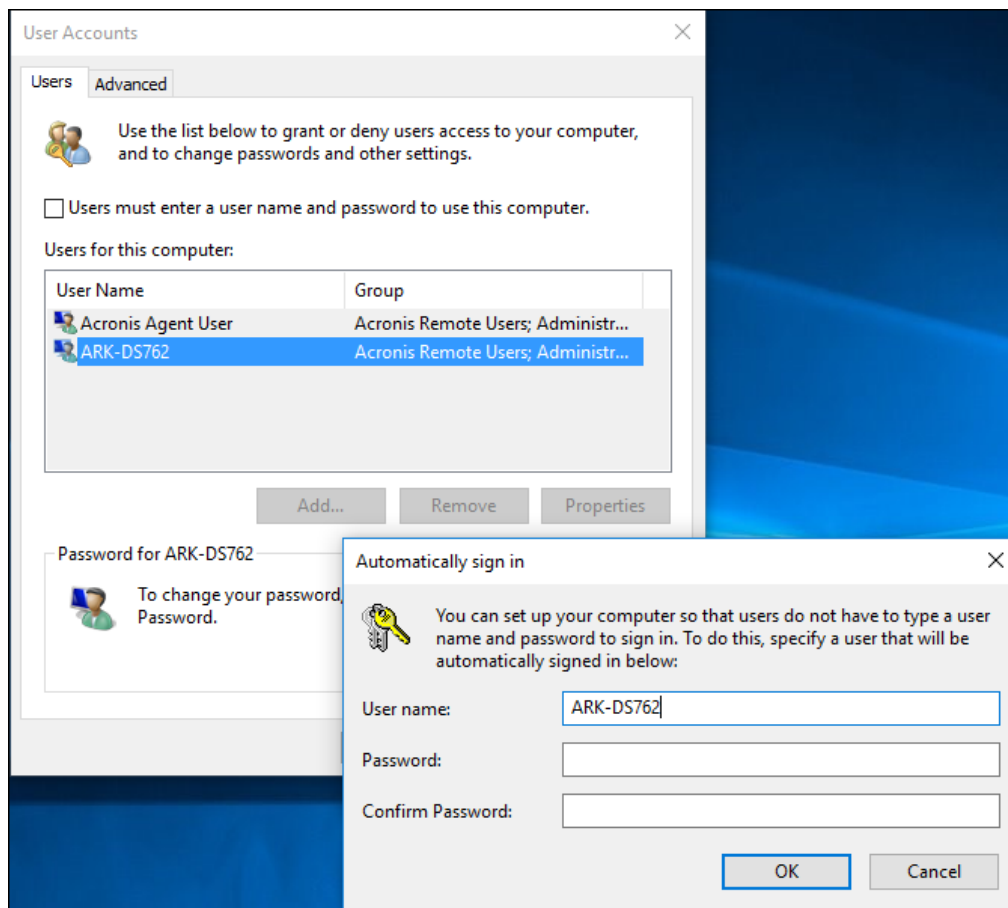


Step 2, Now Then Type: **netplwiz** and hit Enter or click OK.




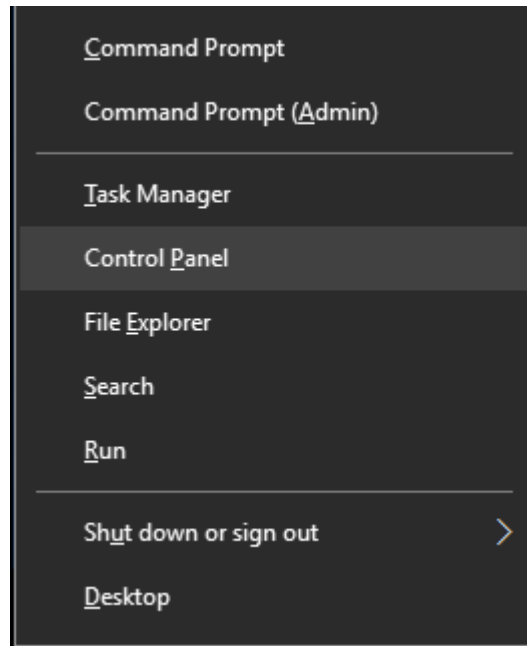
Step 3, Uncheck Users must enter a user name and password to use this computer and click OK.

Step 4, Enter in your user name and the password you use to log into your system twice and click OK.

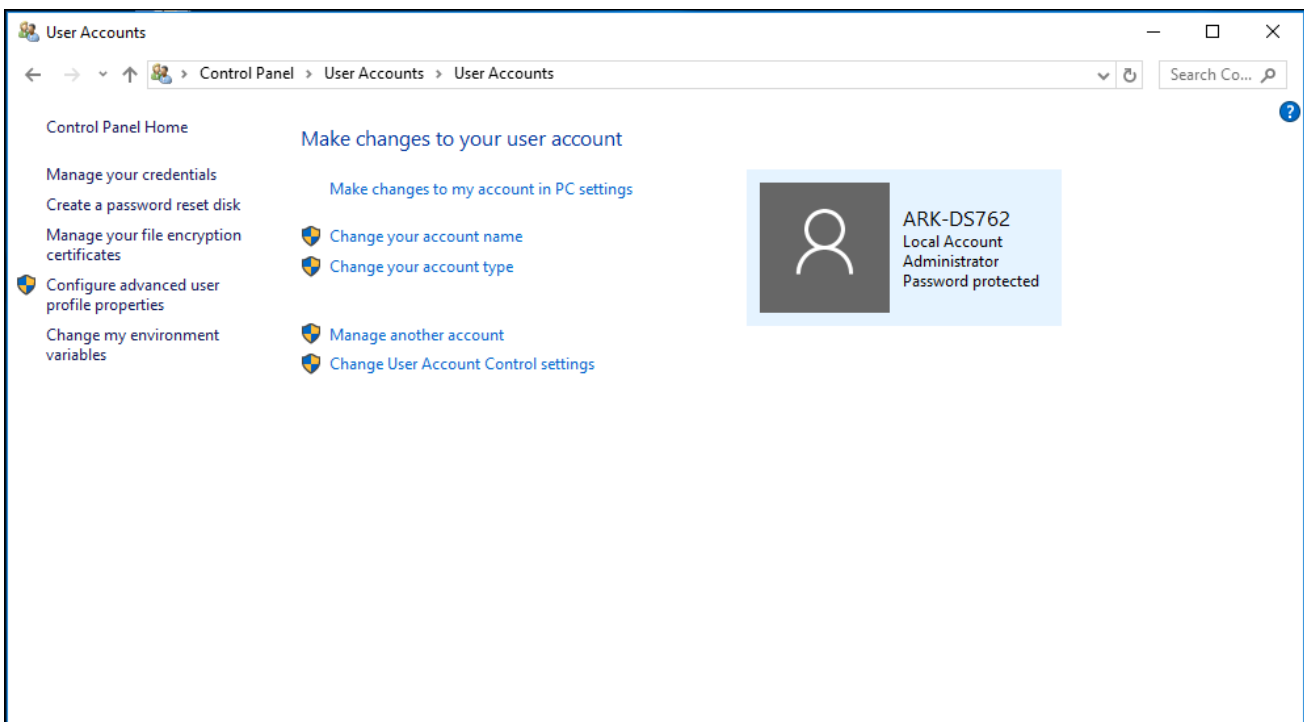


If you still get the "No Login" error or get the "black screen", then you can try to disable the Windows User Account Control (UAC).

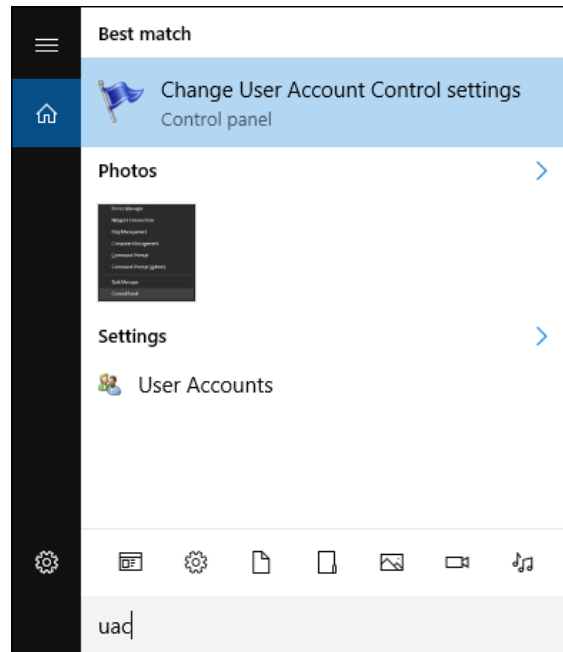
Step 1, Press Windows Key  + X hotkeys together on the keyboard and choose the "Control Panel" item.



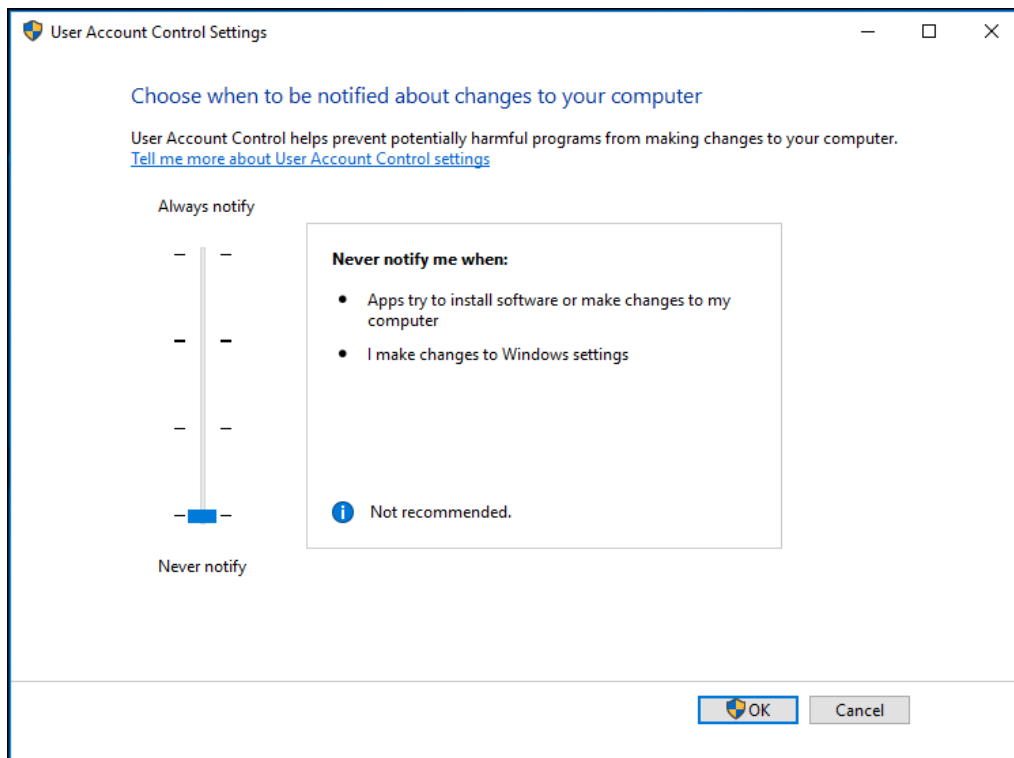
Step 2, Go to the following path: “Control Panel\User Accounts\User Accounts” There you will find the Change User Account Control settings link. Click it.



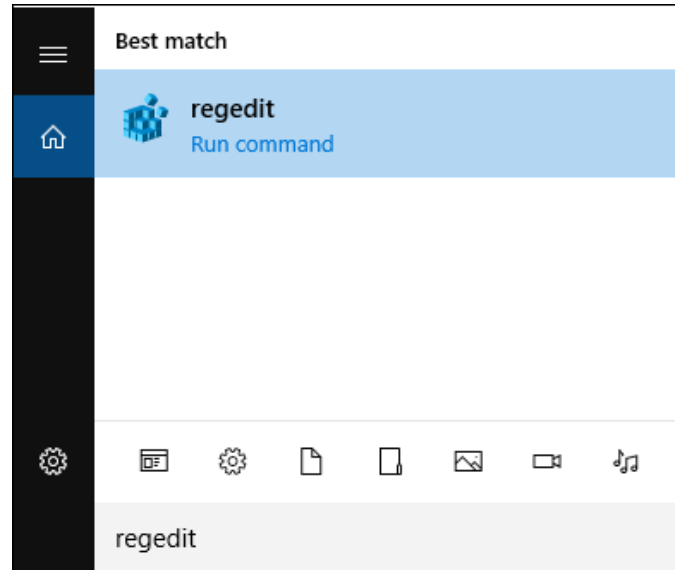
Alternatively, you can enter the “**UAC**” in the Search box to open the User Account Control settings dialog.



Step 3, In the User Account Control settings dialog, move the slider to the bottom (Never Notify).

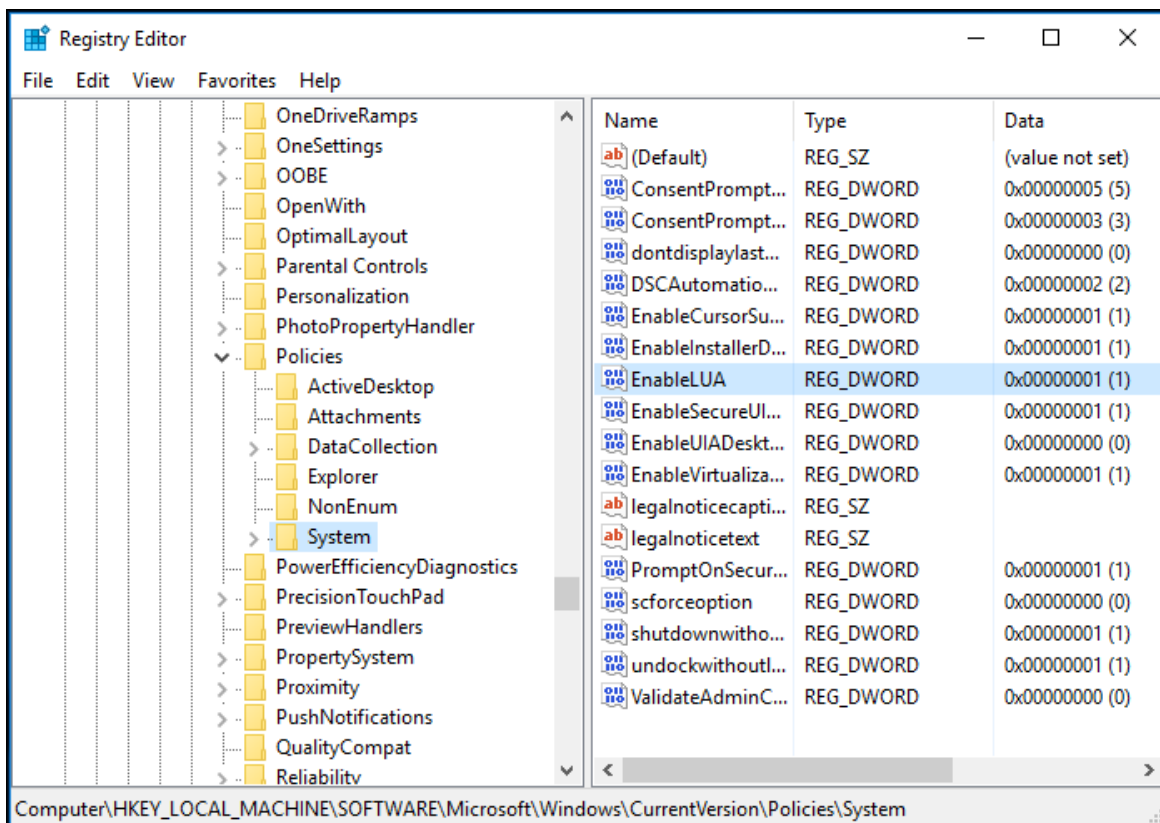


Step 4, Enter the “*regedit*” in the Search box to open the Registry Editor.

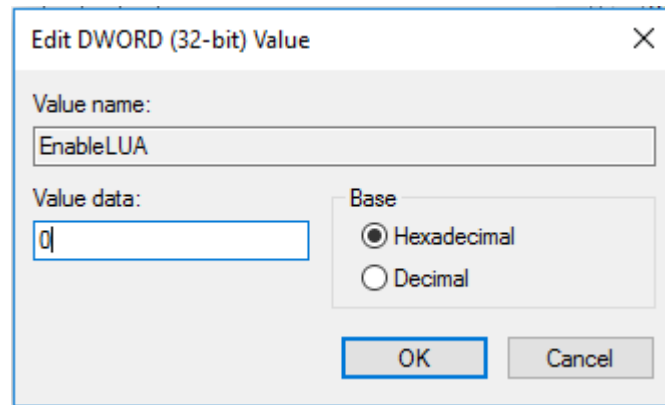


Step 5, Navigate to the following key:

"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"



Step 6, In the right pane, modify the value of the **EnableLUA** DWORD value and set it to **0**.



Step 7, Restart your computer.

6.4 How the Device Data Flow and Debug from Edge to Cloud

The **WISE-PaaS/DeviceOn** offers a general solution of gathering device, equipment and sensor information from the edge device via WISE-Agent. This document will walk you through how the data will be transmitted to **WISE-PaaS/EnSaaS** and the data flow over our architecture. Besides, it also covers how to clarify the issues while using **WISE-PaaS/DeviceOn**.

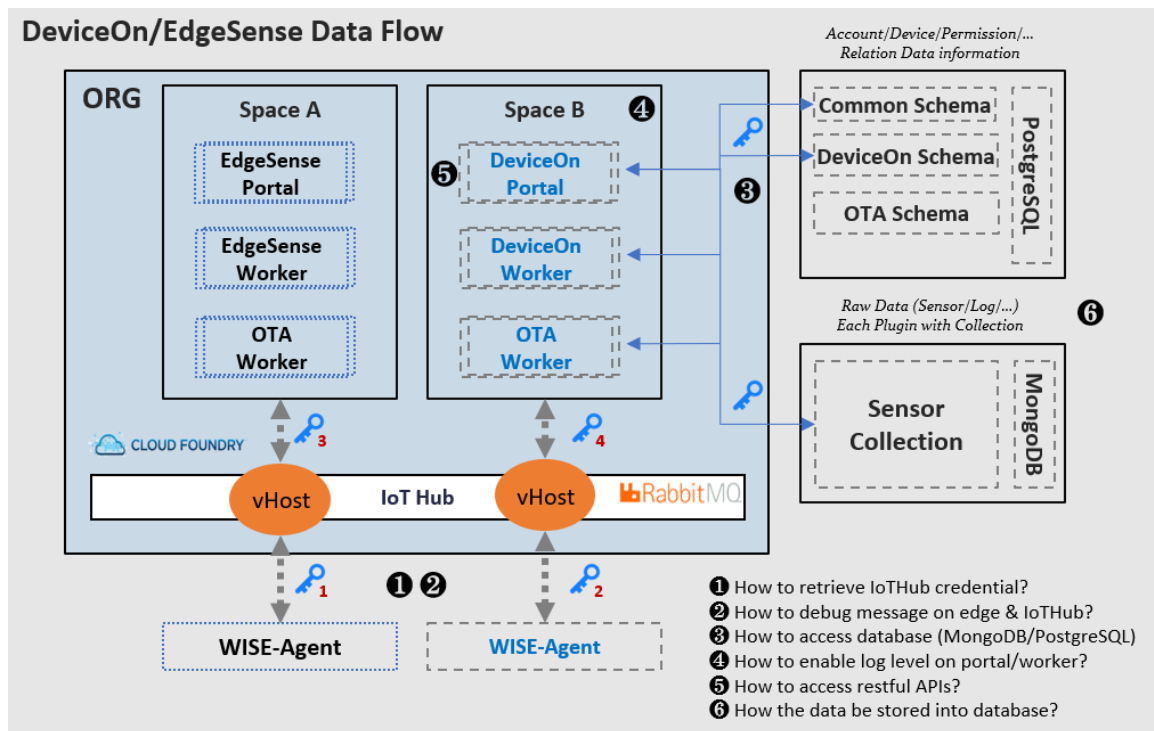
For those advanced system integrators, below figure illustrates an overview of data flow among our software components. You also can access several documents (links of these docs...) that will help you to dive deeper of each item. As an example of document item 1, how to retrieve credential for device to connect to **WISE-PaaS/EnSaaS** IoTHub. We implemented a virtual host mechanism in IoTHub to process messages independently for different space in case data confusion of messages in same topic. Each key can only be used for accessing data for one specific space as below figure. Key No. 1 can neither publish nor subscribe data for space B, but only key No. 4 is available to access IoTHub for space B.

Furthermore, one 3rd party tool **node-RED** can help you to check if all the data are transmitted to IoTHub properly. It's an open source project has been uploaded on the GitLab, as [document](#) item2 will walk you through how to publish node-RED application on our **WISE-PaaS/EnSaaS** and how to monitor messages on edge and IoTHub.

Once the data has been published to target space of **WISE-PaaS/EnSaaS**, the worker will process it and store it into corresponding databases. There are two databases we adopted; one is relational database **PostgreSQL** for storing relational data. For instance, MAC address, device name, platform name, OS information...etc. The other is NoSQL database **MongoDB** for storing sensor raw data. Hence, document as [item 3](#) will walk you through how to access these databases to make sure all the data are stored in databases properly.

In **WISE-PaaS/DevieOn**, we implemented a log system to record each operation. As document [item 4](#) will walk you through how to enable log message for advanced error tracking. Besides, as document [item 5](#), it will also walk you through how to accessing data from database directly by using RESTful APIs for data visualization or application development.

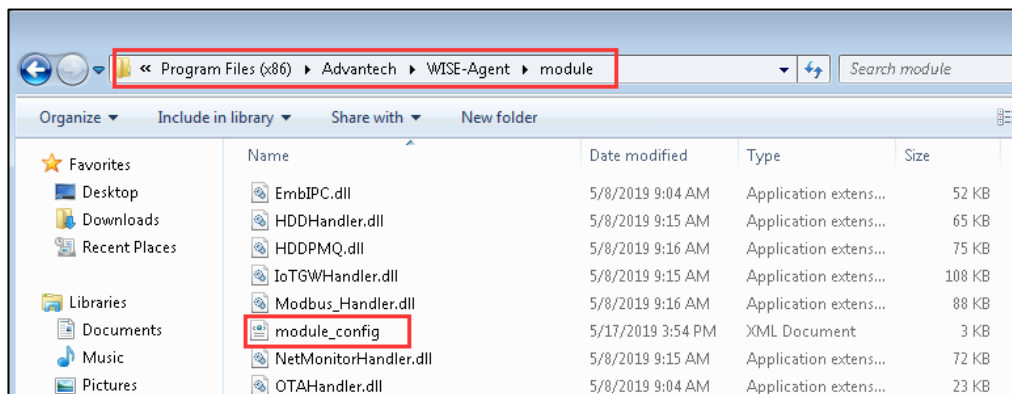
Finally, document [item 6](#) gives an example to show you what kind of data will be stored in **PostgreSQL** and **MongoDB** respectively once edge devices are connected.



6.5 How to Enable and Disable plugins on WISE-Agent

Step 1: Adjust configuration file on WISE-Agent

Open **module_config.xml** on Installation path\module\



Adjust “ModuleEnable” to TRUE/FALSE to enable and disable.

```

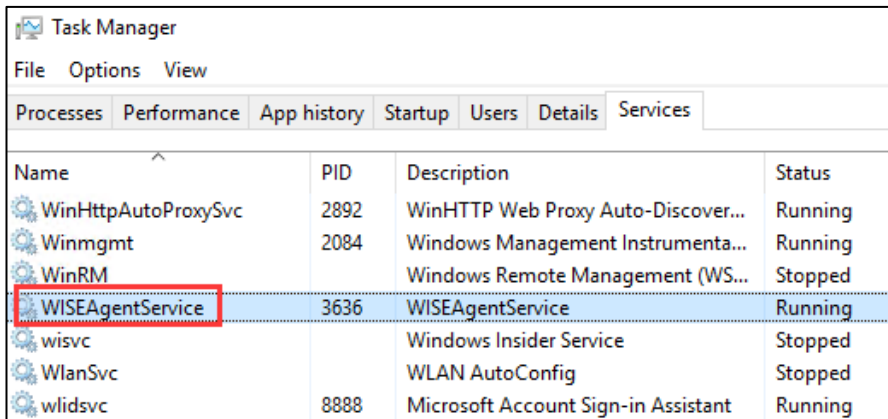
1  <?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
2  <XMLConfigSettings>
3    <BaseSettings>
4      <ModuleNum>15</ModuleNum>
5      <ModuleName1>HDDHandler</ModuleName1>
6      <ModulePath1>\module\HDDHandler.dll</ModulePath1>
7      <ModuleEnable1>TRUE</ModuleEnable1>
8      <ModuleName2>PowerOnOffHandler</ModuleName2>
9      <ModulePath2>\module\PowerOnOffHandler.dll</ModulePath2>
10     <ModuleEnable2>TRUE</ModuleEnable2>
11     <ModuleName3>ScreenshotHandler</ModuleName3>
12     <ModulePath3>\module\ScreenshotHandler.dll</ModulePath3>
13     <ModuleEnable3>TRUE</ModuleEnable3>
14     <ModuleName4>NetMonitorHandler</ModuleName4>
15     <ModulePath4>\module\NetMonitorHandler.dll</ModulePath4>
16     <ModuleEnable4>TRUE</ModuleEnable4>
17     <ModuleName5>ProcessMonitorHandler</ModuleName5>
18     <ModulePath5>\module\ProcessMonitorHandler.dll</ModulePath5>
19     <ModuleEnable5>TRUE</ModuleEnable5>

```

HDD Monitoring

Step 2: Restart WISE-Agent

Open “Task Manager” and switch to “Services”



Task Manager			
File Options View			
Processes Performance App history Startup Users Details Services			
Name	PID	Description	Status
WinHttpAutoProxySvc	2892	WinHTTP Web Proxy Auto-Discover...	Running
Winmgmt	2084	Windows Management Instrumenta...	Running
WinRM		Windows Remote Management (WS...	Stopped
WISEAgentService	3636	WISEAgentService	Running
wisvc		Windows Insider Service	Stopped
WlanSvc		WLAN AutoConfig	Stopped
wlidsvc	8888	Microsoft Account Sign-in Assistant	Running

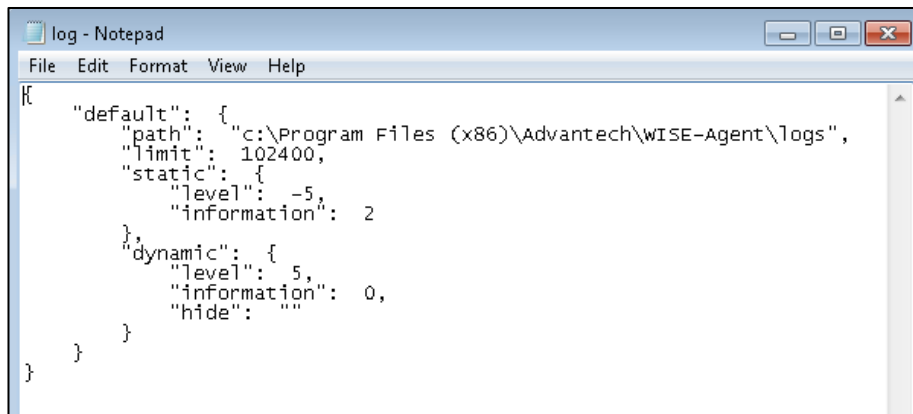
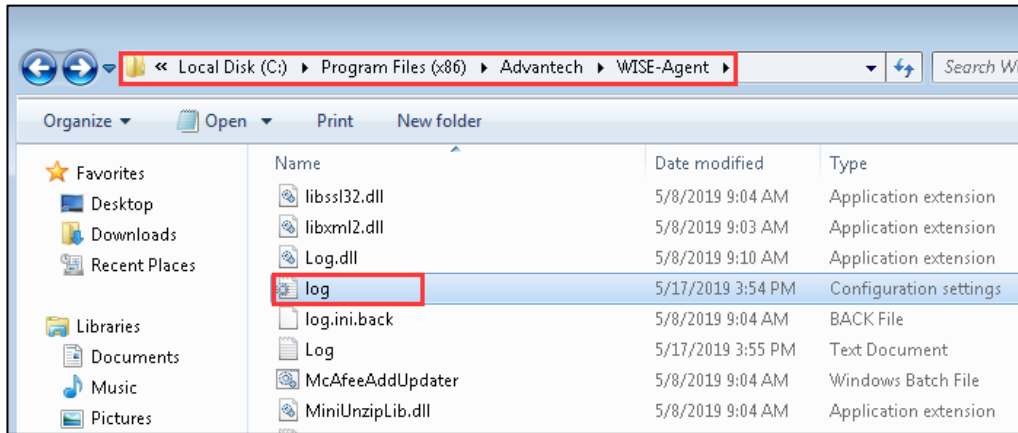
Restart “WISEAgentService” to connect to DeviceOn

6.6 How to Enable and Adjust WISE-Agent Log Levels

[WISE-Agent v-1.3.x & v-1.2.x]

Step 1: Adjust configuration file on WISE-Agent

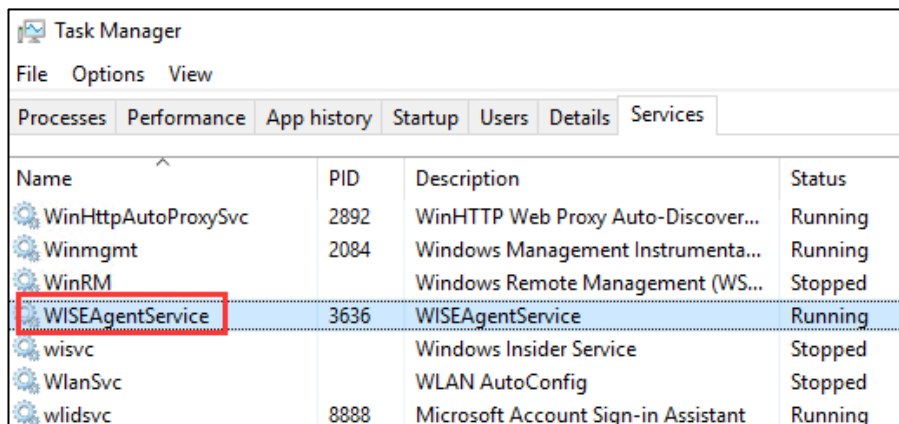
Open **log.ini** on Installation path



Adjust level 5 to 7, minus stand for HTML format.

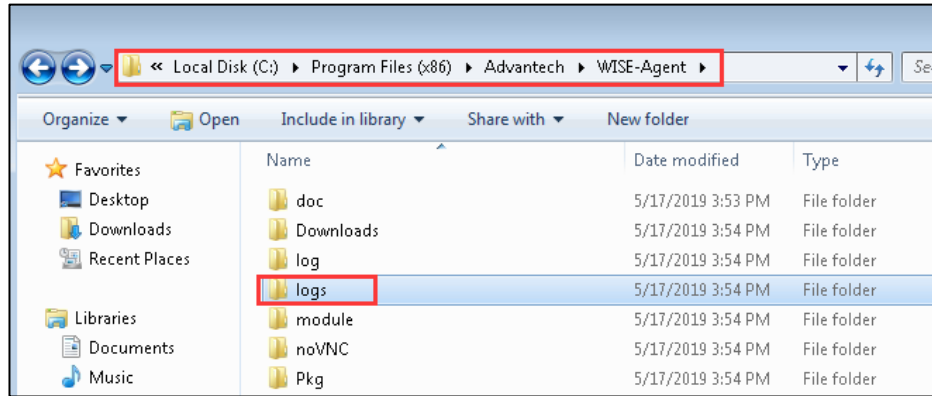
Step 2: Restart WISE-Agent

Open “Task Manager” and switch to “Services”, and restart “WISEAgentService”



Step 3: Retrieve log files from WISE-Agent

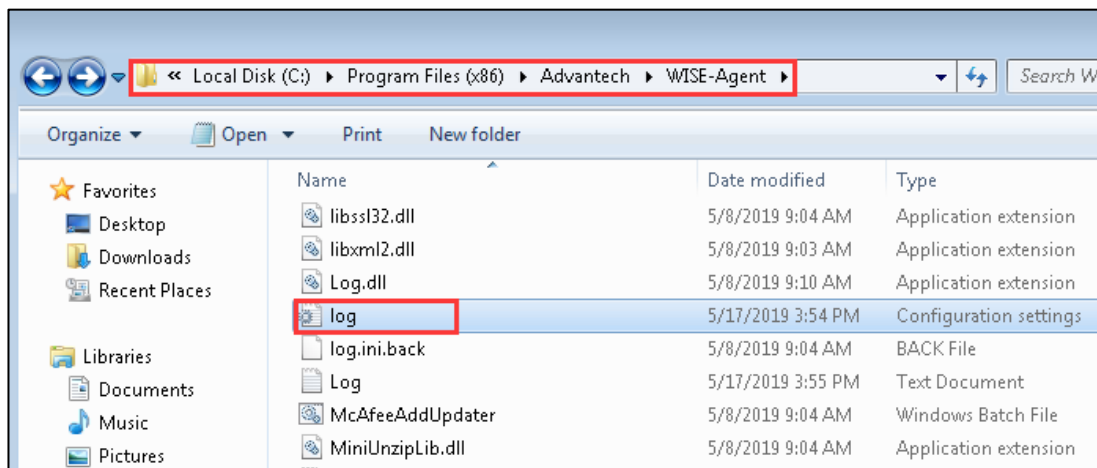
The log files under the Installation path\logs



[WISE-Agent v-1.4.x and above]

Step 1: Adjust configuration file on WISE-Agent

Open **log.ini** on Installation path\module\



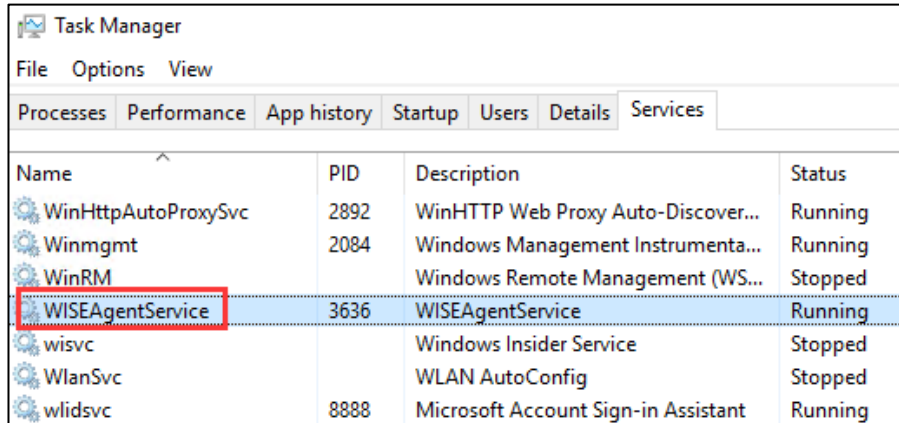
```

[LogClient]
#log_level=4, LOG_FATAL(0), LOG_ALARM(1), LOG_ERROR(2), LOG_WARNING(2), LOG_NORMAL(4), LOG_DEBUG(5)
log_level=5
#to_stderr=1, 1: print to stderr, 0: doesn't print stderr
#logd_ip=127.0.0.1, ip of logd
#logd_port=9278
  
```

Adjust **log_level** from 4 to 5.

Step 2: Restart WISE-Agent

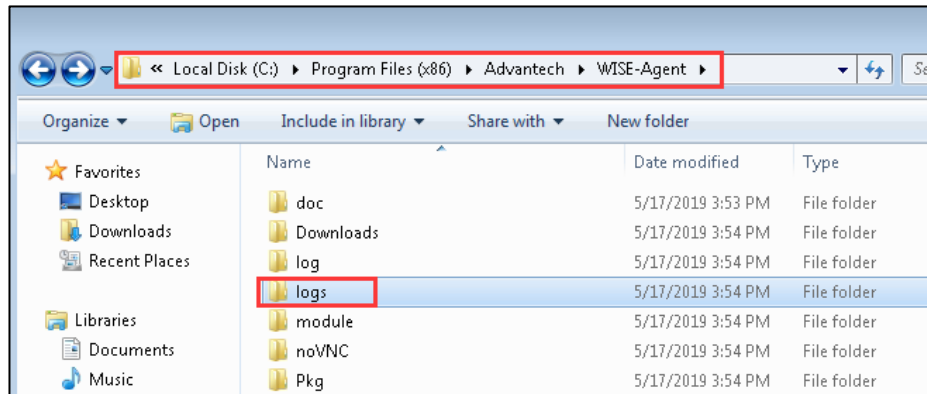
Open "Task Manager" and switch to "Services", and restart "WISEAgentService"



Name	PID	Description	Status
WinHttpAutoProxySvc	2892	WinHTTP Web Proxy Auto-Discover...	Running
Winmgmt	2084	Windows Management Instrumenta...	Running
WinRM		Windows Remote Management (WS...	Stopped
WISEAgentService	3636	WISEAgentService	Running
wisvc		Windows Insider Service	Stopped
WlanSvc		WLAN AutoConfig	Stopped
wlidsvc	8888	Microsoft Account Sign-in Assistant	Running

Step 3: Retrieve log files from WISE-Agent

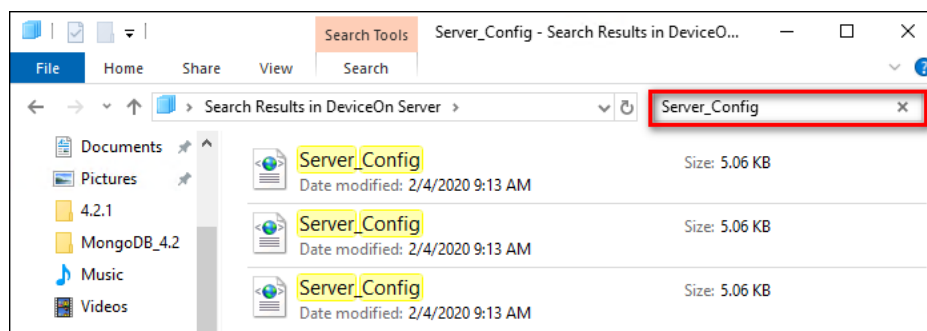
The log files under the Installation path\logs



6.7 How to Change DeviceOn Server Address (Standalone)

If your DeviceOn Server (Standalone) running on public cloud or on-premise environment, and then you would like to update DeviceOn Server address, due to machine/VM IP changed. Here are few steps to update server setting.

Step 1, Search **Server_config.xml** on installation path,
(example, C:\Program Files\Advantech\DeviceOn Server\)

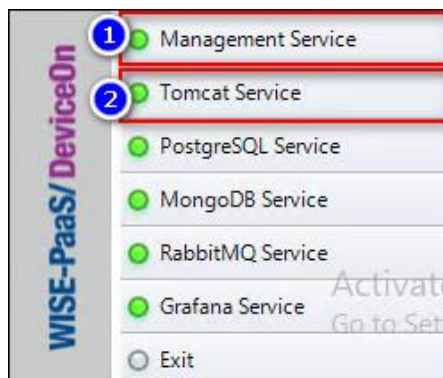


Step 2, Open these files with notepad or other txt editor, and then update host IP address to below path.

```

81      <List>[{"isMaster": true, "name": "wiseagent-upgrade", "url": "http: ^
82    </Storages>
83  </DefaultStorage>
84  <AgentCredential>
85    <BrokerHost>172.22.12.240</BrokerHost>
86    <EndPoint>http://172.22.12.240:8080/rmm/v1/iotHub/credential</EndPo.
87    <KeyName>LzB1qrh3c2cwZzZjS2p2NUU3SXJEdz09</KeyName>
88  </AgentCredential>
89  <SelfProtection>
90    <MemoryLimit>0.9</MemoryLimit>
91  </SelfProtection>
92  <ProvisionInfo>
93    <Org>
94      <Id/>
95      <Name/>
96    </Org>
97    <Space>
98      <Id/>
99      <Name/>
100   </Space>
101  </ProvisionInfo>
102  <UpgradePkgType>
103    <List>[{"pkgType": "RMMAgentSetup", "osType": "Windows"}, {"pkgType": "W.
104  </UpgradePkgType>
105  <Repeater>
106    <Host/>
107    <Port>8443</Port>
108  </Repeater>
109  <WebServer>
110    <IP>172.22.12.240</IP>
111    <HTTPPort>8080</HTTPPort>
112  </WebServer>
113 </Configuration>
  
```

Step 3, Restart the **Tomcat** and **Management Services** through DeviceOn Server Control.



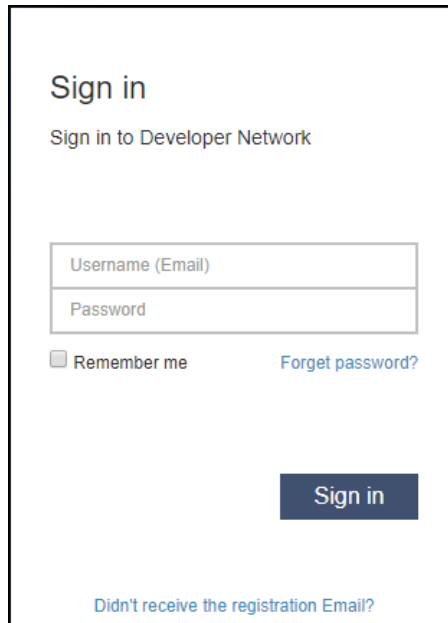
6.8 How to Migrate/Transfer EdgeSense Database to DeviceOn (WISE-PaaS/EnSaaS)

Actually, the DeviceOn is a new product for IoT device management and the backend cores, database structure is based on EdgeSense to develop. In the section, we give a few steps to migrate, transfer database from EdgeSense to DeviceOn. Before the steps, you should prepare the database tool, download and install the program.

[PostgreSQL](#): pg_dump, psql

[MongoDB](#): mongodump, mongorestore

Step 1, Sign in to your WISE-PaaSEnSaaS Management portal



Sign in

Sign in to Developer Network

Username (Email)

Password

☐ Remember me [Forget password?](#)

Sign in

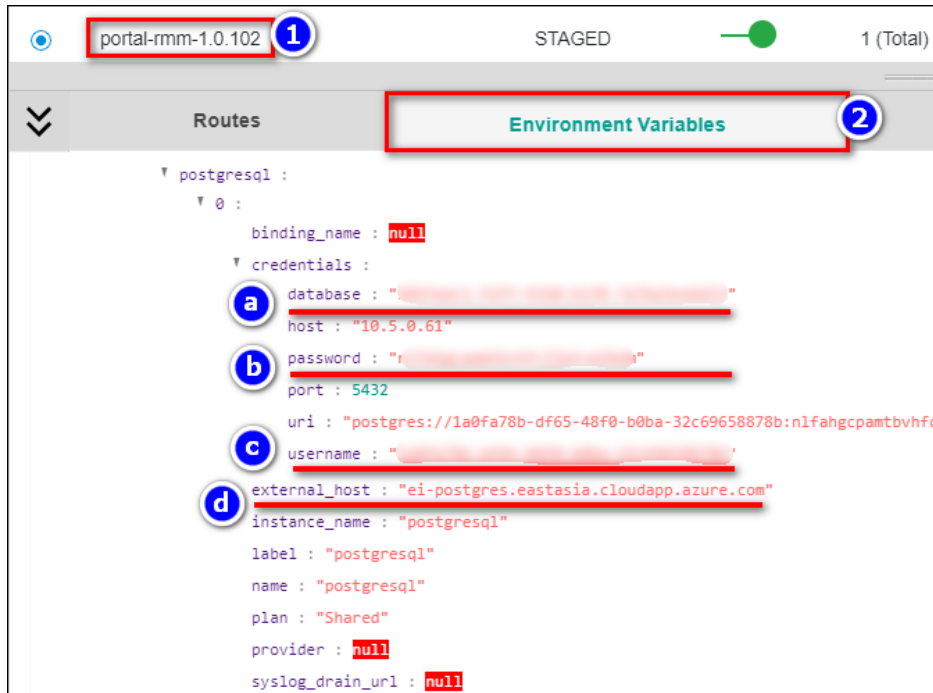
[Didn't receive the registration Email?](#)

Step 2, Enter to your organization, space and listing your applications.

Organization		Space	
Application List	Service Instance List	Route List	Usage
Name	Package State	State	
<input type="radio"/> dashboard-1.2.4	STAGED	<input type="radio"/>	
<input type="radio"/> dashboard-1.3.3	STAGED	<input checked="" type="radio"/>	
<input type="radio"/> ota-worker-1.0.44	STAGED	<input checked="" type="radio"/>	
<input type="radio"/> portal-rmm-1.0.102	STAGED	<input checked="" type="radio"/>	
<input type="radio"/> rmm-worker-1.0.104	STAGED	<input checked="" type="radio"/>	

Step 3, Retrieve PostgreSQL information via Application (“portal-rmm-1.0.x”) environment, click on the application.

- DATABASE_NAME
- DATABASE_PASSWORD
- DATABASE_USERNAME
- DATABASE_HOST

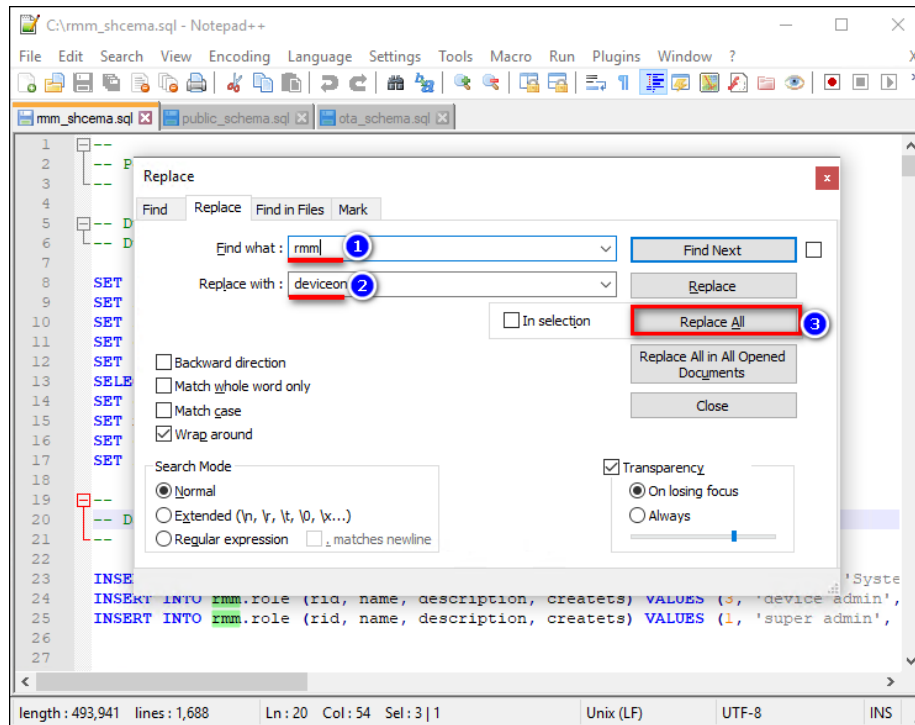


Step 4, Start to backup PostgreSQL data, open the terminal and enter to your PostgreSQL tool path, for example, <INSTALLATION_PATH>\PostgreSQL\11\bin\

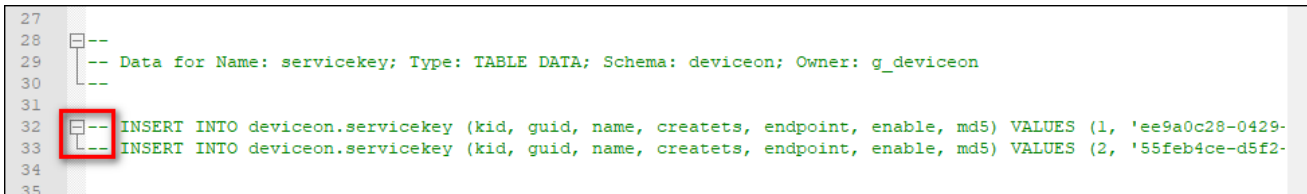
Run the following commands and give a password to backup 3 schema data only.

1. `pg_dump.exe -h DATABASE_HOST -U DATABASE_USERNAME --column-inserts --data-only --schema=rmm --dbname=DATABASE_NAME --file=d:\rmm_schema.sql`
2. `pg_dump.exe -h DATABASE_HOST -U DATABASE_USERNAME --column-inserts --data-only --schema=public --dbname=DATABASE_NAME --file=d:\public_schema.sql`
3. `pg_dump.exe -h DATABASE_HOST -U DATABASE_USERNAME --column-inserts --data-only --schema=ota --dbname=<DATABASE_NAME> --file=d:\ota_schema.sql`

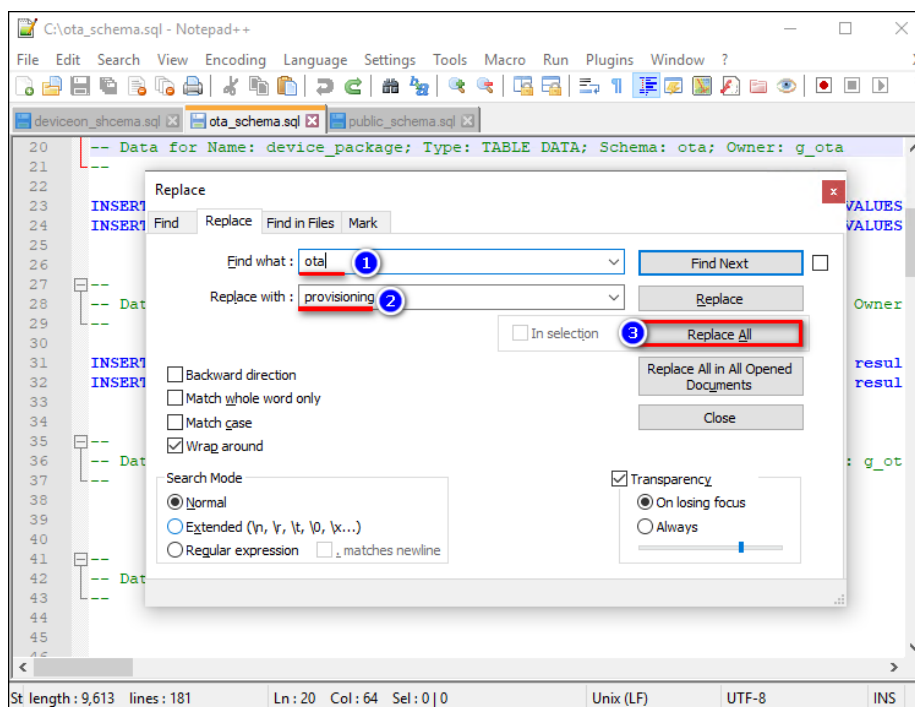
Step 5, Open `rmm_schema.sql` on text editor tool, replace “rmm” word to “deviceon”.



Then, remove or mark the data on “servicekey”, save as another file (**deviceon_schema.sql**)



Step 6, Open **ota_schema.sql** on text editor tool, replace “ota” word to “provisioning”, and save as another file (**provisioning_schema.sql**)



Step 7, Before to restore database to **DeviceOn**, please retrieve related information on Management portal, such as Database name, user name, password and host. On WISE-PaaS 3.0, the steps similar to previous, click on the application (portal-deviceon-1.1.x) and get the information via environment.



Step 8, Start to restore PostgreSQL data, open the terminal and enter to your PostgreSQL tool path, for example, <INSTALLATION_PATH>\PostgreSQL\11\bin\

Run the following commands with the SQL that adjusted and give a password to restore 3 schema data only.

1. `psql.exe -h DATABASE_HOST -U DATABASE_USERNAME -d DATABASE_NAME -f d:\public_schema.sql`
2. `psql.exe -h DATABASE_HOST -U DATABASE_USERNAME -d DATABASE_NAME -f d:\deviceon_schema.sql`
3. `psql.exe -h DATABASE_HOST -U DATABASE_USERNAME -d DATABASE_NAME -f d:\provisioning_schema.sql`

Step 9, For MongoDB backup and restore, you could get the credential on application's environment, and start to run below command to dump collection.

```
1. mongodump.exe --host DATABASE_HOST --db DATABASE_NAME --collection COLLECTION_NAME --  
out d:\mongodb --username DATABASE_USERNAME --password DATABASE_PASSWORD
```

Run the following commands to restore collection to new database.

```
1. mongorestore.exe --host DATABASE_HOST --db DATABASE_NAME --  
collection COLLECTION_NAME D:\mongodb\COLLECTION_NAME.bson --username DATABASE_USERNAME --  
password DATABASE_PASSWORD
```

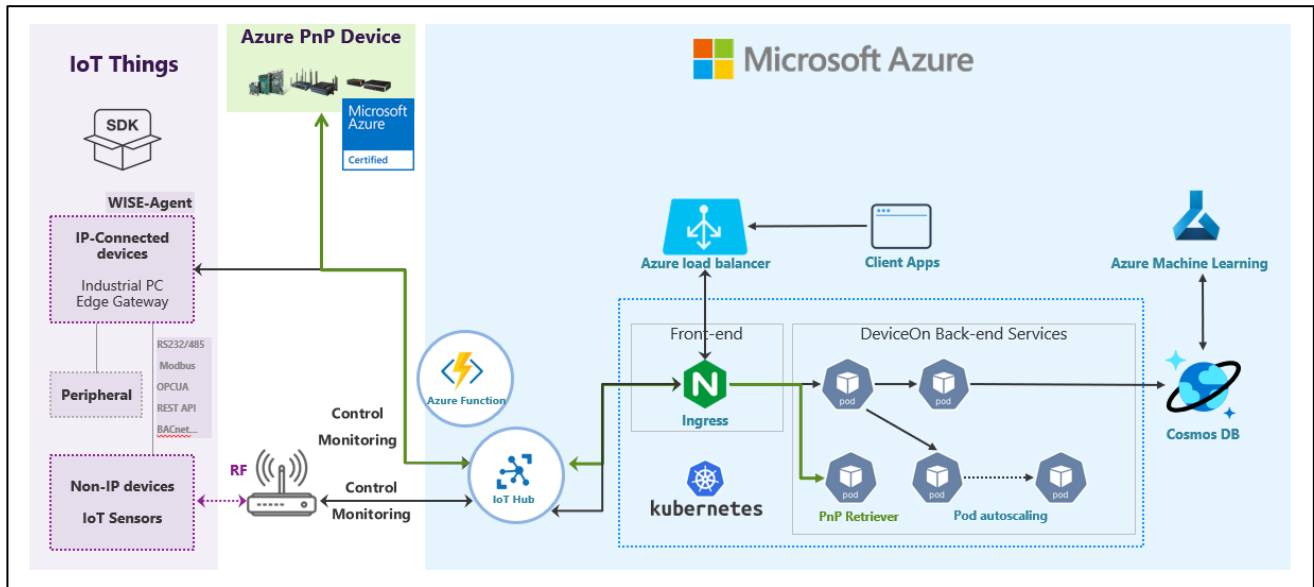
6.9 How Does DeviceOn Interact with AI and Machine Learning

Before to realize the value of data, to export a precise model on your field side, you must collect these raw data from edge side through WISE-Agent. The WISE-Agent not only IPC management but data acquisition for various wire/wireless protocols. DeviceOn could deploy on Azure Kubernetes to leverage Azure PaaS resource, such as Azure Function, IoT Hub, Cosmos DB, meanwhile, much easier to start training via Azure Machine Learning.

Leverage Azure Machine Learning, automated ML is the process of automating the time consuming, iterative tasks of machine learning model development. It allows data scientists, analysts, and developers to build ML models with high scale, efficiency, and productivity all while sustaining model quality. Automated ML is based on a breakthrough from our Microsoft Research division.

Traditional machine learning model development is resource-intensive, requiring significant domain knowledge and time to produce and compare dozens of models. Apply automated ML when you want Azure Machine Learning to train and tune a model for you using the target metric you specify. The service then iterates through ML algorithms paired with feature selections, where each iteration produces a model with a training score. The higher the score, the better the model is considered to "fit" your data.

With automated machine learning, you'll accelerate the time it takes to get production-ready ML models with great ease and efficiency.



6.10 What IS WISE-PaaS Alliance, and How Does One Join

REF: <https://wise-paas.advantech.com/en-us/marketplace/faq>

WISE-PaaS Alliance is a partnership program hosted by Advantech to provide IoT Solutions. Members benefit greatly in their IoT application development by using software developed by Advantech or its strategy partners. Customers can join the VIP member program by paying 20K USD and getting 2K WISE-Points. WISE-Points can be used to purchase software, technical support, or co-marketing events.

6.11 What ARE WISE-Points, and How They Used

REF: <https://wise-paas.advantech.com/en-us/marketplace/faq>

WISE-Points represent virtual currency used by members of the WISE-PaaS Alliance to purchase software in the Marketplace.

1 WISE-Point = 10 USD.

7. Reference

7.1 User Permission

Item	Action	Description	Root	System Admin	Device Admin
------	--------	-------------	------	--------------	--------------

Account Management	Create	Create Account	✓ (Not Include Self)	✓ (Only Device Admin)	
	Edit	Edit Account Basic Information	✓	✓ (Only Self & Device Admin)	✓ (Only Self)
	Edit	Edit Account Role	✓ (Not Include Self)		
	Edit	Disable Account	✓ (Not Include Self)	✓ (Only Device Admin)	
	View	View Account Information	✓	✓ (Only Self & Device Admin)	✓ (Only Self)
Device Group Management	Create	Create Device Group	✓	✓ (Only Self & Device Admin)	✓ (Only Self)
	Edit	Edit Device Group Information	✓	✓ (Only Self & Device Admin)	✓ (Only Self)
	View	View Device Group Information	✓	✓ (Only Self & Device Admin)	✓ (Only Self)
	Delete	Delete Device Group	✓	✓ (Only Self & Device Admin)	✓ (Only Self)
Device Control & Management	Add	Add Unmanaged Device	✓	✓	✓
	Edit	Edit Device Information	✓	✓ (Only Self & Device Admin)	✓ (Only Self-Managed Devices)
	View	View Device Information	✓	✓ (Only Self & Device Admin)	✓ (Only Self-Managed Devices)
	Edit	Remove Device	✓	✓ (Only Self & Device Admin)	✓ (Only Self-Managed Devices)
	View	Search Unmanaged Devices	✓	✓	✓
	Control	Power, Remote	✓	✓ (Only Self &	✓ (Only Self-

		Desktop, Terminal, Screenshot, Backup/Recovery, Protection, Windows Lockdown Actions...		Device Admin)	Managed Devices)
Event Log Management	View	View and Export Device Event	✓	✓ (Only Self- Managed & Device Admin Devices)	✓ (Only Self- Managed Devices)
	View	View and Export System Event	✓	✓	
	View	View and Export Operation Event	✓	✓ (Only Self- Managed & Device Admin Devices)	✓ (Only Self- Managed Devices)
	View	Long-polling, Web-Socket	✓	✓	✓
OTA Management	Create	Create Storage Repository	✓	✓	
	Edit	Edit Storage Repository	✓	✓	
	View	View Storage Repository	✓	✓	✓
	Delete	Delete Storage Repository	✓	✓	
	Upload	Upload OTA Package	✓ (Only Self)	✓ (Only Self)	✓ (Only Self)
	View	View OTA Package	✓ (Only Self)	✓ (Only Self)	✓ (Only Self)
	Delete	Delete OTA Package	✓ (Only Self)	✓ (Only Self)	✓ (Only Self)
	Deploy	Deploy OTA	✓	✓ (Only Self-	✓ (Only Self-

		Package		Managed & Device Admin Devices)	Managed Devices)
	Edit	Edit OTA Deploy Configuration	✓	✓	
System Setting Management	Create	Create an Action	✓ (All Groups) on Self Account	✓ (Only Self-Groups & Device Admin Groups) on Self Account	✓ (Only Self-Groups)
	Edit	Update an Action	✓ (All Groups) on Self Account	✓ (Only Self-Groups & Device Admin Groups) on Self Account	✓ (Only Self-Groups)
	View	View Action	✓ Self Account	✓ Self Account	✓ Self Account
	Delete	Delete Action	✓ Self Account	✓ Self Account	✓ Self Account
	Provisioning	Power Management	✓	✓ (Only Self-Managed & Device Admin Devices)	✓ (Only Self-Managed Devices)
		Backup/Recovery	✓	✓ (Only Self-Managed & Device Admin Devices)	✓ (Only Self-Managed Devices)
		Protection	✓	✓ (Only Self-Managed & Device Admin Devices)	✓ (Only Self-Managed Devices)
	Edit	Edit Event Alert Setting	✓ (Only Self)	✓ (Only Self)	✓ (Only Self)
	Edit	Configure Alert Service	✓	✓	
	Create	Create Rule Engine	✓	✓ (Only Self & Device Admin)	✓ (Only Self-Managed Devices)
	Update	Edit Rule Engine	✓	✓ (Only Self & Device Admin)	✓ (Only Self-Managed)

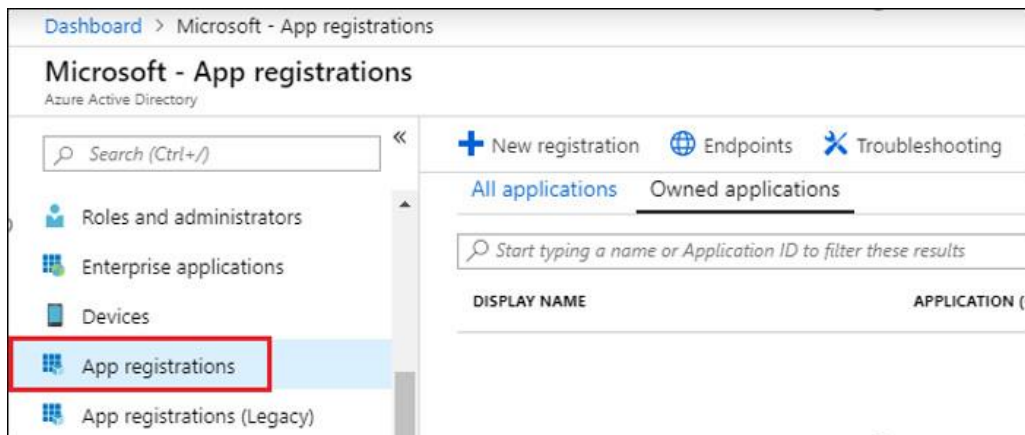
					Devices)
	View	View Rule Engine	✓	✓ (Only Self & Device Admin)	✓ (Only Self-Managed Devices)
	Delete	Delete Rule Engine	✓	✓ (Only Self & Device Admin)	✓ (Only Self-Managed Devices)
	Edit/View	Edit/View System UI	✓	✓	
	Edit	Activate DeviceOn License (Perpetual Only)	✓	✓	

7.2 Retrieve My Azure Account Information

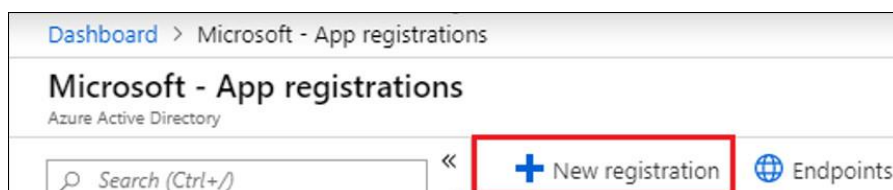
7.2.1 Method 1 – Create & Get Information on Azure Portal

Step 1: Create Your Application

- 1.1. Log into your [Azure Portal](#)
- 1.2. Select **[Azure Active Directory]**
- 1.3. Select **[App registrations]**



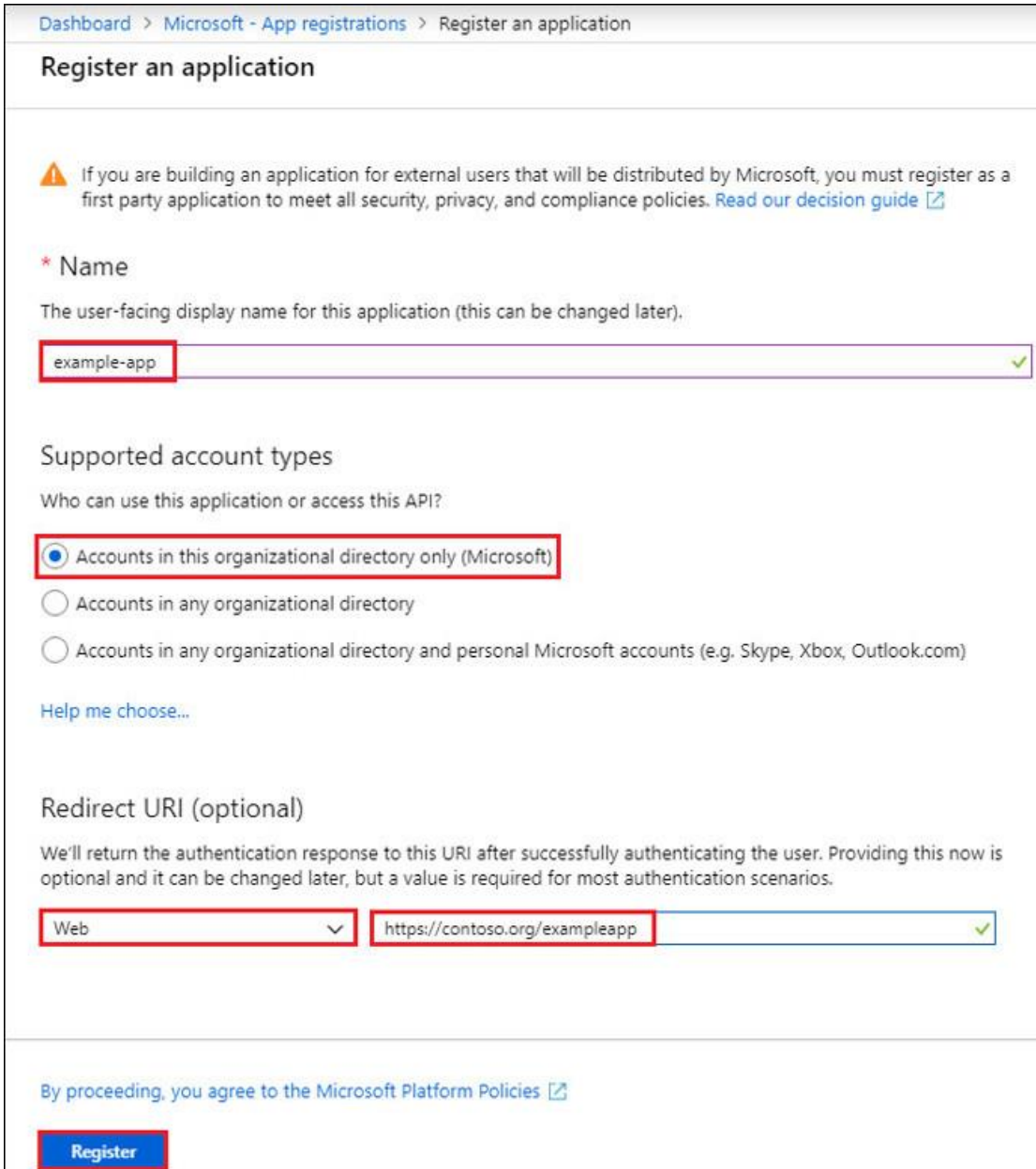
- 1.4. Add **[New Registration]**



- 1.5. Setup your **Application Name** then click **[Register]**.
 - Enter your Application display name in **Name** field.


- Setup **Supported account types** by selecting the respective account type for this API.
- Under **Redirect URI**, select Web for the type of application you want to create. Enter the URI where the access token is sent to.

Note: You cannot create a Native application credential nor use the type for an automated application.



Dashboard > Microsoft - App registrations > Register an application

Register an application

 If you are building an application for external users that will be distributed by Microsoft, you must register as a first party application to meet all security, privacy, and compliance policies. [Read our decision guide](#)

*** Name**
The user-facing display name for this application (this can be changed later).

example-app

Supported account types
Who can use this application or access this API?

☒ Accounts in this organizational directory only (Microsoft)

☐ Accounts in any organizational directory

☐ Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)

[Help me choose...](#)

Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web

[By proceeding, you agree to the Microsoft Platform Policies](#)

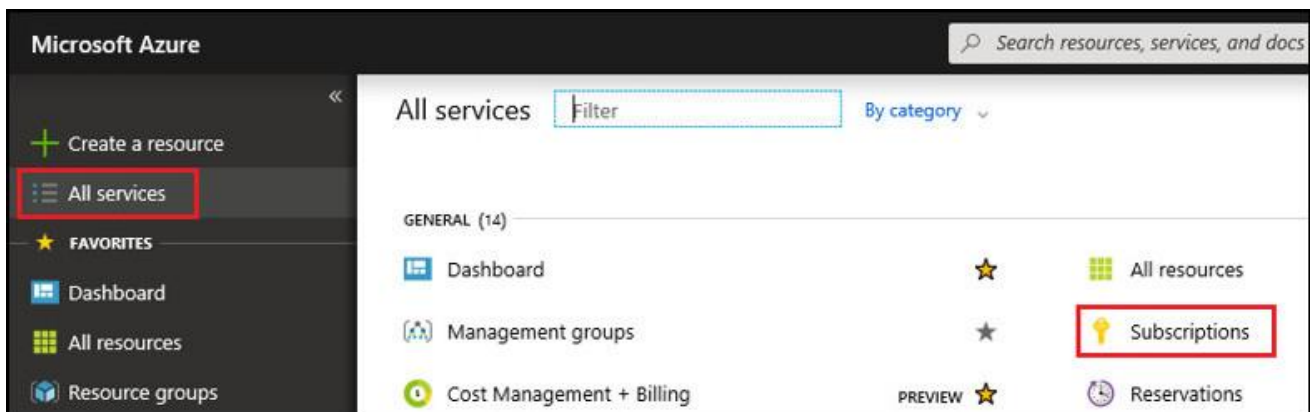
Register

Step 2: Get Subscription ID

To access resources in your subscription, you must assign a role to the Application. You can pick between Subscription, Resource Group or Resource. Permissions are inherited to lower scope levels. [For more details, see RBAC: Built in Roles](#)

- 2.1. Select **All services** then select **Subscriptions** to set up the level of scope you wish to assign

this application.

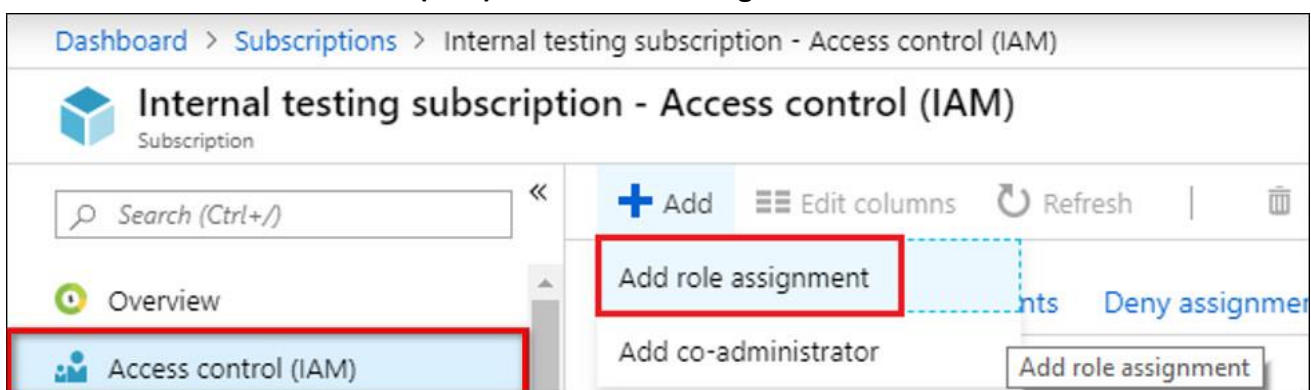


2.2. Find the Subscription you would like to assign to the Application created in the Step 1. Copy the **Subscription ID**, as this is one of the Azure data fields required on the WISE-PaaS Marketplace later. (Ref: [Marketplace field #A](#))

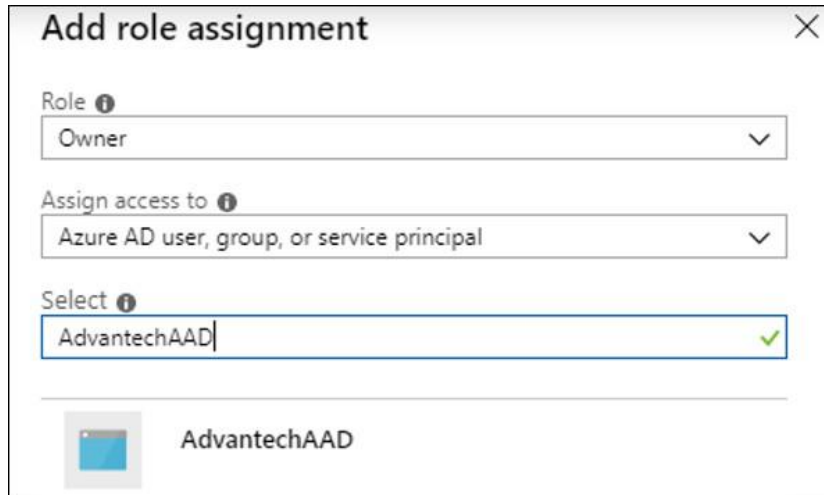
SUBSCRIPTION	SUBSCRIPTION ID
Visual Studio Enterprise – MPN	

! Troubleshoot: If you do not see the subscription you're looking for, select global subscriptions filter. Make sure the subscription you want is selected for the portal.

2.3. Select **Access control (IAM)** then **Add role assignment**



2.4. Select the **Owner** role. By default, Azure AD applications are not displayed in the available options. To find your application, search for the name.




Add role assignment [X]

Role ⓘ
Owner

Assign access to ⓘ
Azure AD user, group, or service principal

Select ⓘ
AdvantechAAD ✓

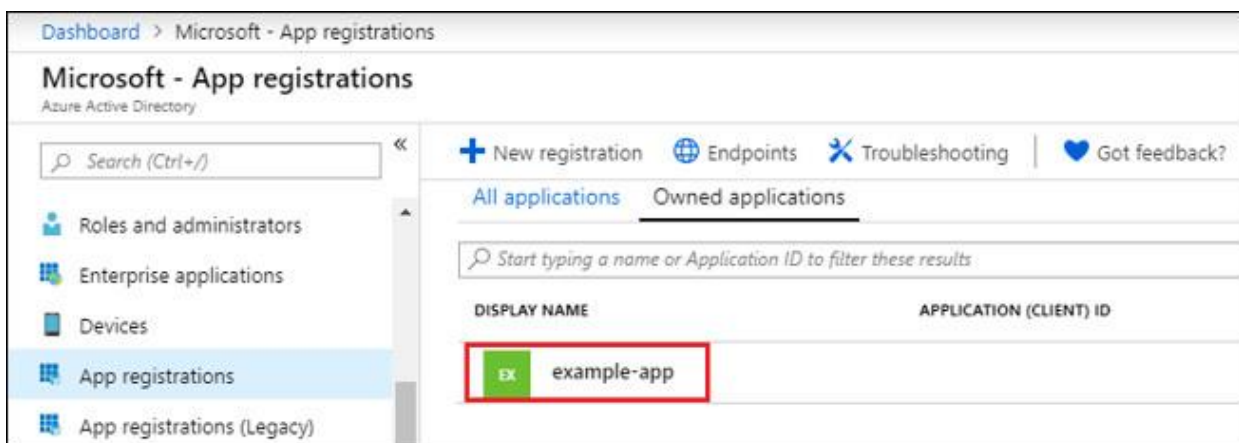
 AdvantechAAD

2.5. Click **Save** to finish assigning the role. You will be able to see your application in the list of users assigned to a role for that scope.

Step 3: Get Application & Tenant ID

3.1. Select **Azure Active Directory**

3.2. From **App registrations** in Azure AD, select your application



Dashboard > Microsoft - App registrations

Microsoft - App registrations
Azure Active Directory


Search (Ctrl+/)

Roles and administrators
Enterprise applications
Devices
App registrations
App registrations (Legacy)

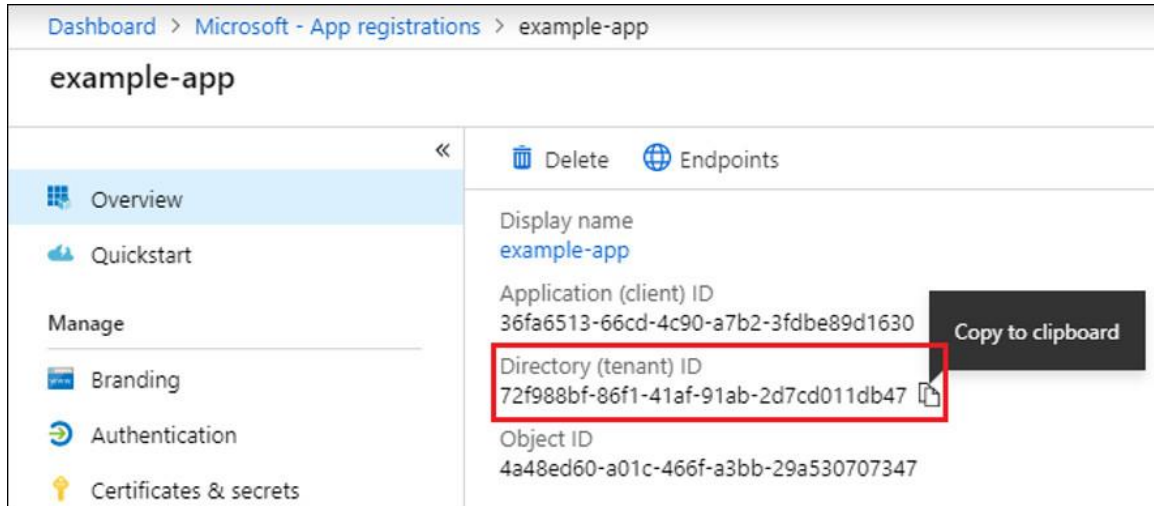
+ New registration | Endpoints | Troubleshooting | Got feedback?

All applications | Owned applications

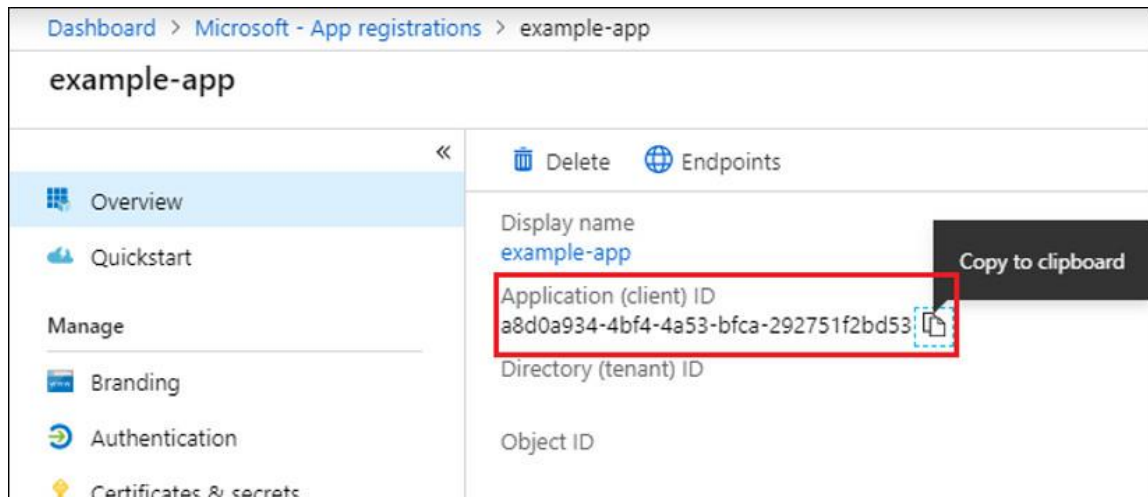
Start typing a name or Application ID to filter these results

DISPLAY NAME	APPLICATION (CLIENT) ID
 example-app	

3.3. Copy the **Directory (tenant) ID** as another piece of Azure information that will be required on the WISE-PaaS Marketplace later. (Ref: [Marketplace field #C](#))

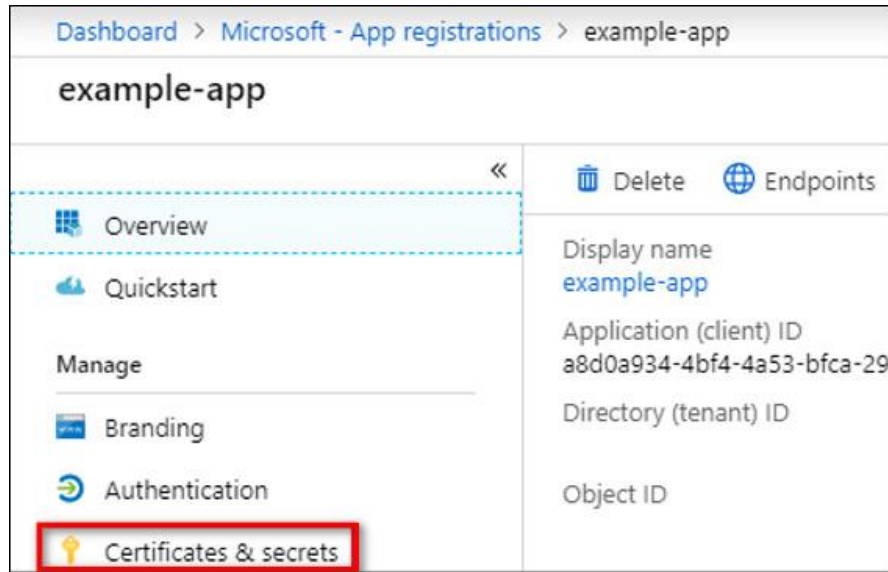


3.4. Copy the **Application (client) ID** as part of Azure information that will be required on the WISE-PaaS Marketplace later. ([Ref: Marketplace field #B](#))

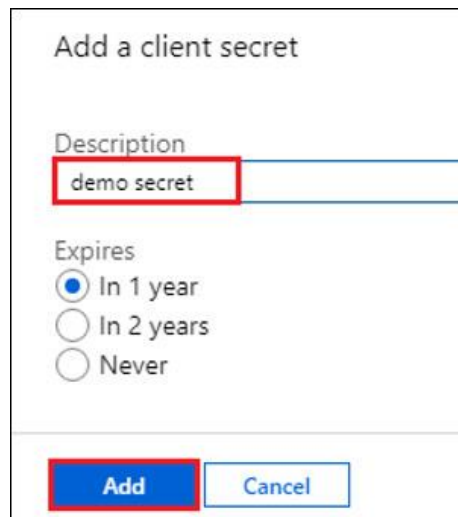


Step 4: Add & Get Client Secret

- 4.1. Select **[Certificates & secrets]**
- 4.2. Select **Client secrets** then **New client secret**



4.3. Provide a description for the new client secret, set up the expiration period. Then Click **[Add]**



The screenshot shows the 'Add a client secret' dialog box. It contains a 'Description' field with the text 'demo secret' entered, which is highlighted with a red box. Below the description field, there are three radio button options for the expiration period: 'In 1 year' (selected), 'In 2 years', and 'Never'. At the bottom of the dialog, there are two buttons: 'Add' (highlighted with a red box) and 'Cancel'.

Copy Client Secret (**Ref: Marketplace field #D**)

Client secrets		
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.		
+ New client secret		
DESCRIPTION	EXPIRES	VALUE
demo secret	5/14/2020	nWu9HVZ7Rnj.2y7XSkVyUngZ][x9Z:e 

7.2.2 Method 2 – Create via Azure CLI (Command-line Tool)

Step 1: Install Azure CLI

[For details, please view this step by step guide](#)

Step 2: Sign in to the Azure Account

1. C:\>az login

Note: If the CLI can open your default browser, it will do so and load a sign-in page. Otherwise, you need to open a browser page and follow the instructions on the command line to enter an authorization code after navigating to <https://aka.ms/devicelogin> in your browser. Sign in with your account credentials in the browser.

Step 3: Get Subscription ID & Copy Output

2. C:\>az account show --query id

```
C:\>az login
Note, we have launched a browser for you to login. For old experience with device code, use "az login --use-device-code"
You have logged in. Now let us find all the subscriptions to which you have access...
[
  {
    "cloudName": "AzureCloud",
    "id": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
    "isDefault": true,
    "name": "Visual Studio Enterprise \u2013 2013 MPN",
    "state": "Enabled",
    "tenantId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
    "user": {
      "name": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
      "type": "user"
    }
  }
]
```

Step 4: Create service principal and get Application ID, Tenant ID and Client Secret

3. C:\>az ad sp create-for-rbac --name ServicePrincipalName

```
C:\>az ad sp create-for-rbac --name AdvantechAD
Retrying role assignment creation: 1/36
Retrying role assignment creation: 2/36
{
  "appId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
  "displayName": "AdvantechAD",
  "name": "http://AdvantechAD",
  "password": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
  "tenant": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
}
```

Reference: [Create an Azure service principal with Azure CLI >](#)